Notas de Álgebra

Mariano Suárez-Álvarez

31 de octubre de 2023

Contenido

Capítulo 1

Conjuntos

§1.1. Conjuntos

1.1.1. Un ***conjunto*** es una colección de objetos, a los que nos referimos como sus ***elementos***. Cuando un objeto x es un elemento de un conjunto A decimos que x ***pertenece*** a A y escribimos

$$x \in A.$$

Si, por el contrario, x no es un elemento de A, decimos que x no pertenece a A y escribimos

$$x \notin A.$$

Un conjunto queda completamente determinado por sus elementos. Como consecuencia de esto, dos conjuntos son iguales si y solamente si tienen exactamente los mismos elementos.

1.1.2. Si un conjunto tiene un número finito de elementos y estos no son muchos, entonces podemos describir el conjunto simplemente listando sus elementos y en ese caso lo hacemos entre llaves $\{\cdots\}$. Por ejemplo, si escribimos

$$\{1, 3, 101, 7\} \tag{1}$$

estamos mencionando el conjunto que tiene por elementos a los números 1, 3, 101 y 7, y a ninguna otra cosa más — observemos que de esta forma el conjunto queda completamente determinado. Cuando usamos este tipo de descripción de un conjunto — listar sus elementos — decimos que lo describimos por ***enumeración*** o por ***extensión***. Si llamamos A al conjunto de (1), entonces claramente tenemos que

$$1 \in A, \qquad 99 \notin A, \qquad 101 \in A, \qquad 0 \notin A.$$

Cada una de estas afirmaciones puede verificarse simplemente por inspección: por ejemplo, 0 no es un elemento de A porque 0 no es ninguno de los objetos listados entre las llaves en (1).

Es importante tener en cuenta que el orden en que listamos los elementos de un conjunto cuando lo damos por enumeración es irrelevante — ya que lo único importante es qué cosas pertenecen al conjunto y qué cosas no — y, por lo tanto, que podríamos haber escrito

$$\{7, 101, 1, 3\}$$

para describir exactamente el mismo conjunto que el de (1). De manera similar, la cantidad de veces que aparece un objeto en la lista de elementos de un conjunto en una descripción como (1) es irrelevante: otra vez, lo único importante es si un objeto aparece o no en la lista. Esto significa que el conjunto

$$\{1, 1, 101, 3, 3, 3, 7, 101, 7, 7\}$$

es exactamente el mismo que el conjunto de (1). Por supuesto, casi siempre es preferible evitar repeticiones inútiles, pero esto puede no ser fácil o posible.

1.1.3. En ciertas situaciones usamos la palabra ***familia*** en lugar de *conjunto*. Por ejemplo, cuando tenemos un conjunto cuyos elementos son conjuntos, como $\{\{1, 2\}, \{3, 4\}, \{5\}\}$, preferimos decir «familia de conjuntos» a decir «conjunto de conjuntos», pero las dos frases significan exactamente lo mismo. Encontraremos algunos ejemplos de este uso en lo que sigue — por ejemplo, en el Ejercicio 1.6.3.

1.1.4. Los elementos de un conjunto pueden ser de cualquier tipo. Por ejemplo, el conjunto

$$\{1, \bigcirc, \clubsuit, (2, 3)\}$$

tiene cuatro elementos: el número 1, el disco rojo $\bigcirc$, el palo de trébol $\clubsuit$ de la baraja francesa y el par ordenado $(2, 3)$. Los elementos de un conjunto pueden ser ellos mismos conjuntos: así, los elementos del conjunto

$$\{1, \{2, 3\}, 4, \{5, 6\}\}$$

son cuatro: los números 1 y 4 y los conjuntos $\{2, 3\}$ y $\{5, 6\}$. Es importante observar que, por ejemplo, el número 2 no es un elemento de este conjunto. De manera similar, el conjunto

$$\{\{1, 2\}\}$$

tiene exactamente *un* elemento, el conjunto $\{1, 2\}$, y

$$\{\{1\}, 1\}$$

tiene *dos*: el número 1 y el conjunto $\{1\}$. Finalmente,

$$\{1, \{1\}, \{1, \{1\}\}, \{\{1, \{1\}\}\}\}$$

denota el conjunto que tiene cuatro elementos: el número 1 y los conjuntos $\{1\}$, $\{1, \{1\}\}$ y $\{\{1, \{1\}\}\}$, que tienen 1, 2 y 1 elementos, respectivamente.

1.1.5. Un conjunto puede no tener elementos: decimos en ese caso que es ***vacío***. Si A y B son dos conjuntos que son vacíos, entonces tienen exactamente los mismos elementos — a saber, ninguno — y esto implica, como observamos arriba, que A y B son de hecho el mismo conjunto. Vemos así que hay exactamente un conjunto que es vacío y no hay ninguna ambigüedad si nos referirnos a él como *el* conjunto vacío.

Podemos dar el conjunto vacío por enumeración: de acuerdo a las convenciones que describimos arriba, el símbolo

$$\{\}$$

denota al conjunto vacío. En efecto, como no hay ningún objeto listado entre estas llaves ningún objeto pertenece a este conjunto. Casi siempre, sin embargo, usamos el símbolo especial

$$\varnothing$$

para representar al conjunto vacío. Este símbolo fue propuesto por André Weil, inspirado en la letra ø del idioma noruego, y fue usado por primera vez en 1939 en el libro sobre la teoría de conjuntos de Nicolás Bourbaki[1]. El concepto de conjunto vacío, sin embargo, es muy anterior: el primero en usar explícitamente el conjunto vacío fue Georges Boole en 1847.

Observemos que el conjunto $\{\varnothing\}$ tiene un elemento — el conjunto vacío — así que no es vacío. De manera similar, $\{\varnothing, \{\varnothing\}\}$ tiene dos, ya que $\varnothing$ y $\{\varnothing\}$ son dos cosas distintas: se trata de dos conjuntos, pero no son el mismo, ya que uno es vacío mientras que el otro, el segundo, tiene exactamente un elemento.

1.1.6. Si un conjunto es finito pero tiene muchos elementos o, peor, si tiene infinitos elementos, entonces no es práctico o posible darlo por enumeración. En ese caso, podemos describirlo dando alguna condición que permita decidir si un objeto pertenece o no al conjunto. Por ejemplo, escribimos

$$A = \{x : x \text{ es un entero positivo y par}\} \tag{2}$$

para decir que A es el conjunto de todos los objetos x que satisfacen la condición «x es un entero positivo y par». Así, los números 2 y 1928 pertenecen a este conjunto A mientras que el número 7,

[1] En su autobiografía, Weil cuenta: «Wisely, we had decided to publish an installment establishing the system of notation for set theory, rather than wait for the detailed treatment that was to follow: it was high time to fix these notations once and for all, and indeed the ones we proposed, which introduced a number of modifications to the notations previously in use, met with general approval. Much later, my own part in these discussions earned me the respect of my daughter Nicolette, when she learned the symbol Ø for the empty set at school and I told her that I had been personally responsible for its adoption. The symbol came from the Norwegian alphabet, with which I alone among the Bourbaki group was familiar.»

el número -4 o el conjunto $\{4, 9\}$ no: el número 7 es un entero positivo pero no es par, el número -4 es un entero y es par, pero no es positivo, y el conjunto $\{4, 9\}$ no es ni siquiera un entero. De manera similar, al conjunto

$$\{x : x \text{ es un número real y } 0 < x \leq 3\} \tag{3}$$

pertenecen los números 1, $\sqrt{2}$ y 3, pero no el número -9, el número 12 o el par ordenado $(1, 2)$.

Los conjuntos de (2) y (3) son infinitos, así que no sería posible darlos por enumeración de sus elementos. Por otro lado, el conjunto

$$\{x : x \text{ es un entero positivo menor que } 1\,000\,000\}$$

es finito pero tiene 999 999 elementos, así que aunque es en principio posible describirlo por enumeración hacerlo no es muy práctico.

1.1.7. Cuando describimos un conjunto dando una condición que permite decidir si cada objeto pertenece o no a él, decimos que lo damos ***por comprensión***. El símbolo «:» que usamos en (2) y en (3) se lee «tal que», y entonces leemos en voz alta lo que aparece a la derecha del símbolo igual de (2) «el conjunto de los objetos x tales que x es un entero positivo y par». A veces se usa una barra vertical «|» en lugar de «:», y se escribe, por ejemplo,

$$\{x \mid x \text{ es un entero positivo y par}\}.$$

En estas notas usaremos exclusivamente el símbolo «:», ya que reservaremos la barra vertical para denotar la relación de divisibilidad entre números enteros.

1.1.8. Casi siempre que damos un conjunto por comprensión, parte de la condición que lo determina es que los objetos tienen que pertenecer a algún conjunto ya conocido. Así, la condición que aparece en el conjunto (2) incluye la de que x pertenezca al conjunto $\mathbb{Z}$ de los números enteros, mientras que la de (3) que x pertenezca al conjunto $\mathbb{R}$ de los números reales. Cuando es ese el caso y queremos enfatizarlo, preferimos escribir

$$\{x \in \mathbb{Z} : x \text{ es positivo y par}\}$$

y

$$\{x \in \mathbb{R} : 0 < x \leq 3\}$$

en lugar de las fórmulas de (2) y (3). Cuando leemos en voz alta la primera de estas fórmulas, por ejemplo, decimos «el conjunto de los elementos x de $\mathbb{Z}$ tales que x es positivo y par».

§1.2. Subconjuntos

1.2.1. Decimos que un conjunto A es un ***subconjunto*** de un conjunto B o también que A está ***contenido*** o ***incluido*** en B, y en ese caso escribimos $A \subseteq B$, si todo elemento de A es un elemento de B, esto es, si para todo objeto x vale la implicación

$$x \in A \implies x \in B.$$

Si además es $A \neq B$, decimos que A es un subconjunto ***propio*** de B y escribimos, si queremos enfatizar esto, $A \subsetneq B$.

Muchos autores usan el símbolo $\subset$ en lugar de $\subseteq$ para denotar la contención de conjuntos, y escriben $A \subset B$ en lugar de $A \subseteq B$. En estas notas no usaremos nunca este símbolo.

1.2.2. Usaremos la siguiente observación todo el tiempo en lo que sigue, y casi siempre sin referir a ella explícitamente:

Proposición. *Sean A y B dos conjuntos. Es $A \subseteq B$ si y solamente si para todo objeto x vale que $x \notin B \implies x \notin A$.*

Demostración. La afirmación $A \subseteq B$ significa que para todo x vale la implicación $x \in A \implies x \in B$, y la afirmación contrarrecíproca de esta implicación es precisamente la del enunciado de la proposición, así que la proposición es trivialmente cierta. □

1.2.3. Es importante distinguir a los *elementos* de un conjunto de sus *subconjuntos*. Esto lo hacemos tanto en la notación como en el lenguaje: si x es un elemento de un conjunto B, decimos que x pertenece a B y escribimos $x \in B$, y si A es un subconjunto del conjunto B decimos que A está contenido en B y escribimos $A \subseteq B$.

Así, por ejemplo, 1 pertenece al conjunto $\{1, 2, 3\}$ y $\{1\}$ está incluido en ese conjunto. De todas formas, es bien posible que algo simultáneamente pertenezca y esté incluido en un conjunto: así, $\{1, 2\}$ es un subconjunto del conjunto $\{1, 2, \{1, 2\}\}$ y a la vez es uno de sus elementos.

1.2.4. La siguiente proposición describe las propiedades más sencillas de la relación de inclusión entre conjuntos.

Proposición. *Sean A, B y C conjuntos.*

(*i*) *Se tiene que $A \subseteq A$.*

(*ii*) *Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$.*

(*iii*) *Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.*

Demostración. (*i*) Si x es un elemento de A, entonces claramente x es un elemento de A: esto significa, precisamente, que A está contenido en A, es decir, que $A \subseteq A$.

(*ii*) Supongamos que $A \subseteq B$ y que $B \subseteq A$, y mostremos que $A = B$. Si x es un elemento de A, entonces, como $A \subseteq B$, tenemos que $x \in B$; se manera similar, si x es un elemento de B, entonces como $B \subseteq A$ podemos deducir que $x \in A$. Vemos así que todo elemento de A es un elemento de B y que todo elemento de B es un elemento de A, por lo que A y B tienen exactamente los mismos elementos y, por lo tanto, es $A = B$.

(*iii*) Supongamos que $A \subseteq B$ y que $B \subseteq C$, y sea x un elemento de A. Como $A \subseteq B$, de que x pertenezca a A se deduce que x pertenece a B. De esto y de que $B \subseteq C$ se deduce, a su vez, que x pertenece a C. Vemos así que todo elemento de A es un elemento de C y, por lo tanto, que $A \subseteq C$, como afirma el enunciado. □

1.2.5. La primera afirmación de la Proposición 1.2.4 que acabamos de probar nos dice que todo conjunto A es un subconjunto de sí mismo, esto es, que $A \subseteq A$. Por el contrario, ningún conjunto es un *elemento* de sí mismo: en otras palabras, vale que

cualquiera sea el conjunto A se tiene que $A \notin A$.

Esta afirmación es, de hecho, el llamado *Axioma de Fundación* de la Teoría Axiomática de Conjuntos de John von Neumann y Ernst Zermelo, que es la formalización más usual de la teoría de conjuntos.

1.2.6. El conjunto vacío se comporta de una manera especial con respecto a la relación de inclusión:

Proposición. *Sea A un conjunto.*
(*i*) *Se tiene que $\varnothing \subseteq A$.*
(*ii*) *Si $A \subseteq \varnothing$, entonces $A = \varnothing$.*

Demostración. Todo elemento de $\varnothing$ pertenece a A, simplemente porque no hay ningún elemento en $\varnothing$: esto nos dice que $\varnothing \subseteq A$. Esto prueba la afirmación (*i*). Para probar la afirmación (*ii*), por su parte, probaremos la afirmación contrarrecíproca, a saber, que

si $A \neq \varnothing$, entonces $A \not\subseteq \varnothing$.

Sea entonces A un conjunto que no es vacío. Como no es vacío, posee algún elemento x: ahora bien, como $x \notin \varnothing$, es claro que $A \not\subseteq \varnothing$. □

1.2.7. Si A es un conjunto, el ***conjunto de partes*** de A es el conjunto $\mathscr{P}(A)$ cuyos elementos son los subconjuntos de A. Así, se tiene que

$$B \in \mathscr{P}(A) \iff B \subseteq A.$$

Proposición. *Sean A y B dos conjuntos.*

(*i*) *El conjunto vacío $\varnothing$ y el conjunto A son elementos de $\mathscr{P}(A)$ y, en particular, el conjunto $\mathscr{P}(A)$ no es vacío.*

(*ii*) *Si $A \subseteq B$, entonces $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.*

Demostración. (*i*) Sabemos de la Proposición **1.2.6**(*i*) y de la Proposición **1.2.4**(*i*) que $\varnothing \subseteq A$ y que $A \subseteq A$, así que $\varnothing \in \mathscr{P}(A)$ y $A \in \mathscr{P}(A)$.

(*ii*) Supongamos que $A \subseteq B$ y sea $C \in \mathscr{P}(A)$, de manera que $C \subseteq A$. Usando la Proposición **1.2.4**(*iii*) y el hecho de que $C \subseteq A$ y $A \subseteq B$, vemos que $C \subseteq B$, esto es, que $C \in \mathscr{P}(B)$. Así, todo elemento de $\mathscr{P}(A)$ está en $\mathscr{P}(B)$ y, por lo tanto, $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, como afirma el enunciado. □

1.2.8. El único subconjunto del conjunto vacío es el conjunto vacío — esto es precisamente lo que nos dice la Proposición **1.2.6**(*ii*)— así que $\mathscr{P}(\varnothing)$ tiene exactamente un elemento, el conjunto vacío mismo:

$$\mathscr{P}(\varnothing) = \{\varnothing\}.$$

Los subconjuntos del conjunto $\{1\}$ son

$$\varnothing \quad \text{y} \quad \{1\}$$

así que estos son los elementos de $\mathscr{P}(\{1\})$, que tiene, por lo tanto, 2 elementos. De manera similar, los subconjuntos de $\{1, 2\}$ y de $\{1, 2, 3\}$ son, respectivamente,

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{1, 2\},$$

y

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{1, 2\}, \quad \{1, 3\}, \quad \{2, 3\}, \quad \{1, 2, 3\},$$

así que los conjuntos de partes $\mathscr{P}(\{1, 2\})$ y $\mathscr{P}(\{1, 2, 3\})$ tienen $4 = 2^2$ y $8 = 2^3$ elementos. Veremos un poco más adelante que este patrón se cumple con toda generalidad, de manera que tenemos el siguiente resultado:

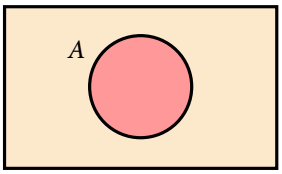
Proposición. *Si A es un conjunto finito y $n \in \mathbb{N}_0$ es el número de elementos de sus elementos, entonces el conjunto de partes $\mathscr{P}(A)$ es finito y tiene exactamente 2^n elementos.*

Daremos la prueba de esta proposición cuando tengamos a nuestra disposición el principio de inducción.

§1.3. Diagramas de Venn

Cuando tenemos unos pocos conjuntos es frecuente usar una idea de John Venn para hacer un diagrama que refleje las relaciones entre ellos. Dedicaremos esta sección a los llamados *diagramas de Venn*, que aparecerán frecuentemente en todo lo que sigue.

Cuando tenemos un conjunto A podemos representarlo gráficamente con un diagrama como el siguiente:



La idea es que el rectángulo contiene todos los objetos sobre los que estamos hablando, mientras que el círculo, que representa al conjunto A, divide a esos objetos en dos: los que están adentro son los que pertenecen a A y los que están afuera son los que no pertenecen a A.

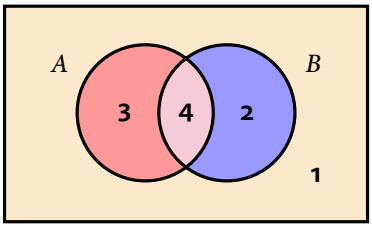
Supongamos ahora tenemos dos conjuntos A y B. Cada objeto puede pertenecer o no a A y puede pertenecer o no a B. En total, hay cuatro posibilidades, correspondientes a las cuatro entradas de la siguiente tabla:

		$¿x \in B?$	
		No	Sí
$¿x \in A?$	No	1	2
	Sí	3	4

Una forma alternativa y más conveniente de presentar estas mismas cuatro posibilidades es la siguiente tabla:

	$¿x \in A?$	$¿x \in B?$
1	No	No
2	No	Sí
3	Sí	No
4	Sí	Sí

Gráficamente podemos representar estas cuatro opciones usando el siguiente diagrama:



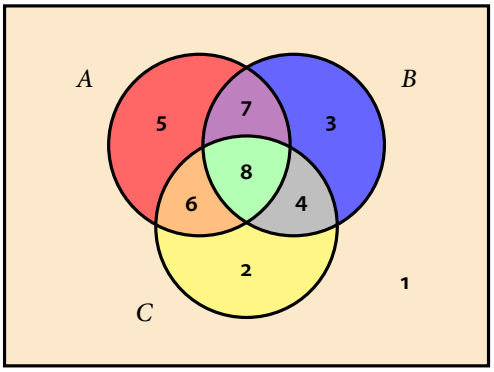
Tenemos aquí el mismo rectángulo que antes, que representa la clase de todos los objetos sobre los que estamos hablando, y dos círculos que corresponden a los conjuntos A y B. Cada uno de estos círculos dividen al rectángulo en dos regiones, que representan los elementos que pertenecen al conjunto corresponden y los que no pertenecen a él. Entre los dos, los círculos dividen al rectángulo en cuatro regiones: cada una de ellas se corresponde a una de las cuatro opciones que tabulamos arriba. Por ejemplo, la región que pintamos de azul ● es la parte del rectángulo que está dentro del círculo que representa a B y fuera del que representa a A.

Si en lugar de dos conjuntos tenemos tres, A, B y C, entonces un elemento x puede o no pertenecer a A, puede o no pertenecer a B y puede o no pertenecer a C: en total esto nos da ocho casos, que son los que aparecen en la siguiente tabla:

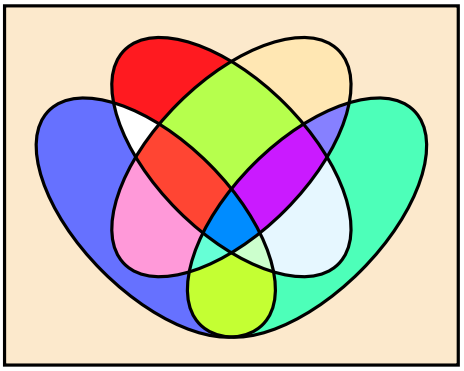
	$¿x \in A?$	$¿x \in B?$	$¿x \in C?$
1	No	No	No
2	No	No	Sí
3	No	Sí	No
4	No	Sí	Sí
5	Sí	No	No
6	Sí	No	Sí
7	Sí	Sí	No
8	Sí	Sí	Sí

Como en el caso anterior, cada una de las filas de esta tabla se corresponde con una de las regiones

del siguiente diagrama de Venn:



Si tenemos más conjuntos, es más difícil hacer diagramas de Venn que los representen, pero Venn probó en [Ven1880] que siempre es posible. Por ejemplo, si tenemos cuatro conjuntos A, B, C, D y un elemento x que puede pertenecer o no a cada uno de ellos, hay en total 16 posibles casos a considerar. Es imposible hacer un diagrama de Venn para esta situación usando círculos — esencialmente porque dos círculos se intersecan en como mucho dos puntos[2] — pero sí es posible hacerlo con otras figuras. Por ejemplo, el siguiente es un diagrama de Venn con cuatro elipses congruentes:



Notemos que este diagrama no tiene la misma simetría rotacional que el diagrama de arriba para tres conjuntos, y esto es inevitable: David Henderson [Hen1963] y Stan Wagon y Peter Webb [WW2008] probaron que si hay un diagrama de Venn para n conjuntos que tiene simetría

[2] Que dos círculos se intersequen en como mucho dos puntos implica que si tenemos un diagrama con k círculos y agregamos un círculo más, entonces agregaremos como mucho $2k$ nuevos puntos de intersección y, por lo tanto, el número de regiones en las que queda dividido el plano puede aumentar, como mucho, en $2k$. Con un solo círculo tenemos 2 regiones, así que agregando uno tenemos como mucho $2 + 2 \cdot 1 = 4$ regiones, agregando uno más como mucho $4 + 2 \cdot 2 = 8$, y agregando uno más como mucho $8 + 2 \cdot 3 = 14$. Como 14 es ciertamente menor que 16, es imposible hacer un diagrama de Venn con 4 círculos.

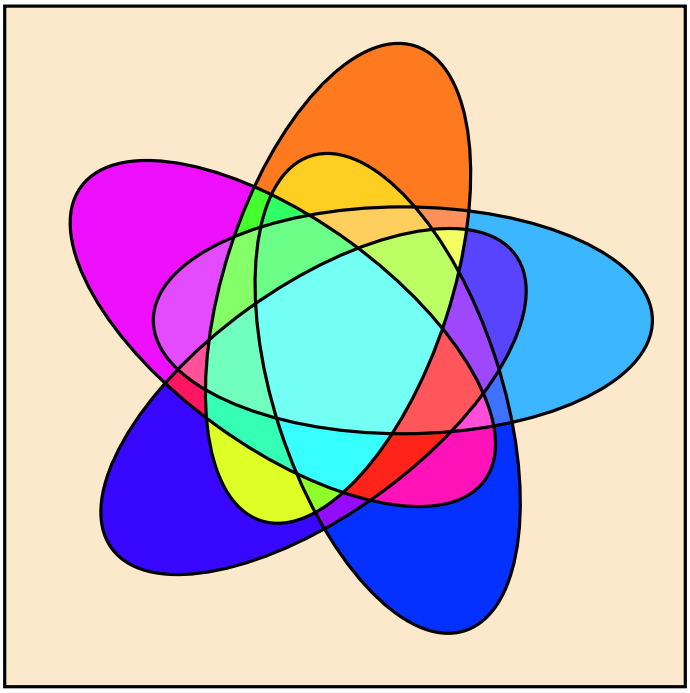


Figura 1.1. Un diagrama de Venn para cinco conjuntos usando elipses congruentes.

rotacional de $360/n$ grados, entonces el número n es necesariamente primo. No se conocen diagramas simétricos para todos los primos, de todas formas. En la Figura 1.1 mostramos un diagrama de Venn para cinco conjuntos representados por elipses congruentes que tiene simetría rotacional — la construcción es debida a Branko Grünbaum [Grü1992a, Grü1992b].

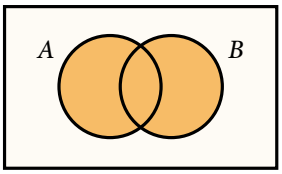
§1.4. Operaciones entre conjuntos

Unión

1.4.1. Si A y B son conjuntos, la ***unión*** de A y B es el conjunto $A \cup B$ tal que un elemento pertenece a $A \cup B$ si y solamente si pertenece a A o a B, esto es, tal que

$$x \in A \cup B \iff x \in A \text{ o } x \in B.$$

En términos de diagramas de Venn, la unión de A y B es



1.4.2. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) $A \subseteq A \cup B$ *y* $B \subseteq A \cup B$.

(*ii*) *Si* $A \subseteq C$ *y* $B \subseteq C$, *entonces* $A \cup B \subseteq C$.

(*iii*) *Se tiene que* $A \subseteq B$ *si y solamente si* $A \cup B = B$.

Demostración. (*i*) Si x es un elemento de A, entonces claramente se tiene que $x \in A$ o $x \in B$, y esto significa que $x \in A \cup B$: vemos así que $A \subseteq A \cup B$. Para ver la veracidad de la segunda parte del enunciado procedemos de exactamente la misma manera.

(*ii*) Supongamos que $A \subseteq C$ y que $B \subseteq C$ y mostremos que $A \cup B \subseteq C$. Sea x un elemento de $A \cup B$, de manera que $x \in A$ o $x \in B$. En el primer caso, de que $x \in A$ y que $A \subseteq C$ podemos deducir que $x \in C$; en el segundo, de que $x \in B$ y que $B \subseteq C$, que también $x \in C$. Así, en cualquier caso se tiene que $x \in C$ y esto prueba que todo elemento de $A \cup B$ es un elemento de C, esto es, que $A \cup B \subseteq C$, como queremos.

(*iii*) Supongamos primero que $A \subseteq B$. Como además es $B \subseteq B$, usando la parte (*ii*) que acabamos de probar podemos deducir que $A \cup B \subseteq B$. Por otro lado, la parte (*i*) nos dice que $B \subseteq A \cup B$. Juntando estas dos cosas, la Proposición 1.2.4(*ii*) nos permite concluir que $A \cup B = B$. Vemos así que si $A \subseteq B$, entonces $A \cup B = B$.

Probemos ahora la implicación recíproca: que si $A \cup B = B$, entonces $A \subseteq B$. Supongamos entonces que $A \cup B = B$. De la parte (*i*) de la proposición sabemos que $A \subseteq A \cup B$ y, por hipótesis, este último conjunto es igual a B, así que $A \subseteq B$, que es lo que queremos. □

1.4.3. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) $A \cup A = A$.

(*ii*) $A \cup \varnothing = A$.

(*iii*) $A \cup B = B \cup A$.

(*iv*) $(A \cup B) \cup C = A \cup (B \cup C)$.

Demostración. (*i*) De la Proposición 1.4.2(*i*) sabemos que $A \subseteq A \cup A$, y de la Proposición 1.4.2(*ii*), como $A \subseteq A$ y $A \subseteq A$, que $A \cup A \subseteq A$. Estas dos inclusiones nos dicen que $A \cup A = A$.

(*ii*) Como $A \subseteq A$ y $\varnothing \subseteq A$, de la Proposición 1.4.2(*ii*) tenemos que $A \cup \varnothing \subseteq A$. Por otro lado, de la Proposición 1.4.2(*i*) sabemos que $A \subseteq A \cup \varnothing$. Vemos así que $A \cup \varnothing = A$.

(*iii*) De la Proposición 1.4.2(*i*) sabemos que $A \subseteq B \cup A$ y que $B \subseteq B \cup A$ y entonces, gracias a la Proposición 1.4.2(*ii*), podemos concluir que $A \cup B \subseteq B \cup A$. Exactamente el mismo argumento pero intercambiando los roles de A y de B muestra que $B \cup A \subseteq A \cup B$ y, juntando todo, que $A \cup B = B \cup A$.

(*iv*) Sea x un elemento de $(A \cup B) \cup C$, de manera que o $x \in A \cup B$ o $x \in C$.

- En el segundo caso, tenemos que $x \in B \cup C$ y, por lo tanto que $x \in A \cup (B \cup C)$.
- En el primer caso, tenemos que o $x \in A$ o $x \in B$. Si $x \in A$, entonces claramente $x \in A \cup (B \cup C)$. Si en cambio $x \in B$, entonces $x \in B \cup C$ y, por lo tanto, $x \in A \cup (B \cup C)$.

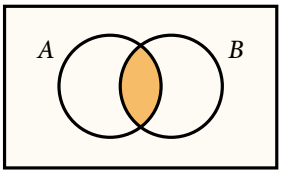
Vemos así que en cualquier caso se tiene que x pertenece a $A \cup (B \cup C)$, y esto prueba que $(A \cup B) \cup C \subseteq A \cup (B \cup C)$. Razonando de la misma manera podemos ver que también vale la inclusión recíproca, $A \cup (B \cup C) \subseteq (A \cup B) \cup C$, y concluir entonces que $(A \cup B) \cup C = A \cup (B \cup C)$, como afirma el enunciado. □

Intersección

1.4.4. Si A y B son conjuntos, la ***intersección*** de A y B es el conjunto $A \cap B$ de los elementos que pertenecen simultáneamente a A y a B, esto es, el conjunto tal que

$$x \in A \cap B \iff x \in A \text{ y } x \in B.$$

En términos de diagramas de Venn, la intersección de A y B es



Decimos que A y B son ***disjuntos*** si la intersección $A \cap B$ es vacía.

1.4.5. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) *$A \cap B \subseteq A$ y $A \cap B \subseteq B$.*

(*ii*) *Si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cap B$.*

(*iii*) *Se tiene que $A \subseteq B$ si y solamente si $A \cap B = A$.*

Demostración. (*i*) Si x es un elemento de $A \cap B$, entonces $x \in A$ y $x \in B$, así que, en particular, x es un elemento de A. Esto nos dice que todo elemento de $A \cap B$ es elemento de A, esto es, que se tiene que $A \cap B \subseteq A$. Que $A \cap B \subseteq B$ se prueba de la misma forma.

(*ii*) Supongamos que $C \subseteq A$ y que $C \subseteq B$ y mostremos que $C \subseteq A \cap B$. Sea x un elemento de C. Como $C \subseteq A$, de que x pertenezca a C podemos deducir que $x \in A$; de manera similar, de que

$C \subseteq B$ y $x \in C$ vemos que $x \in B$. Como x pertenece tanto a A como a B, pertenece a $A \cap B$. Esto muestra que bajo nuestras hipótesis es $C \subseteq A \cap B$, que es lo que queremos.

(*iii*) Mostremos primero que si $A \subseteq B$ entonces $A \cap B = A$. Supongamos, para ello, que $A \subseteq B$. De la parte (*i*) de la proposición sabemos que $A \cap B \subseteq A$. Por otro lado, si x es un elemento de A, entonces $x \in B$ porque $A \subseteq B$ y, en consecuencia, $x \in A \cap B$: esto muestra que todo elemento de A es pertenece a $A \cap B$, es decir, que $A \subseteq A \cap B$. Como valen las dos inclusiones, vemos de esta forma que $A \cap B = A$.

Mostremos ahora que si $A \cap B = A$ entonces $A \subseteq B$. Supongamos para ello que $A \cap B = A$ y sea x un elemento de A. Como x pertenece a A y $A = A \cap B$, tenemos por supuesto que $x \in A \cap B$ y, en particular, que x pertenece a B. Esto prueba que $A \subseteq B$. □

1.4.6. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) $A \cap A = A$.

(*ii*) $A \cap \varnothing = \varnothing$.

(*iii*) $A \cap B = B \cap A$.

(*iv*) $(A \cap B) \cap C = A \cap (B \cap C)$.

Demostración. (*i*) De la Proposición 1.4.5(*i*) sabemos que $A \cap A \subseteq A$. Por otro lado, como $A \subseteq A$, de la Proposición 1.4.5(*ii*) sabemos también que $A \subseteq A \cap A$. En definitiva, tenemos que $A = A \cap A$.

(*ii*) Es $A \cap \varnothing \subseteq \varnothing$ por la Proposición 1.4.5(*i*) y entonces, de acuerdo a la Proposición 1.2.6(*ii*), es $A \cap \varnothing = \varnothing$.

(*iii*) Sabemos que $A \cap B \subseteq B$ y que $A \cap B \subseteq A$, así que la Proposición 1.4.5(*ii*) implica que $A \cap B \subseteq B \cap A$. Intercambiando los roles de A y B en este razonamiento, vemos que también $B \cap A \subseteq A \cap B$ y, por lo tanto, que $A \cap B = B \cap A$.

(*iv*) Sea x un elemento de $(A \cap B) \cap C$. Se tiene entonces que $x \in A \cap B$ y que $x \in C$, y que x pertenezca a $A \cap B$ implica que $x \in A$ y que $x \in B$. Ahora bien, como $x \in B$ y $x \in C$, es $x \in B \cap C$; como además $x \in A$, tenemos que $x \in A \cap (B \cap C)$. Vemos de esta forma que

$$(A \cap B) \cap C \subseteq A \cap (B \cap C). \tag{4}$$

Para probar la inclusión recíproca, observemos que

$$\begin{aligned}
A \cap (B \cap C) &= A \cap (C \cap B) && \text{porque } B \cap C = C \cap B, \text{ en vista de la parte } (iii)\\
&= (C \cap B) \cap A && \text{otra vez por la parte } (iii)\\
&\subseteq C \cap (B \cap A) && \text{porque ya sabemos que } (4) \text{ vale}\\
&= (B \cap A) \cap C && \text{por } (iii)\\
&= (A \cap B) \cap C && \text{por la misma razón.}
\end{aligned}$$

En definitiva, tenemos que $(A \cap B) \cap C = A \cap (B \cap C)$, como afirma el enunciado. □

1.4.7. Las Proposiciones 1.4.5 y 1.4.6 sobre la intersección de conjuntos son completamente paralelas a las Proposiciones 1.4.2 y 1.4.3, que se refieren a la unión. El siguiente resultado, por su parte, nos dice cómo se relacionan entre sí las operaciones de unión e intersección.

Proposición. *Sean A, B y C tres conjuntos.*
(*i*) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
(*ii*) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

La primera parte de esta proposición nos dice que la unión se ***distribuye*** sobre intersecciones, de manera similar a como el producto de números de distribuye sobre sumas: sabemos que si a, b y c son números, vale que $(a + b) \cdot c = a \cdot c + b \cdot c$. De manera similar, la segunda parte de la proposición afirma que la intersección se distribuye sobre uniones.

Demostración. (*i*) Probaremos la igualdad que afirma el enunciado mostrando que los dos conjuntos que aparecen a los lados del signo = se contienen mutuamente.

Empezamos probando que $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$. Para ello, supongamos que x es un elemento de $(A \cap B) \cup C$, de manera que x está en $A \cap B$ o x están en C.

- Si $x \in C$, entonces claramente $x \in A \cup C$ y $x \in B \cup C$, así que $x \in (A \cup C) \cap (B \cap C)$.
- Si en cambio $x \in A \cap B$, entonces sabemos que tanto $x \in A$ como $x \in B$. De lo primero deducimos que $x \in A \cup C$ y de lo segundo que $x \in B \cup C$ y, juntando estas dos cosas, que $x \in (A \cup C) \cap (B \cup C)$.

En cualquier caso, entonces, se tiene que $x \in (A \cup C) \cap (B \cup C)$ y esto prueba que, como queríamos,

$$(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C). \tag{5}$$

Veamos ahora la inclusión recíproca: supongamos que x es un elemento de $(A \cap C) \cup (B \cap C)$ y mostremos que necesariamente es también un elemento de $(A \cup B) \cap C$. La hipótesis nos dice, otra vez, que x pertenece a $A \cap C$ o a $B \cap C$.

- Si $x \in A \cap C$, entonces tenemos que $x \in A$ y que $x \in C$. De lo primero se deduce que $x \in A \cup B$, y de todo que $x \in (A \cup B) \cap C$.
- Si $x \in B \cap C$, entonces tenemos que $x \in B$ y que $x \in C$. Lo primero implica que $x \in A \cup B$ y esto y lo segundo que $x \in (A \cup B) \cap C$.

Vemos así que x pertenece a $(A \cup B) \cap C$ independientemente de en qué caso estemos, y esto muestra que

$$(A \cup C) \cap (B \cup C) \ \subseteq (A \cap B) \cup C. \tag{6}$$

Finalmente, de (5) y de (6) vemos que $(A \cup C) \cap (B \cup C) \ \subseteq (A \cap B) \cup C$, como queremos.

(*ii*) Probaremos esta igualdad, como la anterior, mostrando que ambos conjuntos se contienen mutuamente. Sea x un elemento de $(A \cup B) \cap C$. Sabemos que $x \in C$ y que $x \in A \cup B$, de manera que $x \in A$ o $x \in B$. En el primer caso tenemos que $x \in A \cap C$ y, por lo tanto, que $x \in (A \cap C) \cup (B \cap C)$. En el segundo tenemos que $x \in B \cap C$ y, por lo tanto, que $x \in (A \cap C) \cup (B \cap C)$. En cualquier caso, entonces, es $x \in (A \cap C) \cup (B \cap C)$, de manera que

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C). \tag{7}$$

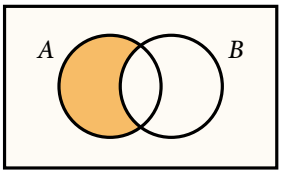
Supongamos ahora que x es un elemento de $(A \cap C) \cup (B \cap C)$. Si $x \in A \cap C$, entonces $x \in A$ y $x \in C$, así que $x \in A \cup B$ y, más aún, que $x \in (A \cup B) \cap C$. Si en cambio $x \in B \cap C$, entonces $x \in B$ y $x \in C$, así que $x \in A \cup B$ y $x \in (A \cup B) \cap C$. Vemos de esta forma que $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$ y esto, junto con (7), prueba que $(A \cap C) \cup (B \cap C) = (A \cup B) \cap C$, completando la prueba de la proposición. □

Diferencia

1.4.8. Si A y B son conjuntos, la ***diferencia*** de A y B es el conjunto $A \setminus B$ cuyos elementos son precisamente los elementos de A que no son elementos de B, esto es, el conjunto tal que

$$x \in A \setminus B \iff x \in A \text{ y } x \notin B.$$

En términos de diagramas de Venn, la diferencia de $A \setminus B$ es



Muchos autores escriben $A - B$ a lo que nosotros aquí escribimos $A \setminus B$.

1.4.9. Observemos que de la definición del conjunto $A \setminus B$ se siguen inmediatamente que

$$x \notin A \setminus B \implies x \notin A \text{ o } x \in B.$$

En efecto, esta implicación es la contrarrecíproca de la implicación

$$x \in A \text{ y } x \notin B \implies x \in A \setminus B$$

que es parte de la definición de $A \setminus B$.

1.4.10. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) *El conjunto $A \setminus B$ está contenido en A y es disjunto de B.*

(*ii*) $A \setminus A = \varnothing$, $A \setminus \varnothing = A$ *y* $\varnothing \setminus A = \varnothing$.
(*iii*) *Si* $A \setminus B = B \setminus A$, *entonces* $A = B$.
(*iv*) *Es* $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$.

Demostración. (*i*) Si x es un elemento de $A \setminus B$, entonces de la definición misma de la diferencia de conjuntos sabemos que x pertenece a A: esto significa que $A \setminus B \subseteq A$ y prueba la primera afirmación. Para probar la segunda, supongamos por un momento que el conjunto $(A \setminus B) \cap B$ no es vacío, de manera que posee algún elemento x. Por supuesto se tiene en ese caso que $x \in B$. Por otro lado, es $x \in A \setminus B$ y, por lo tanto, $x \notin B$: esto es imposible. Esta contradicción muestra que nuestra suposición de que $(A \setminus B) \cap B$ no es vacío no puede ser cierta y podemos concluir de esto que $(A \setminus B) \cap B = \varnothing$, esto es, que los conjuntos $A \setminus B$ y B son disjuntos.

(*ii*) Supongamos que la diferencia $A \setminus A$ no es vacía, de manera que posee algún elemento x. Como $x \in A \setminus A$, de la definición de la diferencia tenemos que $x \in A$ y $x \notin A$: esto es imposible y esta contradicción provino de haber supuesto que el conjunto $A \setminus A$ no es vacío. Vemos así que debe ser $A \setminus A = \varnothing$.

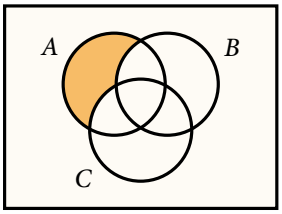
De la parte (*i*) sabemos que $A \setminus \varnothing \subseteq A$. Por otro lado, si x es un elemento de A, entonces claramente $x \notin \varnothing$, así que $x \in A \setminus \varnothing$: esto nos dice que $A \subseteq A \setminus \varnothing$ y, juntando todo, que $A \setminus \varnothing = A$. Finalmente, de la parte (*i*) sabemos que $\varnothing \setminus A \subseteq \varnothing$, así que usando la Proposición **1.2.6**(*ii*) podemos deducir que $\varnothing \setminus A = \varnothing$.

(*iii*) Supongamos que $A \setminus B = B \setminus A$ y mostremos que $A = B$ probando que los conjuntos A y B se contienen mutuamente. Sea x un elemento de A: si fuese $x \notin B$, entonces tendríamos que $x \in A \setminus B$ y como este último conjunto coincide con $B \setminus A$ por hipótesis y sabemos que $B \setminus A \subseteq B$, tendríamos que $x \in B$, lo que es absurdo. Vemos así que x necesariamente pertenece a B y, en definitiva, que $A \subseteq B$. Razonando de manera similar pero intercambiando los roles de A y de B vemos que además es $B \subseteq A$, así que, como queríamos, $A = B$.

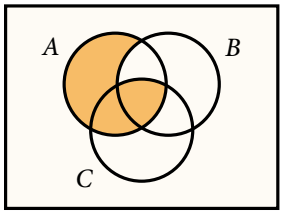
(*iv*) Sea x un elemento de $(A \setminus B) \setminus C$, de manera que $x \in A \setminus B$ y $x \notin C$. Como $x \in A \setminus B$, entonces $x \in A$ y $x \notin B$. En particular, de que x no pertenezca a B deducimos que $x \notin B \setminus C$ y, juntando todo, que $x \in A \setminus (B \setminus C)$. □

1.4.11. Observemos que no es cierto que valga la igualdad en la Proposición **1.4.10**(*iv*). Por ejemplo, si tomamos $A = C = \{1\}$ y $B = \varnothing$, entonces el conjunto $(A \setminus B) \setminus C = \varnothing$ esta contenido propiamente en $A \setminus (B \setminus C) = \{1\}$. En general, los conjuntos que aparecen en ese enunciado tienen los diagramas

de Venn siguientes:



$(A \setminus B) \setminus C$



$A \setminus (B \setminus C)$

Esto nos dice que la operación de diferencia de conjuntos no es, en general, asociativa y, más aún, nos sugiere cuándo sí lo es.

1.4.12. Ejercicio. Sean A, B y C tres conjuntos. Pruebe que $(A \setminus B) \setminus C = A \setminus (B \setminus C)$ si y solamente si $A \cap C = \varnothing$.

1.4.13. La siguiente proposición nos describe algunas de las formas en las que la diferencia interactúa con las otras operaciones de conjuntos.

Proposición. *Sean A, B y C tres conjuntos.*

(*i*) *Es* $(A \setminus B) \setminus C = A \setminus B \cup C$.
(*ii*) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
(*iii*) $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.
(*iv*) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Demostración. Probaremos cada una de las cuatro igualdades que afirma esta proposición mostrando que los dos conjuntos involucrados se contienen mutuamente.

(*i*) Sea x un elemento de $(A \setminus B) \setminus C$, de manera que $x \in A \setminus B$ y $x \notin C$. Se tiene entonces que $x \in A$ y que $x \notin B$, así que $x \notin B \cup C$ y, por lo tanto, podemos concluir, como queremos, que $x \in A \setminus B \cup C$. Vemos así que $(A \setminus B) \setminus C \subseteq A \setminus B \cup C$.

Sea, por otro lado, x un elemento de $A \setminus B \cup C$, de forma que $x \in A$ y $x \notin B \cup C$. De esto último se deduce que $x \notin B$ y que $x \notin C$, así que tenemos que $x \in A \setminus B$ y, finalmente, que $x \in (A \setminus B) \setminus C$. Esto nos dice que $A \setminus B \cup C \subseteq (A \setminus B) \setminus C$.

(*ii*) Sea x un elemento de $A \setminus (B \setminus C)$. Se tiene entonces que $x \in A$ y $x \notin B \setminus C$ y, por lo tanto, que $x \notin B$ o $x \in C$. En el primer caso tenemos que $x \in A \setminus B$ y en el segundo que $x \in A \cap C$: vemos así que en cualquier caso es $x \in (A \setminus B) \cup (A \cap C)$. Esto muestra que $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup (A \cap C)$.

Supongamos, por otro lado, que x es un elemento de $(A \setminus B) \cup (A \cap C)$. Si $x \in A \setminus B$, entonces $x \in A$ y $x \notin B$, así que $x \notin B \setminus C$ y, en definitiva, $x \in A \setminus (B \setminus C)$. Si en cambio es $x \in A \cap C$, entonces $x \in A$ y $x \notin B \setminus C$, así que $x \in A \setminus (B \setminus C)$. Esto prueba que $(A \setminus B) \cup (A \cap C) \subseteq A \setminus (B \setminus C)$ y, junto con la inclusión que probamos antes, que vale la igualdad del enunciado.

(*iii*) Sea x un elemento de $A \cup (B \setminus C)$. Si $x \in A$, entonces $x \in A \cup B$ y $x \notin C \setminus A$ y, por lo tanto, $x \in (A \cup B) \setminus (C \setminus A)$. Por otro lado, si $x \in B \setminus C$, entonces $x \in B$, de manera que $x \in A \cup B$, y $x \notin C$, de manera que $x \notin C \setminus A$ y, otra vez, $x \in (A \cup B) \setminus (C \setminus A)$. Concluimos de esta forma que $A \cup (B \setminus C) \subseteq (A \cup B) \setminus (C \setminus A)$.

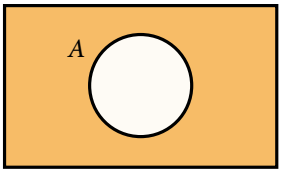
Sea ahora $x \in (A \cup B) \setminus (C \setminus A)$. Es $x \in A \cup B$ y $x \notin C \setminus A$. Si $x \in A$, entonces claramente $x \in A \cup (B \setminus C)$. Si $x \notin A$, entonces debe ser $x \in B$, ya que $x \in A \cup B$, y, como $x \notin C \setminus A$, debe ser también $x \notin C$, así que $x \in B \setminus C$ y, por lo tanto, $x \in A \cup (B \setminus C)$. Esto nos dice que $A \cup (B \setminus C) \subseteq (A \cup B) \setminus (C \setminus A)$ y, junto con la inclusión anterior, prueba lo que queremos.

(*iv*) Sea x un elemento de $A \cap (B \setminus C)$, de manera que $x \in A$ y $x \in B \setminus C$, es decir, $x \in B$ y $x \notin C$. Como $x \in A$ y $x \in B$, sabemos que $x \in A \cap B$; por otro lado, como $x \in A$ y $x \notin C$, es $x \notin A \cap C$. Estas dos cosas implican que $x \in A \cap B \setminus A \cap C$ y, en definitiva, que $A \cap (B \setminus C) \subseteq A \cap B \setminus A \cap C$.

Sea, para verificar la inclusión recíproca, x un elemento de $A \cap B \setminus A \cap C$, de forma que $x \in A \cap B$ y $x \notin A \cap C$. Lo primero nos dice que $x \in A$ y $x \in B$, mientras que lo segundo nos dice, dado que x pertenece a A, que $x \notin C$. Tenemos así que $x \in B \setminus C$ y, en consecuencia, que $x \in A \cap (B \setminus C)$. Esto prueba que $A \cap B \setminus A \cap C \subseteq A \cap (B \setminus C)$ y, en vista de la inclusión que ya probamos, que vale de hecho la igualdad. □

Complemento

1.4.14. Fijemos un conjunto $\mathscr{U}$, al que llamaremos en este contexto el ***conjunto de referencia*** o ***universal***, y representémoslo en los diagramas de Venn por el rectángulo exterior. Si A es un subconjunto de $\mathscr{U}$, llamamos ***complemento*** de A (con respecto al conjunto de referencia $\mathscr{U}$) al conjunto $A^c := \mathscr{U} \setminus A$. El diagrama de Venn de A^c es el siguiente.



Es importante observar que el complemento A^c depende de la elección del conjunto de referencia $\mathscr{U}$ y que solamente está definido para subconjuntos de este.

1.4.15. Proposición. *Sea $\mathscr{U}$ un conjunto de referencia y sean A y B dos subconjuntos de $\mathscr{U}$.*

(*i*) *Es $A \cup A^c = \mathscr{U}$ y $A \cap A^c = \varnothing$.*
(*ii*) *$\varnothing^c = \mathscr{U}$ y $\mathscr{U}^c = \varnothing$.*
(*iii*) *$(A^c)^c = A$.*
(*iv*) *$A \setminus B = A \cap B^c$.*

Observemos que si A es un subconjunto de $\mathscr{U}$, entonces su complemento A^c con respecto

a $\mathscr{U}$ también lo es, así que tiene sentido considerar su complemento $(A^c)^c$, como hicimos en la parte (*iii*) de esta proposición.

Demostración. (*i*) Es

$$\begin{aligned} A \cup A^c &= A \cup (\mathscr{U} \setminus A) \\ &= (A \cup \mathscr{U}) \setminus (A \setminus A) && \text{por la Proposición 1.4.13(iii)} \\ &= \mathscr{U} \setminus \varnothing && \text{porque } A \subseteq \mathscr{U} \\ &= \mathscr{U} \end{aligned}$$

y

$$\begin{aligned} A \cap A^c &= A \cap (\mathscr{U} \setminus A) \\ &= A \cap \mathscr{U} \setminus A \cap A && \text{por la Proposición 1.4.13(iv)} \\ &= A \setminus A && \text{porque } A \subseteq \mathscr{U} \\ &= \varnothing. \end{aligned}$$

(*ii*) Claramente $\varnothing^c = \mathscr{U} \setminus \varnothing = \mathscr{U}$ y $\mathscr{U}^c = \mathscr{U} \setminus \mathscr{U} = \varnothing$.
(*iii*) Es

$$\begin{aligned} (A^c)^c &= \mathscr{U} \setminus A^c \\ &= \mathscr{U} \setminus (\mathscr{U} \setminus A) \\ &= (\mathscr{U} \setminus \mathscr{U}) \cup (\mathscr{U} \cap A) && \text{por la Proposición 1.4.13(ii)} \\ &= \varnothing \cup A && \text{porque } A \subseteq \mathscr{U} \\ &= A. \end{aligned}$$

(*iv*) Sea x un elemento de $A \setminus B$, de manera que $x \in A$ y $x \notin B$. Como $A \subseteq \mathscr{U}$, de que $x \in A$ obtenemos que $x \in \mathscr{U}$ y, por lo tanto, que $x \in \mathscr{U} \setminus B = B^c$. Así, $x \in A \cap B^c$. Recíprocamente, si x es un elemento de $A \cap B^c$, entonces $x \in A$ y $x \in B^c = \mathscr{U} \setminus B$, de manera que $x \notin B$: vemos de esta forma que $x \in A \setminus B$. □

1.4.16. Las dos afirmaciones de la siguiente proposición son conocidas como las Leyes de Dualidad de De Morgan, por Augustus De Morgan, uno de los fundadores de la lógica moderna.

Proposición. *Sea $\mathscr{U}$ un conjunto de referencia y sean A y B dos subconjuntos de $\mathscr{U}$.*
(*i*) $(A \cup B)^c = A^c \cap B^c$.
(*ii*) $(A \cap B)^c = A^c \cup B^c$.

Observemos que si A y B son subconjuntos de $\mathscr{U}$, entonces $A \cup B$ y $A \cap B$ también lo son, así que tiene sentido considerar, como en esta proposición, los complementos $(A \cup B)^c$ y $(A \cap B)^c$

con respecto al conjunto $\mathscr{U}$.

Demostración. (*i*) Supongamos que x es un elemento de $(A \cup B)^c$, de manera que $x \in \mathscr{U}$ y $x \notin A \cup B$, y, por lo tanto, $x \notin A$ y $x \notin B$. Vemos así que $x \in \mathscr{U} \setminus A = A^c$ y que $x \in \mathscr{U} \setminus B = B^c$ y, entonces, que $x \in A^c \cap B^c$.

Recíprocamente, sea x un elemento de $A^c \cap B^c$. Es $x \in A^c$ y $x \in B^c$, así que $x \in \mathscr{U}$, $x \notin A$ y $x \notin B$: de esto se deduce que $x \notin A \cup B$ y, por lo tanto, que $x \in \mathscr{U} \setminus A \cup B = (A \cup B)^c$.

(*ii*) Podríamos probar esta afirmación procediendo de manera totalmente similar a como probamos la parte (*i*) — dejamos eso al lector — pero preferimos, para variar, seguir un camino alternativo. Tenemos que

$$\begin{aligned}(A \cap B)^c &= ((A^c)^c \cap (B^c)^c)^c && \text{porque } A = (A^c)^c \text{ y } B = (B^c)^c \\ &= ((A^c \cup B^c)^c)^c && \text{por la parte } (i) \text{ de la proposición} \\ &= A^c \cup B^c.\end{aligned}$$

Esta última igualdad es consecuencia de que $(X^c)^c = X$ para todo conjunto X y, en particular, cuando X es el conjunto $A^c \cup B^c$. □

1.4.17. Los resultados anteriores describen de qué manera se relaciona la operación de tomar el complemento de un conjunto con las demás operaciones entre conjuntos. El siguiente, por su parte, nos dice qué hace con las inclusiones: «las da vuelta».

Proposición. *Sea $\mathscr{U}$ un conjunto de referencia. Si A y B son dos subconjuntos de $\mathscr{U}$, entonces*

$$A \subseteq B \iff B^c \subseteq A^c.$$

Demostración. Sean A y B dos subconjuntos de $\mathscr{U}$, supongamos que $A \subseteq B$ y sea x un elemento de B^c. Como $x \in \mathscr{U}$ y $x \notin B$, entonces $x \notin A$ y, por lo tanto, $x \in \mathscr{U} \setminus A = A^c$. Esto prueba que

$$A \subseteq B \implies B^c \subseteq A^c.$$

Ahora bien, esto vale cualesquiera sean los conjuntos A y B: en particular, si como A elegimos a B^c y como B a A^c, nos dice que

$$B^c \subseteq A^c \implies (A^c)^c \subseteq (B^c)^c$$

y, como $(A^c)^c = A$ y $(B^c)^c = B$, que

$$B^c \subseteq A^c \implies A \subseteq B.$$

Con esto quedan probadas las dos implicaciones de la proposición. □

El principio de dualidad

1.4.18. Usando las Leyes de Dualidad de la Proposición 1.4.16 y la Proposición 1.4.17 podemos hacer una observación útil, que es conocida como el *principio de dualidad*. Antes que nada, demos dos ejemplos para mostrar de qué hablamos.

1.4.19. La primera parte de la Proposición 1.4.7 nos dice que

> *si A, B y C son tres conjuntos, entonces* $(A \cap B) \cup C = (A \cup C) \cap (B \cap C)$.

Esto es cierto cualesquiera sean los conjuntos A, B y C. En particular, si tenemos tres conjuntos X, Y y Z y como A, B y C elegimos a X^c, Y^c y Z^c, respectivamente, entonces sabemos que

$$(X^c \cap Y^c) \cup Z^c = (X^c \cup Z^c) \cap (Y^c \cup Z^c).$$

Ahora bien, usando las leyes de dualidad de De Morgan de la Proposición 1.4.16 podemos ver que el lado izquierdo de esta igualdad es

$$(X^c \cap Y^c) \cup Z^c = (X \cup Y)^c \cup Z^x = \big((X \cup Y) \cap Z\big)^c,$$

mientras que el lado derecho es

$$(X^c \cup Z^c) \cap (Y^c \cup Z^c) = (X \cap Z)^c \cap (Y \cap Z)^c = \big((X \cap Z) \cup (Y \cap Z)\big)^c,$$

así que aquella igualdad nos dice que

$$\big((X \cup Y) \cap Z\big)^c = \big((X \cap Z) \cup (Y \cap Z)\big)^c.$$

Esto implica — usando otra vez las leyes de dualidad — que

$$(X \cup Y) \cap Z = \Big(\big((X \cup Y) \cap Z\big)^c\Big)^c = \Big(\big((X \cap Z) \cup (Y \cap Z)\big)^c\Big)^c = (X \cap Z) \cup (Y \cap Z).$$

Hemos probado así que

> *si X, Y y Z son tres conjuntos, entonces* $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$.

Esta afirmación es, más allá de la elección de los nombres de los conjuntos, la segunda afirmación de la Proposición 1.4.7. Vemos así que podemos deducir la segunda afirmación de esa proposición de la primera usando las leyes de dualidad. Dejamos al lector la tarea de mostrar que usando esas leyes de dualidad podemos, recíprocamente, deducir la primera de la segunda y, en definitiva, que esas dos afirmaciones son equivalentes — al menos, si tenemos a mano las leyes de dualidad.

1.4.20. La Proposición 1.4.5 afirma en parte que que

si A y B son conjuntos, entonces $A \subseteq B$ exactamente cuando $A \cap B = A$.

Si X e Y son dos conjuntos cualesquiera, entonces podemos elegir en esa afirmación como A y B a los conjuntos Y^c y X^c: tenemos entonces que

$Y^c \subseteq X^c$ exactamente cuando $Y^c \cap X^c = Y^c$.

De la Proposición 1.4.17 sabemos que la afirmación $Y^c \subseteq X^c$ es equivalente a la afirmación $X \subseteq Y$. Por otro lado, de acuerdo a las leyes de dualidad de la Proposición 1.4.16 sabemos que $Y^c \cap X^c = (Y \cup X)^c$, así que la afirmación $Y^c \cap X^c = Y^c$ es equivalente a la afirmación $(Y \cup X)^c = Y^c$ y, por lo tanto, a la afirmación $Y \cup X = Y$. Juntando todo, vemos que lo que tenemos es que

$X \subseteq Y$ exactamente cuando $Y \cup X = Y$.

En definitiva, hemos probado que

si X e Y son conjuntos, entonces $X \subseteq Y$ exactamente cuand $Y \cup X = Y$,

y esto es esencialmente la tercera afirmación de la Proposición 1.4.2.

1.4.21. Estos dos ejemplos son parte de un fenómeno general: siempre que tenemos una afirmación sobre conjuntos podemos construir otra usando las leyes de dualidad de De Morgan de la Proposición 1.4.16 y la Proposición 1.4.17 de la misma forma en que lo hicimos en estos dos ejemplos, y el resultado es una nueva afirmación que es tan cierta como aquella con la que empezamos.

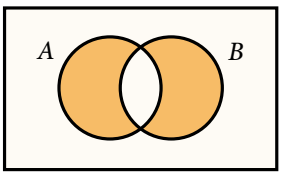
No es difícil probar esto — la dificultad consiste, sobre todo, en describir exactamente qué es lo que queremos decir cuando decimos «una afirmación sobre conjuntos» — y nos contentaremos con usar esta idea como forma de encontrar información.

Diferencia simétrica

1.4.22. Si A y B son dos conjuntos, la ***diferencia simétrica*** de A y B es el conjunto

$$A \triangle B \coloneqq A \cup B \setminus A \cap B.$$

En otras palabras, $A \triangle B$ es el conjunto de todos los elementos de A y de B que no están simultáneamente en A y en B. Por otro lado, en términos de diagramas de Venn, la diferencia simétrica de A y B es



1.4.23. Proposición. *Si A y B son conjuntos, entonces*

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Muchas veces, la diferencia simétrica de dos conjuntos se define usando la igualdad que nos da esta proposición.

Demostración. Sea x un elemento de $A \triangle B = A \cup B \setminus A \cap B$, de manera que $x \in A \cup B$ y $x \notin A \cap B$. Hay dos posibilidades:

- Puede ser que $x \in A$ y, como $x \notin A \cap B$, necesariamente es entonces $x \notin B$ y, por lo tanto, $x \in A \setminus B$.
- Si no, puede ser que $x \in B$, y entonces de que $x \notin A \cap B$ podemos deducir ahora que $x \notin A$ y que $x \in B \setminus A$.

En cualquiera de estos dos casos tenemos que $x \in (A \setminus B) \cup (B \setminus A)$ y, en definitiva, concluimos que $A \triangle B \subseteq (A \setminus B) \cup (B \setminus A)$.

Para probar la inclusión recíproca, sea x un elemento de $\in (A \setminus B) \cup (B \setminus A)$. Otra vez tenemos que considerar dos casos:

- Si $x \in A \setminus B$, entonces $x \in A$ y $x \notin B$, así que $x \in A \cup B$ y $x \notin A \cap B$, y podemos concluir que $x \in A \cup B \setminus A \cap B = A \triangle B$.
- Si $x \in B \setminus A$, entonces $x \in B$ y $x \notin A$, así que $x \in B \setminus A$ y $x \notin A \cap B$ y, como consecuencia de esto, otra vez tenemos que $x \in A \cup B \setminus A \cap B = A \triangle B$.

Vemos así que $(A \setminus B) \cup (B \setminus A) \subseteq A \triangle B$. □

1.4.24. Proposición. *Sean A, B y C tres conjuntos.*

(*i*) $A \triangle \varnothing = A$ *y* $A \triangle A = \varnothing$.
(*ii*) $A \triangle B = B \triangle A$.
(*iii*) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

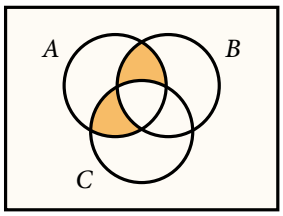
El conjunto de la parte (*iv*) de esta proposición está ilustrado en la Figura 1.2 en la página siguiente.

Demostración. Es

$$A \triangle \varnothing = A \cup \varnothing \setminus A \cap \varnothing = A \setminus \varnothing = A$$

y

$$A \triangle A = A \cup A \setminus A \cap A = A \setminus A = \varnothing,$$



$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$

Figura 1.2. El conjunto de la Proposición 1.4.24(*iii*).

y, de manera similar, tenemos que

$$A \triangle B = A \cup B \setminus A \cap B = B \cup A \setminus B \cap B = B \triangle A.$$

Por otro lado, es

$$\begin{aligned} A \cap (B \triangle C) &= A \cap (B \cup C \setminus B \cap C) \\ &= A \cap (B \cup C) \setminus A \cap B \cap C \\ &= (A \cap B) \cup (A \cap C) \setminus (A \cap B) \cap (A \cap C) \\ &= (A \cap B) \triangle (A \cap C). \end{aligned}$$

Con esto hemos probado todas las afirmaciones de la proposición. □

1.4.25. Proposición. *Sea $\mathscr{U}$ un conjunto de referencia. Si A y B son subconjuntos de $\mathscr{U}$, entonces*

$$(A \triangle B)^c = A^c \triangle B = A \triangle B^c.$$

Demostración. Sean A y B dos subconjuntos de U. Tenemos que

$$\begin{aligned} A^c \triangle B &= (\mathscr{U} \setminus A) \triangle B \\ &= ((\mathscr{U} \setminus A) \setminus B) \cup (B \setminus (\mathscr{U} \setminus A)) \\ &= (\mathscr{U} \setminus A \cup B) \cup ((B \setminus \mathscr{U}) \cup (A \cap B)) && \text{por 1.4.13(}i\text{) y 1.4.13(}ii\text{)} \\ &= (\mathscr{U} \setminus A \cup B) \cup (\varnothing \cup (A \cap B)) && \text{ya que } B \subseteq \mathscr{U} \\ &= (\mathscr{U} \setminus A \cup B) \cup (A \cap B), && (8) \end{aligned}$$

que

$$A \triangle B^c = B^c \triangle A \qquad \text{por 1.4.24(}ii\text{)}$$

$$= (\mathscr{U} \smallsetminus B \cup A) \cup (B \cap A) \qquad \text{por la igualdad (8)}$$
$$= (\mathscr{U} \smallsetminus A \cup B) \cup (A \cap B) \qquad \text{por 1.4.3(iii) y 1.4.6(iii)} \tag{9}$$

y que

$$\begin{aligned}(A \triangle B)^c &= \mathscr{U} \smallsetminus A \triangle B \\ &= \mathscr{U} \smallsetminus (A \cup \smallsetminus A \cap B) \\ &= (\mathscr{U} \smallsetminus A \cup B) \cup (\mathscr{U} \cap (A \cap B)) && \text{por 1.4.13(ii)} \\ &= (\mathscr{U} \smallsetminus A \cup B) \cup (A \cap B) && \text{porque } A \cap B \subseteq \mathscr{U}. \end{aligned} \tag{10}$$

Comparando (8), (9) y (10) obtenemos las igualdades del enunciado. □

§1.5. Tablas de verdad

1.5.1. Muchas de las demostraciones que hicimos en la sección anterior requirieron la consideración de varios casos. Cada vez que hacemos eso es importante ser sistemáticos, para asegurarnos de que no estamos dejando de lado alguna posibilidad. Hay varias estrategias para lograr eso. Veamos una de ellas.

1.5.2. Supongamos que queremos verificar que para cada par de conjuntos A y B se tiene que

$$A \smallsetminus A \triangle B = A \cap B. \tag{11}$$

Una forma de hacer esto es mostrar que cualquiera sea un objeto x vale que x pertenece a $A \smallsetminus A \triangle B$ exactamente cuando pertenece a $A \cap B$. Ahora bien: ¿cuándo pertenece a $A \smallsetminus A \triangle B$? Sabemos que pertenece a este conjunto si y solamente si pertenece a A y no a $A \triangle B$ y, más aún, que no pertenece a $A \triangle B$ si y solamente si o bien pertenece simultáneamente a A y a B o bien no pertenece a ninguno de esos dos conjuntos. Más allá de los detalles, es claro de todo esto que para decidir si x pertenece a $A \smallsetminus A \triangle B$ o no es suficiente con saber responder a las preguntas de si x pertenece o no a A y de si pertenece o no a B.

Ahora bien, ya observamos en la Sección 1.3 que hay cuatro posibilidades para las respuestas a

estas dos preguntas, que son las descriptas en cada una de las filas de la siguiente tabla.

¿$x \in A$?	¿$x \in B$?
No	No
No	Sí
Sí	No
Sí	Sí

En otras palabras, una vez que fijamos un objeto x, hay exactamente una fila de esta tabla que contiene la respuesta a las dos preguntas. Eso significa, entonces, que solo con saber cuál es la fila de la tabla que corresponde a x podemos decidir si x pertenece a $A \setminus A \triangle B$ o no. Mostremos cómo podemos hacer esto en detalle.

Primero, sabiendo qué fila corresponde a x ciertamente podemos decidir si x pertenece o no a $A \triangle B$. Extendemos entonces la tabla anterior con una columna que contiene la respuesta:

¿$x \in A$?	¿$x \in B$?	¿$x \in A \triangle B$?
No	No	No
No	Sí	Sí
Sí	No	Sí
Sí	Sí	No

Hecho eso, podemos extender la tabla una vez más con una columna en la que tabulamos, en cada uno de los casos representados por las filas de la tabla, la respuesta a la pregunta de si x pertenece o no a la diferencia $A \setminus A \triangle B$:

¿$x \in A$?	¿$x \in B$?	¿$x \in A \triangle B$?	¿$x \in A \setminus A \triangle B$?
No	No	No	No
No	Sí	Sí	No
Sí	No	Sí	No
Sí	Sí	No	Sí

(12)

Podemos hacer, por otro lado, una tabla que nos diga, para cada uno de los cuatro casos

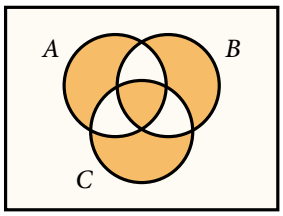


Figura 1.3. El conjunto $(A \triangle B) \triangle C$, que, de acuerdo a la Proposición 1.5.3, coincide con $A \triangle (B \triangle C)$.

representados por las filas, si x pertenece o no a $A \cap B$:

¿$x \in A$?	¿$x \in B$?	¿$x \in A \cap B$?
No	No	No
No	Sí	No
Sí	No	No
Sí	Sí	Sí

(13)

Observemos ahora que en las tablas (12) y (13) las columnas «¿$x \in A \setminus A \triangle B$?» y «¿$x \in A \cap B$?» son iguales: esto significa que en cada uno de los cuatro casos correspondientes a las filas de esas tablas el elemento x o bien pertenece a los dos conjuntos $A \setminus A \triangle B$ y $A \cap B$, o bien no pertenece a ninguno de los dos. El punto de todo esto es, por supuesto, que esto prueba que vale la igualdad (11): nos dice que no importa cuál de los cuatro casos corresponda a x, la respuesta a las dos preguntas «¿$x \in A \setminus A \triangle B$?» y «¿$x \in A \cap B$?» es la misma, así que los conjuntos $A \setminus A \triangle B$ y $A \cap B$ contienen exactamente los mismos elementos.

1.5.3. Veamos un ejemplo un poco más complicado de aplicación de esta idea:

Proposición. *Si A, B y C son tres conjuntos, entonces*

$$A \triangle (B \triangle C) = (A \triangle B) \triangle C.$$

En la Figura 1.3 ilustramos el conjunto que aparece en esta proposición.

Demostración. En este caso tenemos tres conjuntos, A, B y C, así que cuando consideramos las distintas posibilidades que hay de que un elemento x pertenezca a cada uno de ellos, tenemos ocho casos distintos. En cada uno de ellos tenemos que decidir si x pertenece o no a $A \triangle (B \triangle C)$ y a $(A \triangle B) \triangle C$: si en todos los casos la respuesta de las dos preguntas es la misma, entonces los dos conjuntos son iguales.

$¿x \in A?$	$¿x \in B?$	$¿x \in C?$	$¿x \in B \triangle C?$	$¿x \in A \triangle (B \triangle C)?$	$¿x \in A \triangle B?$	$¿x \in (A \triangle B) \triangle C?$
No	No	No	No	No	No	No
No	No	Sí	Sí	Sí	No	Sí
No	Sí	No	Sí	Sí	Sí	Sí
No	Sí	Sí	No	No	Sí	No
Sí	No	No	No	Sí	Sí	No
Sí	No	Sí	Sí	No	Sí	Sí
Sí	Sí	No	Sí	No	No	No
Sí	Sí	Sí	No	Sí	No	Sí

Tabla 1.1. La tabla de verdad de la prueba de la Proposición 1.5.3.

La Tabla 1.1 contiene todos los resultados necesarios. Notemos que incluimos columnas con la respuesta a las preguntas «¿$x \in A \triangle B$?» y «¿$x \in B \triangle C$?» en cada uno de los ocho casos, ya que estas sirven como pasos intermedios para calcular las columnas que verdaderamente nos interesan, que son la quinta y la séptima. Esas dos columnas son iguales, y esto significa que un elemento x pertenece a $A \triangle (B \triangle C)$ si y solamente si pertenece a $(A \triangle B) \triangle C$. Esto nos dice que estos dos conjuntos son iguales, como afirma la proposición. □

1.5.4. Consideremos otro ejemplo de cómo podemos usar estas «tablas de verdad», esta vez no para probar que dos conjuntos *son iguales*, sino que *son iguales bajo una hipótesis*.

Proposición. *Sean A, B y C tres conjuntos. Si $C \subseteq A$, entonces*

$$(A \cup B) \cap C^c = (B \setminus C) \cup (A \triangle C).$$

Demostración. Sean A, B y C tres conjuntos y supongamos que $C \subseteq A$. Otra vez tenemos tres conjuntos, así que hay en principio ocho posibilidades para la pertenencia de un elemento x a cada uno de ellos. La hipótesis que hicimos de que C está contenido en A hace, sin embargo, que algunos de esos casos sean imposibles: no puede ser que x pertenezca a C y no a A. Esto significa

¿$x \in A$?	¿$x \in B$?	¿$x \in C$?	¿$x \in A \cup B$?	¿$x \in (A \cup B) \cap C^c$?	¿$x \in B \setminus C$?	¿$x \in A \triangle C$?	¿$x \in (B \setminus C) \cup (A \triangle C)$?
No	No	No	No	No	No	No	No
No	No	Sí	No	No	No	Sí	Sí
No	Sí	No	Sí	Sí	Sí	No	Sí
No	Sí	Sí	Sí	No	No	Sí	Sí
Sí	No	No	Sí	Sí	No	Sí	Sí
Sí	No	Sí	Sí	No	No	No	No
Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	No	No	No	No

Tabla 1.2. La tabla de verdad de la prueba de la Proposición 1.5.4. Las filas marcadas en rojo son aquellas que corresponden a situaciones que no pueden ocurrir bajo la hipótesis de la proposición.

que cuando armemos la tabla que tabule todos los casos posibles hay que excluir todos aquellos en los que esa condición no se cumpla, que son dos: las marcamos en rojo en la Tabla 1.2.

Si comparamos la quinta columna de esa tabla con la octava, vemos que coinciden en todas sus entradas no marcadas en rojo. Esto prueba la proposición. □

Es importante notar que esas dos columnas no son completamente iguales: sus entradas correspondientes a las filas rojas son efectivamente distintas, y eso significa que la igualdad

$$(A \cup B) \cap C^c = (B \setminus C) \cup (A \triangle C)$$

es falsa en general. La tabla nos permite encontrar un ejemplo de esto: las dos columnas difieren en las entradas correspondientes a la primera de las filas rojas, así que basta encontrar tres conjuntos A, B y C tales que haya un elemento x que corresponda a esa fila, es decir, tal que $x \notin A$, $x \notin B$ y $x \in C$. Por ejemplo, podemos elegir $A = B = \varnothing$ y $C = \{1\}$. En ese caso es $(A \cup B) \cap C^c = C^c$ mientras que $(B \setminus C) \cup (A \triangle C) = C$, y estos dos conjuntos son efectivamente distintos.

Las columnas también difieren en sus entradas correspondientes a la segunda fila roja, en la que $x \notin A$, $x \in B$ y $x \in C$: esto nos sugiere otro ejemplo, con $A = \varnothing$ y $B = C = \{1\}$. Ahora

$(A \cup B) \cap C^c = \varnothing$ mientras que $(B \setminus C) \cup (A \triangle C) = C$.

1.5.5. Para terminar, demos un ejemplo de cómo podemos usar tablas de verdad para probar una inclusión de conjuntos.

Proposición. *Si A, B y C tres conjuntos, entonces* $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$.

Demostración. Fijemos tres conjuntos A, B y B, y sea x un objeto cualquiera. Como antes, si nos preguntamos si x pertenece o no a A, a B y a B, las tres respuestas que obtenemos determinan una de ocho posibilidades, y sabiendo las respuestas a esas preguntas podemos decidir si x pertenece o no a $(A \setminus B) \setminus C$ y si pertenece o no a $A \setminus (B \setminus C)$. La Tabla 1.3 tiene los resultados de hacer esto.

Sus columnas correspondientes a las preguntas «¿$x \in (A \setminus B) \setminus C$?» y «¿$x \in A \setminus (B \setminus C)$?» son distintas, y esto nos dice que los conjuntos $(A \setminus B) \setminus C$ y $A \setminus (B \setminus C)$ son, en general, distintos. Esto no es lo que nos interesa, de todas formas: queremos probar que el conjunto $(A \setminus B) \setminus C$ está contenido en $A \setminus (B \setminus C)$, no que es igual a él. Lo que tenemos que mostrar es que cada vez que elegimos un objeto x y este es un elemento de $(A \setminus B) \setminus C$, entonces x también es un elemento de $A \setminus (B \setminus C)$. En términos de nuestra Tabla 1.3: lo que tenemos que hacer es verificar que cada vez que elegimos una fila de esa tabla que tiene un Sí en la columna «¿$x \in (A \setminus B) \setminus C$?» también tiene un Sí en la columna «¿$x \in A \setminus (B \setminus C)$?». Esto efectivamente ocurre — de hecho, la única fila que tiene un Sí en la columna «¿$x \in (A \setminus B) \setminus C$?» es que pintamos de verde. Esto prueba la proposición. □

Como dijimos, los conjuntos $(A \setminus B) \setminus C$ y $A \setminus (B \setminus C)$ son en general distintos — ya que las columnas correspondientes en nuestra tabla son distintas. Tiene sentido, de todas formas, preguntarse *cuándo* son iguales — ciertamente es posible que lo sean, como ocurre cuando los tres conjuntos A, B y C son vacíos.

Supongamos por un momento que los conjuntos A, B y C son tales que $(A \setminus B) \setminus C = A \setminus (B \setminus C)$. Si elegimos un objeto cualquiera x, entonces las preguntas «¿$x \in (A \setminus B) \setminus C$?» y «¿$x \in A \setminus (B \setminus C)$?» tienen la misma respuesta. Mirando nuestra Tabla 1.3 notamos inmediatamente que no puede ser que x determine una de las filas que pintamos de rojo: en los casos descriptos por ellas x no pertenece a $(A \setminus B) \setminus C$ pero sí a $A \setminus (B \setminus C)$.

Vemos así que $(A \setminus B) \setminus C = A \setminus (B \setminus C)$, entonces no puede ser que

- haya algún objeto que pertenezca a A y a C pero no a B, porque a él correspondería la primera fila roja, no que
- hay algún objeto que terminar a A, a B y a C, ya que a él correspondería la segunda fila roja.

En otras palabras, lo que hemos observado es que

si $(A \setminus B) \setminus C = A \setminus (B \setminus C)$, *entonces* $A \cap B^c \cap C = \varnothing$ *y* $A \cap B \cap C = \varnothing$,

¿$x \in A$?	¿$x \in B$?	¿$x \in C$?	¿$x \in A \setminus B$?	¿$x \in (A \setminus B) \setminus C$?	¿$x \in B \setminus C$?	¿$x \in A \setminus (B \setminus C)$?
No	No	No	No	No	No	No
No	No	Sí	No	No	No	No
No	Sí	No	No	No	Sí	No
No	Sí	Sí	No	No	No	No
Sí	No	No	Sí	Sí	No	Sí
Sí	No	Sí	Sí	No	No	Sí
Sí	Sí	No	No	No	Sí	No
Sí	Sí	Sí	No	No	No	Sí

Tabla 1.3. La tabla de verdad de la prueba de la Proposición 1.5.5. Las filas marcadas en rojo son aquellas que corresponden a situaciones que no pueden ocurrir bajo la hipótesis de la proposición.

y esto nos da una condición necesaria para que sea $(A \setminus B) \setminus C = A \setminus (B \setminus C)$. Esta condición también es necesaria, esto es, vale que

> *si* $A \cap B^c \cap C = \varnothing$ *y* $A \cap B \cap C = \varnothing$, *entonces* $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.

Probemos esto, usando otra vez nuestra tabla. Supongamos que $A \cap B^c \cap C = \varnothing$ y $A \cap B \cap C = \varnothing$, y sea x un objeto cualquiera. De acuerdo a que x pertenezca o no a A, a B y a C queda determinada una de las filas de la Tabla 1.3, pero la hipótesis de que es $A \cap B^c \cap C = \varnothing$ y $A \cap B \cap C = \varnothing$ nos dice que, en realidad, los casos correspondientes a las filas que pintamos de rojo no pueden ocurrir. Para saber, entonces, si las respuestas a las preguntas «¿$x \in (A \setminus B) \setminus C$?» y «¿$x \in A \setminus (B \setminus C)$?» son las mismas lo que tenemos que hacer es ver si las columnas correspondientes a estas son iguales salvo, posiblemente, en las filas rojas. Como esto es así, podemos concluir que los dos conjuntos son iguales bajo nuestra hipótesis.

Juntado todo, hemos probado el siguiente resultado:

> *Sean A, B y C tres conjuntos. La igualdad* $(A \setminus B) \setminus C = A \setminus (B \setminus C)$ *vale si y solamente si* $A \cap B^c \cap C = \varnothing$ *y* $A \cap B \cap C = \varnothing$.

El siguiente ejercicio da una leve mejora de esto.

1.5.6. Ejercicio. Sean A, B y C tres conjuntos. Pruebe que $(A \smallsetminus B) \smallsetminus C = A \smallsetminus (B \smallsetminus C)$ si y solamente si $A \cap C = \varnothing$.

§1.6. Ejercicios

Identidades

1.6.1. Ejercicio. Sean A, B y C tres subconjuntos de un conjunto de referencia $\mathscr{U}$. Pruebe las siguientes afirmaciones.

(a) $A \cap B = A \smallsetminus (A \smallsetminus B) = B \smallsetminus (B \smallsetminus A) = A \smallsetminus A \triangle B = A \triangle (A \smallsetminus B)$.

(b) $A \cup B = (A \triangle B) \cup B = (A \triangle B) \triangle (A \cap B) = (A \smallsetminus B) \cup B$.

(c) $A \triangle B = (A \triangle C) \triangle (B \triangle C) = A^c \triangle B^c$.

(d) $A \smallsetminus B = A \smallsetminus (A \cap B) = A \cap (A \triangle B) = A \triangle (A \cap B) = B \triangle (A \cup B)$.

(e) $A \smallsetminus B = B \smallsetminus A \iff A = B$.

(f) $A \subseteq B \implies A \triangle B = B \smallsetminus A$.

(g) $A \cap (B \triangle C) = (A \cap B) \triangle (A \triangle C)$.

(h) $A \cup (B \triangle C) \supseteq (A \cup B) \triangle (A \cup C) = (B \triangle C) \smallsetminus A = (B \smallsetminus A) \triangle (C \smallsetminus A)$.

(i) $A \smallsetminus (B \smallsetminus C) \supseteq (A \smallsetminus B) \smallsetminus (A \smallsetminus C) = A \cap C \smallsetminus B$, y estos tres conjuntos son iguales si y solamente si $A \smallsetminus B = A \cap C$.

(j) $(A \smallsetminus B) \cap (A \smallsetminus C) = A \smallsetminus (B \cup C) \subseteq A \smallsetminus (B \cap C) = (A \smallsetminus C) \cup (A \smallsetminus C)$, y todos estos conjuntos son iguales si y solamente si $A \smallsetminus (B \cap C) \subseteq A \smallsetminus (B \cup C)$.

(k) $(A \star B) \smallsetminus C = (A \smallsetminus C) \star (B \smallsetminus C)$ cuando $\star$ es cualquiera de las operaciones $\cup$, $\cap$, $\triangle$ y $\smallsetminus$.

(l) $(A \smallsetminus B) \smallsetminus C = (A \smallsetminus C) \smallsetminus B$.

(m) $A \smallsetminus (B \smallsetminus C) \subseteq A \smallsetminus (C \smallsetminus B) \iff A \cap C \subseteq M \iff A \smallsetminus (C \smallsetminus B) = A$.

(n) $(A \cup B) \triangle (B \cup C) = (A \cup C) \smallsetminus B$.

(o) $(A \cap B) \triangle (B \cap C) = (A \cap B) \cup (B \cap C) \smallsetminus (A \cap B \cap C)$.

(p) $(A \smallsetminus B) \smallsetminus (B \smallsetminus C) = A \smallsetminus B$.

(q) $(A \cup B) \triangle (C \smallsetminus B) = B \cup (A \triangle C)$.

Uniones e intersecciones de familias de conjuntos

1.6.2. Si $\mathscr{F}$ es una familia de conjuntos, la ***unión*** de $\mathscr{F}$ y la ***intersección*** de $\mathscr{F}$ son los conjuntos que denotamos con los símbolos

$$\bigcup_{A\in\mathscr{F}} A \qquad \text{y} \qquad \bigcap_{A\in\mathscr{F}} A$$

tales que

$$x \in \bigcup_{A\in\mathscr{F}} A \iff \text{existe } A \in \mathscr{F} \text{ tal que } x \in A$$

y

$$x \in \bigcap_{A\in\mathscr{F}} A \iff \text{para cada } A \in \mathscr{F} \text{ se tiene que } x \in A.$$

Estas construcciones generalizan la unión y la intersección que ya vimos. En efecto, si X e Y son dos conjuntos, entonces la intersección y la unión de la familia $\mathscr{F} = \{X, Y\}$ son, respectivamente,

$$\bigcup_{A\in\mathscr{F}} A = X \cup Y, \qquad \bigcap_{A\in\mathscr{F}} A = X \cap Y.$$

1.6.3. Ejercicio. Si $\mathscr{F}$ es una familia de conjuntos y B es un conjunto, entonces

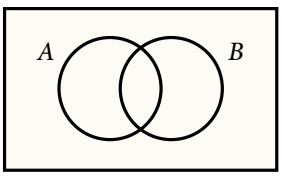
$$\bigcap_{A\in\mathscr{F}} (A \cup B) = \left(\bigcap_{A\in\mathscr{F}} A\right) \cup B, \qquad \bigcup_{A\in\mathscr{F}} (A \cap B) = \left(\bigcup_{A\in\mathscr{F}} A\right) \cap B$$

y si todos los miembros de la familia $\mathscr{F}$ están contenidos en un conjunto de referencia $\mathscr{U}$, entonces además

$$\left(\bigcap_{A\in\mathscr{F}} A\right)^c = \bigcup_{A\in\mathscr{F}} A^c, \qquad \left(\bigcup_{A\in\mathscr{F}} A\right)^c = \bigcap_{A\in\mathscr{F}} A^c.$$

Sistemas completos de operaciones

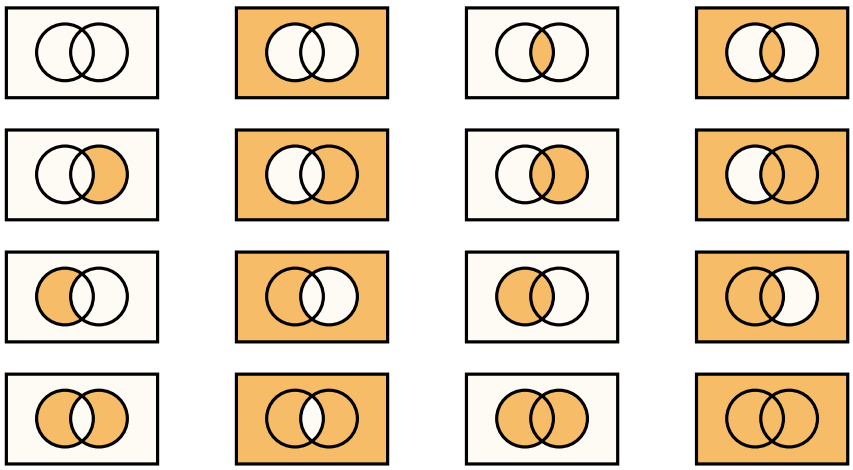
1.6.4. Sea $\mathscr{U}$ un conjunto de referencia y sean A y B dos subconjuntos de $\mathscr{U}$. Consideremos el diagrama de Venn correspondiente a esta situación:



El conjunto $\mathscr{U}$ queda divido así en 4 regiones:

$$A \setminus B, \qquad B \setminus A, \qquad A \cap B, \qquad (A \cup B)^c$$

y considerando uniones de ellas podemos armar 16 conjuntos distintos.



Esto significa que podemos describir estos 16 conjuntos a partir de A y de B usando las operaciones de unión, intersección, diferencia y complemento.

1.6.5. Ejercicio.

(*a*) Muestre que para describir estos 16 conjuntos a partir de A y B es suficiente usar únicamente las operaciones de unión y complemento, o las de intersección y complemento.

(*b*) Si X e Y son subconjuntos de $\mathscr{U}$, definimos dos nuevas operaciones $\downarrow$ y $\uparrow$ poniendo

$$X \downarrow Y = (X \cup Y)^c, \qquad X \uparrow Y = (X \cap Y)^c$$

Muestre que es posible describir cada uno de los 16 conjuntos del diagrama anterior a partir de A y B usando únicamente la operación $\downarrow$ y también usando únicamente la operación $\uparrow$. Así, por ejemplo, se tiene que

$$A \cap B = (A \downarrow A) \downarrow (B \downarrow B), \qquad A \cap B = (A \uparrow B) \uparrow (A \uparrow B).$$

Capítulo 2

Relaciones

§2.1. El producto cartesiano

2.1.1. Si A y B son dos conjuntos, el ***producto cartesiano*** de A y B es el conjunto $A \times B$ cuyos elementos son los pares ordenados (a, b) con $a \in A$ y $b \in B$.

Así, por ejemplo, si $A = \{1, 2\}$ y $B = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, entonces el producto cartesiano $A \times B$ tiene por elementos a los ocho pares

$$(1, \clubsuit) \quad (1, \diamondsuit) \quad (1, \heartsuit) \quad (1, \spadesuit) \quad (2, \clubsuit) \quad (2, \diamondsuit) \quad (2, \heartsuit) \quad (2, \spadesuit).$$

De manera similar, el conjunto $\mathbb{N} \times \mathbb{R}$ es el de todos los pares (n, r) con n un número natural y r un número real, $\mathbb{Z} \times \mathbb{Z}$ es el de todos los pares (a, b) con a y b números enteros y $\mathbb{R} \times \mathbb{R}$ es el conjunto de pares ordenados (x, y) de números reales.

2.1.2. Es fácil decidir cuándo el producto cartesiano de dos conjuntos es vacío:

Proposición. *Sean A y B dos conjuntos. El producto cartesiano $A \times B$ es vacío si y solamente si A es vacío o B es vacío.*

Demostración. Supongamos primero que $A \times B$ no es vacío. Esto significa que existe algún par ordenado (a, b) con $a \in A$ y $b \in B$ y, en particular, que ni A ni B son vacíos, ya que contienen, respectivamente, a a y a b.

Recíprocamente, supongamos que $A \times B$ es vacío y que A no lo es, de manera que existe un elemento a en A. Si B no fuera vacío, habría también un elemento b en B y podríamos, por lo tanto, construir el par ordenado (a, b): este par sería en ese caso un elemento de $A \times B$ y esto es

absurdo, ya que estamos suponiendo que el producto cartesiano es vacío. Vemos así que B debe ser necesariamente vacío y esto prueba la proposición. □

2.1.3. En el caso en que ambos factores son conjuntos finitos, el producto cartesiano es él mismo finito y podemos precisar su número de elementos:

Proposición. *Sean A y B dos conjuntos. Si A y B son finitos y poseen, respectivamente, n y m elementos, entonces el producto cartesiano $A \times B$ es finito y tiene exactamente nm elementos.*

Observemos que si A y B son finitos y alguno de los dos es vacío, de manera que $n = 0$ o $m = 0$, entonces esta proposición nos dice que $A \times B$ tiene $nm = 0$ elementos; recíprocamente, si $A \times B$ es vacío, es $nm = 0$ y, por lo tanto, alguno de n o m tiene que ser nulo. Esto es compatible, por supuesto, con lo que afirma la Proposición **2.1.2**.

Demostración. Supongamos que A y B son finitos y que tienen n y m elementos, respectivamente. Si alguno de A o B es vacío, de manera que alguno de los dos números n o m es nulo, ya sabemos que $A \times B$ es vacío y, por lo tanto, tiene $0 = nm$ elementos. Nos queda considerar, entonces, el caso en el que ni A ni B es vacío y, por lo tanto, en el que los números n y m son positivos.

Sean

$$a_1, \quad a_2, \quad \ldots, \quad a_n \tag{1}$$

los elementos de A listados en algún orden y sin repeticiones, sean

$$b_1, \quad b_2, \quad \ldots, \quad b_m \tag{2}$$

los de B en algún orden y, otra vez, sin repeticiones y consideremos los nm pares ordenados

$$\begin{array}{llll} (a_1, b_1), & (a_1, b_2), & \ldots, & (a_1, b_m), \\ (a_2, b_1), & (a_2, b_2), & \ldots, & (a_2, b_m), \\ \vdots & \vdots & \ddots & \vdots \\ (a_n, b_1), & (a_n, b_2), & \ldots, & (a_n, b_m). \end{array} \tag{3}$$

Todos ellos pertenecen a $A \times B$ y, de hecho, todo elemento de $A \times B$ es uno de ellos. En efecto, si (a, b) es un elemento de $A \times B$, entonces a es un elemento de A, así que aparece en la lista (1) y hay un índice i en $\{1, \ldots, n\}$ tal que $a = a_i$, y b es un elemento de B, así que aparece en la lista (2) y hay un índice j en $\{1, \ldots, m\}$ tal que $b = b_j$: el par (a, b) es entonces el par (a_i, b_j) y es uno de los que están listados en (3).

Por otro lado, los nm pares ordenados que escribimos en (3) son distintos dos a dos. Supongamos, por ejemplo, que los pares $x = (a_i, b_j)$ e $y = (a_k, b_l)$ son iguales. Eso significa que son iguales componente a componente: esto es, que $a_i = a_k$ y que $b_j = b_l$. Ahora bien, los elementos

de la lista (1) son distintos dos a dos y entonces como a_i y a_k son iguales se debe tener que los índices i y k mismos son iguales. Por la misma razón, los índices j y l son iguales, y vemos así que les pares x e y con los que empezamos aparecen en la tabla (3) en la misma posición.

Concluimos así que la lista (3) incluye todos los elementos de $A \times B$ sin repeticiones: como hay allí nm elementos, vemos que $A \times B$ tiene nm elementos y, en particular, que es un conjunto finito. Esto prueba la proposición. □

2.1.4. Observación. El lector atento habrá notado que en ningún momento dijimos qué es exactamente un *par ordenado*. Nos ocupamos aquí de esta cuestión.

Lo que queremos es alguna forma de poder construir a partir de dos objetos x e y un tercero, al que escribimos (x, y), de manera tal que se satisfaga la siguiente propiedad característica: cualesquiera sean los objetos x, y, x' e y',

$$(x, y) = (x', y') \iff x = x' \text{ e } y = y'.$$

Es importante observar que lo único que importa es que se cumpla esta propiedad, que esencialmente nos dice que podemos recuperar a partir de (x, y) a los objetos x e y.

Una forma de hacer esto es usar una idea propuesta originalmente por Kazimierz Kuratowski en 1921: si x e y son dos objetos cualesquiera, definimos

$$(x, y)_K \coloneqq \{\{x\}, \{x, y\}\}.$$

Veamos que esta definición tiene la propiedad que nos interesa. Sean x, y, x' e y' cuatro objetos cualesquiera. Es claro, por supuesto, que si $x = x'$ e $y = y'$, entonces

$$(x, y)_K = \{\{x\}, \{x, y\}\} = \{x', \{\{x'\}, y'\}\} = (x', y')_K.$$

Lo realmente interesante es que vale la implicación recíproca. Supongamos, para verlo, que $(x, y)_K = (x', y')_K$, esto es, que $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$, y consideremos los siguientes dos casos.

- Supongamos primero que $x = y$. En este caso es

  $$\{x', \{x', y'\}\} = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\},$$

  y, en particular, como $\{x', y'\}$ pertenece a $\{x', \{x', y'\}\}$, también pertenece a $\{\{x\}\}$ y, por lo tanto, tiene que ser igual a $\{x\}$. La igualdad $\{x', y'\} = \{x\}$ implica inmediatamente que $x' = x$ y que $y' = x = y$.
- Supongamos ahora que $x \neq y$. Tenemos que $\{x'\} \in \{\{x'\}, \{x', y'\}\} = \{\{x\}, \{x, y\}\}$, así que $\{x'\}$ es igual a $\{x\}$ o a $\{x, y\}$. En el segundo caso es $\{x'\} = \{x, y\}$, así que $x = x' = y$, y esto contradice nuestra hipótesis. Debe ser entonces $\{x'\} = \{x\}$ y, por lo tanto, $x' = x$.

De manera similar, tenemos que $\{x', y'\} \in \{\{x'\}, \{x', y'\}\} = \{\{x\}, \{x, y\}\}$, así que $\{x', y'\}$ es igual a $\{x\}$ o a $\{x, y\}$. En el primer caso es $\{x', y'\} = \{x\}$, de manera que $x' = x$ e $y' = x$: esto implica que

$$\{x, y\} \in \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} = \{\{x\}, \{x, x\}\} = \{\{x\}\}$$

y, por lo tanto, que $\{x, y\} = \{x\}$ y, en definitiva, que $y = x$, contradiciendo nuestra hipótesis. La conclusión de esto es que necesariamente vale que $\{x', y'\} = \{x, y\}$.

En particular, tenemos que $y' \in \{x', y'\} = \{x, y\}$, así que $y' = x$ o $y' = y$. Si $y' = x$, entonces $y' = x'$, porque ya sabemos que $x = x'$, y

$$\{x, y\} \in \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} = \{\{x'\}\},$$

así que $\{x, y\} = \{x'\}$ y, en consecuencia, $x = y$: esto otra vez contradice nuestra hipótesis. Debe ser entonces $y' = y$.

En cualquiera de los dos casos tenemos que $x = x'$ e $y = y'$, y esto prueba lo que queremos.

2.1.5. Ejercicio. Hay varias formas alternativas de construir pares ordenados a partir de conjuntos. Pruebe que si para cada para de objetos x e y definimos

$$(x, y)_W \coloneqq \{\{\{x\}, \varnothing\}, \{\{y\}\}\}$$

vale que

$$(x, y)_W = (x', y')_W \iff x = x' \text{ e } y = y'.$$

Esto nos dice que esta es una definición alternativa para los pares ordenados en términos de conjuntos — esta es debida a Robert Wiener.

§2.2. Relaciones

2.2.1. Si A y B son dos conjuntos, una ***relación de A a B*** es simplemente un subconjunto R del producto cartesiano $A \times B$. Llamamos a A el ***dominio*** de la relación R y a B su ***codominio***. Si a y b son elementos de A y de B, respectivamente, entonces cuando el par ordenado (a, b) pertenece a R decimos que a ***está relacionado*** con b por R y escribimos

$$a \; R \; b.$$

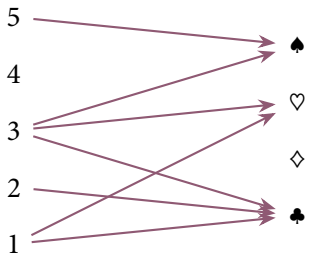
Si en cambio $(a, b) \notin R$, escribimos

$$a \not R\ b.$$

2.2.2. Consideremos un ejemplo sencillo. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{\clubsuit, \spadesuit, \diamond, \heartsuit\}$. El conjunto

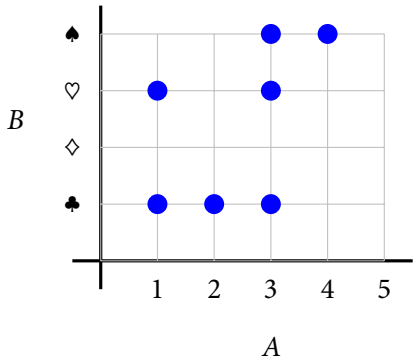
$$R = \{(1, \clubsuit),\ (1, \heartsuit),\ (2, \clubsuit),\ (3, \heartsuit),\ (3, \clubsuit),\ (3, \spadesuit),\ (4, \spadesuit)\}$$

es una relación de A a B. Una forma más eficiente de describir una relación como ésta, que va de un conjunto finito a otro, es dar un diagrama — al que llamamos el ***grafo*** de R — construido de la siguiente manera: ponemos a la izquierda del diagrama los elementos de A encolumnados, a la derecha los de B y conectamos un elemento a de A con uno b de B con una flecha si y solamente si el par ordenado (a, b) está en R. En el ejemplo anterior, si hacemos esto obtenemos el siguiente diagrama:



Observemos que en este dibujo bien puede haber elementos de A o de B que no estén conectados con ningún elemento del otro conjunto y elementos que estén conectados con más de uno.

También podemos usar para representar gráficamente nuestra relación R un diagrama — el ***gráfico*** de la relación — como

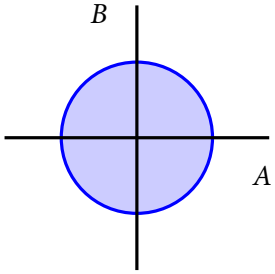


Aquí el eje horizontal y el vertical listan en algún orden y sin repeticiones los elementos de A y de B, respectivamente, y ponemos un punto por cada par ordenado de R de la manera evidente.

Esta última idea, a diferencia de la primera, puede usarse en ciertos casos para representar gráficamente relaciones entre conjuntos infinitos. Por ejemplo, si $A = B = \mathbb{R}$, entonces el conjunto

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 1\}$$

es una relación de $\mathbb{R}$ a $\mathbb{R}$ y podemos representarla gráficamente usando el dibujo



Aquí, como siempre, vemos a los puntos del plano como pares ordenados (x, y) con coordenadas $x \in A$ y $y \in B$, y pintamos los puntos que pertenecen a la relación.

2.2.3. Si A y B son conjuntos, siempre hay relaciones de A a B: esto es simplemente la observación de que el conjunto $\mathscr{P}(A \times B)$ de $A \times B$ no es vacío. Hay dos ejemplos extremos:

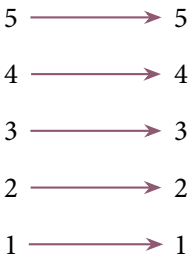
- la ***relación vacía*** de A a B es la relación $E = \varnothing \subseteq A \times B$, y
- la ***relación total*** de A a B es la relación $T = A \times B$.

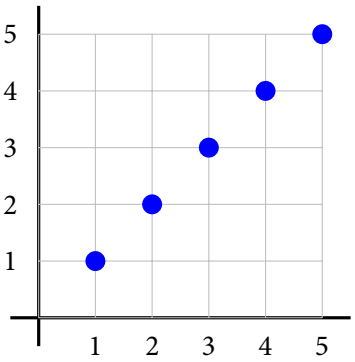
Es posible que la relación vacía de A a B y la relación total sean la misma relación: esto pasa exactamente cuando alguno de los conjuntos A o B es vacío.

2.2.4. Si A es un conjunto, llamamos a la relación

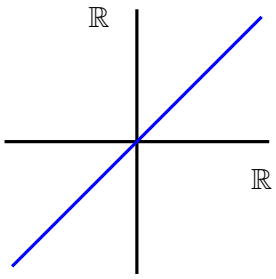
$$I_A = \{(a, b) \in A \times A : a = b\}$$

de A a A la ***relación identidad*** de A. Si por ejemplo $A = \{1, 2, 3, 4\}$, el grafo y el gráfico de la relación I_A son, respectivamente,





En cambio, el gráfico de la relación identidad $I_{\mathbb{R}}$ del conjunto $\mathbb{R}$ de los números reales es



§2.3. Operaciones entre relaciones

Composición de relaciones

2.3.1. Si A, B y C son conjuntos, y $R \subseteq A \times B$ y $S \subseteq B \times C$ son relaciones de A a B y de B a C, respectivamente, entonces podemos construir una nueva relación de A a C, la ***composición*** $S \circ R$ de S y R, poniendo

$$S \circ R \coloneqq \{(a, c) \in A \times C : \text{existe } b \in B \text{ tal que } a\ R\ b \text{ y } b\ S\ c\}.$$

Es importante observar que solamente consideramos esta construcción cuando el codominio de la relación R coincide con el dominio de la relación S.

2.3.2. Por ejemplo, si $A = \{\clubsuit, \diamond, \spadesuit, \heartsuit\}$, $B = \{1, 2, 3, 4, 5, 6\}$ y $C = \{$🔴, 🔵, 🟡, 🟢$\}$ y tenemos las relaciones

$$R = \{(\heartsuit, 1), (\heartsuit, 4), (\heartsuit, 6), (\spadesuit, 3), (\spadesuit, 6), (\clubsuit, 1), (\clubsuit, 2), (\clubsuit, 4)\}$$

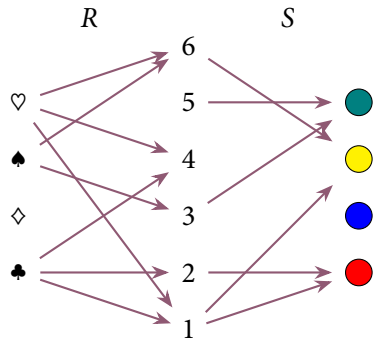
y

$$S = \{(1, 🔴), (1, 🟡), (2, 🔴), (3, 🟢), (5, 🟢), (6, 🟡)\},$$

entonces la composición de S y R es la relación de A a C

$$S \circ R = \{(\clubsuit, 🔴), (\spadesuit, 🟢), (\spadesuit, 🟡), (\heartsuit, 🔴), (\heartsuit, 🟡)\}. \tag{4}$$

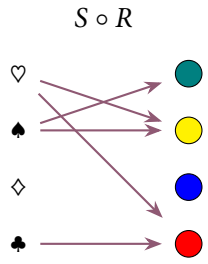
La forma más sencilla de verlo es construir el siguiente diagrama, que contiene simultáneamente el grafo de la relación R y el de la relación S:



(5)

Ahora bien, de acuerdo a la definición de la composición $S \circ R$, un elemento a de A está relacionado con uno c de C por la relación $S \circ R$ exactamente cuando hay un elemento b en B tal que $a\ R\ b$ y $b\ R\ c$. Así, por ejemplo, el par ordenado $(\heartsuit, \bigcirc)$ pertenece a $S \circ R$ porque existe un elemento en B — a saber, el 6 — tal que $(\heartsuit, 6) \in R$ y $(6, \bigcirc) \in S$: en términos del diagrama anterior, podemos decir que ♡ está conectado con ● en la relación $S \circ R$ porque se puede llegar del primero al segundo pasando por 6 a lo largo de las flechas. De la misma forma, como se puede llegar de ♣ a ● pasando por 1, el par $(\clubsuit, \bigcirc)$ pertenece a $S \circ R$. Notemos que también es posible llegar de ♣ a ● pasando por 2, pero esto no es importante: es suficiente con que haya *alguna* forma de llegar de uno al otro para que el correspondiente par ordenado esté en $S \circ R$. Finalmente, el par ordenado $(\spadesuit, \bigcirc)$ no es un elemento de $S \circ R$, ya que no hay forma de ir de ♠ a ● en el diagrama.

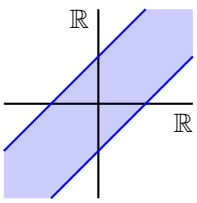
Considerando con cuidado todos los pares, fácilmente construimos el grafo de la relación $S \circ R$ a partir del diagrama (5), y obtenemos



La descripción de $S \circ R$ que dimos en (4) es simplemente una transcripción de esto.

2.3.3. Veamos otro ejemplo: sean los conjuntos A, B y C todos iguales a $\mathbb{R}$ y sea

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x - y| \leq 1\},$$



que es una relación de $\mathbb{R}$ a $\mathbb{R}$. Si x e y son elementos de $\mathbb{R}$, entonces $x\ R\ y$ si y solamente si la distancia entre x e y es a lo sumo 1. Afirmamos que

$$R \circ R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x - y| \leq 2\}. \tag{6}$$

Llamemos por un momento T a la relación de $\mathbb{R}$ a $\mathbb{R}$ que aparece en el miembro derecho de esta igualdad y probemos que $R \circ R = T$ probando las dos inclusiones entre los conjuntos $R \circ R$ y T.

Supongamos primero que (x, y) es un elemento de $R \circ R$, de manera que, de acuerdo a la definición de la composición, existe $z \in \mathbb{R}$ tal que $x\ R\ z$ y $z\ R\ y$. Esto significa que $|x - z| \leq 1$ y que $|z - y| \leq 1$ y entonces, gracias a la desigualdad triangular, tenemos que

$$|x - y| = |(x - z) - (z - y)| \leq |x - z| + |z - y| \leq 1 + 1 = 2.$$

Esto muestra que $(x, y) \in T$ y, en definitiva, que $R \circ R \subseteq T$.

Recíprocamente, supongamos que (x, y) es un elemento de T, de manera que $x, y \in \mathbb{R}$ y $|x - y| \leq 2$. Si ponemos $z = (x + y)/2$, tenemos que

$$|x - z| = \left|x - \frac{x + y}{2}\right| = \left|\frac{x - y}{2}\right| = \frac{|x - y|}{2} \leq \frac{2}{2} = 1$$

y, de manera similar, que

$$|z - y| \leq 1.$$

Esto nos dice que $x\ R\ z$ y que $z\ R\ y$ y, por lo tanto, que $(x, y) \in R \circ R$. Esto completa la prueba de nuestra afirmación (6).

2.3.4. La composición de relaciones es una operación asociativa:

Proposición. *Sean A, B, C y D conjuntos y $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$ relaciones de A a B, de B a C y de C a D, respectivamente. Se tiene que*

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Demostración. Sean $a \in A$ y $d \in D$.

Supongamos primero que (a, d) es un elemento de $T \circ (S \circ R)$. Esto significa que existe $c \in C$ tal que $(a, c) \in S \circ R$ y $(c, d) \in T$. La primera de estas dos cosas significa, a su vez, que existe $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Ahora bien, de que $(b, c) \in S$ y $(c, d) \in T$ podemos deducir que $(b, d) \in T \circ S$ y de esto y de que $(a, b) \in R$, que $(a, d) \in (T \circ S) \circ R$. Concluimos de esta forma que $T \circ (S \circ R) \subseteq (T \circ S) \subseteq R$.

Supongamos ahora que (a, d) es un elemento de $(T \circ S) \circ R$, de manera que existe $b \in B$ tal que $(a, b) \in R$ y $(b, d) \in T \circ S$. Esto último nos dice que existe $c \in C$ tal que $(b, c) \in S$ y $(c, d) \in T$. Como $(a, b) \in R$ y $(b, c) \in S$, sabemos que $(a, c) \in S \circ R$ y de esto y de que $(c, d) \in T$, que

$(a, d) \in T \circ (S \circ R)$. Esto prueba que $(T \circ S) \circ R \subseteq T \circ (S \circ R)$ y, junto con la inclusión anterior, la igualdad que aparece en el enunciado. □

2.3.5. Las relaciones identidades se comportan como elementos neutros para la composición:

Proposición. *Sean A y B dos conjuntos. Si $R \subseteq A \times B$ es una relación de A a B, entonces*

$$I_B \circ R = R = R \circ I_A.$$

Demostración. Mostremos la primera de las dos igualdades — la segunda puede probarse de exactamente la misma forma. Sean a y b elementos de A y de B, respectivamente, y supongamos primero que $(a, b) \in I_B \circ R$: esto significa que existe $b' \in B$ tal que $(b, b') \in I_B$ y $(a, b') \in R$. Pero si (b, b') está en I_B, entonces necesariamente $b' = b$ y, por lo tanto, tenemos que $(a, b) \in R$. Esto nos dice que $I_B \circ R \subseteq R$.

Recíprocamente, si (a, b) es un elemento de R, como además $(b, b) \in I_B$, tenemos que $(a, b) \in I_B \circ R$: vemos así que $R \subseteq I_B \circ R$, y esto prueba lo que queremos. □

Inversión de relaciones

2.3.6. Si A y B son dos conjuntos y R es una relación de A a B, la ***relación inversa*** de R es la relación de B a A

$$R^{-1} \coloneqq \{(x, y) \in B \times A : y \; R \; x\}.$$

Observemos que esto significa que si $x \in A$ e $y \in B$, entonces

$$y \; R^{-1} \; x \iff x \; R \; y.$$

El dominio y el codominio de la relación R^{-1} son, respectivamente, el codominio y el dominio de la relación de partida R.

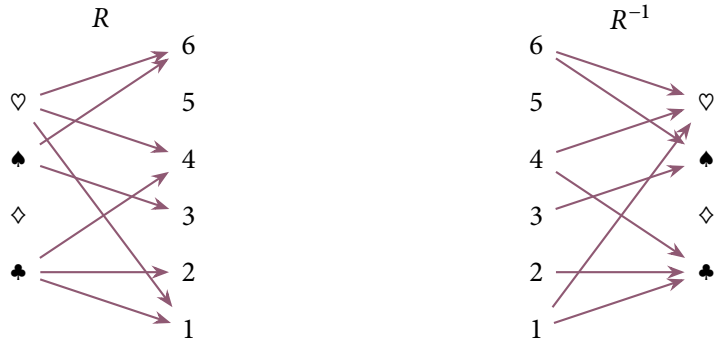
2.3.7. Por ejemplo, si $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ y $B = \{1, 2, 3, 4, 5, 6\}$, la relación inversa de

$$R = \{(\heartsuit, 1), (\heartsuit, 4), (\heartsuit, 6), (\spadesuit, 3), (\spadesuit, 6), (\clubsuit, 1), (\clubsuit, 2), (\clubsuit, 4)\}$$

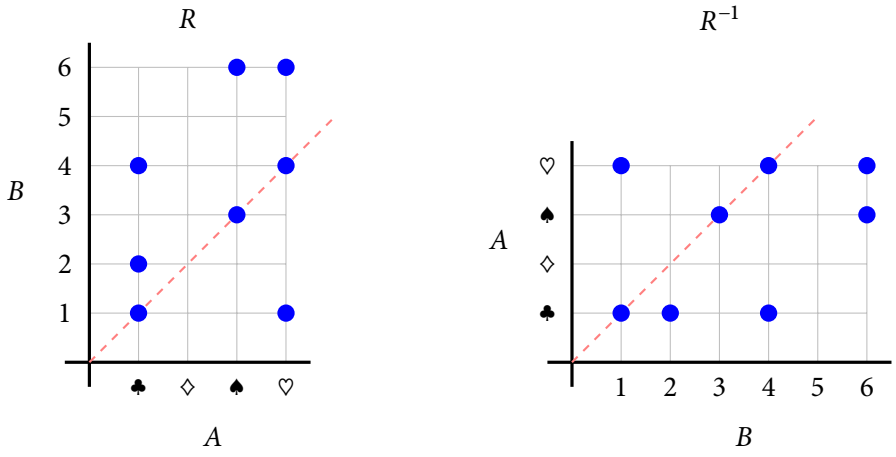
es

$$R^{-1} = \{(1, \heartsuit), (4, \heartsuit), (6, \heartsuit), (3, \spadesuit), (6, \spadesuit), (1, \clubsuit), (2, \clubsuit), (4, \clubsuit)\}.$$

Los grafos de estas relaciones son



y sus gráficos son



Es claro que el grafo de R^{-1} se obtiene del de R dando vuelta la dirección de las flechas e intercambiando de lugar las dos columnas de elementos, mientras que el gráfico de R^{-1} se obtiene del de R reflejando el diagrama con respecto a la diagonal — la linea punteada roja.

2.3.8. Proposición. *Sean A, B y C tres conjuntos. Si $R \subseteq A \times B$ es una relación de A a B y $S \subseteq B \times C$ una de B a C, entonces la relación inversa de la composición $S \circ R \subseteq A \times C$ es*

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Demostración. Sea R una relación de A a B y S una de B a C. Sean $c \in C$ y $a \in A$.

Supongamos primero que (c, a) es un elemento de $(S \circ R)^{-1}$. Esto significa que $(a, c) \in S \circ R$ y, por lo tanto, que existe $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Pero entonces tenemos que $(b, a) \in R^{-1}$ y $(c, b) \in S^{-1}$, así que $(c, a) \in S^{-1} \circ R^{-1}$. Vemos así que $(S \circ R)^{-1} \subseteq S^{-1} \circ R^{-1}$.

Supongamos ahora que (c, a) es un elemento de $R^{-1} \circ S^{-1}$. Esto significa que existe $b \in B$ tal que

$(c, b) \in S^{-1}$ y $(b, a) \in R^{-1}$, es decir, tal que $(b, c) \in S$ y $(a, b) \in R$. Estas dos cosas implican entonces que $(a, c) \in S \circ R$, de manera que $(c, a) \in (S \circ R)^{-1}$, y esto prueba que $R^{-1} \circ S^{-1} \subseteq (S \circ R)^{-1}$. □

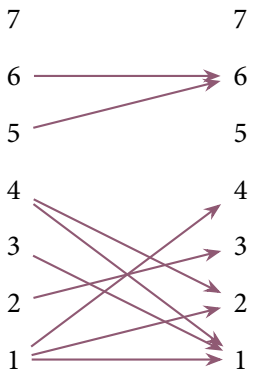
§2.4. Relaciones en un conjunto

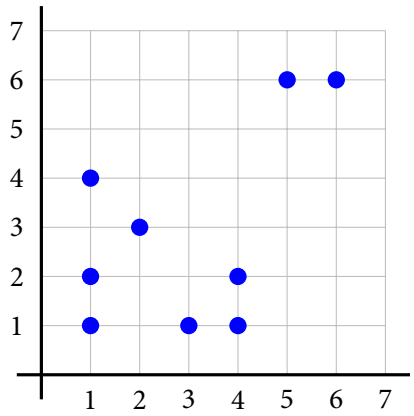
2.4.1. Si A es un conjunto y $R \subseteq A \times A$ es una relación de A a A, decimos que R es una ***relación en*** A. En esta situación A es tanto el dominio como el codominio de R.

Por ejemplo, si $A = \{1, 2, 3, 4, 5, 6, 7\}$, la relación

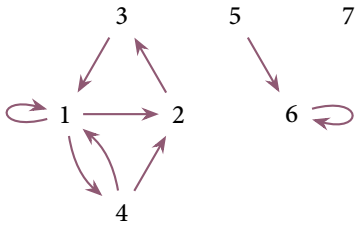
$$R = \{(1,1), (1,2), (2,3), (3,1), (1,4), (4,1), (4,2), (5,6), (6,6)\}$$

es una relación en A. Su grafo y su gráfico, respectivamente, son





En este caso, como el dominio y el codominio de R son ambos el mismo conjunto A, podemos dibujar el grafo poniendo una sola copia de cada elemento de A, de la siguiente manera:



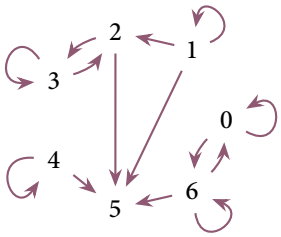
No hay ya necesidad de encolumnar los elementos de A y generalmente los ubicamos de la manera que haga que el diagrama sea lo más claro posible.

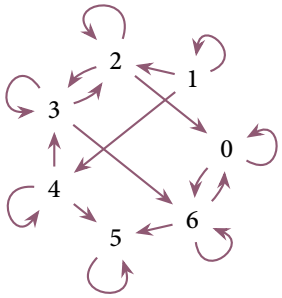
Casi siempre que hacemos un diagrama para una relación *en* un conjunto lo hacemos de esta forma. Observemos que es importante marcar la dirección de cada una de las flechas: bien puede ser que una relación tenga un par (x, y) pero no el par inverso (y, x), como en este ejemplo en el que $(1, 2)$ pertenece a R pero $(2, 1)$ no. De manera similar, la relación de nuestro ejemplo contiene el par $(1, 1)$ pero no el $(3, 3)$: marcamos en el diagrama la presencia del primero usando lo que llamamos un ***bucle***, una flecha que sale y llega al mismo lugar, como 1 ↻.

En el grafo de una relación R en un conjunto puede haber a lo sumo *dos* flechas entre dos elementos distintos x e y del su dominio: las que van en una y en otra dirección, correspondiendo a los pares (x, y) e (y, x) que, por supuesto, pueden o no pertenecer a la relación. Por otro lado, puede haber a lo sumo *una* flecha de un elemento x a sí mismo, correspondiendo a que el par ordenado (x, x) puede o no estar en R.

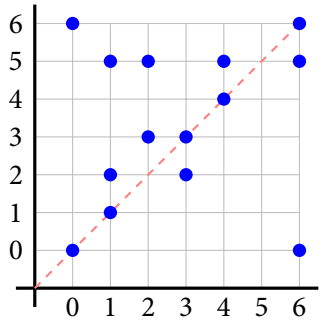
Relaciones reflexivas

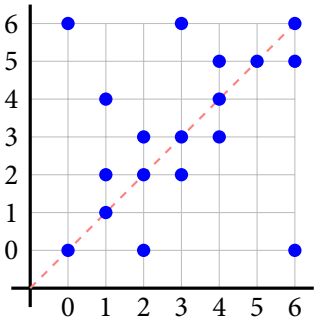
2.4.2. Una relación $R \subseteq A \times A$ en un conjunto A es ***reflexiva*** si para todo elemento a de A se tiene que $a \; R \; a$, es decir, que el par (a, a) pertenece a R. En términos del grafo de la relación R, esto significa que en cada uno de los puntos que representan a los elementos de A hay un bucle: así, de los siguientes dos grafos de relaciones en el conjunto $\{0, 1, 2, 3, 4, 5, 6\}$





sólo el de la derecha representa una que es reflexiva. En términos de los gráficos también es inmediato reconocer la reflexividad: por ejemplo, las dos relaciones que acabamos de considerar tienen gráficos





y que el segundo corresponda a una relación que es reflexiva mientras que el primero no se refleja en que todos los puntos que están sobre la diagonal roja están marcados en él, mientras que ése no es el caso en el primero.

2.4.3. La siguiente observación es inmediata:

Proposición. *Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A. La relación R es reflexiva si y solamente si contiene a la relación identidad I_A.*

Demostración. En efecto, esto es consecuencia directa de la definición de I_A. □

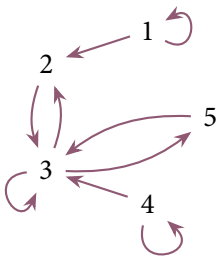
Relaciones simétricas

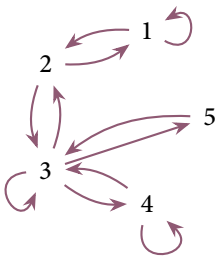
2.4.4. Una relación $R \subseteq A \times A$ en un conjunto A es ***simétrica*** si cada vez que a y b son elementos de A se tiene que

$$a \; R \; b \implies b \; R \; a.$$

En términos del grafo de la relación, esto significa que si a y b son dos elementos de A tales que hay una flecha que va de a a b en el grafo, entonces necesariamente hay también otra que va en la dirección contraria, esto es, de b a a.

2.4.5. Los siguientes grafos representan dos relaciones en el conjunto $A = \{1, 2, 3, 4, 5\}$





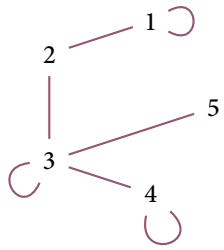
(7)

La primera no es simétrica: contiene la flecha que va de 4 a 3 pero no la que va de 3 a 4. En cambio, la segunda de estas relaciones es simétrica.

Cuando dibujamos el grafo de una relación simétrica cada flecha viene acompañada siempre de su flecha inversa. Para simplificar el dibujo podemos convenir en dibujar simplemente una linea entre dos elementos, sin dirección,

en lugar del par de flechas mutuamente inversas

Usando esta convención, podemos representar la relación del segundo diagrama de (7) con el dibujo más sencillo



Observemos que aquí también eliminamos la orientación de las flechas que forman bucles: claramente esa orientación no agrega información alguna.

2.4.6. Proposición. *Sea A un conjunto. Una relación $R \subseteq A \times A$ en A es simétrica si y solamente si es igual a su relación inversa, esto es, si y solamente si $R = R^{-1}$.*

Demostración. Sea R una relación en A y supongamos primero que R es simétrica: tenemos que mostrar que $R = R^{-1}$. Si (a, b) es un elemento de R, de manera que $a\ R\ b$, entonces la simetría de R nos dice que $b\ R\ a$, esto es, que $(b, a) \in R$: de acuerdo a la definición de R^{-1}, entonces, tenemos que $(a, b) \in R^{-1}$. Vemos así que $R \subseteq R^{-1}$, y un razonamiento exactamente análogo prueba que también $R^{-1} \subseteq R$, de manera que $R = R^{-1}$, como queremos.

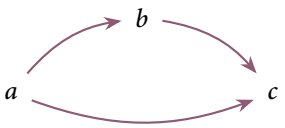
Supongamos ahora que $R = R^{-1}$ y probemos que R es necesariamente simétrica. Sean a y b dos elementos de R tales que $a\ R\ b$, esto es, tales que $(a, b) \in R$. Como $R = R^{-1}$ por nuestra hipótesis, esto nos dice que $(a, b) \in R^{-1}$ y, de acuerdo a la definición de la relación R^{-1}, que $(b, a) \in R$: la relación R es por lo tanto simétrica. □

Relaciones transitivas

2.4.7. Una relación $R \subseteq A \times A$ en un conjunto A es ***transitiva*** si cada vez que a, b y c son elementos de A se tiene que

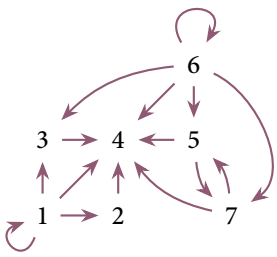
$$a\ R\ b \text{ y } b\ R\ c \implies a\ R\ c.$$

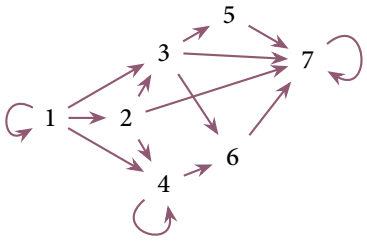
En términos del grafo de R, esto significa que si hay una flecha que va de a hasta b y otra que va de b hasta c, entonces tiene que haber también una flecha que va de a a c:



Así, la condición de transitividad es que si se puede llegar de un vértice a otro en dos pasos siguiendo las flechas, también se puede llegar en uno — en otras palabras, que siempre podemos tomar un "atajo".

2.4.8. Veamos algunos ejemplos. Si $A = \{1, 2, 3, 4, 5, 6, 7\}$, la primera de las dos relaciones siguientes es transitiva, mientras que la segunda no lo es.





En efecto, en la segunda tenemos por ejemplo la flecha que va de 2 a 4 y la de 4 a 6, pero no la de 2 a 6.

2.4.9. Proposición. *Sea A un conjunto. Una relación $R \subseteq A \times A$ en A es transitiva si y solamente si $R \circ R \subseteq R$.*

Demostración. Sea $R \subseteq A \times A$ una relación en el conjunto A.

Supongamos primero que R es transitiva y sea (a, c) un elemento de $R \circ R$, de manera que existe $b \in A$ tal que $(a, b) \in R$ y $(b, c) \in R$. Como R es transitiva, de esto se deduce que $(a, c) \in R$: vemos así que $R \circ R \subseteq R$.

Recíprocamente, supongamos que $R \circ R \subseteq R$ y veamos que R es una relación transitiva. Supongamos que a, b y c son tres elementos de A tales que $a \; R \; b$ y $b \; R \; c$. Se tiene entonces que los pares ordenados (a, b) y (b, c) están en R, así que el par (a, c) está en $R \circ R$. Ahora bien, estamos suponiendo que $R \circ R \subseteq R$, así que esto último implica que $(a, c) \in R$, es decir, que $a \; R \; c$. Concluimos de esta manera que R es transitiva, como queremos. □

§2.5. Relaciones de equivalencia

2.5.1. Una relación R en un conjunto A es una ***relación de equivalencia*** si es reflexiva, simétrica y transitiva.

2.5.2. Veamos algunos ejemplos de relaciones de equivalencia:

(*a*) La relación identidad I_A y la relación total $A \times A$ en un conjunto A son relaciones de equivalencia.

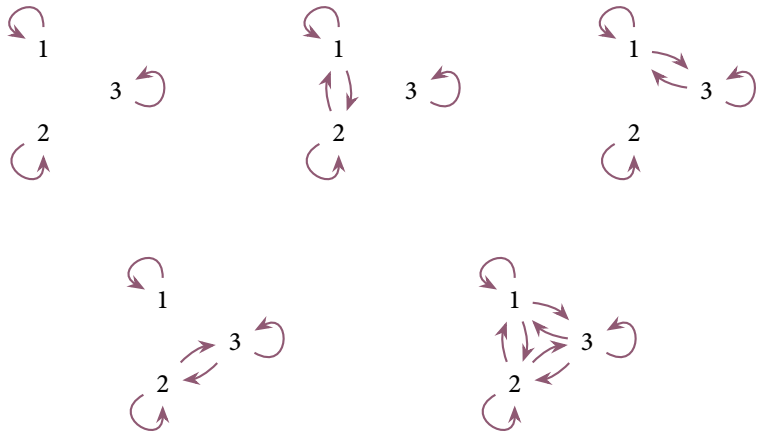
(*b*) Si $A = \{1\}$ tiene un único elemento, entonces hay dos relaciones en A — la vacía y la identidad — y la segunda de ellas es la única de las dos que es de equivalencia.

Si $A = \{1, 2\}$ tiene dos elementos, entonces sabemos que $A \times A$ tiene 4 elementos y, por lo tanto, que el conjunto de partes $\mathscr{P}(A \times A)$ tiene $2^4 = 16$: esto nos dice que hay 16 relaciones sobre el conjunto A. De todas ellas, hay exactamente *dos* que son relaciones de equivalencia: la relación identidad y la relación total. En efecto, supongamos que R es una relación de equivalencia sobre A. Como es reflexiva, sabemos que los pares $(1, 1)$ y $(2, 2)$ están en R. Por otro lado, puede ser que $(1, 2)$ esté o no en R. En el primer caso, como R es simétrica también está en ella el par $(2, 1)$ y vemos que están todos los pares: la relación es, por lo tanto, la relación total

Si en cambio el par $(1, 2)$ no está en R, entonces el par $(2, 1)$ tampoco — ya que la relación es simétrica — y, por lo tanto, la relación es la relación identidad de A,

Razonando de la misma forma, es fácil ver que sobre el conjunto $A = \{1, 2, 3\}$ hay cinco

relaciones de equivalencia:



En general, si un conjunto A es finito y tiene n elementos, llamamos n-ésimo ***número de Bell*** a la cantidad de relaciones de equivalencia que hay en A y lo escribimos B_n. El nombre recuerda a Eric Temple Bell, matemático y autor de ciencia ficción. Los primeros números de Bell son

n	1	2	3	4	5	6	7	8	9	10	11
B_n	1	2	5	15	52	203	877	4 140	21 147	115 975	678 570

Por supuesto, para contar las 115 975 relaciones de equivalencia que hay sobre un conjunto de 10 elementos se requiere una estrategia más eficiente que la que usamos arriba! En [OEI2023, A000110] puede encontrarse mucha información sobre esa secuencia de números.

(*c*) La relación $R \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto $\mathbb{Z}$ tal que para cada $x, y \in \mathbb{Z}$ se tiene que

$$x \; R \; y \iff |x| = |y|.$$

(*d*) La relación $R \subseteq \mathbb{R} \times \mathbb{R}$ en el conjunto $\mathbb{R}$ tal que cada vez que x e y son elementos de $\mathbb{R}$ se tiene que

$$x \; R \; y \iff x^2 - 2x + 2 = y^2 - 2y + 2.$$

(*e*) La relación $R \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto $\mathbb{Z}$ dada por

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y - x \text{ es par}\}.$$

Más generalmente, si $m \in \mathbb{N}$ tenemos una relación de equivalencia $R_m \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto $\mathbb{Z}$ dada por

$$R_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : m \text{ divide a } y - x\}.$$

Probemos que esto es, en efecto, una relación de equivalencia.

- Si x es un elemento de $\mathbb{Z}$, entonces $x - x = 0 \cdot m$, así que m divide a $x - x$ y, por lo tanto, tenemos que $x \; R_m \; x$. Vemos así que la relación R_m es reflexiva.
- Supongamos que x e y son elementos de $\mathbb{Z}$ tales que $x \; R_m \; y$, es decir, tales que m divide a $y - x$. Esto significa que existe $u \in \mathbb{Z}$ tal que $y - x = u \cdot m$. Por supuesto, tenemos entonces que $x - y = (-u) \cdot m$, así que m divide a la diferencia $x - y$ y, por lo tanto, $y \; R_m \; y$: vemos así que la relación R_m es simétrica.
- Finalmente, supongamos que x, y y z son elementos de $\mathbb{Z}$ tales que $x \; R_m \; y$ e $y \; R_m \; z$, de manera que m divide a $y - x$ y a $z - y$. Esto significa que existen enteros $u, v \in \mathbb{Z}$ tales que $y - x = u \cdot m$ e $z - y = v \cdot m$: usando esto, vemos que

  $$z - x = (z - y) + (y - x) = v \cdot m + u \cdot m = (v + u) \cdot m,$$

  así que m también divide a la diferencia $z - x$ y, por lo tanto, es $x \; R_m \; z$. Concluimos de esta forma que R_m es una relación transitiva.

Cuando x e y son dos enteros y se tiene que $x \; R_m \; y$, decimos que x e y son ***congruentes módulo*** m y normalmente escribimos

$$x \equiv y \mod m$$

en lugar de $x \; R_m \; y$. Esta relación de equivalencia es de extraordinaria importancia en teoría de los números enteros. Fue considerada de manera sistemática por primera vez por Carl Friedrich Gauss en su libro *Disquisitiones Arithmeticæ* — escrito en 1798, cuando tenía 21 años, y publicado 1801 — que es la fundación de la teoría moderna de números. La definición de la relación de congruencia ocupa, de hecho, la primera linea de ese texto — véase la Figura 2.1 en la página siguiente.

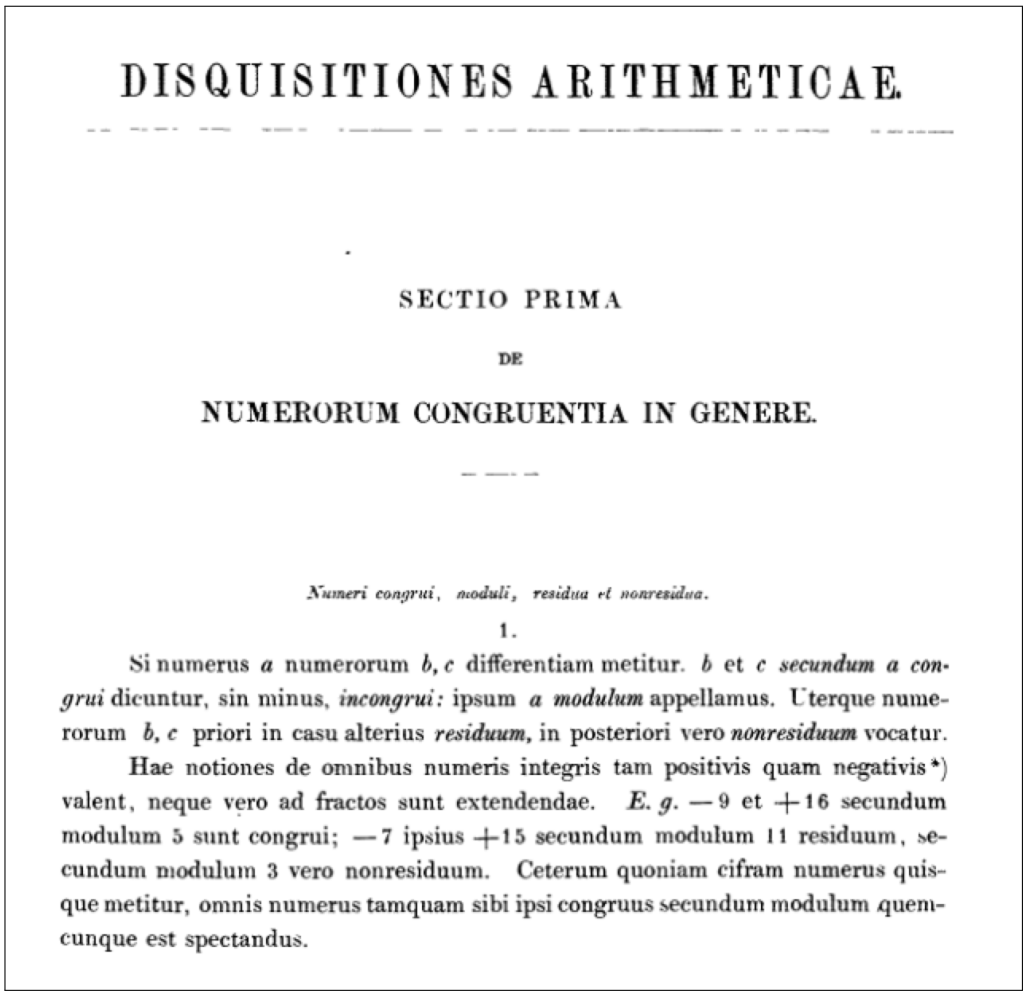
Clases de equivalencia

2.5.3. Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia sobre A. Si x es un elemento de A, entonces la ***clase de equivalencia*** de x en A con respecto a la relación R es el conjunto

$$[x] \coloneqq \{y \in A : x \; R \; y\}.$$

En otras palabras, la clase de equivalencia de x es el conjunto de todos los elementos de A que están relacionados por R con x. Llamamos ***conjunto cociente*** de A por R, y escribimos A/R, al conjunto de las clases de equivalencia de R en A:

$$A/R \coloneqq \{[x] : x \in A\}.$$



DISQUISITIONES ARITHMETICAE.

SECTIO PRIMA

DE

NUMERORUM CONGRUENTIA IN GENERE.

Numeri congrui, moduli, residua et nonresidua.

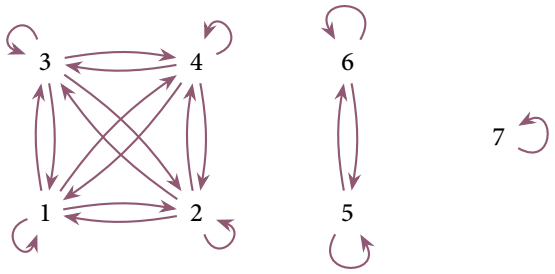
1.

Si numerus a numerorum b, c differentiam metitur. b et c ***secundum a congrui*** dicuntur, sin minus, ***incongrui:*** ipsum a ***modulum*** appellamus. Uterque numerorum b, c priori in casu alterius ***residuum,*** in posteriori vero ***nonresiduum*** vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis*) valent, neque vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

Figura 2.1. El primer párrafo de las *Disquisitiones Arithmeticæ* de Carl Friedrich Gauss, con la definición de la relación de congruencia. «Si un numero a divide la diferencia de números b y c, b y c se dicen congruentes y si no incongruentes. Llamamos a a el módulo y a cada uno de los números b y c residuos del otro en el primer caso y no residuos en el segundo. [...] Por ejemplo, -9 y 16 son congruentes módulo 5; -7 es residuo de 15 módulo 11 y no residuo módulo 3. Como 0 es divisible por todos los enteros, se sigue que podemos considerar a todo número congruente consigo mismo con respecto a un módulo cualquiera.»

Así, por ejemplo, si A es el conjunto $\{1, 2, 3, 4, 5, 6, 7\}$ y la relación R es la que tiene grafo



que es ciertamente una relación de equivalencia en A, entonces las clases de equivalencia de los elementos de A son

$$[1] = \{1, 2, 3, 4\}, \qquad [2] = \{1, 2, 3, 4\}, \qquad [3] = \{1, 2, 3, 4\}, \qquad [4] = \{1, 2, 3, 4\},$$
$$[5] = \{5, 6\}, \qquad [6] = \{5, 6\}, \qquad [7] = \{7\}.$$

En este ejemplo, entonces, las clases de equivalencia de la relación R son tres, a saber:

$$\{1, 2, 3, 4\}, \qquad \{5, 6\}, \qquad \{7\}.$$

El conjunto cociente de A por R es, por lo tanto,

$$A/R = \big\{\{1, 2, 3, 4\},\ \{5, 6\},\ \{7\}\big\}.$$

2.5.4. La siguiente es la observación más importante que podemos hacer sobre las clases de equivalencia de una relación de equivalencia:

Proposición. *Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia en A. Si x e y son elementos de A tales que $x \in [y]$, entonces $[x] = [y]$.*

Demostración. Sean x e y elementos de A tales que $x \in [y]$, es decir, tales que

$$y \ R \ x. \tag{8}$$

Queremos probar que $[x] = [y]$ y para ello probamos, como es usual, las inclusiones mutuas de los dos conjuntos $[x]$ e $[y]$. Supongamos entonces primero que u es un elemento de $[x]$, de manera que $x \ R \ u$. Como la relación R es transitiva, de esto y de la hipótesis (8) tenemos que $y \ R \ u$, esto es, que $u \in [y]$: esto muestra que $[x] \subseteq [y]$.

Recíprocamente, supongamos que u es un elemento de $[y]$, de manera que $y \ R \ u$ y, como R es simétrica, que $u \ R \ y$. De esto y de la hipótesis (8) tenemos que $u \ R \ x$ y, otra vez por la simetría, que $x \ R \ u$, es decir, que $u \in [x]$. Esto muestra que $[y] \subseteq [x]$ y completa la prueba de la proposición. □

2.5.5. Vamos cuáles son las clases de equivalencia de las relaciones de equivalencia que listamos en 2.5.2.

(*a*) Sea A un conjunto y sea $R = I_A$ la relación identidad de A. Si $x \in A$, entonces la clase de equivalencia $[x]$ es el conjunto $\{x\}$. En efecto, si $y \in A$ es tal que $x\ R\ y$, entonces se sigue inmediatamente de la definición de la relación que necesariamente $y = x$: esto muestra que $[x] \subseteq \{x\}$. Por otro lado, como $x\ R\ x$ porque R es reflexiva, tenemos que $x \in [x]$ y, en consecuencia, que $\{x\} \subseteq [x]$. Vemos así que $[x] = \{x\}$, como dijimos. En este ejemplo, entonces, hay tantas clases de equivalencia como elementos hay en A y el conjunto cociente es

$$A/R = \big\{\{x\} : x \in A\big\}.$$

(*b*) Sea A un conjunto y consideremos ahora la relación total $R = A \times A$ en A. En este caso, cualquiera sea el elemento x en A la clase de equivalencia de x es $[x] = A$ y, por lo tanto, hay exactamente una clase de equivalencia, todos los elementos de A tienen la misma clase de equivalencia y el conjunto cociente es

$$A/R = \{A\}.$$

(*c*) Sea $A = \mathbb{Z}$ y sea $R \subseteq \mathbb{Z} \times \mathbb{Z}$ la relación de equivalencia tal que si x e y están en $\mathbb{Z}$ entonces

$$x\ R\ y \iff |x| = |y|.$$

Sea $x \in \mathbb{Z}$. Un entero $y \in \mathbb{Z}$ pertenece a $[x]$ si $x\ R\ y$, es decir, si $|x| = |y|$, y esto ocurre exactamente cuando o $y = x$ o $y = -x$. Vemos así que la clase de equivalencia de x es $[x] = \{x, -x\}$. Esta clase tiene dos elementos, x y $-x$, cuando x es distinto de 0, y uno solo en caso contrario.

En este ejemplo dos elementos de $\mathbb{Z}$ tienen la misma clase de equivalencia si y solamente si son o iguales u opuestos. La clase de equivalencia de 0 tiene un único elemento, ya que $[0] = \{0\}$, mientras que todas las otras clases de equivalencia tienen exactamente dos. El conjunto cociente es

$$A/R = \{[x] : x \in \mathbb{N}_0\}.$$

(*d*) Sea ahora $A = \mathbb{R}$ y $R \subseteq \mathbb{R} \times \mathbb{R}$ la relación de equivalencia en $\mathbb{R}$ tal que si x e y son dos elementos de $\mathbb{R}$, entonces

$$x\ R\ y \iff x^2 - 2x + 2 = y^2 - 2x + 2.$$

Fijemos $x \in \mathbb{R}$ y encontremos la clase de equivalencia $[x]$ de x con respecto a R. Un número $y \in \mathbb{R}$ pertenece a $[x]$ si y solamente si $x\ R\ y$, es decir, si y solamente si

$$x^2 - 2x + 2 = y^2 - 2x + 2.$$

Observemos que podemos reescribir esta igualdad en la forma

$$(x-1)^2+1=(y-1)^2+1,$$

y entonces es claro que esa igualdad se cumple si y solamente si $y-1$ es igual a $x-1$ o a $-(x-1)$, es decir, si y es igual a x o a $2-x$. Vemos así que

$$[x]=\{x,2-x\}.$$

Si $x\neq 1$, entonces $x\neq 2-x$ y la clase de equivalencia $[x]$ tiene exactamente dos elementos; si en cambio es $x=1$, entonces $x=1=2-x$ y $[x]$ tiene un único elemento. Afirmamos que el conjunto cociente es, en este ejemplo,

$$A/R=\{[x]:x\in\mathbb{R},\ x\geq 1\}. \tag{9}$$

En efecto, sea $y\in\mathbb{R}$. Si $y\geq 1$, entonces claramente la clase $[y]$ es uno de los elementos del conjunto que aparece a la derecha en (9). Si en cambio $y<1$, entonces $2-y>1$ y $[y]=\{y,2-y\}=[2-y]$, así que $[y]$ también es uno de los elementos de ese conjunto.

(*e*) Sea $A=\mathbb{Z}$ y $R\subseteq\mathbb{Z}\times\mathbb{Z}$ la relación tal que si x e y son elementos de $\mathbb{Z}$ entonces

$$x\ R\ y \iff y-x \text{ es par.}$$

Fijemos un entero $x\in\mathbb{Z}$. Si $y\in[x]$, entonces $y-x$ es par, es decir, existe $k\in\mathbb{Z}$ tal que $y-x=2k$ y, por lo tanto, $y=x+2k$. Vemos así que $[x]\subseteq\{x+2k:k\in\mathbb{Z}\}$ y vale, de hecho, la igualdad. En efecto, si y es un entero de la forma $x+2k$ para algún $k\in\mathbb{Z}$, entonces la diferencia $y-x=2k$ es un número par y, en consecuencia, $x\ R\ y$, de manera que $y\in[x]$.

Concluimos de esta forma que para cada $x\in\mathbb{Z}$ la clase de equivalencia de x con respecto a R es

$$[x]=\{x+2k:k\in\mathbb{Z}\}.$$

Afirmamos que el conjunto cociente en este caso es

$$A/R=\{[0],[1]\}$$

y que éste tiene dos elementos distintos. Para verlo, tenemos que mostrar, por un lado, que toda clase de equivalencia de la relación R es igual o a $[0]$ o a $[1]$ y, por otro, que $[0]\neq[1]$.

Sea $y\in\mathbb{Z}$ un entero. Si y es par, entonces por supuesto la diferencia $y-0$ es par, de manera que $0\ R\ y$ y, por lo tanto, $y\in[0]$: esto implica, como sabemos, que $[y]=[0]$. Si en cambio y es impar, entonces la diferencia $y-1$ es par y ahora tenemos que $y\in[1]$ y que $[y]=[1]$. Esto prueba la primera de las dos cosas que queremos. Para ver la segunda basta observar que como la diferencia $1-0$ no es par, entonces $0\not R\ 1$ y, por lo tanto $1\notin[0]$: como $1\in[1]$, es claro que esto muestra que las clases $[0]$ y $[1]$ son distintas.

2.5.6. Proposición. *Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia en A.*

(*i*) *Toda clase de equivalencia de R es no vacía.*

(*ii*) *Todo elemento de A pertenece a alguna una clase de equivalencia de R.*

(*iii*) *Dos clases de equivalencia de R son o bien disjuntas o bien iguales.*

Observemos que de (*ii*) y (*iii*) se deduce que, de hecho, todo elemento de A pertenece a *exactamente* una clase de equivalencia de R.

Demostración. (*i*) Si c es una clase de equivalencia de R, entonces existe $x \in A$ tal que $c = [x]$ y, por lo tanto, $x \in c$: en efecto, la relación R es reflexiva, así que $x \mathrel{R} x$ y, en consecuencia, $x \in [x]$.

(*ii*) Si x es un elemento de A, entonces $[x]$ es una clase de equivalencia de R que contiene a x.

(*iii*) Sean c y d dos clases de equivalencia de la relación R, de manera que existen elementos x e y de A tales que $c = [x]$ y $d = [y]$, y supongamos que c y d no son conjuntos disjuntos. Existe entonces $z \in c \cap d = [x] \cap [y]$ y, en particular, $z \in [x]$ y $z \in [y]$. De acuerdo a la Proposición 2.5.4, esto implica que $[z] = [x]$ y que $[z] = [y]$, así que, por supuesto, tenemos que $[x] = [y]$. □

Ejemplos

2.5.7. Ejemplo. En el conjunto $A = \mathbb{N} \times \mathbb{N}$ consideremos la relación

$$R \coloneqq \{((x, y), (x', y')) \in A \times A : x + y' = x' + y\}.$$

Mostremos que se trata de una relación de equivalencia.

- Si (x, y) es un elemento de A, entonces claramente es $x + y = x + y$, así que $(x, y) \mathrel{R} (x, y)$. Esto nos dice que la relación R es reflexiva.
- Sean (x, y) y (x', y') dos elementos de A y supongamos que $(x, y) \mathrel{(} x', y')$, de manera que $x + y' = x' + y$. Esto implica, por supuesto, que también $x' + y = x + y'$ y, por lo tanto, vale que $(x', y') \mathrel{R} (x, y)$. Vemos así que la relación R es simétrica.
- Sean (x, y), (x', y') y (x'', y'') tres elementos de A y supongamos que $(x, y) \mathrel{R} (x', y')$ y que $(x', y') \mathrel{R} (x'', y'')$, de manera que es $x + y' = x' + y$ y $x' + y'' = x'' + y'$. De esto se sigue que

  $$x + y'' + x' + y' = x' + y'' + x' + y = x'' + y + x' + y'$$

  así que $x + y'' = x'' + y$ y $(x, y) \mathrel{R} (x'', y'')$. La relación R es, por lo tanto, transitiva.

Afirmamos que el conjunto cociente A/R tiene como elementos a las siguientes clases de equivalencia

$$[(1,1)], \quad [(2,1)], \quad [(3,1)], \quad [(4,1)], \quad \ldots, \quad [(1,2)], \quad [(1,3)], \quad [(1,4)], \quad \ldots \tag{10}$$

y que, más aún, estas clases de equivalencia son distintas dos a dos — notemos que estas son las clases de los elementos de A que tienen al menos una componente igual a 1. Esto nos dice que toda clase de equivalencia de R en A coincide con una y una sola de las clases de estos elementos.

- Sea (x, y) un elemento cualquiera de A. Sabemos que o bien $x \leq y$, o bien $x > y$. Consideremos separadamente estas dos posibilidades.
  - Si $x \leq y$, entonces el número $z \coloneqq y - x$ pertenece a $\mathbb{N}_0$, así que $(1, z+1)$ es un elemento de A y, como $x + z + 1 = x + y - x + 1 = y + 1$, tenemos que $(x, y)\ R\ (1, z+1)$ y, por lo tanto, que la clase de equivalencia de (x, y) coincide con la de $(1, z+1)$, que es una de las de (10).
  - Si $x > y$, entonces $z \coloneqq x - y$ es un elemento de $\mathbb{N}$ tal que $x + 1 = x - y + y + 1 = z + 1 + y$, así que $(x, y)\ R\ (z+1, 1)$ y la clase de equivalencia de (x, y) coincide con la de $(z+1, 1)$, que es una de las listadas en (10).

  Vemos así que en cualquier caso la clase de (x, y) coincide con alguna de las clases listadas en (10). Esto prueba, claro, que todas las clases de equivalencia de la relación R están en esa lista.
- Para ver que las clases listadas en (10) son distintas dos a dos es suficiente que mostremos que si (x, y) y (x', y') son dos elementos de A tales que *(i)* alguno de x e y es igual a 1, y *(ii)* alguno de x' e y' es igual a 1, entonces $[(x, y)] = [(x', y')]$ solamente si $(x, y) = (x', y')$.

  Sean para ello (x, y) y (x', y') dos elementos que satisfacen esas condiciones y supongamos que $[(x, y)] = [(x', y')]$, de manera que $(x, y)\ R\ (x', y')$, esto es, $x + y' = x' + y$.
  - Si $x = 1$ y $x' = 1$, esto nos dice que $y' = y$, así que $(x, y) = (x', y')$.
  - Si $y = 1$ y $x' = 1$, esto implica que $x + y' = 2$ y, como x e y' pertenecen a $\mathbb{N}$, que también $x = 1$ e $y' = 1$. Tenemos entonces que $(x, y) = (1, 1) = (x', y')$.
  - Si $x = 1$ e $y' = 1$, entonces $2 = x' + y$ y, como antes, tenemos que $x' = 1$, que $y = 1$ y, por lo tanto, que $(x, y) = (1, 1) = (x', y')$.
  - Finalmente, si $y = 1$ e $y' = 1$, tenemos que $x = x'$, así que $(x, y) = (x', y')$.

  Así, en cualquier caso tenemos que $(x, y) = (x', y')$, y esto prueba lo que queremos.

2.5.8. Ejemplo. Sea ahora A el conjunto $\mathbb{Z} \times \mathbb{N}$, y consideremos sobre A la relación $R \subseteq A \times A$ tal que siempre que (x, y) y (x', y') son elementos de A se tiene que

$$(x, y)\ R\ (x', y') \iff xy' = x'y.$$

Mostremos que se trata de una relación de equivalencia en A.

- Si (x, y) es un elemento de A, entonces ciertamente vale que $xy = xy$, así que $(x, y)\ R\ (x, y)$.

Esto nos dice que la relación R es reflexiva.

- Sean (x, y) y (x', y') dos elementos de A y supongamos que $(x, y)\ R\ (x', y')$, de manera que $xy' = x'y$. Por supuesto, esto implica que $x'y = xy'$ y, por lo tanto, que $(x', y') = (x, y)$. Vemos así que la relación R es simétrica.
- Sean finalmente (x, y), (x', y') y (x'', y'') tres elementos de A tales que $(x, y)\ R\ (x', y')$ y $(x', y')\ R\ (x'', y'')$. Esto nos dice que $xy' = x'y$ y que $x'y'' = x''y'$, así que

  $$xy''y'x' = x'yy''x' = x''yy'x'$$

  y, como $y'x' \neq 0$, esto implica que $xy'' = x''y$, esto es, que $(x, y)\ R\ (x'', y'')$. Podemos concluir con esto que la relación R es transitiva.

2.5.9. Ejemplo. Sea X un conjunto finito y consideremos el conjunto $A \coloneqq \mathscr{P}(X)$ de sus partes. Por supuesto, todos los subconjuntos de X son finitos, así que para cada elemento U de A podemos hablar del cardinal $|U|$ de U, que es un elemento de $\mathbb{N}_0$.

Consideremos en A la relación

$$R \coloneqq \{(U, V) \in A \times A : |U \triangle V| \text{ es par}\}.$$

Notemos que esto tiene sentido: en efecto, si U y V son elementos de A, entonces se trata de subconjuntos de X, así que su diferencia simétrica $U \triangle V$ también es un subconjunto de A y tiene, en consecuencia, cardinal $|U \triangle V|$ finito, que puede ser o no un elemento par de $\mathbb{N}_0$.

Queremos probar que R es una relación de equivalencia.

- Sea U un elemento de A, esto es, un subconjunto de X. La diferencia simétrica $U \triangle U$ es vacía, así que su cardinal es $|U \triangle U| = 0$, que es un número par. Esto nos dice que $U\ R\ U$ y, en definitiva, que la relación R es reflexiva.
- Sean ahora U y V dos elementos de A y supongamos que $U\ R\ V$, de manera que el conjunto $U \triangle V$ tiene un número par de elementos. Como $V \triangle U = U \triangle V$, es claro entonces que $V \triangle U$ tiene un número par de elementos y, en consecuencia, que $V \triangle RU$. Vemos así que la relación R es simétrica.
- Finalmente, sean U, V y W tres elementos de A y supongamos que $U\ R\ V$ y $V\ R\ W$, de manera que los cada uno de los conjuntos $U \triangle V$ y $V \triangle W$ tiene un número par de elementos. Sabemos del Ejercicio 1.6.1 que

  $$U \triangle W = (U \triangle V) \triangle (V \triangle W)$$

  Como $U \triangle V$ y $V \triangle W$ tienen cada un número par de elementos, esta igualdad junto con la siguiente observación implican que $U \triangle W$ también tiene un número par de elementos,

de manera que $U \; R \; W$.

> *si G y H son dos conjuntos finitos y cada uno de ellos tiene un número par de elementos, entonces $G \triangle H$ también tiene un número par de elementos.*

Para terminar, entonces, tenemos que probar esta observación.

Consideremos para ello dos conjuntos finitos G y H y supongamos que cada uno de ellos tiene un número par de elementos. Sabemos que $G = (G - H) \cup (G \cap H)$ y que $(G - H) \cap (G \cap H) = \varnothing$, así que

$$|G| = |G - H| + |G \cap H|. \tag{11}$$

De manera similar, es $H = (H - G) \cup (G \cap H)$ y $(H - H) \cap (G \cap H) = \varnothing$, así que

$$|H| = |H - G| + |G \cap H|. \tag{12}$$

Por otro lado, como $G \triangle H = (G - H) \cup (H - G)$ y $(G - H) \cap (H - G) = \varnothing$, también tenemos que

$$|G \triangle G| = |G - H| + |H - G|. \tag{13}$$

El número $|G \cap H|$ puede ser par o no.

- Si es par, como $|G|$ y $|H|$ también son pares, de las igualdades (11) y (12) podemos deducir que los cardinales $|G - H|$ y $|H - G|$ también son pares, y usando eso y la igualdad (13) que el cardinal de $G \triangle H$ es par.
- Si en cambio $|G \cap H|$ es impar, las igualdades (11) y (12) implican que $|G - H|$ y $|H - H|$ son números impares y, a su vez, la igualdad (13) que el cardinal de $G \triangle H$ es par.

En cualquiera de los dos casos, por lo tanto, el conjunto $G \triangle H$ tiene cardinal par, como queremos.

Particiones

2.5.10. Si A es un conjunto, una ***partición*** de A es un conjunto $\mathscr{F}$ contenido en $\mathscr{P}(A)$ — de manera que los elementos de $\mathscr{F}$ son subconjuntos de A — que satisface las siguientes tres condiciones:

- $\varnothing \notin \mathscr{F}$;
- todo elemento de A pertenece a algún elemento de $\mathscr{F}$;
- dos elementos de $\mathscr{F}$ son o bien iguales o disjuntos.

Llamamos a los elementos de $\mathscr{F}$ las ***partes*** de la partición.

2.5.11. Por ejemplo, el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ tiene a

$$\mathscr{F}_1 = \{\{1, 2, 5\}, \{4, 6\}, \{3\}\},$$
$$\mathscr{F}_2 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$$

y a

$$\mathscr{F}_3 = \{\{1, 2, 3, 4, 5, 6\}\}$$

como particiones, entre otras. En cambio, ni

$$\mathscr{F}_4 = \{\{1, 2\}, \{4, 6\}, \{3\}\}$$

ni

$$\mathscr{F}_5 = \{\{1, 2\}, \{2, 3\}, \{3, 4, 5, 6\}\}$$

son particiones de A.

2.5.12. El conjunto vacío $\varnothing$ tiene exactamente una partición, la partición vacía $\varnothing$. Mostremos esto.

- Primero, supongamos que $\mathscr{F}$ es una partición de $\varnothing$. Todo elemento de $\mathscr{F}$ es un subconjunto de $\varnothing$, así que es vacío y, al mismo tiempo, como $\mathscr{F}$ es una partición no tiene elementos vacíos: esto nos dice que $\mathscr{F}$ no tiene ningún elemento, esto es, $\mathscr{F} = \varnothing$.
- Por otro lado, la familia vacía $\mathscr{F} = \varnothing$ es ciertamente una partición de $\varnothing$: no contiene a $\varnothing$, todo elemento de $\varnothing$ pertenece a algún elemento de $\varnothing$, y dos elementos cualesquiera de $\varnothing$ son o iguales o vacíos — todo esto por razones triviales.

2.5.13. La razón que hace que nos interesen las particiones de conjuntos es que están estrechamente relacionadas con las relaciones de equivalencia. En primer lugar, podemos obtener una partición de un conjunto a partir de una relación de equivalencia:

Proposición. *Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia en A. El conjunto cociente A/R es una partición de A.*

Demostración. En efecto, que las tres condiciones de la definición 2.5.10 se cumplen es precisamente lo que afirma la Proposición 2.5.6. □

2.5.14. Recíprocamente, si tenemos una partición en un conjunto, podemos construir de manera natural una relación de equivalencia:

Proposición. *Sea A un conjunto y sea $\mathscr{F}$ una partición de A. La relación $R \subseteq A \times A$ tal que si x e y son elementos de A entonces*

$$x \; R \; y \iff \text{existe una parte } P \in \mathscr{F} \text{ tal que } x \in P \text{ e } y \in P$$

es una relación de equivalencia en A y su conjunto cociente es $A/R = \mathscr{F}$.

Demostración. Mostremos primero que la relación R definida en el enunciado de esta proposición es una relación de equivalencia.

- Si x es un elemento de A, entonces como $\mathscr{F}$ es una partición, existe una parte $P \in \mathscr{F}$ tal que $x \in P$ y, por lo tanto, $x \ R \ x$.
- Sean x e y dos elementos de A tales que $x \ R \ y$, de manera que existe una parte $P \in \mathscr{F}$ tal que $x \in P$ e $y \in P$. Por supuesto, tenemos entonces que $y \in P$ y $x \in P$, así que $y \ R \ x$.
- Finalmente, sean x, y y z elementos de A tales que $x \ R \ y$ e $y \ R \ z$. Existen entonces partes P y Q en la partición $\mathscr{F}$ tales que $x \in P$, $y \in P$, $y \in Q$ y $z \in Q$. En particular, vemos de esto que $y \in P \cap Q$, de manera que las partes P y Q no son disjuntas: como $\mathscr{F}$ es una partición y satisface por lo tanto la tercera de las condiciones de la definición **2.5.10**, vemos que tiene que ser $P = Q$. Pero en ese caso tenemos que $x \in P$ y $z \in P$ y, por lo tanto, que $x \ R \ z$.

Como consecuencia de todo esto, la relación R es reflexiva, simétrica y transitiva y, por lo tanto, se trata de una relación de equivalencia.

Veamos ahora que $A/R = \mathscr{F}$. Para ello, tenemos que mostrar las dos inclusiones entre los conjuntos A/R y $\mathscr{F}$.

- Sea primero c un elemento de A/R, es decir, una clase de equivalencia de la relación R, de manera que existe $x \in A$ tal que $c = [x]$. Como $\mathscr{F}$ es una partición del conjunto A, sabemos que existe una parte $P \in \mathscr{F}$ tal que $x \in P$. Afirmamos que c y P son el mismo conjunto y, en particular, que $c \in \mathscr{F}$. Cuando probemos esto tendremos, por lo tanto, que $A/R \subseteq \mathscr{F}$.

  Sea y un elemento de $c = [x]$: esto significa que $x \ R \ y$ y, de acuerdo a la definición de la relación R, que existe una parte $Q \in \mathscr{F}$ tal que $x \in Q$ e $y \in Q$. Ahora bien, como $x \in P \cap Q$, las partes P y Q no son disjuntas, así que tienen que ser iguales, esto es, debe ser $P = Q$. En particular, como $y \in Q$ tenemos que $y \in P$, y en definitiva esto muestra que $c \subseteq P$.

  Por otro lado, sea y un elemento de P. Como $x \in P$ e $y \in P$, la definición de R nos dice que $x \ R \ y$, así que $y \in [x]$: esto implica que $P \subseteq c$.
- Sea ahora P una parte de $\mathscr{F}$. Como $\mathscr{F}$ es una partición, P no es el conjunto vacío y, por lo tanto, existe $x \in A$ tal que $x \in P$. Para ver que P pertenece a A/R es suficiente con que mostremos que $P = [x]$.

  Si y es un elemento de P, entonces tenemos que $x \in P$ e $y \in P$, así que $x \ R \ y$ y, por lo tanto, $y \in [x]$. Esto muestra que $P \subseteq [x]$. Recíprocamente, si y es un elemento de $[x]$, de manera que $x \ R \ y$, entonces existe una parte Q de $\mathscr{F}$ tal que $x \in Q$ e $y \in Q$. Como la intersección $P \cap Q$ no es vacía, ya que contiene a x, debe ser $P = Q$ y, por lo tanto, tenemos que $y \in P$. Concluimos de esta forma que $[x] \subseteq P$.

Esto completa la prueba de la proposición. □

2.5.15. Ejercicio. Sea A un conjunto. La Proposición 2.5.13 nos permite construir una partición de A a partir de una relación de equivalencia en A, y la Proposición 2.5.14 nos permite construir una relación de equivalencia en A a partir de una partición de A. Veamos cómo están relacionadas estas dos construcciones.

(*a*) Sea R una relación de equivalencia en A, sea $\mathscr{P}$ la partición de A que se obtiene a partir de R como en la Proposición 2.5.13, y sea R' la relación de equivalencia en A que se obtiene a partir de la partición $\mathscr{P}$ como en la Proposición 2.5.14. Pruebe que $R = R'$.

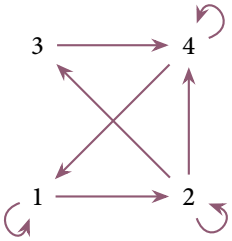
(*b*) Sea ahora $\mathscr{P}$ una partición del conjunto A, sea R la relación de equivalencia en A que se obtiene de $\mathscr{P}$ como en la Proposición 2.5.14, y sea $\mathscr{P}'$ la partición de A que se obtiene de la relación R como en la Proposición 2.5.13. Pruebe que $\mathscr{P} = \mathscr{P}'$.

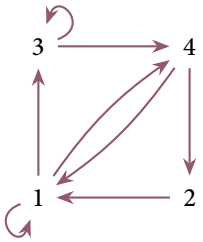
§2.6. Relaciones de orden

2.6.1. Si A es un conjunto y $R \subseteq A \times A$ es una relación en A, entonces decimos que R es ***anti-simétrica*** si cada vez que a y b son elementos de A se tiene que

$$a\ R\ b \text{ y } b\ R\ a \implies a = b.$$

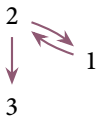
En términos del grafo de la relación, esta condición nos dice que hay a lo sumo *una* flecha entre dos elementos *distintos* de A. De las siguientes dos relaciones en el conjunto $\{1, 2, 3, 4\}$ sólo la primera es anti-simétrica:





Es importante observar que la propiedad de anti-simetría de una relación es independiente de la de simetría y, en particular, que no es lo mismo que la de no ser simétrica. La siguiente tabla

muestra relaciones que tienen las cuatro posibles combinaciones de estas dos propiedades.

		¿Es anti-simétrica? Sí	¿Es anti-simétrica? No
¿Es simétrica?	Sí		
	No		

2.6.2. Una relación $R \subseteq A \times A$ en un conjunto A es una ***relación de orden*** si es reflexiva, anti-simétrica y transitiva.

2.6.3. Ejemplo. La relación identidad I_A en un conjunto cualquiera A.

2.6.4. Ejemplo.

Si $A = \mathbb{N}$, entonces la relación

$$R \coloneqq \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \leq b\}$$

en $\mathbb{N}$ es una relación de orden. Podemos reemplazar al conjunto $\mathbb{N}$ por $\mathbb{Z}$, por $\mathbb{R}$ y, más generalmente, por cualquier subconjunto de $\mathbb{R}$. Este ejemplo es el que motiva el nombre de «relación de orden» de la propiedad que estamos estudiando.

2.6.5. Ejemplo. Si B es un conjunto, podemos considerar la relación $R \subseteq \mathscr{P}(B) \times \mathscr{P}(B)$ en el conjunto de partes $\mathscr{P}(B)$ de B dada por

$$R \coloneqq \{(X, Y) \in \mathscr{P}(B) \times \mathscr{P}(B) : X \subseteq Y\}.$$

Es inmediato verificar que se trata de una relación de orden en $\mathscr{P}(B)$. En efecto, ya sabemos que es reflexiva y transitiva, y la Proposición 1.2.4(*ii*) nos dice precisamente que es anti-simétrica.

2.6.6. Ejemplo.

En el conjunto $\mathbb{N}$ consideremos la relación $R \subseteq \mathbb{N} \times \mathbb{N}$ tal que si x e y son elementos de $\mathbb{N}$ entonces

$$x \; R \; y \iff x \text{ divide a } y.$$

Sabemos que se trata de una relación reflexiva y transitiva y es, de hecho, una relación de orden. Para verlo, bastará que mostremos que es anti-simétrica.

Supongamos que x e y son elementos de $\mathbb{N}$ tales que $x \ R \ y$ e $y \ R \ x$, es decir, tales que $x \mid y$ e $y \mid x$. Existen entonces k y l en $\mathbb{N}$ tales que $y = lx$ y $x = ky$, y se tiene entonces que

$$x = ky = klx,$$

de manera que $(1 - kl)x = 0$. Como x no es nulo, esta igualdad implica que $1 - kl$ sí lo es, es decir, que $kl = 1$. Como tanto k como l están en $\mathbb{N}$, vemos así que necesariamente $k = 1$ y, por lo tanto, que $x = ky = y$. Esto prueba que la relación es anti-simétrica, como queríamos.

Notemos que si definimos en $\mathbb{Z}$ una relación $R' \subseteq \mathbb{Z} \times \mathbb{Z}$ de manera que para cada x e $y \in \mathbb{Z}$ se tenga que vale

$$x \ R' \ y \iff x \text{ divide a } y,$$

entonces *no* obtenemos una relación de orden: por ejemplo, $2 \ R' \ (-2)$ y $(-2) \ R' \ 2$, pero ciertamente 2 y -2 no son iguales.

2.6.7. Ejemplo. Sea $A = \mathbb{R} \times \mathbb{R}$ y consideremos la relación $R \subseteq A \times A$ tal que cada vez que (x_1, x_2) e (y_1, y_2) son dos elementos de A se tiene que

$$(x_1, x_2) \ R \ (y_1, y_2) \iff \begin{cases} x_1 > y_1 \\ \quad \text{o} \\ x_1 = y_1 \text{ e } x_2 \geq y_2. \end{cases} \tag{14}$$

Veamos que se trata de una relación de orden en el conjunto A. Observemos antes que claramente se tiene que

$$(x_1, x_2) \ R \ (y_1, y_2) \implies x_1 \geq y_1 \tag{15}$$

siempre que (x_1, x_2) e (y_1, y_2) son elementos de A.

- Si (x_1, x_2) es un elemento de A, entonces es claro que $(x_1, x_2) \ R \ (x_1, x_2)$, así que la relación es reflexiva.
- Sean (x_1, x_2) e (y_1, y_2) dos elementos de A para los que se tiene que

  $$(x_1, x_2) \ R \ (y_1, y_2) \tag{16}$$

  y

  $$(y_1, y_2) \ R \ (x_1, x_2). \tag{17}$$

  De nuestra observación (15) y de esto deducimos que $x_1 \geq y_1$ y que $y_1 \geq x_1$, así que, de hecho, es $x_1 = y_1$.

Ahora bien, de (16) y de esto vemos que debe ser $x_2 \geq y_2$, ya que la primera de las alternativas de la definición (14) no puede valer. De la misma forma, de (17) y de que $x_1 = y_1$ deducimos que $y_2 \geq x_2$. Juntando las dos desigualdades, vemos que, de hecho, $x_2 = y_2$ y, por lo tanto, que $(x_1, x_2) = (y_1, y_2)$. Esto prueba que la relación R es anti-simétrica.

- Finalmente, supongamos que (x_1, x_2), (y_2, y_2) y (z_1, z_2) son elementos de A tales que

$$(x_1, x_2)\ R\ (y_1, y_2) \tag{18}$$

y

$$(y_1, y_2)\ R\ (z_1, z_2). \tag{19}$$

En particular, de acuerdo a nuestra observación (15), tenemos que $x_1 \geq y_1$ y que $y_1 \geq z_1$. Si alguna de estas dos desigualdades es estricta, entonces tenemos que $x_1 > z_1$ y, por lo tanto, que $(x_1, x_2)\ R\ (z_1, z_2)$. Supongamos entonces que ninguna de esas dos desigualdades es estricta, de manera que $x_1 = y_1$ e $y_1 = z_1$. De la definición de la relación R y de (18) y de (19) podemos deducir entonces que $x_2 \geq y_2$ y que $y_2 \geq z_2$. Tenemos en consecuencia que $x_1 = z_1$ y que $x_2 \geq z_2$, así que otra vez $(x_1, x_2)\ R\ (z_1, z_2)$.

En cualquier caso, entonces, es $(x_1, x_2)\ R\ (z_1, z_2)$ y, por lo tanto, la relación R es transitiva.

Vemos de esta forma que la relación R es una relación de orden en el conjunto A, como queríamos.

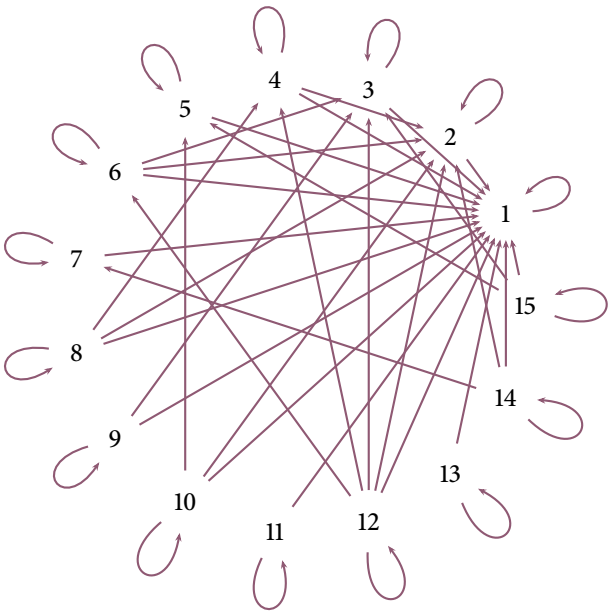
2.6.8. Sea A un conjunto y consideremos en A una relación de orden R. Si a y b son dos elementos de A, decimos que a y b son ***comparables*** con respecto a R si $a\ R\ b$ o $b\ R\ a$. En general, este no es el caso: con respecto a la relación de divisibilidad en $\mathbb{N}$ que vimos en el Ejemplo 2.6.6 los números 2 y 3 no son comparables. Cuando, por el contrario, todo par de elementos de A es comparable con respecto a la relación de orden R decimos que R es una relación de orden ***total***.

La relación usual de orden sobre el conjunto $\mathbb{N}$ es total, por ejemplo.

2.6.9. Cuando tenemos una relación de orden R sobre un conjunto A y hacemos el grafo de R, como explicamos en 2.4.1, normalmente hacemos algunas convenciones para simplificar el dibujo resultando. Supongamos, por ejemplo, que A es el conjunto $\{1, 2, \ldots, 15\}$ y que R es la relación en A dada por

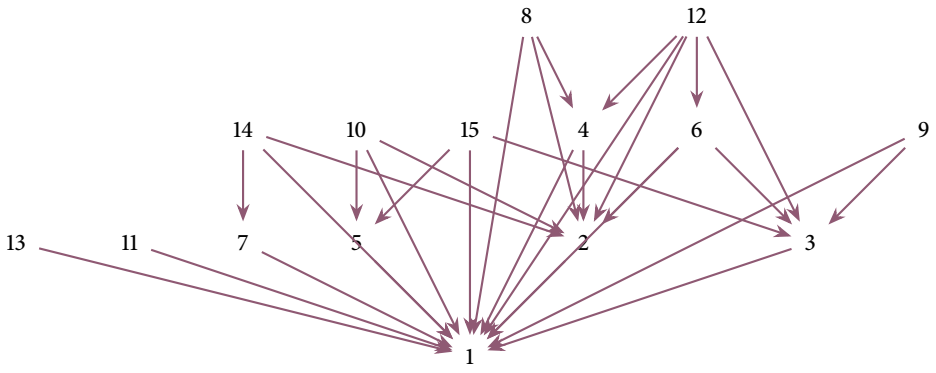
$$R = \{(a, b) \in A \times A : a \text{ divide a } b\}.$$

Si disponemos los elementos de A en un círculo, entonces el grafo de A es el siguiente:



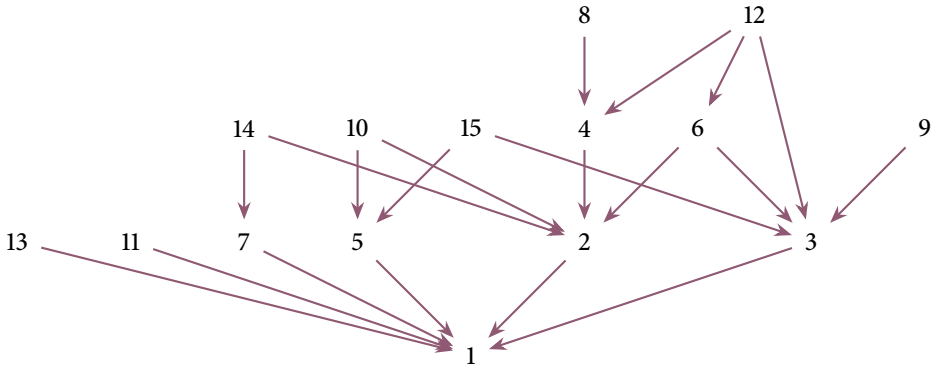
Es claro que este diagrama no es particularmente útil…

Una primera convención que hacemos al dibujar relaciones de orden es omitir todos los bucles: como una relación de orden es reflexiva, sabemos que en todo elemento del conjunto tiene que haber un bucle, así que incluirlo en el dibujo no agrega nada. En segundo lugar, normalmente disponemos los elementos de A en el dibujo de manera que siempre que (a, b) es un elemento de R el elemento a está más abajo que el elemento b. En el ejemplo de arriba, si usamos estas dos convenciones obtenemos un dibujo como el siguiente:



Finalmente, como R es una relación de orden sabemos que siempre es $a \ R \ b$ y $b \ R \ c$ vale que $a \ R \ c$, así que convenimos en no poner en el diagrama la flecha que corresponde a esta última

relación. Así, por ejemplo, como 1 R 2 y 2 R 4, no incluiremos la flecha que corresponde a que 1 R 4. Si hacemos esto sistemáticamente obtenemos el siguiente diagrama:



Por supuesto, este ya no es el grafo de la relación R, pero podemos reconstruir a R a partir de este dibujo. Llamamos a este diagrama un ***diagrama de Hasse*** del orden R, por Helmut Hasse.

El diagrama de Hasse de una relación de orden casi siempre es mucho más sencillo que el grafo de esa relación. Por ejemplo, si $A = \{1, 2, 3, 4, 5, 6\}$ y $R = \{(a, b) \in A \times A : a \leq b\}$, en el grafo de R hay 21 flechas, contando 6 bucles, mientras que el el correspondiente diagrama de Hasse hay solo 5:

Por otro lado, el diagrama de Hasse de una relación de orden usualmente deja de manifiesto la estructura de este. En la Figura 2.3 damos dos diagramas de Hasse para la situación en que $A = \mathscr{P}(\{1, 2, 3, 4\})$ y $R = \{(X, Y) \in A \times A : X \subseteq Y\}$. Por otro lado, podemos considerar el conjunto D de todos los divisores positivos de 210, que es

$$D = \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\},$$

y considerar la relación S en D determinada por la divisibilidad, esto es,

$$S := \{(x, y) \in D \times D : x \text{ divide a } y\},$$

que es una relación de orden en D. En la Figure 2.2 dibujamos un posible diagrama de Hasse para S. Comparando este último diagrama con el tercero de la Figura 2.3 vemos inmediatamente ambos coinciden, salvo por el nombre de los elementos que aparecen en ellos. Este tipo de coincidencia es extremadamente útil en muchas situaciones, y los diagramas de Hasse hacen posible encontrarlas gráficamente.

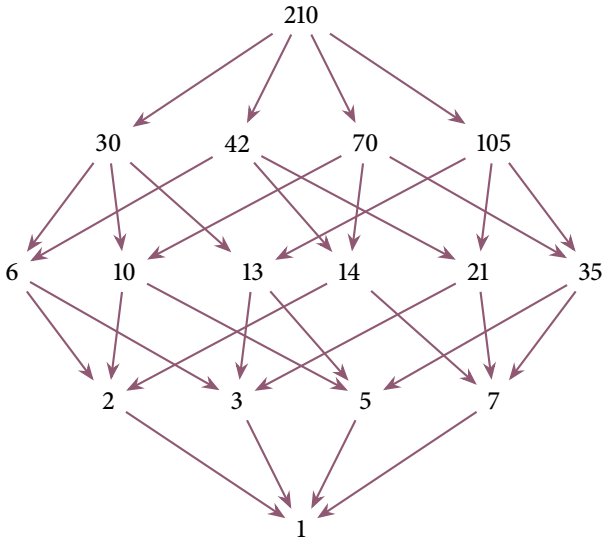


Figura 2.2. Un diagrama de Hasse para la relación de divisibilidad en el conjunto de los divisores positivos de 210.

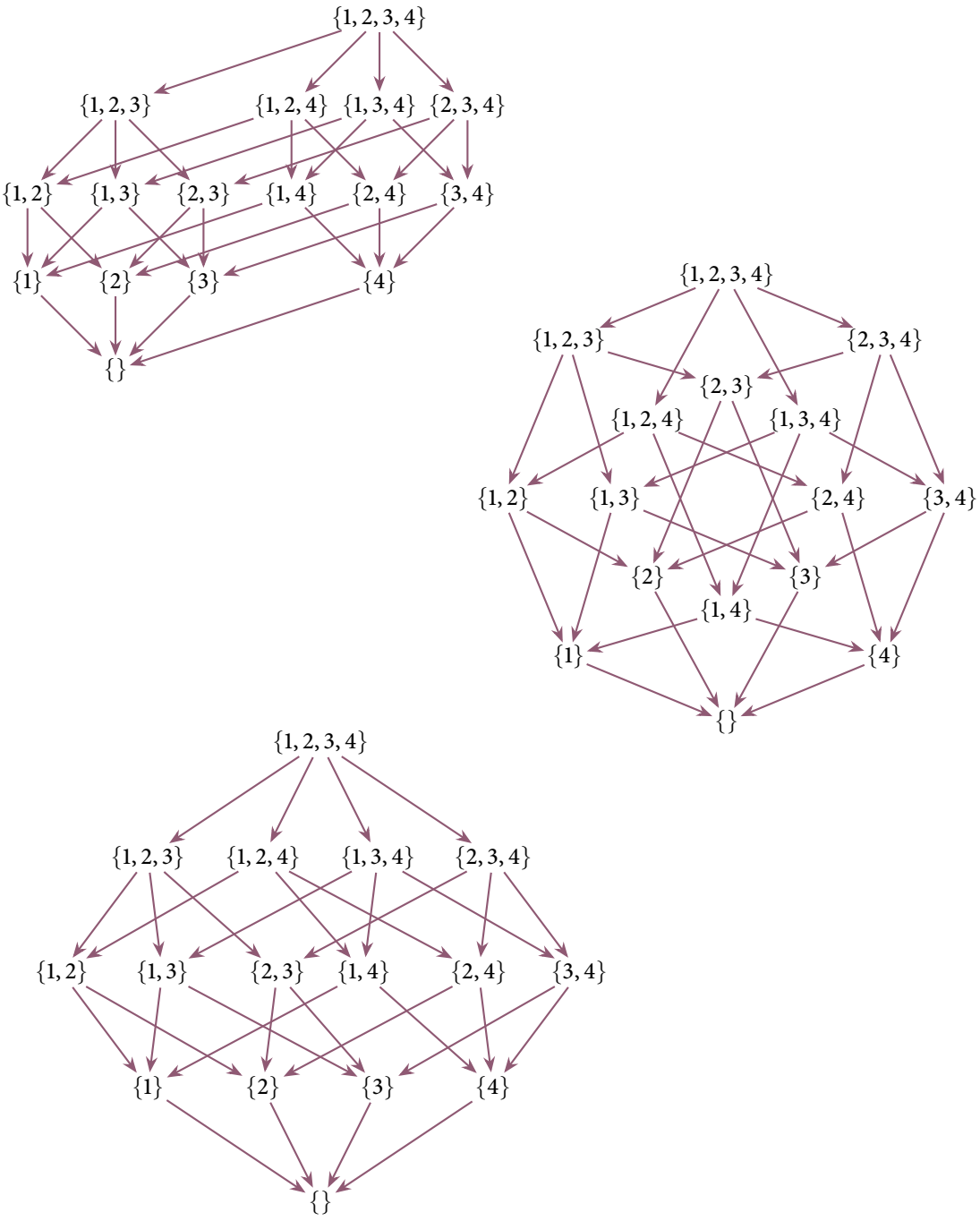


Figura 2.3. Dos diagramas para la relación de orden $R = \{(X, Y) \in A \times A : X \subseteq Y\}$ sobre el conjunto $A = \mathscr{P}(\{1, 2, 3, 4\})$.

§2.7. Ejercicios

Independencia

2.7.1. Decimos que una relación R en un conjunto A es

- ***irreflexiva*** si para todo $a \in A$ se tiene que $(a, a) \notin R$, y que es
- ***intransitiva*** si para toda elección de a, b y c en A vale que

$$a \mathrel{R} b,\ b \mathrel{R} c \implies a \not{R}\, c.$$

2.7.2. Ejercicio. Si R es una relación en un conjunto A, entonces puede tener o no cada una de las siguientes propiedades

reflexividad, irreflexividad, simetría, antisimetría, transitividad, intransitividad.

Sea P el conjunto de estas seis propiedades. Determine para qué subconjuntos S de P existe una relación no vacía en algún conjunto que tenga las propiedades de S y no las de $P - S$.

El conjunto P tiene $2^6 = 64$ subconjuntos, así que en principio hacer esto requiere examinar 64 casos distintos. De todas formas, hay ciertas combinaciones de propiedades que son incompatibles: por ejemplo, una relación no vacía claramente no puede ser a la vez reflexiva e irreflexiva. Observaciones como esta permiten reducir la cantidad total de trabajo necesario para hacer este ejercicio.

Intersección de relaciones

2.7.3. Ejercicio. Sea A un conjunto.

(*a*) Si R y S son dos relaciones en A que son reflexivas, simétricas, transitivas o anti-simétricas, entonces la intersección $R \cap S$, que es una relación en A, tiene la misma propiedad. Si R y S son relaciones de equivalencia o de orden, entonces $R \cap S$ también lo es.

(*b*) Más generalmente, si $\mathscr{F}$ es una familia no vacía de relaciones en A y todos los miembros de $\mathscr{F}$ son relaciones reflexivas, simétricas, transitivas o anti-simétricas, entonces la intersección

$$\bigcap_{R \in \mathscr{F}} R,$$

que también es una relación en A, tiene la misma propiedad. Si todos los miembros de la familia $\mathscr{F}$ son relaciones de equivalencia o de orden, entonces la intersección de la familia también lo es.

(*c*) ¿Hay resultados como los de las dos partes anteriores de este ejercicio pero con respecto a la unión de relaciones?

Productos

2.7.4. Si A y B son dos conjuntos y R y S son una relación en A y una relación en B, respectivamente, entonces podemos hay una relación T en el conjunto $A \times B$ tal que

$$(a, b)\ T\ (a', b') \iff a\ R\ a' \text{ y } b\ S\ b'$$

cualesquiera sean los elementos (a, b) y (a', b') de $A \times B$. Llamamos a T el ***producto cartesiano*** de las relaciones R y S.

2.7.5. Ejercicio. Sean A y B dos conjuntos, sean R y S una relación en A y una relación en B, y sea T la relación en $A \times B$ que es el producto cartesiano de R y S. Pruebe que T es una relación de equivalencia o de orden si tanto R como S son relaciones de equivalencia o de orden, respectivamente.

2.7.6. Sean ahora A y B dos conjuntos y sean R y S relaciones de orden en A y en B, respectivamente. El ***producto lexicográfico*** de R y S es la relación T en el conjunto $A \times B$ tal que cualesquiera sean los elementos (a, b) y (a', b') de $A \times B$ se tiene que

$$(a, b)\ T\ (a', b') \iff \begin{cases} a\ R\ a' \text{ y } a \neq a' \\ \text{o} \\ a = a' \text{ y } b\ S\ b'. \end{cases}$$

2.7.7. Ejercicio. Sean A y B dos conjuntos, y sean R y S relaciones de orden en A y en B, respectivamente. Pruebe que el producto lexicográfico de R y S es una relación de orden en $A \times B$, y que es total si R y S lo son.

2.7.8. Ejercicio. Sean n y m dos enteros positivos, sean $A \coloneqq \{1, \ldots, n\}$ y $B \coloneqq \{1, \ldots, m\}$, y consideremos sobre A y B las relaciones de orden R y S usuales. Dibuje diagramas de Hasse para estas dos relaciones de orden, y para las relaciones de orden en $A \times B$ dadas por el producto cartesiano y por el producto lexicográfico.

Clausura transitiva

2.7.9. Ejercicio. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A.

(*a*) La familia $\mathscr{F}$ de todas las relaciones $S \subseteq A \times A$ que son transitivas y tales que $R \subseteq S$ es no vacía, ya que contiene a la relación total. Podemos entonces considerar la relación

$$\bar{R} = \bigcap_{S \in \mathscr{F}} S.$$

Esta relación $\bar{R}$ es una relación transitiva en A que contiene a R y es la menor relación en A con esa propiedad, en el sentido de que

si $S \subseteq A \times A$ es una relación transitiva en el conjunto A y $R \subseteq S$, entonces $\bar{R} \subseteq S$.

Llamamos a la relación $\bar{R}$ la ***clausura transitiva*** de R.

(*b*) Sea $R \subseteq \mathbb{N} \times \mathbb{N}$ la relación en $\mathbb{N}$ tal que si x e y son elementos de $\mathbb{N}$ entonces

$$x \; R \; y \iff y = x + 1.$$

Describa la clausura transitiva $\bar{R}$ de R.

2.7.10. Ejercicio. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A. Consideremos la relación $R' \subseteq A \times A$ tal que si x e y son elementos de A, entonces se tiene que

$$x \; R' \; y$$

si y solamente si se cumple la siguiente condición:

existen $n \in \mathbb{N}$ y elementos $z_0, z_1, \ldots, z_n \in A$ tales que $z_0 = x$, $z_n = y$ y para cada $i \in \{1, \ldots, n\}$ es $z_{i-1} \; R \; z_i$.

Muestre que R' es una relación transitiva en A, que $R \subseteq R'$ y que, de hecho, R' es la clausura transitiva de R.

Relación de equivalencia generada por una relación

2.7.11. Ejercicio. Sea A un conjunto y sea $R \subseteq A \times A$ una relación.

(*a*) La familia $\mathscr{F}$ de todas las relaciones $S \subseteq A \times A$ que contienen a R y que son relaciones de equivalencia no es vacía, ya que contiene a la relación total en A, y podemos, por lo tanto, considerar la intersección

$$\bar{R} = \bigcap_{S \in \mathscr{F}} S.$$

Esta relación en A es una relación de equivalencia, contiene a R y es la menor relación de equivalencia en A que contiene a R, en el sentido de que

si $S \subseteq A \times A$ es una relación de equivalencia en el conjunto A y $R \subseteq S$, entonces $\bar{R} \subseteq S$.

Llamamos a esta relación $\bar{R}$ la relación de equivalencia ***generada*** por R.

(*b*) Sea $R' \subseteq A \times A$ la relación en A tal que si x e y son elementos de A, entonces se tiene que

$$x \; R' \; y$$

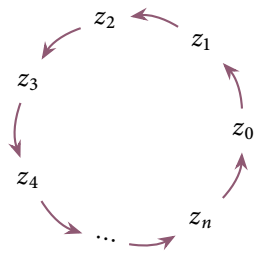
si y solamente si se cumple la condición de que

> *existen* $n \in \mathbb{N}_0$ *y elementos* $z_0, z_1, \ldots, z_n \in A$ *tales que* $z_0 = x$, $z_n = y$ *y para cada* $i \in \{1, \ldots, n\}$ *es* $z_{i-1}\ R\ z_i$ *o* $z_i\ R\ z_{i-1}$.

Muestre que R' es una relación de equivalencia en A, que $R \subseteq R'$ y que R' es, de hecho, la relación de equivalencia en A generada por R.

Relación de orden generada por una relación acíclica

2.7.12. Si A es un conjunto y $R \subseteq A \times A$ es una relación en A decimos que R es ***posee un ciclo*** si existen $n \in \mathbb{N}$ y elementos $z_0, \ldots, z_n \in A$ tales que $z_{i-1}\ R\ z_i$ para cada $i \in \{1, \ldots, n\}$ y $z_n\ R\ z_0$.



Si R no posee un ciclo, entonces decimos que R es ***acíclica***.

2.7.13. Ejercicio. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A.

(*a*) Si la relación R posee un ciclo, entonces no existe ninguna relación de orden $S \subseteq A \times A$ tal que $R \subseteq S$.

(*b*) Supongamos ahora que R es acíclica. Si R^+ es la clausura transitiva de la relación $R \cup I_A$, entonces R^+ es una relación de orden en A y $R \subseteq R^+$.

(*c*) En particular, esto muestra que si R es acíclica, entonces la familia $\mathscr{F}$ de todas las relaciones de orden S en A tales que $R \subseteq S$ no es vacía y que, por lo tanto, podemos considerar la intersección

$$\bigcap_{S \in \mathscr{F}} S,$$

que es una relación en A. Esta relación es precisamente la relación R^+ construida en la parte (*b*) y es la menor relación de orden en A que contiene a R, en el sentido de que

> *si* $S \subseteq A \times A$ *es una relación de orden en el conjunto* A *y* $R \subseteq S$, *entonces* $R^+ \subseteq S$.

Llamamos a esta relación R^+ la relación de orden ***generada*** por R.

La relación de cubrimiento de una relación de orden

2.7.14. Sea A un conjunto y sea $R \subseteq A \times A$ una relación de orden en A. Definimos una nueva relación $R^\circ \subseteq A \times A$ en A de la siguiente manera: si x e y son elementos de A, entonces $x \; R^\circ \; y$ si y solamente se cumplen las siguientes dos condiciones

- es $x \; R \; y$, y
- cada vez que $z \in R$ es tal que $x \; R \; z$ y $z \; R \; y$ se tiene que $z = x$ o $z = y$.

En otras palabras, si x e y son elementos de A, entonces se tiene que $x \; R^\circ \; y$ si y solamente si $x \; R \; y$ y no hay elementos z de R distintos de x y de y que sean «intermedios» entre x e y, en el sentido que se tengan las relaciones

$$x \; R \; z, \qquad z \; R \; y.$$

Llamamos a la relación R° la ***relación de cubrimiento*** correspondiente a la relación R de partida.

2.7.15. Ejercicio. Describa en cada uno de los siguientes ejemplos la relación de cubrimiento correspondiente.

(*a*) Sea $R \subseteq \mathbb{Z} \times \mathbb{Z}$ la relación de orden en $\mathbb{Z}$ tal que si x e y son elementos de $\mathbb{Z}$ entonces

$$x \; R \; y \iff x \leq y.$$

(*b*) Sea B un conjunto y sea $R \subseteq \mathscr{P}(B) \times \mathscr{P}(B)$ la relación de orden en el conjunto de partes $\mathscr{P}(B)$ tal que si X e Y son elementos de $\mathscr{P}(B)$ entonces

$$X \; R \; Y \iff X \subseteq Y.$$

(*c*) Sea $R \subseteq \mathbb{Q} \times \mathbb{Q}$ la relación de orden en $\mathbb{Q}$ tal que si x e y son elementos de $\mathbb{Q}$ entonces

$$x \; R \; y \iff x \leq y.$$

Capítulo 3

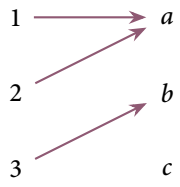
Funciones

§3.1. Funciones

3.1.1. Sean A y B dos conjuntos. Una relación $f \subseteq A \times B$ de A a B es una ***función*** de A a B si

- para cada $a \in A$ existe $b \in B$ tal que $(a, b) \in f$, y
- si $a \in A$ y $b, b' \in B$ son tales que los pares ordenados (a, b) y (a, b') están en f, entonces necesariamente $b = b'$.

En términos del grafo de la relación f, la primera de estas condiciones dice que de cada elemento de A sale *al menos* una flecha, mientras que la segunda que sale *a lo sumo* una: juntas, entonces, nos dicen que de cada elemento del dominio de la relación f sale *exactamente* una flecha. Observemos que ambas condiciones son sobre lo que sucede con los elementos del *dominio* de f: bien puede suceder que haya elementos del *codominio* de f, el conjunto B, a los que no llegue ninguna flecha en el grafo de f o elementos a los que llegue más de una. Así, por ejemplo, si $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$, entonces la relación $f \subseteq A \times B$ cuyo grafo es



es una función. En efecto, en este grafo de cada elemento de A sale exactamente una flecha.

3.1.2. Cuando una relación $f \subseteq A \times B$ de un conjunto A a otro B es una función, escribimos

$$f : A \to B.$$

Esta notación nos dice cuál es el dominio de f, cuál es su codominio, y deja en claro que se trata de una función.

Por otro lado, si $f : A \to B$ es una función de A a B y a es un elemento de A, sabemos que existe un elemento b en B y uno solo tal que $(a, b) \in f$: a ese elemento lo escribimos

$$f(a)$$

y lo llamamos el ***valor*** de f en a o la ***imagen*** de a por f. En otras palabras, cuando escribimos que

$$b = f(a)$$

estamos diciendo, ni más ni menos, que el par ordenado (a, b) pertenece a f.

3.1.3. Ejemplo. Sean A y B dos conjuntos y probemos que la relación identidad $I_A \subseteq A \times A$ es una función, a la que llamamos la ***función identidad*** de A. Para hacerlo, verificamos las dos condiciones de la definición 3.1.1.

- Si a es un elemento de A, entonces el par ordenado (a, a) pertenece a I_A.
- Supongamos que $a \in A$ y $b, b' \in A$ son tales que los pares ordenados (a, b) y (a, b') están en I_A. De la definición de I_A se sigue, claro, que $a = b$ y que $a = b'$ y, en particular, que $b = b'$.

Esto prueba lo que queremos.

3.1.4. Ejemplo. Sean A y B dos conjuntos, y sea b_0 es un elemento de B. La relación

$$f = \{(a, b_0) \in A \times B : a \in A\}$$

es una función $f : A \to B$, a la que llamamos la ***función constante*** de valor b. En efecto, si a es un elemento cualquiera de A, entonces el par (a, b_0) pertenece a b, así que la primera condición de la definición 3.1.1 se cumple. Por otro lado, si a es un elemento de A y b y b' son elementos de B tales que los pares ordenados (a, b) y (a, b') están en f, entonces claramente tiene que ser $b = b_0 = b'$. La segunda condición de la definición, por lo tanto, también se cumple.

3.1.5. Ejemplo. Sean A y B dos conjuntos y sea $R = \varnothing \subseteq A \times B$ la relación vacía de A a B. Nos preguntamos cuándo R es una función.

Supongamos primero que R es una función. De acuerdo a la primera condición de la definición 3.1.1, entonces, para todo elemento a de A existe un elemento b de B tal que el par ordenado (a, b) pertenece a R. Ahora bien, como el conjunto R es vacío, esto implica claramente que no puede haber en A ningún elemento, esto es, que el conjunto A tiene que ser vacío.

Esto nos da una condición necesaria para que la relación vacía de A a B sea una función: que A

sea vacío. También es una condición suficiente. En efecto, si A vacío, entonces las dos condiciones de la definición 3.1.1 se cumplen trivialmente. Podemos concluir, en definitiva, que

la relación vacía de A a B es una función si y solamente si el conjunto A es vacío.

Notemos que cuando esa condición se cumple, el conjunto $A \times B$ es vacío, así que la única relación de A a B es la vacía.

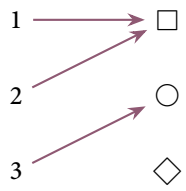
3.1.6. Ejemplo. Sean otra vez A y B dos conjuntos, consideremos ahora la relación total $R = A \times B$ de A a B. Si A es vacío, entonces esta relación R coincide con la relación vacía de A a B y vimos en el ejemplo anterior que se trata de una función. Supongamos entonces que el conjunto A no es vacío, de manera que hay algún elemento a en A.

La primera condición de la definición 3.1.1 nos dice que hay entonces un elemento b en B tal que $(a, b) \in R$ y, en particular, que el conjunto B no es vacío. Más aún, B tiene en este caso exactamente un elemento. En efecto, si por el contrario hubiera dos elementos distintos b y b' en B, tendríamos que (a, b) y (a, b') están los dos en R, contradiciendo la segunda condición de la definición 3.1.1. Vemos así que una condición necesaria para que R sea una función es que B tenga exactamente un elemento. Esta condición también es suficiente — dejamos la verificación de esto al lector.

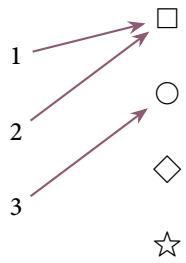
3.1.7. Si $f : A \to B$ y $g : C \to D$ son dos funciones, entonces decimos que f y g son ***iguales*** si

- los dominios de f y de g coinciden, esto es, si $A = C$;
- los codominios de f y de g coinciden, esto es, si $B = D$; y
- f y g coinciden como conjuntos.

Es importante no olvidar que insistimos aquí en que los dominios y los codominios coincidan. Así, por ejemplo, si $A = \{1, 2, 3\}$, $B = \{\square, \bigcirc, \diamondsuit\}$ y $C = \{\square, \bigcirc, \diamondsuit, \star\}$, entonces hay una función $f : A \to B$ cuyo grafo es



y hay una función $g : A \to B$ cuyo grafo es



y estas dos funciones son *distintas* porque sus codominios son diferentes. Notemos que sus dominios coinciden y que tanto f como g corresponden al conjunto

$$\{(1, \square), (2, \square), (3, \bigcirc)\}.$$

3.1.8. En la práctica, usamos casi siempre el siguiente criterio para comparar funciones:

Proposición. *Sean A y B dos conjuntos. Dos funciones $f : A \to B$ y $g : A \to B$ son iguales si y solamente si para todo elemento a de A se tiene que $f(a) = g(a)$.*

Demostración. Sean $f : A \to B$ y $g : A \to B$ dos funciones. Que si f es igual a g entonces $f(a) = g(a)$ para todo elemento a de A es evidente, así que bastará que probemos la implicación recíproca a esta.

Supongamos que $f(a) = g(a)$ para todo elemento a de A. Para ver que $f = g$, como f y g tienen el mismo dominio y el mismo codominio, tenemos que probar que f y g coinciden como conjuntos. Ahora bien, si (a, b) es un elemento de f, entonces a es un elemento de A y $b = f(a)$: pero entonces la hipótesis nos dice que también $b = g(a)$ y, por lo tanto que $(a, b) \in g$. Esto prueba que $f \subseteq g$. Por supuesto, un razonamiento similar prueba que $g \subseteq f$ y, por lo tanto, que $f = g$, como queremos. □

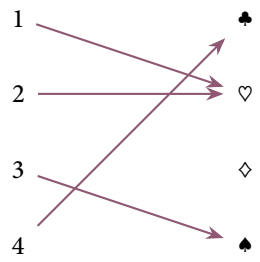
§3.2. Formas de describir funciones

3.2.1. Una función de un conjunto A a un conjunto B es una relación de A a B, así que no es otra cosa que un subconjunto de $A \times B$. Esto significa que para dar una función tenemos a nuestra disposición todas las formas que hay para describir conjuntos.

Así, podemos describir una función por enumeración. Por ejemplo, si $A = \{1, 2, 3, 4\}$ y $B = \{\clubsuit, \heartsuit, \diamondsuit, \spadesuit\}$, entonces podemos dar una función $f : A \to B$ dando el correspondiente subconjunto de $A \times B$ por enumeración, como

$$f = \{(1, \heartsuit), (2, \heartsuit), (3, \spadesuit), (4, \clubsuit)\}.$$

Por supuesto, como f es una relación, también podemos describirla dando su grafo, que en este case es el siguiente:



Muchas veces, en lugar de hacer alguna de estas dos cosas, tabulamos los elementos del conjunto f en una tabla como la siguiente:

a	$f(a)$
1	♡
2	♡
3	♠
4	♣

Cada fila de esta tabla describe uno de los pares ordenados del conjunto f.

Estas estrategias para describir una función solo se aplican si su dominio es un conjunto finito, por supuesto, ya que es exactamente en ese caso que tenemos que dar un número finito de pares ordenados al describirla.

3.2.2. También podemos dar una función por comprensión. Por ejemplo,

$$f \coloneqq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = x^2\}$$

es la descripción por comprensión de un subconjunto de $\mathbb{Z} \times \mathbb{Z}$, esto es, de una relación de $\mathbb{Z}$ a $\mathbb{Z}$, y se trata de una función. Probémoslo.

- Si x es un elemento cualquiera de $\mathbb{Z}$, entonces claramente el par ordenado (x, x^2) pertenece a f, y esto nos dice que la primera condición de la definición 3.1.1 se cumple.
- Por otro lado, supongamos que x, y e y' son elementos de $\mathbb{Z}$ tales que los pares (x, y) y (x, y') pertenecen a f. Esto significa que $y = x^2$ y que $y' = x^2$: por supuesto, de estas dos igualdades podemos deducir que $y = y'$ y, en definitiva, que la segunda condición de la definición 3.1.1 también se cumple.

Para esta función f se tiene claramente que para todo elemento x de $\mathbb{Z}$ es

$$f(x) = x^2.$$

En efecto, lo que estamos afirmando es que para todo elemento x de $\mathbb{Z}$ el par ordenado (x, x^2) pertenece a f, y eso es evidente, dada la definición de f!

3.2.3. En la practica, casi siempre definimos las funciones como en el ejemplo que acabamos de ver, aunque usando una notación distinta para hacerlo. En lugar de describir a una función f de un conjunto A a un conjunto B por comprensión en la forma

$$f = \left\{(a, b) \in A \times B : b = \boxed{E}\right\}, \tag{1}$$

con $\boxed{E}$ alguna expresión conveniente[1], escribimos

$$f : a \in A \mapsto \boxed{E} \in B. \tag{2}$$

Es importante tener siempre en mente que esto último significa *exactamente* lo mismo que la descripción por comprensión (1). Podemos leer la expresión escrita en (2) diciendo «la función f que a cada elemento a de A lo manda al elemento $\boxed{E}$ de B».

Así, por ejemplo, a la función de 3.2.2 podemos describirla escribiendo

$$f : x \in \mathbb{Z} \mapsto x^2 \in \mathbb{Z},$$

y si escribimos

$$g : n \in \mathbb{N} \mapsto n^2 - 10n \in \mathbb{Z}$$

nos estamos refiriendo a la función, a la que llamamos g, de dominio $\mathbb{N}$ y codominio $\mathbb{Z}$, dada por el conjunto

$$\{(n, m) \in \mathbb{N} \times \mathbb{Z} : m = n^2 - 10n\}.$$

De la misma forma, si escribimos

$$h : t \in \mathbb{R} \mapsto \operatorname{sen} t \in \mathbb{R}$$

estamos refiriéndonos a la función h de $\mathbb{R}$ a $\mathbb{R}$ dada por el conjunto de pares ordenados

$$\{(t, u) \in \mathbb{R} \times \mathbb{R} : u = \operatorname{sen} t\}.$$

[1] No entraremos aquí en los detalles sobre qué significa exactamente «conveniente» en este contexto.

Algo que es muchas veces útil es que esta notación nos permite referirnos a una función sin necesidad de ponerle un nombre. Así, por ejemplo, podemos decir cosas como

las funciones $n \in \mathbb{N} \mapsto n^2 \in \mathbb{N}$ *y* $n \in \mathbb{N} \mapsto n^3 \in \mathbb{N}$ *son distintas.*

Otra forma de dar por comprensión una función f de un conjunto a A a otro B es describir explícitamente el valor de f en cada elemento de su dominio. Así, podemos decir

sea $f : \mathbb{N} \to \mathbb{Z}$ *la función que en cada elemento* n *de* $\mathbb{N}$ *toma el valor* $f(n) = n^2 - 10n$.

La función a la que nos estamos refiriendo es, claramente, la determinada por el conjunto $\{(n, m) \in \mathbb{N} \times \mathbb{Z} : m = n^2 - 10n\}$, que podemos escribir, como vimos, $n \in \mathbb{N} \mapsto n^2 - 10n \in \mathbb{Z}$.

3.2.4. Recordemos que en 2.3.1 definimos la operación de relaciones: si A, B y C son tres conjuntos y R y S son una relación de A a B y una relación de B a C, respectivamente, entonces construimos allí una nueva relación $S \circ R$ de A a C, la composición de S con R. La segunda parte de la siguiente proposición nos dice que si las relaciones R y S son funciones, también lo es su composición.

Proposición. *Sean A, B y C tres conjuntos.*

(*i*) *La relación identidad $I_A \subseteq A \times A$ es una función.*

(*ii*) *Si $f : A \to B$ y $g : B \to C$ son funciones, entonces la relación $g \circ f \subseteq A \times C$ es una función de A a C.*

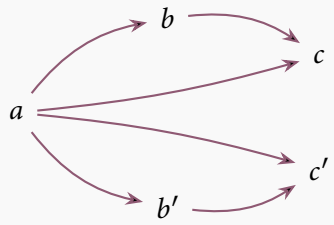
Demostración. (*i*) Veamos que I_A es una función, verificando las dos condiciones de la definición 3.1.1.

- Si a es un elemento de A, entonces el par ordenado (a, a) pertenece a I_A.
- Supongamos que $a \in A$ y $b, b' \in A$ son tales que los pares ordenados (a, b) y (a, b') están en I_A. De la definición de I_A se sigue, claro, que $a = b$ y que $a = b'$ y, en particular, que $b = b'$.

(*ii*) Otra vez, para mostrar que la relación compuesta $g \circ f$ de A a C es una función verificamos las dos condiciones de la definición 3.1.1.

- Sea $a \in A$. Como f es una función, existe un elemento $b \in B$ tal que $(a, b) \in f$ y, por otro lado, como g es una función, existe un elemento $c \in C$ tal que $(b, c) \in g$. De acuerdo a la definición de la composición de relaciones, entonces, se tiene que $(a, c) \in g \circ f$.
- Sean $a \in A$ y $c, c' \in C$ tales que los pares ordenados (a, c) y (a, c') están en $g \circ f$. Esto significa que existen elementos b y b' en B tales que (a, b) y (a, b') están en f y (b, c) y

(b', c') están en g.



Ahora bien, como f es una función, de que los pares (a, b) y (a, b') estén en f se deduce que $b = b'$. Tenemos entonces que los pares (b, c) y (b, c') están en g y, como g también es una función, vemos que $c = c'$.

Esto completa la prueba de la proposición. □

3.2.5. Si A, B y C son tres conjuntos y $f : A \to B$ y $g : B \to C$ son dos funciones, esta proposición nos dice que la composición $g \circ f : A \to C$ es también una función. Si a es un elemento de A, entonces tenemos la imagen de a por f, el elemento $b \coloneqq f(a)$ de B y, a su vez, tenemos la imagen de b por g, el elemento $c \coloneqq g(b)$. En otras palabras, tenemos que $(a, b) \in f$ y que $(b, c) \in g$, así que la definición de $g \circ f$ implica que $(a, c) \in g \circ f$. Vemos así que

$$(g \circ f)(a) = c = g(b) = g(f(a)).$$

3.2.6. La Proposición 2.3.4 nos dice que la composición de relaciones es una operación asociativa. Como la composición de funciones no es más que la composición de relaciones, vemos así que, en particular, la composición de funciones es una operación asociativa. Explícitamente, esto significa que si A, B, C y D son cuatro conjuntos y $f : A \to B$, $g : B \to C$ y $h : C \to D$ son tres funciones, entonces vale que

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Casi siempre escribimos simplemente $h \circ g \circ f$ a la función $h \circ (g \circ g)$. Su valor en un elemento a de su dominio es $h(g(f(a)))$.

§3.3. Inyectividad, sobreyectividad, biyectividad

3.3.1. Sean A y B dos conjuntos y sea $f : A \to B$ una función de A a B. Decimos que

- f es ***inyectiva*** si cada vez que a y a' son dos elementos de A tales que $f(a) = f(a')$ se tiene que $a = a'$, que
- f es ***sobreyectiva*** si para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$, y que
- f es ***biyectiva*** si es a la vez inyectiva y sobreyectiva.

En términos del grafo de la función f, la condición de inyectividad es que a cada elemento de b llegue *a lo sumo* una flecha desde un elemento de A, mientras que la de sobreyectividad que a cada elemento de B llegue *al menos* una flecha.

3.3.2. La definición que acabamos de dar nos dice que una función $f : A \to B$ es inyectiva si siempre que a y a' son elementos de su dominio A vale que

$$f(a) = f(a') \implies a = a'.$$

Equivalentemente, la función f es inyectiva si siempre que a y a' son elementos de su dominio vale que

$$a \neq a' \implies f(a) \neq f(a').$$

En efecto, esta implicación es la contrarrecíproca de la anterior, así que es equivalente a ella.

3.3.3. Ejemplo. Si A es un conjunto cualquiera, entonces la función identidad $I_A : A \to A$ es inyectiva, sobreyectiva y, por lo tanto, biyectiva.

3.3.4. Las tres propiedades descriptas en 3.3.1 se preservan al componerlas:

Proposición. *Sean A, B y C conjuntos y sean $f : A \to B$ y $g : B \to C$ funciones.*

(*i*) *Si las funciones f y g son inyectivas, entonces la composición $g \circ f$ es inyectiva.*
(*ii*) *Si las funciones f y g son sobreyectivas, entonces la composición $g \circ f$ es sobreyectiva.*
(*iii*) *Si las funciones f y g son biyectivas, entonces la composición $g \circ f$ es biyectiva.*

Demostración. (*i*) Supongamos que las funciones f y g son inyectivas, y sean a y a' elementos de A tales que $(g \circ f)(a) = (g \circ f)(a')$, es decir, tales que $g(f(a)) = g(f(a'))$. Como g es inyectiva, esto implica que $f(a) = f(a')$ y, a su vez, como f es inyectiva, esto implica que $a = a'$: vemos así que la composición $g \circ f$ es inyectiva.

(*ii*) Supongamos ahora que las funciones f y g son sobreyectivas, y sea $c \in C$. Como g es sobreyectiva, hay un elemento b de B tal que $g(b) = c$ y, por otro lado, como f es sobreyectiva,

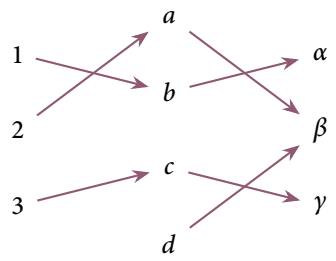
hay un elemento a de A tal que $f(a) = b$. Tenemos entonces que

$$(g \circ f)(a) = g(f(a)) = g(b) = c,$$

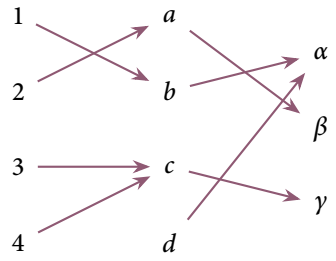
y esto nos dice que $g \circ f$ es sobreyectiva.

(*iii*) Supongamos finalmente que f y g son biyectivas. Como f y g son entonces inyectivas, la primera parte de esta proposición nos dice que la composición $g \circ f$ es inyectiva; por otro lado, como f y g son sobreyectivas, la segunda parte nos dice que esa composición es sobreyectiva. Vemos así que $g \circ f$ es biyectiva, como queremos. □

3.3.5. Las implicaciones recíprocas a las de la Proposición 3.3.4 son falsas. Así, por ejemplo, la composición indicada en el gráfico



es inyectiva, pero la segunda función no lo es. De manera similar, la composición



es ciertamente sobreyectiva pero la primera de las dos funciones que estamos componiendo no lo es. Sin embargo, tenemos el siguiente resultado parcial:

3.3.6. Proposición. *Sean A, B y C conjuntos y sean $f : A \to B$ y $g : B \to C$ funciones.*

(*i*) *Si la composición $g \circ f$ es inyectiva, entonces la función f es inyectiva.*

(*ii*) *Si la composición $g \circ f$ es sobreyectivas, entonces la función g es sobreyectiva.*

Demostración. (*i*) Probaremos la implicación contrarrecíproca, esto es, que

si f no es inyectiva, entonces la composición $g \circ f$ tampoco lo es.

Supongamos entonces que f no es inyectiva, de manera que hay elementos a y a' en A tales que $a \neq a'$ y $f(a) = f(a')$. Se tiene entonces que

$$(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a'),$$

y, como $a \neq a'$, que la composición $g \circ f$ no es inyectiva.

(*ii*) Supongamos que la composición $g \circ f$ es una función sobreyectiva y sea $c \in C$. La hipótesis nos dice que existe $a \in A$ tal que $c = (g \circ f)(a)$, es decir, que $c = g(f(a))$. El elemento $b = f(a)$ de B es entonces tal que $g(b) = c$: esto muestra que la función g es sobreyectiva. □

§3.4. Funciones inversibles y funciones inversas

3.4.1. Sea $f : A \to B$ una función de un conjunto A a otro B. Decimos que f es ***inversible*** si existe una función $g : B \to A$ tal que $g \circ f = I_A$ y que $f \circ g = I_B$ y en ese caso decimos que g es una ***función inversa*** de f.

Notemos que en esta situación el dominio de g tiene que ser el codominio de f y el codominio de g tiene que ser el dominio de f: si no es ese el caso, ni siquiera podemos hablar de las composiciones $g \circ f$ y $f \circ g$.

3.4.2. Una observación importante es la siguiente:

Lema. *Si una función es inversible, entonces posee exactamente una función inversa.*

En vista de esto, cuando tengamos una función inversible podremos hablar de *la* función inversa y no solamente de *una* función inversa, ya que esta está bien determinada.

Demostración. Sea $f : A \to B$ una función, y supongamos que f es inversible y que las funciones $g_1, g_2 : B \to A$ son funciones inversas de f, de manera que se tiene que

$$g_1 \circ f = g_2 \circ f = I_A, \qquad f \circ g_1 = f \circ g_2 = I_B.$$

Usando estas igualdades, vemos que

$$g_1 = g_1 \circ I_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2.$$

Como g_1 y g_2 tienen el mismo dominio y el mismo codominio, esto prueba el lema. □

3.4.3. La siguiente proposición establece la conexión fundamental entre la condición de inversibilidad de una funciones y su biyectividad:

Proposición. *Sean A y B dos conjuntos. Una función $f : A \to B$ es inversible si y solamente si es biyectiva. Cuando ese es el caso, la relación inversa $f^{-1} \subseteq B \times A$ es una función y es, de hecho, la función inversa de f.*

Demostración. Sea $f : A \to B$ una función y supongamos primero que f es inversible, de manera que existe una función $g : B \to A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$. Como la composición $g \circ f$ es inyectiva, ya que es la función identidad de A, la Proposición 3.3.6(*i*) nos dice que f es inyectiva. De manera similar, como la composición $f \circ g$ es sobreyectiva, ya que es la función identidad de B, la Proposición 3.3.6(*ii*) nos dice que f es sobreyectiva. Vemos así que f es biyectiva.

Supongamos en segundo lugar que f es biyectiva y consideremos la relación inversa $f^{-1} \subseteq B \times A$. Se trata de una función: para verlo, verificamos las dos condiciones de la definición 3.1.1.

- Si b es un elemento de B, entonces, como f es sobreyectiva, existe $a \in A$ tal que $b = f(a)$, esto es, tal que el par ordenado (a, b) pertenece a f. Esto significa que el par ordenado (b, a) pertenece a la relación f^{-1}.
- Sean b un elemento de B y a, a' elementos de A tales que los pares ordenados (b, a) y (b, a') están en f^{-1}. Esto significa que los pares ordenados (a, b) y (a', b) están en f, es decir, que $f(a) = b$ y que $f(a') = b$. Pero entonces $f(a) = f(a')$ y, como f es inyectiva, tenemos necesariamente que $a = a'$.

Vemos así que, como dijimos, la relación f^{-1} es una función $f^{-1} : B \to A$. Mostremos que f^{-1} es una función inversa de f y, por lo tanto, que la función f es inversible.

- Sea a un elemento de A. Pongamos $b \coloneqq f(a)$, de manera que $(a, b) \in f$ y, por lo tanto, $(b, a) \in f^{-1}$, es decir, $f^{-1}(b) = a$. Usando esto, vemos que

  $$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = I_A(a)$$

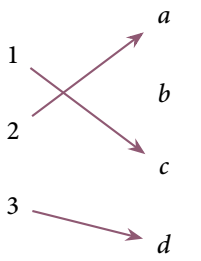
  y concluimos que las funciones $f^{-1} \circ f$ e I_A toman el mismo valor en cada elemento de su dominio común A: esto significa, precisamente, que $f^{-1} \circ f = I_A$.
- Sea ahora b un elemento de B y pongamos $a \coloneqq f^{-1}(b)$, de manera que $(b, a) \in f^{-1}$ y $(a, b) \in f$, es decir, $f(a) = b$. Tenemos que

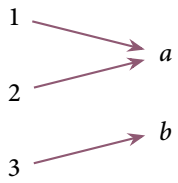
  $$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b = I_B(b)$$

  y, en consecuencia, que $f \circ f^{-1} = I_B$.

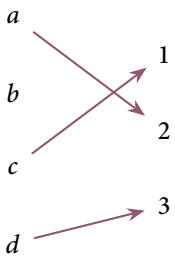
Esto completa la prueba de la proposición. □

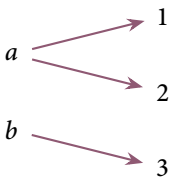
3.4.4. Es importante observar que si $f : A \to B$ es una función que no es biyectiva, entonces la relación inversa $f^{-1} : B \times A$ no es una función. Por ejemplo, las relaciones inversas de las funciones





son, respectivamente,





y ninguna de estas dos últimas es una función.

3.4.5. Ejercicio. Pruebe en detalle que una función $f : A \to B$ es biyectiva, si y solamente si la relación $f^{-1} \subseteq B \to A$ es una función de B a A.

3.4.6. Sabemos que la composición de dos funciones biyectivas biyectivas es ella misma biyectiva, y acabamos de probar que es entonces inversible. El siguiente resultado nos permite calcular su inversa.

Proposición. *Sean $f : A \to B$ y $g : B \to C$ dos funciones inversibles, de manera que poseen funciones inversas $f^{-1} : B \to A$ y $g^{-1} : C \to B$. La composición $g \circ f : A \to C$ es inversible y su función inversa es*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Demostración. Como f y g son inversibles, la Proposición 3.4.3 nos dice que son biyectivas y la Proposición 3.3.4(*iii*), a su vez, que la composición $g \circ f$ es biyectiva. La primera de esas proposiciones, por lo tanto, implica que esta composición es inversible. Esto prueba la primera de las dos afirmaciones del enunciado. Para ver la segunda, es suficiente que mostremos que la

función $h \coloneqq f^{-1} \circ g^{-1}$ es una función inversa de la función $k \coloneqq g \circ f$, y para ello tenemos que probar que $h \circ k = I_A$ y que $k \circ h = I_C$. Ahora bien, es

$$\begin{aligned} h \circ k &= (f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ (g \circ f)) = f^{-1} \circ ((g^{-1} \circ g) \circ f) \\ &= f^{-1} \circ (I_B \circ f) = f^{-1} \circ f = I_A \end{aligned}$$

y, de manera similar,

$$\begin{aligned} k \circ h &= (g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ (f^{-1} \circ g^{-1})) = g \circ ((f \circ f^{-1}) \circ g^{-1}) \\ &= g \circ (I_B \circ g^{-1}) = g \circ g^{-1} = I_C, \end{aligned}$$

y esto prueba lo que queremos. □

§3.5. Ejercicios

Imagen y preimagen de subconjuntos por una función

3.5.1. Sean A y B dos conjuntos y sea $f : A \to B$ una función de A a B. Si X es un subconjunto de A, llamamos ***imagen*** de X por f al subconjunto

$$f[X] \coloneqq \{f(a) : a \in X\}$$

de B, de manera que si $b \in B$ se tiene que

$$b \in f[X] \iff \text{existe } a \in X \text{ tal que } f(a) = b.$$

De manera similar, si Y es un subconjunto de B, llamamos ***preimagen*** o ***imagen inversa*** de Y por f al subconjunto

$$f^{-1}[Y] \coloneqq \{a \in A : f(a) \in Y\}$$

de A, y entonces para cada $a \in A$ se tiene que

$$a \in f^{-1}[Y] \iff f(a) \in Y.$$

3.5.2. Ejercicio. Sea $f : A \to B$ una función.

(*a*) Para cada subconjunto $X \subseteq A$ se tiene que $X \subseteq f^{-1}[f[X]]$ y, más aún, si la función f es inyectiva, entonces $X = f^{-1}[f[X]]$. Esta última igualdad no vale siempre.

(*b*) Para cada subconjunto $Y \subseteq B$ se tiene que $f[f^{-1}[Y]] \subseteq Y$ y, más aún, si la función f es sobreyectiva, entonces $f[f^{-1}[Y]] = Y$. Esta igualdad no vale siempre.

(*c*) Si X_1 y X_2 son subconjuntos de A tales que $X_1 \subseteq X_2$, entonces $f[X_1] \subseteq f[X_2]$.

(*d*) Si Y_1 e Y_2 son subconjuntos de B tales que $Y_1 \subseteq Y_2$, entonces $f^{-1}[Y_1] \subseteq f^{-1}[Y_2]$.

3.5.3. Ejercicio. Sean $f : A \to B$ y $g : B \to C$ dos funciones.

(*a*) Si X es un subconjunto de A, entonces $(g \circ f)[X] = g[f[X]]$.

(*b*) Si Y es un subconjunto de B, entonces $(g \circ f)^{-1}[Y] = f^{-1}[g^{-1}[Y]]$.

3.5.4. Ejercicio. Sea $f : A \to B$ una función.

(*a*) Si X_1 y X_2 son subconjuntos de A, entonces

$$f[X_1 \cup X_2] = f[X_1] \cup f[X_2]$$

y

$$f[X_1 \cap X_2] \subseteq f[X_1] \cap f[X_2],$$

y, más aún, si la función f es inyectiva entonces de hecho se tiene que

$$f[X_1 \cap X_2] = f[X_1] \cap f[X_2].$$

Esta igualdad no vale siempre, sin embargo. Además, se tiene que

$$f[X_1 - X_2] \supseteq f[X_1] - f[X_2]$$

(*b*) Si Y_1 e Y_2 son subconjuntos de B, entonces

$$f^{-1}[Y_1 \cup Y_2] = f^{-1}[Y_1] \cup f^{-1}[X_2],$$
$$f^{-1}[Y_1 \cap Y_2] = f^{-1}[Y_1] \cap f^{-1}[Y_2]$$

y

$$f^{-1}[Y_1 - Y_2] = f^{-1}[Y_1] - f^{-1}[Y_2].$$

3.5.5. Ejercicio. Si $f : A \to B$ es una función y X e Y son subconjuntos de A y de B, respectivamente, entonces se tiene que

$$X \subseteq f^{-1}(Y) \iff f(X) \subseteq Y$$

y vale que

$$f[X] \cap Y = f[X \cap f^{-1}[Y]], \qquad f[X] \cup Y \supseteq f[X \cup f^{-1}[Y]],$$

$$X \cap f^{-1}[Y] \subseteq f^{-1}[f[X] \cap Y], \qquad X \cup f^{-1}[Y] \subseteq f^{-1}[f[X] \cup Y].$$

Ninguna de las últimas tres inclusiones es en general una igualdad: encuentre ejemplos en los que sean estrictas y condiciones sobre f que garanticen las igualdades.

Restricción y correstricción de funciones

3.5.6. Ejercicio. Sea $f : A \to B$ una función y recordemos que, como f es una relación de A a B, se trata de un subconjunto del producto cartesiano $A \times B$.

(*a*) Si C es un subconjunto de A, entonces el subconjunto $f \cap (C \times B)$ de $A \times B$ es una función de C a B. La llamamos la ***restricción*** de f a C y la escribimos $f|_C$.

(*b*) Si D es un subconjunto de B tal que $D \supseteq f[A]$, entonces el subconjunto $f \cap (A \times D)$ de $A \times B$ es una función de A a D. La llamamos la ***correstricción*** de f a B y la escribimos $f|^D$.

(*c*) Más generalmente, si C y D son subconjuntos de A y de B, respectivamente, y se tiene que $f[C] \subseteq D$, entonces la intersección $f \cap (C \times D)$ es una función de C a D, a la que escribimos $f|^D_C$.

3.5.7. Ejercicio. Sea $f : A \to B$ una función. Muestre que si f es inyectiva, entonces la correstricción $f|^{f[A]} : A \to f[A]$ es biyectiva.

"Pegado" de funciones

3.5.8. Muchas veces necesitamos construir funciones $f : A \to B$ «por partes». El siguiente ejercicio es la forma más sencilla en la que podemos hacer eso.

Ejercicio. Sean A y B dos conjuntos, y supongamos que A_1 y A_1 son dos subconjuntos de A tales que $A = A_1 \cup A_2$ y $A_1 \cap A_2 = \varnothing$. Muestre que si $f_1 : A_1 \to B$ y $f_2 : A_2 \to B$ son dos funciones, entonces hay exactamente una función $f : A \to B$ tal que $f|_{A_1} = f_1$ y $f|_{A_2} = f_2$.

3.5.9. Muchas veces necesitamos definir funciones por partes como en el ejercicio anterior pero los subconjuntos A_1 y A_2 que son dominio de las funciones f_1 y f_2 no son disjuntos. En general esto es imposible. Por ejemplo, si $A = \{1, 2, 3\}$, $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $B = \{\square, \bigcirc\}$ y las funciones $f_1 : A_1 \to B$ y $f_2 : A_2 \to B$ están dadas por las siguientes tablas

a	$f_1(a)$
1	$\square$
2	$\square$

a	$f_2(a)$
2	$\bigcirc$
3	$\bigcirc$

entonces es fácil verificar que no existe ninguna función $f : A \to B$ tal que $f|_{A_1} = f_1$ y $f|_{A_2} = f_2$.

Podemos, sin embargo, hacer lo que queremos si hacemos una hipótesis natural.

Ejercicio. Sean A_1, A_2 y B tres conjuntos y sean $f : A_1 \to B$ y $g : A_2 \to B$ dos funciones. Si las restricciones $f|_{A_1 \cap A_2}$ y $g|_{A_1 \cap A_2}$ coinciden, entonces existe una y sólo una función $h : A_1 \cup A_2 \to B$ tal que $h|_{A_1} = f$ y $h|_{A_2} = g$. En esta situación, decimos que la función h se obtiene por "pegado" de las funciones f y g.

3.5.10. Este último resultado puede generalizarse al caso en que tenemos más que dos partes descomponiendo el dominio de la función que queremos construir:

Ejercicio. Sean A y B dos conjuntos, sea $\mathscr{F}$ una familia de subconjuntos de A tal que

$$A = \bigcup_{X \in \mathscr{F}} X,$$

y supongamos que para cada $X \in \mathscr{F}$ tenemos una función $f_X : X \to B$. Pruebe que si

$$\textit{siempre que } X \textit{ e } Y \textit{ son dos elementos de } \mathscr{F} \textit{ tenemos que } f_X|_{X \cap Y} = f_Y|_{X \cap Y} \tag{3}$$

entonces existe exactamente una función $F : A \to B$ tal que $F|_X = f_X$ para todo elemento X de $\mathscr{F}$.

Llamamos a la condición (3) la *condición de cociclo* o *de pegado*. Notemos que tiene sentido: si X e Y son dos elementos de $\mathscr{F}$, entonces $X \cap Y$ es un subconjunto tanto de X como de Y, así que podemos considerar las restricciones $f_X|_{X \cap Y}$ y $f_Y|_{X \cap Y}$ de las funciones $f_X : X \to B$ y $f_Y : Y \to B$ a $X \cap Y$.

Caracterizaciones alternativas de la inyectividad y la sobreyectividad

3.5.11. Ejercicio. Sea $f : A \to B$ una función.

(*a*) La función f es inyectiva si y solamente si cada vez que $g_1 : C \to A$ y $g_2 : C \to A$ son funciones tales que $f \circ g_1 = g \circ f_2$ se tiene que $g_1 = g_2$.

(*b*) La función f es sobreyectiva si y solamente si cada vez que $g_1 : B \to C$ y $g_2 : B \to C$ son funciones tales que $g_1 \circ f = g_2 \circ f$ se tiene que $g_1 = g_2$.

3.5.12. Ejercicio. Si $f : A \to B$ es una función, entonces las siguientes tres condiciones son equivalentes:

(*a*) La función f es inyectiva.

(*b*) Cada vez que X e Y son subconjuntos de A se tiene que $f[X \cap Y] = f[X] \cap f[Y]$.

(*c*) Cada vez que X e Y son subconjuntos de A tales que $X \subseteq Y$ es $f[Y - X] = f[Y] - f[X]$.

Funciones inversas a izquierda y a derecha

3.5.13. Sea $f : A \to B$ una función. Decimos que una función $g : B \to A$ es

- una ***inversa a izquierda*** de f si $g \circ f = I_A$, y
- una ***inversa a derecha*** de f si $f \circ g = I_B$.

Claramente una función $g : B \to A$ es una función inversa para f si y solamente si es a la vez una función inversa a izquierda para f y una función inversa a derecha para f.

3.5.14. Ejercicio. Sea $f : A \to B$ una función.

(*a*) La función f posee una función inversa a izquierda si y solamente si f es inyectiva, pero en general no tiene una sola.

(*b*) La función f posee una inversa a derecha si y solamente si f es sobreyectiva, pero en general no tiene una sola.

(*c*) Si f posee una inversa a izquierda $g : B \to A$ y una inversa a derecha $h : B \to A$, entonces f es inversible y se tiene que $g = h = f^{-1}$.

Relaciones de equivalencia inducidas por funciones

3.5.15. Ejercicio. Sea $f : A \to B$ una función. La relación $R_f \subseteq A \times A$ en el conjunto A tal que si x e y son elementos de A entonces

$$x \; R_f \; y \iff f(x) = f(y)$$

es una relación de equivalencia. Llamamos a R_f la relación de equivalencia ***inducida*** por la función f.

3.5.16. Ejercicio. Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia en A. Hay una función $f : A \to A/R$ con codominio en el conjunto cociente de A por R tal que

$$f(a) = [a]$$

para cada $a \in A$, esta función es sobreyectiva, y la relación de equivalencia $R_f \subseteq A \times A$ inducida por f es precisamente la relación R con la que empezamos. Llamamos a la función f la ***proyección canónica*** de A al cociente A/R.

Observemos que este resultado nos dice que *toda* relación de equivalencia es la relación de equivalencia inducida por alguna función.

---

§3.6. Funciones definidas sobre un conjunto cociente

3.6.1. Terminaremos este capítulo probando el siguiente resultado, que tiene un rol verdaderamente fundamental.

Proposición. *Sean A y B dos conjuntos, sea $R \subseteq A \times A$ una relación de equivalencia en A y sea $f : A \to B$ una función. Si cada vez que a y a' son elementos de A se tiene que*

$$a \; R \; a' \implies f(a) = f(a'),$$

entonces existe una y una sola función $F : A/R \to B$ con dominio en el conjunto cociente A/R de A por R tal que para cada $a \in A$ es

$$F([a]) = f(a).$$

Demostración. Supongamos que la hipótesis de la proposición se satisface y consideremos el conjunto

$$F \coloneqq \{([a], b) \in A/R \times B : a \in A, b = f(a)\}.$$

Se trata de un subconjunto de $A/R \times B$, así que es una relación del conjunto cociente A/R a B. Mostremos que es, de hecho una función.

- Sea α un elemento de A/R, de manera que existe un elemento a en A tal que α es la clase de equivalencia de a con respecto a la relación R, esto es, $\alpha = [a]$. De la definición de la relación F, entonces, es claro que $(c, f(a))$ es un elemento de F.
- Sean ahora α un elemento de A/R y b y b' dos elementos de B tales que los pares ordenados (α, b) y (α, b') pertenecen a F. Como (α, b) es un elemento de F, existe un elemento a en A tal que $\alpha = [a]$ y $b = f(a)$; de manera similar, como (α, b') es un elemento de F, hay un elemento a' tal que $\alpha = [a']$ y $b' = f(b')$. En particular, esto nos dice que $[a] = \alpha = [a']$, así que $a \; R \; a'$ y, de acuerdo a la hipótesis, es también $b = f(a) = f(a') = b'$

Esto prueba que lo que tenemos es, como dijimos, una función $F : A/R \to B$. Más aún, si a es un elemento cualquiera de A, entonces de la definición misma de F es claro que el par ordenado $([a], f(a))$ está en F, así que tenemos que $F([a]) = f(a)$. Esto nos dice que la función F satisface la condición descripta en la proposición.

Para terminar de probar la proposición, entonces, tenemos que mostrar que F es la única función $A/R \to B$ que satisface esa condición. Sea para ello $G : A/R \to B$ otra función tal que $G([a]) = f(a)$ para todo elemento a de A. Si α es un elemento cualquiera de A/R, entonces existe un elemento a de A tal que $\alpha = [a]$, y tenemos en consecuencia que $G(\alpha) = G([a]) = f(a) = F([a]) = F(\alpha)$. Vemos así que F y G toman el mismo valor en cada

elemento de su dominio común — como tienen el mismo codominio, esto nos dice que F y G son, de hecho, la misma función. □

Demos un ejemplo de aplicación de este resultado.

3.6.2. Ejemplo. En el Ejemplo 2.5.7 consideramos el conjunto $A = \mathbb{N} \times \mathbb{N}$, la relación

$$R \coloneqq \{((x,y),(x',y')) \in A \times A : x + y' = x' + y\},$$

y mostramos que se trata de una relación de equivalencia. Consideremos ahora la función

$$f : (x,y) \in A \mapsto x - y \in \mathbb{Z}.$$

Esta función satisface la condición de la Proposición 3.6.1, esto es,

> *si* (x,y) *y* (x',y') *son elementos de* A *tales que* $(x,y)\ R\ (x',y')$*, entonces* $f(x,y) = f(x',y')$.

En efecto, si (x,y) y (x',y') son dos elementos del conjunto A tales que $(x,y)\ R\ (x',y')$, de manera que $x + y' = x' + y$, entonces tenemos que $f(x,y) = x - y = x' - y' = f(x',y')$. La proposición nos dice, entonces, que hay una y solo una función $F : A/R \to \mathbb{Z}$ tal que $F([x,y]) = f(x,y)$ para todo elemento (x,y) de A.

Mostremos que esta función F es biyectiva.

- Supongamos que α y α' son dos elementos de A/R tales que $F(\alpha) = F(\alpha')$. Hay elementos (x,y) y (x',y') de A tales que $\alpha = [(x,y)]$ y $\alpha' = [(x',y')]$, y tenemos entonces que

  $$x - y = f(x,y) = F([(x,y)]) = F(\alpha) = F(\alpha') = F([(x',y')]) = f(x',y') = x' - y'.$$

  Esta igualdad implica que también $x + y' = x' + y$ y, por lo tanto, que $(x,y)\ R\ (x',y')$, así que $\alpha = [(x,y)] = [(x',y')] = \alpha'$. Podemos concluir de todo esto que la función F es inyectiva.

- Sea ahora z un elemento cualquiera de $\mathbb{Z}$. Si es $z \geq 0$, entonces el par ordenado $(z+1,1)$ es un elemento de A y $z = (z+1)-1 = f(z+1,1) = F([(z+1,1)])$. Si, por el contrario, es $z < 0$, entonces el par ordenado $(1,1-z)$ es un elemento de A y $z = 1-(1-z) = f(1,1-z) = F([(1,1-z)])$. En cualquier caso, el elemento z de $\mathbb{Z}$ está en la imagen de la función F. Esto prueba que esta función es sobreyectiva.

3.6.3. Ejercicio. Sean A y B dos conjuntos, sea $R \subseteq A \times A$ una relación de equivalencia en A, y sea $F : A/R \to B$ una función. Pruebe que la función $f : a \in A \mapsto F([a]) \in B$ satisface la condición de la Proposición 3.6.1, esto es, que cualesquiera sean a y a' en A vale que

$$a \; R \; a' \implies f(a) = f(a').$$

Esto muestra que la condición que aparece en esa proposición es necesaria para la conclusión de esta. Explícitamente, lo que tenemos es que

> *si $f : A \to B$ es una función tal que existe una función $F : A/R \to B$ con la propiedad de que $F([a]) = f(a)$ cualesquiera sea el elemento a de A, entonces la función f satisface la condición de la Proposición 3.6.1.*

3.6.4. Ejercicio. Sea A un conjunto y sea $\mathscr{F}$ una partición de A. Hay exactamente una función $f : A \to \mathscr{F}$ tal que $a \in f(a)$ para todo $a \in A$ y se trata de una función sobreyectiva.

Capítulo 4

Inducción

§4.1. El principio de inducción

4.1.1. Decimos que un subconjunto S de $\mathbb{N}$ es ***inductivo*** si tiene las siguientes dos propiedades:

- $1 \in S$, y
- para cada $k \in \mathbb{N}$ vale que

$$k \in S \implies k+1 \in S.$$

Es evidente que el conjunto $\mathbb{N}$ es inductivo y una propiedad fundamental del conjunto $\mathbb{N}$ de los números naturales es que, de hecho, este es el único ejemplo:

Proposición. *Si S es un subconjunto inductivo de $\mathbb{N}$, entonces $S = \mathbb{N}$.* □

Llamamos a este resultado el *principio de inducción*. Veamos por qué es cierto. Sea S un subconjunto inductivo de $\mathbb{N}$ y supongamos que S no es igual a $\mathbb{N}$, de manera que la diferencia $T \coloneqq \mathbb{N} \setminus S$ es un conjunto no vacío. Ahora bien, como T es un subconjunto no vacío de $\mathbb{N}$, posee un menor elemento m: es decir, existe un elemento $m \in T$ tal que para todo $n \in T$ se tiene que $m \leq n$. Como 1 pertenece a S, es $m \neq 1$ y, en consecuencia, el número $m-1$ pertenece a $\mathbb{N}$. Más aún, como $m-1$ es estrictamente menor que m, la forma en que elegimos a m implica que $m-1 \notin T$, es decir, que $m-1 \in S$. Usando esto y el hecho de que S es inductivo, entonces, podemos deducir que $m \in S$: esto es absurdo, ya que m pertenece a T. Esta contradicción provino de suponer que S es un subconjunto propio de $\mathbb{N}$ y todo esto prueba, en consecuencia, que $S = \mathbb{N}$, como queremos.

Este argumento es convincente pero adolece de un problema: depende de que sepamos que la

afirmación

todo subconjunto no vacío de $\mathbb{N}$ *posee un menor elemento*

es cierta y — más allá de que es intuitivamente plausible — no sabemos que esto es así. El problema es que para poder establecer formalmente el principio de inducción necesitamos hacer antes un tratamiento formal de qué es el conjunto $\mathbb{N}$ y de sus propiedades básicas. En estas notas no haremos esto. Usaremos, de todas formas, con total libertad ese principio.

4.1.2. La razón por la que estamos interesados en el principio de inducción es que nos da un mecanismo muy efectivo para probar que un subconjunto de $\mathbb{N}$ coincide con $\mathbb{N}$. Vamos un ejemplo sencillo de por qué esto es útil.

Supongamos que queremos probar la siguiente afirmación:

$$\textit{para todo } n \in \mathbb{N} \textit{ se tiene que } 2^n + 3^n \leq 5^n. \tag{1}$$

Esto puede hacerse de muchas formas. Una de ellas consiste en considerar el subconjunto

$$S = \{n \in \mathbb{N} : 2^n + 3^n \leq 5^n\}$$

de $\mathbb{N}$ y probar que coincide con $\mathbb{N}$: claramente, esto es lo mismo que probar que la afirmación (1) vale. Para ver que S es igual a $\mathbb{N}$ es suficiente, de acuerdo al principio de inducción, con mostrar que se trata de un conjunto inductivo, es decir, que tiene las dos propiedades de la definición **4.1.1**. Así, tenemos que probar que $1 \in S$ y que para todo $k \in \mathbb{N}$ se tiene que

$$k \in S \implies k+1 \in S. \tag{2}$$

La primera de estas dos cosas puede verificarse por un cálculo directo: en efecto, basta observar que $2^1 + 3^1 = 5 \leq 5^1$. Veamos la segunda. Para ello, supongamos que k es un elemento de $\mathbb{N}$ tal que $k \in S$, es decir, tal que

$$2^k + 3^k \leq 5^k. \tag{3}$$

Tenemos que

$$2^{k+1} + 3^{k+1} = 2^k \cdot 2 + 3^k \cdot 3$$

y, como $2 \leq 5$ y $3 \leq 5$, esto es

$$\leq 2^k \cdot 5 + 3^k \cdot 5 = (2^k + 3^k) \cdot 5 \tag{4}$$

Ahora bien, estamos suponiendo que k pertenece a S, así que vale la desigualdad (3), y entonces tenemos que el último miembro de la igualdad (4) es

$$\leq 5^k \cdot 5 = 5^{k+1}.$$

Esto nos dice, precisamente, que $k+1$ pertenece a S. Hemos probado así que vale la segunda condición (2).

4.1.3. Demos otro ejemplo de este procedimiento: probemos que

$$\textit{para todo } n \in \mathbb{N} \textit{ se tiene que } 1 + \cdots + n = \frac{n(n+1)}{2}. \tag{5}$$

A la izquierda de la igualdad que aparece en esta afirmación tenemos la suma de los primeros n números naturales, del 1 hasta n. Como hicimos antes, consideramos el subconjunto

$$S = \left\{ n \in \mathbb{N} : 1 + \cdots + n = \frac{n(n+1)}{2} \right\}$$

de $\mathbb{N}$, mostramos que es inductivo y entonces gracias al principio de inducción, podemos concluir que $S = \mathbb{N}$, que es precisamente lo que se afirma en (5).

La verificación de la primera condición de la definición 4.1.1 es, como en el ejemplo anterior, un simple cálculo directo: cuando $n = 1$, la suma de los primeros n números naturales es claramente igual a 1 y, por otro lado, es

$$\frac{n(n+1)}{2} = \frac{1 \cdot 2}{2} = 1.$$

Esto muestra que $1 \in S$.

Probemos ahora que la segunda condición de 4.1.1 también se cumple. Supongamos que k es un elemento de $\mathbb{N}$ tal que $k \in S$, es decir, tal que

$$1 + \cdots + k = \frac{k(k+1)}{2}. \tag{6}$$

La suma de los primeros $k+1$ números naturales es

$$1 + \cdots + (k+1) = \underbrace{1 + \cdots + k}_{} + (k+1)$$

Ahora bien, los primeros k sumandos de esta suma son precisamente los primeros k números naturales y estamos suponiendo que vale (6), así que

$$1 + \cdots + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

y, observando que $k+1$ es un factor común en los dos términos del miembro derecho de esta igualdad, podemos reescribirlo:

$$= (k+1)\left(\frac{k}{2} + 1\right) = (k+1)\frac{k+2}{2} = \frac{(k+1)(k+2)}{2}.$$

Hemos probado que, bajo la hipótesis de que vale (6), se tiene que

$$1 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2},$$

y esto nos permite concluir que

$$k \in S \implies k+1 \in S.$$

Esto completa la prueba de que el conjunto S es inductivo y, como dijimos antes, de la afirmación (5).

4.1.4. En estos dos ejemplos el procedimiento que seguimos fue completamente similar. En efecto, en ambos casos tenemos un predicado $P(n)$ que depende de un número natural n y queremos probar que

$$\text{para todo } n \in \mathbb{N} \text{ vale } P(n). \tag{7}$$

En el primer ejemplo $P(n)$ es el predicado «$2^n + 3^n \leq 5^n$» mientras que en el segundo es «$1 + \cdots + n = n(n+1)/2$». Consideramos entonces el subconjunto $S = \{n \in \mathbb{N} : P(n)\}$ de $\mathbb{N}$ y mostramos que se trata de un subconjunto inductivo, esto es, que $1 \in S$ y que para cada $k \in \mathbb{N}$ vale $k \in S \implies k+1 \in S$. En vista de la definición del conjunto S, esto es lo mismo que mostrar que

- la afirmación $P(1)$ vale, y que
- para cada $k \in \mathbb{N}$ se tiene que si la afirmación $P(k)$ vale entonces también vale la afirmación $P(k+1)$.

Hecho esto, el principio de inducción nos permite concluir que $S = \mathbb{N}$, esto es, que vale (7), como queremos. En la próxima sección daremos varios ejemplos más de este procedimiento.

Una demostración hecha de esta forma es llamada una *prueba por inducción*. La parte en que probamos que vale la afirmación $P(1)$ es llamada el *paso inicial* o *caso base* de la inducción, mientras que la prueba de la implicación $P(k) \implies P(k+1)$ para cada $k \in \mathbb{N}$ es llamada el *paso inductivo*. Habitualmente, la prueba del paso inductivo procede de la siguiente forma: elegimos un número natural $k \in \mathbb{N}$ y suponemos que la afirmación $P(k)$ se cumple — esta hipótesis es la *hipótesis inductiva* — y de alguna manera, usando esa hipótesis inductiva, probamos que en ese caso también vale la afirmación $P(k+1)$.

§4.2. Algunos ejemplos de pruebas por inducción

Sumas geométricas

4.2.1. Fijemos un número $a \in \mathbb{R}$ distinto de 1 y mostremos que

$$\text{para cada } n \in \mathbb{N} \text{ se tiene que } 1 + a + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}. \tag{8}$$

El miembro izquierdo de esta igualdad es la suma de las primeras n potencias de a, desde la 0-ésima, $a^0 = 1$, hasta la $(n-1)$-ésima, a^{n-1}: la llamamos la ***suma geométrica*** de razón a. Para probar (8), para cada n llamamos $P(n)$ a la afirmación

$$1 + a + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

y procedemos por inducción.

- Vemos que vale $P(1)$ calculando directamente: si $n = 1$, entonces por un lado es

$$1 + a + \cdots + a^{n-1} = 1$$

y, por otro, $(a^n - 1)/(a - 1) = 1$. Esto establece el caso base de la inducción.

- Veamos ahora el paso inductivo. Sea k un elemento de $\mathbb{N}$ y supongamos que vale $P(k)$, de manera que

$$1 + a + \cdots + a^{k-1} = \frac{a^k - 1}{a - 1}.$$

Usando esto, podemos ver que

$$\begin{aligned} 1 + a + \cdots + a^k &= \left(1 + a + \cdots + a^{k-1}\right) + a^k = \frac{a^k - 1}{a - 1} + a^k \\ &= \frac{a^k - 1 + a^k(a - 1)}{a - 1} = \frac{a^{k+1} - 1}{a - 1}, \end{aligned}$$

y esto significa, precisamente, que vale la afirmación $P(k + 1)$.

La inducción queda así completa y prueba, como queríamos, la afirmación (8).

La suma de los cuadrados de los primeros números naturales

4.2.2. Probemos que

$$\textit{para todo } n \textit{ de } \mathbb{N} \textit{ vale que } 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Para ello, para cada $n \in \mathbb{N}$ llamemos $P(n)$ a la afirmación de que

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

y probemos que $P(n)$ vale cualquiera sea n por inducción.

- Cuando $n = 1$ el lado izquierdo de la igualdad de la afirmación $P(1)$ es $1^2 = 1$, mientras que el derecho es

$$\frac{n(n+1)(2n+1)}{6} = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = 1,$$

así que esa igualdad vale.

- Sea ahora k un elemento cualquiera de $\mathbb{N}$ y supongamos que la afirmación $P(k)$ vale, de manera que

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Tenemos entonces que

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 &= 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}, \end{aligned}$$

y esto nos dice que vale la afirmación $P(k+1)$.

La suma alternada de los cuadrados de los primeros números naturales

4.2.3. Probemos que

$$\textit{para todo } n \textit{ de } \mathbb{N} \textit{ vale que } \sum_{i=1}^{n} (-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}. \tag{9}$$

Para cada elemento n de $\mathbb{N}$ llamemos $P(n)$ a la afirmación

$$\sum_{i=1}^{n} (-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}$$

y procedamos por inducción.

- La afirmación $P(1)$ vale, ya que

$$\sum_{i=1}^{1} (-1)^i i^2 = -1$$

y

$$\frac{(-1)^1 1(1+1)}{2} = -1.$$

- Supongamos que k es un elemento de $\mathbb{N}$ y que vale a afirmación $P(k)$, de manera que

$$\sum_{i=1}^{k} (-1)^i i^2 = \frac{(-1)^k k(k+1)}{2}.$$

Separando el último término de la suma, tenemos que

$$\sum_{i=1}^{k+1} (-1)^i i^2 = \sum_{i=1}^{k} (-1)^i i^2 + (-1)^{k+1}(k+1)^2$$

y entonces, usando la hipótesis inductiva, vemos que esto es

$$
\begin{aligned}
&= \frac{(-1)^k k(k+1)}{2} + (-1)^{k+1}(k+1)^2 \\
&= (-1)^k \left(\frac{k}{2} - (k+1)\right)(k+1) \\
&= (-1)^k \frac{k - 2(k+1)}{2}(k+1) \\
&= (-1)^k \frac{-(k+2)}{2}(k+1) \\
&= \frac{(-1)^{k+1}(k+1)(k+2)}{2}.
\end{aligned}
$$

Esto nos dice que, bajo la hipótesis inductiva, vale la afirmación $P(k+1)$.

De esto podemos concluir, gracias al principio de inducción, que vale la igualdad (9) para todo $n \in \mathbb{N}$.

Una suma de fracciones

4.2.4. Queremos probar que

para cada $n \in \mathbb{N}$ *se tiene que* $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

De manera similar a lo que hicimos antes, para cada elemento n de $\mathbb{N}$ llamamos $P(n)$ a la afirmación de que

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

y probamos por inducción que $P(n)$ vale para todo $n \in \mathbb{N}$.

- Calculando, vemos que cuando $n = 1$ es

  $$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{1}{2} = \frac{n}{n+1},$$

  así que la afirmación $P(1)$ vale.

- Sea ahora k un elemento cualquiera de $\mathbb{N}$ y supongamos que vale la afirmación $P(k)$, es decir, que

  $$\sum_{i=1}^{k} \frac{1}{i(i+1)} = \frac{k}{k+1}. \tag{10}$$

Se tiene entonces que

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \sum_{i=1}^{k} \frac{1}{i(i+1)} + \frac{1}{(k+1)(k+2)}$$

y, en vista de la hipótesis inductiva (10), esto es

$$\begin{aligned} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{1}{k+1}\left(k + \frac{1}{k+2}\right) \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{k+1}{k+2}. \end{aligned}$$

Vemos así que

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k+1}{k+2}$$

y, por lo tanto, que vale la afirmación $P(k+1)$.

Esto prueba lo que queremos, gracias al principio de inducción.

El producto de los primeros números impares

4.2.5. Mostremos que

$$\textit{para todo } n \in \mathbb{N} \textit{ se tiene que } \prod_{i=1}^{n}(2i-1) = \frac{(2n)!}{n! \cdot 2^n} \tag{11}$$

haciendo inducción con respecto a n. Para cada elemento n de $\mathbb{N}$ sea $P(n)$ la afirmación de que

$$\prod_{i=1}^{n}(2i-1) = \frac{(2n)!}{n! \cdot 2^n}$$

- Si $n = 1$, entonces

  $$\prod_{i=1}^{n}(2i-1) = 1 = \frac{2}{2} = \frac{(2n)!}{n! \cdot 2^n},$$

  así que vale la afirmación $P(1)$.

- Supongamos ahora que k es un elemento cualquiera de $\mathbb{N}$ y que vale la afirmación $P(k)$, es decir, que

  $$\prod_{i=1}^{k}(2i-1) = \frac{(2k)!}{k! \cdot 2^k}.$$

Separando el último factor del producto, vemos que

$$\prod_{i=1}^{k+1}(2i-1) = \prod_{i=1}^{k}(2i-1)\cdot(2(k+1)-1)$$

y, usando ahora la hipótesis inductiva, que esto es

$$= \frac{(2k)!}{k!\cdot 2^k}\cdot(2(k+1)-1)$$
$$= \frac{(2k)!}{k!\cdot 2^k}(2k+1).$$

Si multiplicamos al último miembro de esta cadena de igualdades por $1 = \frac{2k+2}{2k+2}$, vemos finalmente que

$$\prod_{i=1}^{k+1}(2i-1) = \frac{(2k)!}{k!\cdot 2^k}(2k+1)\frac{2k+2}{2k+2} = \frac{(2(k+1))!}{(k+1)!\cdot 2^{k+1}},$$

es decir, que vale la afirmación $P(k+1)$.

Esto completa la inducción y, por lo tanto, la prueba de (11).

Una sucesión de enteros divisibles por 5

4.2.6. Probemos que

para todo $n \in \mathbb{N}$ *el número* $8^n - 3^n$ *es divisible por* 5. (12)

Para ello, para cada $n \in \mathbb{N}$ llamamos $P(n)$ a la afirmación

$8^n - 3^n$ *es divisible por* 5

y procedemos por inducción.

- Como $8^1 - 3^1 = 8 - 3 = 5$, y esto es evidentemente divisible por 5, es claro que la afirmación $P(1)$ vale: esto establece el caso base.
- Sea, por otro lado, k un elemento cualquiera de $\mathbb{N}$ y supongamos que la afirmación $P(k)$ vale, de manera que 5 divide a $8^k - 3^k$, esto es, que existe un número $r \in \mathbb{Z}$ tal que $8^k - 3^k = 5r$. Entonces

$$8^{k+1} - 3^{k+1} = 8^k\cdot 8 - 8^k\cdot 3 + 8^k\cdot 3 - 3^k\cdot 3$$
$$= 8^k\cdot(8-3) + (8^k - 3^k)\cdot 3$$

y, de acuerdo a la hipótesis inductiva, esto es

$$= 8^k\cdot 5 + 5r\cdot 3$$
$$= (8^k + 3r)\cdot 5.$$

Vemos así $8^{k+1} - 3^{k+1}$ es divisible por 5, esto es, que vale la afirmación $P(k+1)$.

Esto completa la inducción y, por lo tanto, la prueba de (12).

La cardinalidad del conjunto de partes de un conjunto finito

4.2.7. Mostremos que

> *si $n \in \mathbb{N}$ y A es un conjunto finito de n elementos, entonces el conjunto de partes $\mathscr{P}(A)$ tiene 2^n elementos.* (13)

Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

> *si A es un conjunto finito de n elementos, entonces $\mathscr{P}(A)$ tiene 2^n elementos*

y procedamos por inducción con respecto a n.

- Sea A un conjunto que tiene 1 elemento y sea a ese elemento, de manera que $A = \{a\}$. Es claro que $\mathscr{P}(A) = \{\varnothing, A\}$ y, como $A \neq \varnothing$, que $\mathscr{P}(A)$ tiene exactamente dos elementos. Como $2^1 = 2$, esto nos dice que la afirmación $P(1)$ vale.
- Sea ahora k un elemento cualquiera de $\mathbb{N}$ y supongamos que vale la afirmación $P(k)$. Sea A un conjunto finito con $k+1$ elementos y sean $a_1, \ldots, a_{k+1}$ esos $k+1$ elementos listados en algún orden y sin repeticiones. Un subconjunto de A puede contener a a_{k+1} o no, y exactamente una de estas opciones ocurre: esto significa que si ponemos

  $$P \coloneqq \{X \in \mathscr{P}(A) : a_{k+1} \notin X\}, \qquad Q \coloneqq \{X \in \mathscr{P}(A) : a_{k+1} \in X\}$$

  entonces tenemos que $\mathscr{P}(A) = P \cup Q$ y $P \cap Q = \varnothing$ y, en consecuencia, que el número de elementos de $\mathscr{P}(A)$ es la suma del número de elementos de P y el número de elementos de Q.

  Los subconjuntos de A que no contienen a a_{k+1} son precisamente los subconjuntos del conjunto $B = \{a_1, \ldots, a_k\}$. Como B tiene k elementos, la hipótesis de que vale la afirmación $P(k)$ nos dice que $P = \mathscr{P}(B)$ tiene 2^k elementos.

  Es claro que si X es un elemento de P, entonces $X \cup \{a_{k+1}\}$ es un elemento de Q, así que hay una función

  $$f : X \in P \mapsto X \cup \{a_{k+1}\} \in Q.$$

  Esta función es biyectiva. En efecto, si X y X' son dos elementos de P tales que $f(X) = f(X')$, de manera que $X \cup \{a_{k+1}\}) = X \cup \{a_{k+1}\}$, entonces tenemos que

  $$X = (X \cup \{a_{k+1}) \cap B = (X' \cup \{a_{k+1}\}) \cap B = X',$$

  y esto nos dice que la función f es inyectiva. Por otro lado, si Y es un elemento de Q, entonces $Y \cap B$ es un elemento de P tal que $f(Y \cap B) = Y$, así que la función f es sobreyectiva.

La biyectividad de f nos permite concluir que su dominio y codominio tienen el mismo numero de elementos y, por lo tanto, que Q tiene 2^k elementos. Juntando todo, concluimos que $\mathscr{P}(A)$ tiene $2^k + 2^k = 2^{k+1}$ elementos y, por lo tanto, que vale la afirmación $P(k+1)$.

Queda así completa la prueba de (13)

Veamos en un ejemplo como funciona este argumento. Sea $A = \{1, 2, 3, 4\}$, de manera que $k = 3$, y pongamos $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ y $a_4 = 4$. Dividimos a $\mathscr{P}(A)$ en dos partes: P y Q son los subconjuntos de $\mathscr{P}(A)$ de los subconjuntos X de A que no contienen y que contienen, respectivamente, a 4. Así, los elementos de P son

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{1,2\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{1,2,3\},$$

y los de Q son

$$\{4\}, \quad \{1,4\}, \quad \{2,4\}, \quad \{3,4\}, \quad \{1,2,4\}, \quad \{1,3,4\}, \quad \{2,3,4\}, \quad \{1,2,3,4\}.$$

Es claro que P es precisamente $\mathscr{P}(\{1,2,3\})$ y, gracias a la hipótesis inductiva, tiene entonces 2^3 elementos. Por otro lado, la función $X \in P \mapsto X \cup \{4\} \in Q$ es claramente biyectiva y, por lo tanto, Q tienen la misma cantidad de elementos que P, es decir, 2^3.

Subconjuntos de dos elementos de un conjunto finito

4.2.8. Para cada $n \in \mathbb{N}$ vale que

un conjunto de n elementos posee $n(n-1)/2$ subconjuntos de dos elementos. (14)

Para verlo, llamemos $P(n)$ a esta afirmación y procedamos por inducción.

- Si un conjunto A tiene un elemento, entonces por supuesto A no posee ningún subconjunto de dos elementos. Como $n(n-1)/2$ es 0 si $n = 1$, esto nos dice que el caso base funciona, es decir, que vale la afirmación $P(1)$.
- Supongamos ahora que k es un elemento cualquiera de $\mathbb{N}$ y que vale la afirmación $P(k)$, y sea A un conjunto con $k+1$ elementos. Digamos que los elementos de A, listados en algún orden y sin repeticiones, son $a_1, \ldots, a_{k+1}$. Hay dos tipos de subconjuntos de A de dos elementos:
  - En primer lugar, están los subconjuntos de A de dos elementos que *no* contienen a a_{k+1}. Estos son, por supuesto, los subconjuntos de $\{a_1, \ldots, a_k\}$ de dos elementos. Como el conjunto $\{a_1, \ldots, a_k\}$ tiene k elementos y nuestra hipótesis inductiva es que la afirmación $P(k)$ vale, hay $k(k-1)/2$ subconjuntos de este tipo.
  - En segundo lugar, están los subconjuntos de A de dos elementos que *sí* contienen a a_{k+1}. Éstos son de la forma $\{a_i, a_{k+1}\}$ con i algún elemento de $\{1, \ldots, k\}$ y, por lo tanto, hay k de ellos.

Concluimos así que, en total, hay $k(k-1)/2 + k$ subconjuntos de A de dos elementos, y este número es igual a $(k+1)k/2$. Esto muestra que vale $P(k+1)$.

Gracias al principio de inducción, podemos concluir con todo esto que vale (14).

La dualidad de De Morgan

4.2.9. Fijemos un conjunto de referencia U y mostremos la siguiente generalización de la Proposición 1.4.16(*i*):

si $n \in \mathbb{N}$ y $A_1, \ldots, A_n$ son subconjuntos de U, entonces $(A_1 \cap \cdots \cap A_n)^c = A_1^c \cup \cdots \cup A_n^c$.

Procedamos por inducción. En este caso, si $n \in \mathbb{N}$ la afirmación $P(n)$ que nos interesa es

si $A_1, \ldots, A_n$ son subconjuntos de U, entonces $(A_1 \cap \cdots \cap A_n)^c = A_1^c \cup \cdots \cup A_n^c$.

Observemos que la afirmación $P(1)$ es evidente, así que el caso base se satisface automáticamente. Resta entonces probar que vale el paso inductivo. Sea k un elemento de $\mathbb{N}$, supongamos que vale la afirmación $P(k)$, y sean $A_1, \ldots, A_{k+1}$ subconjuntos de U. Tenemos entonces que

$$\begin{aligned}(A_1 \cap \cdots \cap A_{k+1})^c &= ((A_1 \cap \cdots \cap A_k) \cap A_{k+1})^c \\ &= (A_1 \cap \cdots \cap A_k)^c \cup A_{k+1}^c\end{aligned}$$

porque vale la Proposición 1.4.16(*i*), y esto es, de acuerdo a la hipótesis inductiva, es

$$\begin{aligned}&= (A_1^c \cup \cdots \cup A_k^c) \cup A_{k+1}^c \\ &= A_1^c \cup \cdots \cup A_k^c \cup A_{k+1}^c.\end{aligned}$$

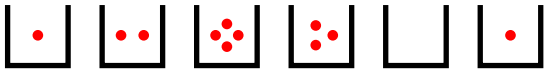
Esto completa la prueba de lo que queremos.

El «principio del palomar»

4.2.10. Mostremos que si n es un elemento de $\mathbb{N}$, entonces vale que

si distribuímos m bolas en n cajas y $m > n$, alguna caja necesariamente contiene dos bolas o más. (15)

Por ejemplo, una posible distribución de 11 bolas en 6 cajas es



y claramente hay cajas que tienen al menos dos bolas.

Llamemos $P(n)$ a la afirmación (15) y procedamos por inducción.

- Consideremos primero el caso en que $n = 1$. Es evidente que si tenemos una sola caja y más que una bola, al distribuir las bolas va a haber más de una bola en esa única caja: esto nos dice que la afirmación $P(1)$, el caso base, vale.
- Supongamos ahora que k es un elemento cualquiera de $\mathbb{N}$ y que sabemos que vale la afirmación $P(k)$. Supongamos que m es un elemento de $\mathbb{N}$ tal que $m > k+1$ y que distribuimos m bolas en $k+1$ cajas, y consideremos tres casos:
  - Si la caja número $k+1$ está vacía, entonces en realidad lo que hicimos fue distribuir las m bolas en las primeras k cajas, y la hipótesis inductiva nos dice, ya que $m > k$, que alguna de estas contiene al menos dos bolas.
  - Si la caja número $k+1$ contiene al menos dos bolas, entonces por supuesto alguna de las cajas contiene al menos dos bolas: por ejemplo, la número $k+1$.
  - Consideremos, finalmente, el caso en que la caja $k+1$ contiene exactamente una bola. En ese caso, distribuimos las otras $m-1$ bolas en las primeras k cajas, y como $m-1 > k$, ya que $m > k+1$, la hipótesis inductiva nos dice que alguna de esas primeras k cajas contiene al menos dos bolas.

  Así, en cualquier caso podemos garantizar que alguna caja contiene al menos dos bolas y, por lo tanto, que vale la afirmación $P(k+1)$. Esto completa la inducción.

Un embaldozado

4.2.11. Supongamos que tenemos muchas piezas de la siguiente forma:

(16)

y que podemos rotarlas 90°, 180° y 270°, de manera que obtenemos

(17)

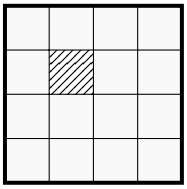
Afirmamos que para cada $n \in \mathbb{N}$ vale que

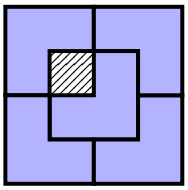
> *si tenemos un tablero de ajedrez de $2^n \times 2^n$ cuadrados al que le falta uno de los cuadrados, podemos taparlo con piezas como la de (16) y sus rotaciones (17) sin que falte cubrir ninguno de los cuadrados restantes ni haya uno cubierto más de una vez.*

(18)

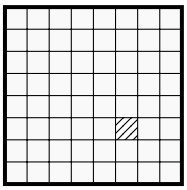
Así, por ejemplo, si $n = 2$ y tenemos un tablero de $2^2 \times 2^2$ cuadrados al que le falta un cuadrado

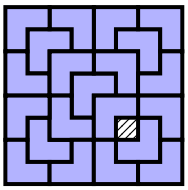
como en el dibujo de la izquierda





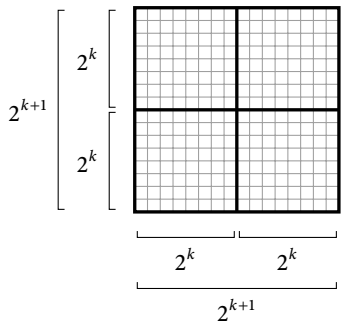
entonces podemos taparlo con fichas como está indicado en la figura derecha. De manera similar, el siguiente dibujo indica como tapar un tablero de $2^3 \times 2^3$ al que le falta el cuadrado gris siguiente:



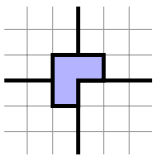


Probemos nuestra afirmación (18) haciendo inducción sobre n. El caso base, en el que $n = 1$, es inmediato: si tenemos un tablero de $2^1 \times 2^1$ al que le falta un cuadrado, el tablero tiene la forma es de una de nuestras piezas, así que ciertamente podemos taparlo de la manera correcta.

Supongamos entonces que $k \in \mathbb{N}$, que la afirmación (18) vale cuando n es k y consideremos un tablero de tamaño $2^{k+1} \times 2^{k+1}$ al que le falta uno de los casilleros. A ese tablero podemos dividirlo en cuatro tableros de tamaño $2^k \times 2^k$, y el casillero faltante está en uno de los cuatro:



Podemos poner una de nuestras piezas en la posición central, de manera que tenga un casillero en cada uno de los subtableros que no contienen el casillero que falta. Por ejemplo, si el casillero que falta el el tablero está en el subtablero que está en la esquina inferior derecha, ponemos una pieza en el centro orientada de la siguiente manera:



Hecho esto, cada uno de los cuatro subtableros es un tablero de tamaño $2^k \times 2^k$ al que le falta un casillero, y la hipótesis inductiva nos dice que podemos taparlo con nuestras piezas de manera que no haya casilleros cubiertos más de una vez. Si hacemos esto con cada uno de estos subtableros, vemos que hemos cubierto el tablero original de la manera que queríamos. Esto significa que vale la afirmación (18) cuando n es $k+1$ y completa la inducción.

§4.3. Dos variaciones del principio de inducción

Inducción «corrida»

4.3.1. Muchas veces tenemos una afirmación $P(n)$ para cada entero positivo n pero, a diferencia de los ejemplos que vimos antes, queremos mostrar no que vale para todo $n \in \mathbb{N}$ sino que vale a partir de algún entero en adelante. Así, por ejemplo, la afirmación «$n! \geq 3^n$» vale para todo entero $n \geq 7$ (y no vale si $1 \leq n \leq 6$). Para probar cosas como esta podemos usar el principio de inducción bajo la siguiente forma:

Proposición. *Sea n_0 un elemento de $\mathbb{Z}$ y consideremos, para cada entero $n \geq n_0$, una afirmación $P(n)$. Si*

- *vale $P(n_0)$ y*
- *para cada entero $k \geq n_0$ se tiene que*

$$P(k) \implies P(k+1),$$

entonces la afirmación $P(n)$ vale para todo entero $n \geq n_0$.

Demostración. Para cada $n \in \mathbb{N}$ sea $Q(n)$ la afirmación $P(n + n_0 - 1)$. Las dos condiciones que aparecen en el enunciado nos dicen que vale $Q(1)$ y que para cada $k \in \mathbb{N}$ se tiene que $Q(k) \implies Q(k+1)$, así que el principio de inducción nos dice que la afirmación $Q(n)$ vale para todo $n \in \mathbb{N}$: esto significa precisamente que la afirmación $P(n)$ vale para todo entero $n \geq n_0$. □

Demos dos ejemplos de cómo usar este resultado.

4.3.2. Ejemplo. Veamos que, como dijimos antes,

para todo $n \geq 7$ se tiene que $n! \geq 3^n$ (19)

usando esta proposición. Llamemos $P(n)$ a la afirmación «$n! \geq 3^n$».

- Calculando, vemos que $7! = 5\,040$ mientras que $3^7 = 2\,187$, así que claramente vale que $3^7 \leq 7!$, es decir, vale la afirmación $P(7)$.
- Por otro lado, supongamos que $k \geq 7$ y que vale la afirmación $P(k)$, de manera que $3^k \leq k!$. Entonces se tiene que

  $$3^{k+1} = 3^k \cdot 3 \leq k! \cdot (k+1)$$

  usando la hipótesis inductiva y el hecho de que $3 \leq k+1$, y esto es

  $$= (k+1)!$$

  Vemos así que para cada entero $k \geq 7$ se tiene que

  $$P(k) \implies P(k+1).$$

Estas dos observaciones y la Proposición 4.3.1 implican que vale (19).

Es de notar que la prueba del segundo punto que hicimos muestra que, de hecho, para todo entero $k \geq 2$ se tiene que $P(k) \implies P(k+1)$: esto no nos permite concluir que $P(r)$ valga para todo $n \geq 2$, ya que $P(2)$ no vale — en efecto, $2! = 2 < 9 = 3^2$.

4.3.3. Ejemplo. Probemos ahora que

para todo $n \in \mathbb{N}$ *tal que* $n \geq 5$ *vale que* $2^n > n^2$. (20)

Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación «$2^n > n^2$» y procedamos por inducción.

- Cuando $n = 5$ es $2^n = 32$ y $n^2 = 25$, así que ciertamente vale que $2^n > n^2$, esto es, la afirmación $P(5)$ es cierta.
- Supongamos ahora que k es un elemento tal que $k \geq 5$ y vale la afirmación $P(k)$, de manera que $2^k > k^2$. Como $k \geq 5$, es $k^2 \geq 5k$ y $3k - 1 \geq 3 \cdot 5 - 1 = 14$, así que

  $$k^2 - 2k - 1 \geq 5k - 2k - 1 = 3k - 1 \geq 14 > 0$$

  y, por lo tanto, $k^2 > 2k + 1$. Por otro lado, como $2^k > k^2$, tenemos que

  $$2^{k+1} = 2 \cdot 2^k \geq 2k^2 = k^2 + k^2 > k^2 + 2k + 1 = (k+1)^2,$$

  y esto nos dice que la afirmación $P(k+1)$ vale.

Esto completa la inducción y prueba (20). Notemos que el segundo punto que hicimos es la prueba de que para todo $k \in \mathbb{N}$ vale

$$k \geq 5 \wedge P(k) \implies P(k+1).$$

y no que vale

$$P(k) \implies P(k+1).$$

De hecho, esta última implicación es falsa: por ejemplo, $P(1)$ vale, ya que $2^1 = 2 > 1 = 1^2$, pero $P(2)$ no, ya que $2^2 = 4 \not> 2^2$.

4.3.4. La proposición anterior nos dice, informalmente, que podemos arrancar la inducción en cualquier entero. Es importante, de todas formas, arrancarla en *alguno*. Por ejemplo, si para cada $n \in \mathbb{N}$ llamamos $P(n)$ a la afirmación

$$n = n + 1,$$

entonces es cierto que si $k \in \mathbb{Z}$ vale que

$$P(k) \implies P(k+1).$$

En efecto, supongamos que k es un elemento de $\mathbb{Z}$ y que vale $P(k)$, esto es, que $k = k + 1$. En ese caso, sumando 1 a ambos lados de esa igualdad vemos inmediatamente que $k + 1 = (k + 1) + 1$, es decir, que vale la afirmación $P(k + 1)$. Por supuesto, no existe *ningún* entero $n_0 \in \mathbb{Z}$ tal que $P(n_0)$ valga, así que no podemos usar la Proposición 4.3.1 para concluir nada.

Inducción «fuerte»

4.3.5. En todos los ejemplos de pruebas por inducción que llevamos vistos hasta ahora, para probar que una afirmación $P(n)$ vale cualquiera sea el entero positivo n mostramos que para cada $k \in \mathbb{N}$ se tiene que

$$P(k) \implies P(k+1).$$

Al hacer eso, fijamos $k \in \mathbb{N}$, supusimos que vale la afirmación $P(k)$ — esta es la llamada «hipótesis inductiva», como dijimos — y de alguna forma, a partir de eso, concluimos que vale la afirmación $P(k + 1)$. La razón por la que esto funciona, en todos los casos que vimos, es que saber que $P(k)$ vale ayuda a probar que $P(k + 1)$ vale. Hay situaciones, sin embargo, en que los que no es suficiente saber que vale $P(k)$ para probar $P(k + 1)$.

4.3.6. Veamos un ejemplo sencillo de esto. Supongamos que tenemos monedas de 3 y de 7 centavos y tratemos de probar que

para cada $n \geq 12$ es posible juntar exactamente n centavos usando estas monedas.

Así, como $2 \cdot 3 + 4 \cdot 7 = 34$, podemos juntar 34 centavos usando 2 monedas de 3 centavos y 4 de 7. Si intentamos proceder por inducción, es natural llamar $P(n)$, para cada $n \in \mathbb{N}$, a la afirmación

es posible juntar n centavos usando monedas de 3 y de 7 centavos.

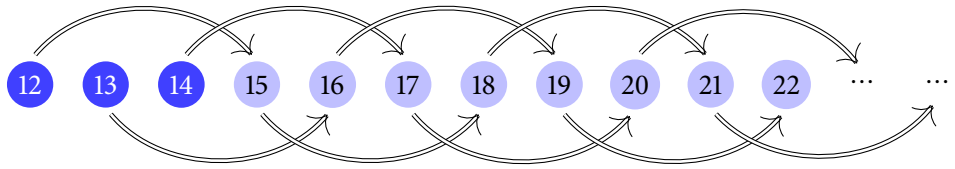
Como $12 = 4 \cdot 3$, con 4 monedas de 3 centavos juntamos 12 centavos: esto significa que vale la afirmación $P(12)$. Tenemos sin embargo un problema cuando intentamos mostrar que vale el paso inductivo: si suponemos que $k \in \mathbb{N}$ es tal que $k \geq 12$ y vale $P(k)$, entonces no hay ninguna forma de concluir que vale $P(k+1)$. En efecto, no es difícil convencerse que no es útil saber cómo juntar k centavos usando nuestras monedas si lo que queremos es juntar $k+1$.

De todas formas, podemos hacer la siguiente observación: si k es un entero positivo, entonces vale que

$$P(k-2) \implies P(k+1). \tag{21}$$

En efecto, si suponemos que la afirmación $P(k-2)$ vale, entonces existen a y b en $\mathbb{N}_0$ tales que $k-2 = 3a+7b$ y, por lo tanto, $k+1 = 3(a+1)+7b$: esto implica que vale la afirmación $P(k+1)$.

Usando que vale la implicación (21) y el hecho de que $P(12)$ vale, podemos concluir que $P(15)$, $P(18)$, $P(21)$ valen y, más generalmente, que $P(12+3c)$ vale para todo $c \in \mathbb{N}_0$, pero no que $P(16)$ vale, por ejemplo. Sin embargo, basta observar que $13 = 2 \cdot 3 + 1 \cdot 7$ y que $14 = 2 \cdot 7$ para deducir que $P(13)$ y $P(14)$ valen, y esto junto a la implicación (21) sí nos permite concluir que $P(n)$ vale para todo $n \geq 12$. El argumento puede representarse gráficamente de la siguiente manera



4.3.7. Estamos en una situación similar cuando queremos probar el siguiente resultado:

todo entero no negativo $n \in \mathbb{N}_0$ puede escribirse como suma de potencias distintas de 2.

Así, $77 = 2^0 + 2^2 + 2^3 + 2^6$, $530 = 2^1 + 2^4 + 2^9$ y 0 puede escribirse como la suma con cero sumandos y esa suma es una suma de potencias distintas de 2. Como ocurre en el ejemplo anterior, no es obvio que saber que el número $k-1$ puede escribirse como suma de potencias distintas de 2 ayude a escribir a k de esa forma. En este caso, podemos proceder de la siguiente manera.

Sea $k \in \mathbb{N}$ y elijamos $r \in \mathbb{N}_0$ de manera que 2^r sea la potencia más grande de 2 que no supera a k, es decir, tal que $2^r \leq k$. El número $k - 2^r$ es un elemento de $\mathbb{N}_0$. Supongamos por un momento que vale $P(k-2^r)$, es decir, que $k-2^r$ puede ser escrito como suma de potencias distintas de 2. Todas las potencias de dos que aparecen en esa suma son menores que 2^r: de no ser así, tendríamos que $k - 2^r \geq 2^r$ y, por lo tanto, que $k \geq 2^{r+1}$, lo que contradice la forma en que elegimos el número r. Como

$$k = (k-2^r) + 2^r$$

y sabemos ahora que podemos escribir a $k - 2^r$ como suma de potencias de 2 distintas dos a dos y distintas de 2^r, es claro que k puede ser escrito como suma de potencias de dos distintas dos a dos: vale por lo tanto $P(k)$.

Lo que esto muestra es lo siguiente: para cada $k \in \mathbb{N}$ vale que

si r es el mayor elemento de $\mathbb{N}_0$ tal que $k \geq 2^r$ y vale $P(k - 2^r)$, entonces vale $P(k)$. (22)

No es difícil convencerse que esto es suficiente para probar que $P(n)$ vale para todo $n \in \mathbb{N}_0$. Así, para ver que vale $P(22)$ observamos que la potencia más grande de 2 menor que 22 es 2^4, así que basta ver que vale $P(22 - 2^4) = P(6)$. Ahora bien, la potencia de 2 más grande que es menor que 6 es 2^2, así que es suficiente verificar que vale $P(6 - 2^2) = P(2)$: como 2 es él mismo una potencia de 2, esto es claro. Este razonamiento puede ilustrarse con el siguiente diagrama:

$$P(0) \rightsquigarrow P(2) \rightsquigarrow P(6) \rightsquigarrow P(22).$$

De manera similar, para ver que vale $P(5785)$ usando (22) hacemos las siguientes reducciones:

$$P(0) \rightsquigarrow P(1) \rightsquigarrow P(9) \rightsquigarrow P(25) \rightsquigarrow P(153) \rightsquigarrow P(665) \rightsquigarrow P(1689) \rightsquigarrow P(5785).$$

En efecto, la potencia de 2 más grande que no supera a 5785 es 2^{12} y $5785 - 2^{12} = 1689$, la potencia de 2 más grande que no supera a 1689 es 2^{10} y $1689 - 1^{10} = 665$, etc. Lo que es importante es que (22) permite reducir la verificación de que la afirmación $P(k)$ vale a la verificación de que $P(l)$ vale para algún número l que es *menor* que k y entonces iterando este proceso un cierto número finito de veces concluimos que para verificar afirmación $P(k)$ es suficiente con verificar $P(0)$.

4.3.8. En general, tenemos el siguiente resultado:

Proposición. *Sea $n_0 \in \mathbb{Z}$ y para cada entero $n \geq n_0$ sea $P(n)$ una afirmación. Si*

- *vale la afirmación $P(n_0)$ y*
- *para cada elemento k de $\mathbb{Z}$ tal que $k \geq n_0$ se tiene que*

  si valen las afirmaciones $P(n_0)$, $P(n_0 + 1)$, …, $P(k)$, entonces también vale la afirmación $P(k + 1)$,

entonces la afirmación $P(n)$ vale para todo entero $n \geq n_0$.

Demostración. Para cada entero $n \geq n_0$ sea $Q(n)$ la afirmación

las afirmaciones $P(n_0)$, $P(n_0 + 1)$, …, $P(n)$ valen.

y mostremos por inducción que $Q(n)$ vale cualquiera sea el entero $n \geq n_0$.

- En primer lugar, la afirmación $Q(n_0)$ vale simplemente porque esta afirmación coincide

con $P(n_0)$ y que esta vale es la primera de las condiciones del enunciado.

- Supongamos ahora que k es un elemento de $\mathbb{Z}$ tal que $k \geq n_0$ y que vale $Q(k)$, es decir, que las afirmaciones $P(n_0)$, $P(n_0+1)$, …, $P(k)$ valen. De acuerdo a la segunda condición del enunciado, esto implica que $P(k+1)$ vale: vemos así que si $Q(k)$ vale, entonces $P(n_0), \ldots, P(k+1)$ valen, es decir, que $Q(k+1)$ vale.

Ahora bien, es claro que si $Q(n)$ vale para todo entero n mayor o igual que n_0 en particular $P(n)$ vale para todo entero n mayor o igual que n_0, y esto es precisamente lo que queríamos probar. □

4.3.9. En la sección siguiente daremos ejemplos de uso de esta proposición. Por ahora mostremos como podemos usarla para formalizar los argumentos que hicimos en 4.3.6 y 4.3.7.

- En el primer caso, para cada $n \geq 12$ llamamos $P(n)$ a la afirmación «es posible juntar n centavos con monedas de 3 y de 7 centavos». Que $P(12)$ vale es consecuencia de que $12 = 4 \cdot 3$, así que con 4 monedas de 3 centavos tenemos 12 centavos. Para usar la Proposición 4.3.8, tenemos que probar ahora que para cada $k \in \mathbb{N}$ tal que $k \geq 12$ se tiene que

  si las afirmaciones $P(12)$, $P(13)$, …, $P(k)$ valen, entonces también vale $P(k+1)$.

  Supongamos entonces que k es un elemento de $\mathbb{N}$ tal que $k \geq 12$ y que valen las afirmaciones $P(12), \ldots, P(k)$. Se nos presentan ahora tres casos.

  - Si $k = 12$, entonces de que $13 = 2 \cdot 3 + 1 \cdot 7$ es claro que $P(k+1)$ vale.
  - Si $k = 13$, entonces de que $14 = 2 \cdot 7$ es claro que $P(k+1)$ vale.
  - Finalmente, si $k \geq 14$, entonces $k - 2 \geq 12$ y la hipótesis inductiva nos dice que $P(k-2)$ vale, así que hay elementos a y b en $\mathbb{N}_0$ tales que $k - 2 = a \cdot 3 + b \cdot 7$ y, por lo tanto $k + 1 = (a+1) \cdot 3 + b \cdot 7$: vemos así que también en este caso $P(k+1)$ vale.

  Esto prueba el enunciado de 4.3.6.

- Veamos ahora cómo usar la Proposición 4.3.8 para probar el enunciado de 4.3.7. En este caso, para cada $n \in \mathbb{N}_0$ escribimos $P(n)$ a la afirmación

  n puede escribirse como suma de potencias distintas de 2.

  Es claro que $P(0)$ vale, ya que cero es suma de cero potencias de dos. Para el paso inductivo, supongamos que k es un elemento de $\mathbb{N}_0$ y que valen $P(0), \ldots, P(k)$. Sea $r \in \mathbb{N}_0$ el mayor entero no negativo tal que $2^r \leq k+1$. Si $k+1 = 2^r$, entonces claramente $k+1$ puede escribirse como suma de potencias distintas de 2. Si en cambio $k+1 > 2^r$, entonces el número $l = k+1-2^r$ es uno de los elementos de $\{0, \ldots, k\}$ y, de acuerdo a la hipótesis, vale $P(l)$, es decir, l puede escribirse como suma de potencias distintas de 2. Más aún, todas las potencias de dos que aparecen en esa suma son menores que 2^r: si no fuese ese el caso,

tendríamos que $k+1-2^r \geq 2^r$ y por lo tanto, $k+1 \geq 2^{r+1}$, lo que es imposible en vista de la forma en que elegimos a r. Como

$$k+1 = (k+1-2^r) + 2^r$$

y ahora sabemos que $k+1-2^r$ puede escribirse como suma de potencias distintas de 2 y todas distintas de 2^r, vemos que $k+1$ puede escribirse como suma de potencias distintas de 2, es decir, que vale $P(k+1)$.

Observemos que en ambos casos no estamos usando la hipótesis inductiva completa: en el primer ejemplo, la hipótesis inductiva es que valen $P(12), \ldots, P(k)$, pero sólo usamos el hecho de que $P(k-2)$ vale, mientras que en el segundo ejemplo la hipótesis inductiva es que valen $P(0), \ldots, P(k)$ pero sólo necesitamos que $P(k+1-2^r)$ valga.

4.3.10. Llamamos a un argumento basado en la Proposición 4.3.8 una *inducción fuerte*, porque es una forma de inducción en la que la hipótesis inductiva es mas fuerte que la usual. De todas formas, es importante notar que este principio es simplemente una aplicación del principio usual que usamos antes — esto queda claro en la prueba que dimos de la Proposición 4.3.8.

§4.4. Tres pruebas por «inducción fuerte»

Potencias de dos

4.4.1. Mostremos que para cada $n \in \mathbb{N}$ vale que

$$\text{existen } r \in \mathbb{N}_0 \text{ y un entero impar } u \text{ tales que } n = 2^r u. \tag{23}$$

Sea $P(n)$, para cada $n \in \mathbb{N}$, esta última afirmación.

- Es claro que $P(1)$ vale: como $1 = 2^0 \cdot 1$, basta tomar $r = 0$ y $u = 1$ en (23).
- Sea $k \in \mathbb{N}$ y supongamos que $P(1), \ldots, P(k)$ valen. Si $k+1$ es impar, entonces podemos tomar $r = 0$ y $u = k+1$ en (23), y $P(k+1)$ vale en ese caso. Si en cambio $k+1$ es par, entonces existe $k' \in \mathbb{N}$ tal que $k+1 = 2k'$. Como $k' = (k+1)/2 < k+1$, la hipótesis inductiva implica que $P(k')$ vale, es decir, que existen $r \in \mathbb{N}_0$ y un entero impar u tales que $k' = 2^r u$. Pero entonces es $k+1 = 2k' = 2^{r+1}u$, y esto muestra que $P(k+1)$ vale también en este caso.

Usando estas dos observaciones y la Proposición 4.3.8 podemos concluir, como queremos, que $P(n)$ vale para todo $n \in \mathbb{N}$.

Números irreducibles

4.4.2. Decimos que un número $n \in \mathbb{N}$ es ***irreducible*** si no puede ser escrito en la forma $n = ab$ con a y b enteros mayores que 1. Por ejemplo, es fácil ver que 2, 3, 5 y 7 son irreducibles, pero 6 o 9 no lo son: en efecto, $6 = 2 \cdot 3$ y $9 = 3 \cdot 3$.

Queremos probar que

todo elemento de $\mathbb{N}$ *es producto de números irreducibles* (24)

usando la Proposición 4.3.8 y para ello llamaremos $P(n)$, para cada $n \in \mathbb{N}$, a la afirmación «n es igual a un producto de números irreducibles» y probaremos que $P(n)$ vale cualquiera sea $n \in \mathbb{N}$.

- La afirmación $P(1)$ vale: en efecto, 1 es igual a un producto con cero factores y — de manera tautológica — cada uno de esos factores es irreducible.
- Sea ahora k un elemento cualquiera de $\mathbb{N}$ y supongamos inductivamente que $P(1), \ldots, P(k)$ valen. El número $k+1$ puede ser o no irreducible. Si es irreducible, entonces ciertamente is igual a un producto de irreducibles — un producto con un único factor, él mismo — así que en ese caso $P(k+1)$ vale. Si, por el contrario, $k+1$ no es irreducible, entonces existen a y b en $\mathbb{N}$ tales que $k+1 = ab$ y $a, b \geq 2$. Observemos que

  $$a = \frac{ab}{b} = \frac{k+1}{b} \leq \frac{k+1}{2} < k+1$$

  y, de manera similar, que $b < k+1$. De acuerdo a la hipótesis inductiva, entonces, las afirmaciones $P(a)$ y $P(b)$ valen: esto significa que a y b son iguales a productos $p_1 \cdots p_u$ y $q_1 \cdots q_v$ de números irreducibles: se sigue de eso, claro, que

  $$k+1 = ab = p_1 \cdots p_u q_1 \cdots q_v,$$

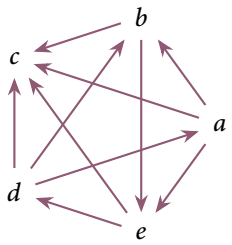
  así que también $k+1$ es igual a un producto de números irreducibles. Vemos así que la afirmación $P(k+1)$ vale.

Estos dos puntos, junto con la Proposición 4.3.8, nos permiten concluir que la afirmación (24) vale.

Caminos

4.4.3. Supongamos que en un país hay n ciudades y que entre cada par de esas ciudades hay una ruta de una sola mano. Por ejemplo, si $n = 5$ y las ciudades se llaman a, b, c, d y e, podríamos

describir las rutas usando el siguiente diagrama



Observemos que en este caso hay un camino que recorre todas las ciudades avanzando en la dirección permitida de las rutas, a saber

$$a \to b \to e \to d \to c.$$

No es el único, ya que también está el camino

$$d \to a \to b \to e \to c,$$

pero lo único que nos interesa es que hay alguno.

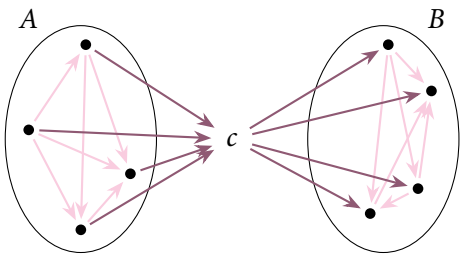
Queremos mostrar que para cada $n \in \mathbb{N}$ se tiene, de hecho, que

> *si hay n ciudades y entre cada dos de ellas hay una ruta de una sola mano, entonces hay al menos un camino que las recorre todas.*

Sea $P(n)$ esta afirmación y procedamos por inducción en n.

- La afirmación $P(1)$ vale: si hay una sola ciudad, entonces hay un camino que recorre todas las ciudades, que consiste en empezar en esa ciudad y no moverse.
- Sea ahora $k \in \mathbb{N}$ y supongamos que todas las afirmaciones $P(1), \ldots, P(k)$ valen. Supongamos además que tenemos $k+1$ ciudades conectadas dos a dos con rutas de una sola mano y llamemos c a una de esas ciudades.

  Sea A al conjunto de ciudades a tales que la ruta que une a y c va desde a a c, y B al conjunto de ciudades b tales que la ruta que une b y c va desde c hasta b. Podemos representar esquemáticamente esta situación de la siguiente manera:



Como cada par de ciudades está conectado por una ruta, es claro que $A \cup B \cup \{c\}$ es el conjunto de todas las ciudades; por otro lado, los conjuntos A, B y $\{c\}$ son disjuntos dos a dos. En otras palabras, el conjunto $\{A, B, \{c\}\}$ es una partición del conjunto de nuestras $k+1$ ciudades.

Supongamos ahora por un momento que tanto A como B son conjuntos no vacíos. Si r es el número de elementos de A, entonces claramente $1 \leq r \leq k$ y, de acuerdo a nuestro hipótesis inductiva, la afirmación $P(r)$ vale: esto significa que hay un camino — llamémoslo α — que recorre todas las ciudades de A. De manera similar, si s es el número de elementos de B, entonces $1 \leq s \leq k$ y la hipótesis inductiva nos dice que hay un camino — que podemos llamar β — que recorre todas las ciudades de B. Pero entonces hay un camino que recorre todas las ciudades: consiste en

- seguir primero el camino α,
- tomar luego la ruta que va desde la última ciudad visitada por α hasta la ciudad c (notemos que esto es posible precisamente porque esa última ciudad visitada por α está en el conjunto A y, por lo tanto, la ruta que la une con c va en dirección de c),
- continuar por la ruta que va desde c hasta la primera ciudad visitada por el camino β (y esto es posible porque esta ciudad está en B) y,
- finalmente, recorrer el camino β.

Si alguno de los conjuntos A o B es vacío, podemos hacer algo parecido. Supongamos, por ejemplo, que A es vacío. En este caso, B tiene exactamente k elementos y la hipótesis inductiva nos dice que hay un camino β que recorre esas ciudades. Un camino que recorre todas las ciudades consiste entonces en empezar en c, tomar la ruta que va desde c hasta el la primera ciudad visitada por ese camino β, y luego recorrer el camino β. Por supuesto, si B es vacío podemos proceder de manera similar.

Esto completa la inducción: gracias a la Proposición **4.3.8** podemos concluir que $P(n)$ vale cualquiera sea $n \in \mathbb{N}$.

§4.5. Ejercicios

4.5.1. Ejercicio. Pruebe las siguientes afirmaciones por inducción con respecto a n.

(*a*) $\displaystyle\sum_{i=1} i(i+1) = \frac{n(n+1)(n+2)}{2}$ para cada $n \geq 1$.

(*b*) $\displaystyle\sum_{i=2}^{n} \frac{1}{i^2-1} = \frac{(n-1)(3n+2)}{4n(n+1)}$ para cada $n \geq 2$.

(*c*) $\displaystyle\sum_{i=n}^{2n-1} (2i+1) = n^2$ para cada $n \geq 1$.

(*d*) $\displaystyle\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$ para cada $n \geq 1$.

(*e*) $\sqrt{n} \leq \displaystyle\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n} - 1$ para cada $n \geq 1$.

4.5.2. Ejercicio. Pruebe que para todo entero positivo n vales las siguientes igualdades:

(*a*) $1^0 + 2^0 + \cdots + n^0 = n$.

(*b*) $1^1 + 2^1 + \cdots + n^1 = \frac{1}{2}n(n+1)$.

(*c*) $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

(*d*) $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$.

(*e*) $1^4 + 2^4 + \cdots + n^4 = \frac{1}{30}n(n+1)(2n+1)\left(3n^2+3n-1\right)$.

(*f*) $1^5 + 2^5 + \cdots + n^5 = \frac{1}{12}n^2(n+1)^2\left(2n^2+2n-1\right)$.

(*g*) $1^6 + 2^6 + \cdots + n^6 = \frac{1}{42}n(n+1)(2n+1)\left(3n^4+6n^3-3n+1\right)$.

(*h*) $1^7 + 2^7 + \cdots + n^7 = \frac{1}{24}n^2(n+1)^2\left(3n^4+6n^3-n^2-4n+2\right)$.

(*i*) $1^8 + 2^8 + \cdots + n^8 = \frac{1}{90}n(n+1)(2n+1)\left(5n^6+15n^5+5n^4-15n^3-n^2+9n-3\right)$.

(*j*) $1^9 + 2^9 + \cdots + n^9 = \frac{1}{20}n^2(n+1)^2\left(n^2+n-1\right)\left(2n^4+4n^3-n^2-3n+3\right)$.

(*k*) $1^{10}+2^{10}+\cdots+n^{10} = \frac{1}{66}n(n+1)(2n+1)\left(n^2+n-1\right)\left(3n^6+9n^5+2n^4-11n^3+3n^2+10n-5\right)$.

Estas identidades son llamadas *fórmulas de Faulhaber*, por Johann Faulhaber, que encontró la fórmula para la suma de las potencias k-ésimas de los primeros n números naturales para cada k de 1 hasta 17 — esos resultados fueron publicados en 1631. Una fórmula valida para todo entero positivo k fue encontrada por Jacob Bernoulli en 1713, que publicó el resultado en un célebre trabajo llamado *Summae Potestatum*. En la página 125 puede verse una reproducción de la página del *Ars Conjectandi*, el libro póstimo de Bernoulli donde se incluyen estos resultados.

La primera prueba completa de que la fórmula dada por Bernoulli es correcta, sin embargo, fue dada recién en 1834 — ¡más de un siglo después! — por Carl Gustav Jacob Jacobi en [Jac1834]. La dificultad en hacer esto está en lograr describir los coeficientes de los polynomios de Faulhaber: la respuesta final es en términos de la sucesión de los llamados ***números de Bernoulli***,

$$-\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, 0, -\frac{1}{30}, 0, \frac{5}{66}, 0, -\frac{691}{2730}, 0, \frac{7}{6}, 0, -\frac{3617}{510}, 0, \frac{43867}{798}, 0, -\frac{174611}{330}, \dots$$

Una discusión de la historia de este problema puede encontrarse en el artículo [Knu1993] de Donald Knuth.

4.5.3. Ejercicio. Muestre que

(*a*) $2^n > n$ si $n \geq 1$;

(*b*) $2^n \geq n^2$ si $n \geq 4$;

(*c*) $n! > 2^n$ si $n \geq 4$;

(*d*) $(1-x)^n \geq 1 - nx$ si $n \geq 0$ y $x \in (0,1)$;

(*e*) $(1+x)^n \geq 1 + nx$ si $n \geq 0$ y $x > 0$.

4.5.4. Ejercicio. Pruebe por inducción los siguientes enunciados:

(*a*) El producto de n números enteros impares es impar.

(*b*) Si $n \in \mathbb{N}$ $x_1, \dots, x_n$ son números reales, entonces

$$\left|\sin\left(\sum_{i=1}^{n} x_i\right)\right| \leq \sum_{i=1}^{n} |\sin x_i|.$$

(*c*) Si $n \in \mathbb{N}$ y $x \in \mathbb{R}$ es tal que $\sin \frac{1}{2}x \neq 0$, entonces

$$\sum_{i=1}^{n} \sin nx = \frac{\sin \frac{1}{2}(n+1)x \cdot \sin \frac{1}{2}nx}{\sin \frac{1}{2}x}$$

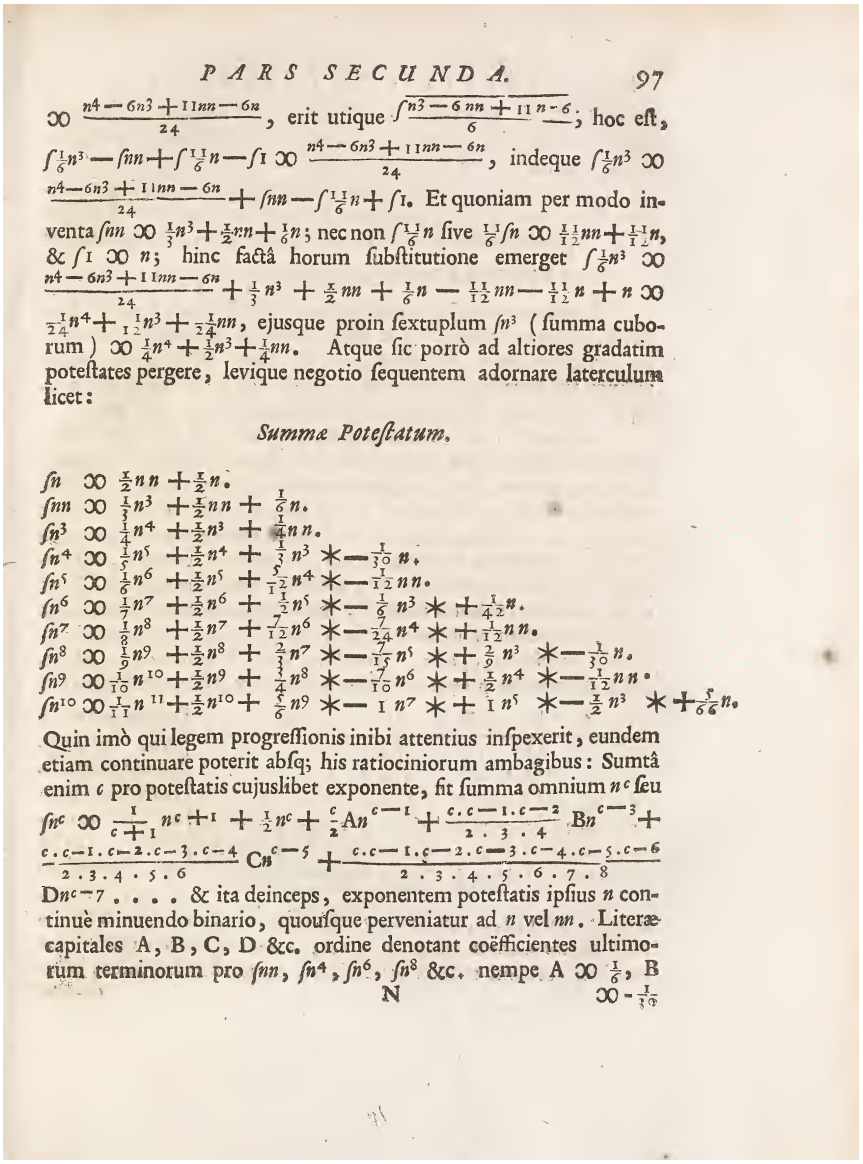
y

$$\frac{1}{2} + \sum_{i=1}^{n} \cos nx = \frac{\sin(n+1\frac{1}{2})x}{2\sin \frac{1}{2}x}.$$

(*d*) Si $n \in \mathbb{N}$ y $x \in \mathbb{R}$ es tal que $\sin x \neq 0$, entonces

$$\prod_{i=1}^{n} \cos 2^i x = \frac{\sin 2^{n+1}x}{2^n \sin x}.$$

4.5.5. Ejercicio. Muestre que para cada entero $n \geq 0$ se tiene que $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$. Usando



PARS SECUNDA. 97

$\infty \frac{n^4 - 6n^3 + 11nn - 6n}{24}$, erit utique $\int \frac{n^3 - 6nn + 11n - 6}{6}$; hoc est, $\int \frac{1}{6}n^3 - \int nn + \int \frac{11}{6}n - \int 1 \infty \frac{n^4 - 6n^3 + 11nn - 6n}{24}$, indeque $\int \frac{1}{6}n^3 \infty \frac{n^4 - 6n^3 + 11nn - 6n}{24} + \int nn - \int \frac{11}{6}n + \int 1$. Et quoniam per modo inventa $\int nn \infty \frac{1}{3}n^3 + \frac{1}{2}nn + \frac{1}{6}n$; nec non $\int \frac{11}{6}n$ sive $\frac{11}{6}\int n \infty \frac{11}{12}nn + \frac{11}{12}n$, & $\int 1 \infty n$; hinc factâ horum substitutione emerget $\int \frac{1}{6}n^3 \infty \frac{n^4 - 6n^3 + 11nn - 6n}{24} + \frac{1}{3}n^3 + \frac{1}{2}nn + \frac{1}{6}n - \frac{11}{12}nn - \frac{11}{12}n + n \infty \frac{1}{24}n^4 + \frac{1}{12}n^3 + \frac{1}{24}nn$, ejusque proin sextuplum $\int n^3$ (summa cuborum) $\infty \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}nn$. Atque sic porrò ad altiores gradatim potestates pergere, levique negotio sequentem adornare laterculum licet:

Summæ Potestatum.

$\int n \infty \frac{1}{2}nn + \frac{1}{2}n.$
$\int nn \infty \frac{1}{3}n^3 + \frac{1}{2}nn + \frac{1}{6}n.$
$\int n^3 \infty \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}nn.$
$\int n^4 \infty \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 * - \frac{1}{30}n.$
$\int n^5 \infty \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 * - \frac{1}{12}nn.$
$\int n^6 \infty \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 * - \frac{1}{6}n^3 * + \frac{1}{42}n.$
$\int n^7 \infty \frac{1}{8}n^8 + \frac{1}{2}n^7 + \frac{7}{12}n^6 * - \frac{7}{24}n^4 * + \frac{1}{12}nn.$
$\int n^8 \infty \frac{1}{9}n^9 + \frac{1}{2}n^8 + \frac{2}{3}n^7 * - \frac{7}{15}n^5 * + \frac{2}{9}n^3 * - \frac{1}{30}n.$
$\int n^9 \infty \frac{1}{10}n^{10} + \frac{1}{2}n^9 + \frac{3}{4}n^8 * - \frac{7}{10}n^6 * + \frac{1}{2}n^4 * - \frac{1}{12}nn.$
$\int n^{10} \infty \frac{1}{11}n^{11} + \frac{1}{2}n^{10} + \frac{5}{6}n^9 * - 1\,n^7 * + 1\,n^5 * - \frac{1}{2}n^3 * + \frac{5}{66}n.$

Quin imò qui legem progressionis inibi attentius inspexerit, eundem etiam continuare poterit absq; his ratiociniorum ambagibus: Sumtâ enim c pro potestatis cujuslibet exponente, fit summa omnium n^c seu $\int n^c \infty \frac{1}{c+1}n^{c+1} + \frac{1}{2}n^c + \frac{c}{2}An^{c-1} + \frac{c.c-1.c-2}{2.3.4}Bn^{c-3} + \frac{c.c-1.c-2.c-3.c-4}{2.3.4.5.6}Cn^{c-5} + \frac{c.c-1.c-2.c-3.c-4.c-5.c-6}{2.3.4.5.6.7.8}Dn^{c-7} \ldots$ & ita deinceps, exponentem potestatis ipsius n continuè minuendo binario, quousque perveniatur ad n vel nn. Literæ capitales A, B, C, D &c. ordine denotant coëfficientes ultimorum terminorum pro $\int nn$, $\int n^4$, $\int n^6$, $\int n^8$ &c. nempe $A \infty \frac{1}{6}$, $B \infty -\frac{1}{30}$

Figura 4.1. La página del *Ars Conjectandi* de Jacob Bernoulli en la que tabula las primeras fórmulas de Faulhaber.

eso, pruebe que todo entero positivo $m \in \mathbb{N}$ puede escribirse en la forma

$$m = d_1 \cdot 1! + d_2 \cdot 2! + \cdots + d_r \cdot r!$$

para algún $r \in \mathbb{N}$ y con $d_i \in \{0, \ldots, i\}$ para cada $i \in \{1, \ldots, r\}$.

4.5.6. Ejercicio.

(*a*) Todo entero positivo puede escribirse en la forma $3a + 5b$ con a y b enteros.

(*b*) Si $n \in \mathbb{N}$, entonces el número $3^{3n} + 5^{4n+2}$ es divisible por 13.

Capítulo 5

Recursión

§5.1. Sucesiones

5.1.1. Si A es un conjunto, una ***sucesión*** de elementos de A es una función $f : \mathbb{N} \to A$. Casi siempre que tenemos una tal sucesión y un número $n \in \mathbb{N}$, preferimos escribir f_n en lugar de $f(n)$ y llamamos a f_n la ***n-ésima componente*** de la sucesión en lugar de «el valor de f en n». Más aún, solemos escribir a una sucesión en la forma

$$(f_n)_{n\geq 1}$$

o, más explícitamente, listando las primeras de sus componentes

$$f_1, f_2, f_3, f_4, \ldots$$

Por ejemplo, la función $f : \mathbb{N} \to \mathbb{R}$ tal que $f(n) = 2^n$ para todo $n \in \mathbb{N}$ es una sucesión de números reales puede ser escrita en la forma

$$(2^n)_{n\geq 1}$$

o en la forma

$$2, 4, 8, 16, 32, \ldots \tag{1}$$

Es importante observar que esta última notación es solamente indicativa y no determina completamente a la sucesión. Así, la sucesión $g : \mathbb{N} \to \mathbb{R}$ tal que

$$g_n = \tfrac{1}{12}(x^4 - 6x^3 + 23x^2 - 18x + 24)$$

para cada $n \in \mathbb{N}$ tiene las mismas primeras cinco componentes que f y podríamos escribirla también en la forma (1). Para evitar ambigüedades, incluimos frecuentemente en la lista de las primeras componentes de una sucesión la expresión de tu componente general: escribimos, por ejemplo,

$$2, 4, 8, 16, 32, \ldots, 2^n, \ldots$$

y

$$2, 4, 8, 16, 32, \ldots, \tfrac{1}{12}(x^4 - 6x^3 + 23x^2 - 18x + 24), \ldots$$

para referirnos a f y a g, respectivamente.

5.1.2. Una pequeña variación de la definición de sucesión que acabamos de dar es la siguiente. Si $n_0 \in \mathbb{Z}$ y A es un conjunto, una ***sucesión de elementos de A que empieza en n_0*** es una función $f : \{n \in \mathbb{Z} : n \geq n_0\} \to A$. Escribimos a una tal sucesión en la forma

$$(f_n)_{n \geq n_0}$$

o listando sus componentes empezando por la n_0-ésima,

$$f_{n_0}, f_{n_0+1}, f_{n_0+2}, \ldots$$

Por ejemplo, la función $f : \mathbb{N}_0 \to \mathbb{Z}$ tal que $f(n) = 2^n$ es una sucesión de enteros

$$1, 2, 3, 4, \ldots, 2^n, \ldots$$

que empieza en la componente 0-ésima y la sucesión

$$\frac{1}{24}, \frac{1}{120}, \frac{1}{360}, \frac{1}{840}, \frac{1}{1680}, \ldots, \frac{1}{n(n-1)(n-2)(n-3)}, \ldots$$

empieza en su componente con índice 4.

§5.2. Definiciones por recursión

5.2.1. Muchas sucesiones se dan de manera explícita, como dimos los todos los ejemplos de sucesiones de la sección anterior, exhibiendo una *fórmula* que determine los valores de cada una de sus componentes. También es posible dar una sucesión de manera ***implícita*** o ***recursiva***. Veamos un ejemplo de qué significa esto: afirmamos que hay exactamente una sucesión $(a_n)_{n \geq 0}$ que empieza en su componente 0-ésima, que tiene

$$a_0 = 1 \tag{2}$$

y tal que para cada $n \geq 1$ vale que

$$a_n = n \cdot a_{n-1}. \tag{3}$$

Observemos que no estamos diciendo con esto *cuál* es el valor de cada componente a_n de la sucesión, sino que estamos dando un *procedimiento* o *algoritmo* que permite calcular esas componentes:

- Así, es claro que la 0-ésima componente de la sucesión es $a_0 = 1$, porque eso es precisamente uno de los dos datos que tenemos sobre ella.
- De la componente a_1 sabemos, gracias a (3), que es igual a $1 \cdot a_0$. Como sabemos ya cuál es el valor de a_0, esto nos permite determinar de manera unívoca el valor de a_1: en efecto, es $a_1 = 1 \cdot a_0 = 1 \cdot 1 = 1$.
- Podemos seguir de esta forma: de la componente a_2 de la sucesión sabemos que es igual a $2 \cdot a_1$ y como la componente a_1 está bien determinada por los datos que tenemos y vale 1, tenemos que $a_2 = 2 \cdot a_1 = 2 \cdot 1 = 2$.
- Por supuesto, de manera similar vemos que $a_3 = 3 \cdot a_2 = 3 \cdot 2 = 6$, que $a_4 = 4 \cdot a_3 = 4 \cdot 6 = 24$, etc.

Vemos así que los datos que tenemos sobre la sucesión implican que las primeras componentes de la sucesión son, necesariamente,

$$1, 1, 2, 6, 24, 120, \ldots$$

Más aún, debería ser intuitivamente claro que con este procedimiento podemos determinar de manera unívoca a partir de las ecuaciones (2) y (3) con las que empezamos *cualquier* componente de la sucesión: es por eso que hay exactamente una sucesión $(a_n)_{n\geq 0}$ que satisface esas dos ecuaciones.

5.2.2. Veamos otro ejemplo de una sucesión definida recursivamente. Afirmamos que hay exactamente una sucesión de números $(C_n)_{n\geq 0}$ tal que

$$C_0 = 1 \tag{4}$$

y, para cada entero $n \geq 1$,

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1}. \tag{5}$$

En efecto, claramente toda sucesión que satisfaga esas dos condiciones tiene necesariamente

$$C_0 = 1, \qquad C_1 = \frac{2(2\cdot 1-1)}{1+1} C_0 = 1, \qquad C_2 = \frac{2(2\cdot 2-1)}{2+1} C_1 = 2,$$
$$C_3 = \frac{2(2\cdot 3-1)}{3+1} C_2 = 5, \qquad C_4 = \frac{2(2\cdot 4-1)}{4+1} C_3 = 14, \qquad \text{etc.}$$

Es fácil ver de esta manera que las primeras componentes de una sucesión que cumple (4) y (5) necesariamente son

n	0	1	2	3	4	5	6	7	8	9	10	11
C_n	1	1	2	5	14	42	132	429	1 430	4 862	16 796	58 786

Estos números se llaman ***números de Catalan***, por Eugène Charles Catalan, y aparecen en los más variados contextos. Hay libros enteros dedicados a estudiar esta sucesión de números, como los libros [Sta2015] y [Kos2009] de Richard Stanley y de Thomas Koshy.

5.2.3. La forma general de las definiciones recursivas de sucesiones del tipo de los dos ejemplos que acabamos de ver es la siguiente. Empezamos con un conjunto A, un elemento $\alpha \in A$ y una función $f : \mathbb{N}_0 \times A \to A$, y consideramos la sucesión $(a_n)_{n\geq 0}$ tal que

$$a_0 = \alpha \tag{6}$$

y

$$a_n = f(n, a_{n-1}) \tag{7}$$

para cada entero positivo n. Así,

- para obtener el ejemplo de la sucesión de 5.2.1, podemos tomar $A \coloneqq \mathbb{Z}$, $\alpha \coloneqq 1$ y $f : \mathbb{N}_0 \times \mathbb{Z} \to \mathbb{Z}$ a la función tal que $f(n, x) = n \cdot x$ para cada $n \in \mathbb{N}_0$ y $x \in \mathbb{Z}$, mientras que
- en el ejemplo de 5.2.2 de los números de Catalan se obtiene eligiendo $A \coloneqq \mathbb{Q}$, $\alpha \coloneqq 1$ y como $f : \mathbb{N}_0 \times \mathbb{Q} \to \mathbb{Q}$ a la función que para cada $n \in \mathbb{N}_0$ y $x \in \mathbb{Q}$ tiene

$$f(n, x) = \frac{2(2n-1)}{n+1} x.$$

Aunque es intuitivamente claro, es sin embargo necesario verificar que una vez que A, α y f están fijos existe efectivamente una sucesión que satisface las condiciones (6) y (7) y que, más aún, existe una sola: esto es lo que justifica usar esas dos ecuaciones para definir la sucesión $(a_n)_{n\geq 0}$. De esto se ocupan las siguientes dos proposiciones.

5.2.4. Empecemos por la unicidad, que es la parte más sencilla:

Proposición. *Sea A un conjunto, sea α un elemento de A y sea $f : \mathbb{N}_0 \times A \to A$ una función. Existe a lo sumo una sucesión $(a_n)_{n\geq 0}$ de elementos de A tal que*

$$a_0 = \alpha, \qquad a_n = f(n, a_{n-1})$$

para cada $n \in \mathbb{N}$.

Demostración. Supongamos que $(a_n)_{n\geq 0}$ y $(b_n)_{n\geq 0}$ son dos sucesiones de elementos de A tales que

$$a_0 = \alpha, \qquad b_0 = \alpha \tag{8}$$

y que para cada $n \in \mathbb{N}$ se tiene que

$$a_n = f(n, a_{n-1}), \qquad b_n = f(n, b_{n-1}). \tag{9}$$

Tenemos que mostrar que en estas condiciones las sucesiones $(a_n)_{n\geq 0}$ y $(b_n)_{n\geq 0}$ son iguales: es decir, que para todo $n \in \mathbb{N}_0$ se tiene que $a_n = b_n$. Para ello, para cada $n \in \mathbb{N}_0$ llamemos $P(n)$ a la afirmación «$a_n = b_n$» y probemos que $P(n)$ vale para todo $n \in \mathbb{N}_0$ procediendo por inducción.

- Que $P(0)$ vale es consecuencia inmediata de las igualdades de (8).
- Supongamos que k es un elemento de $\mathbb{N}_0$ y que $P(k)$ vale, de manera que $a_k = b_k$. En ese caso, tenemos que

$$\begin{aligned} a_{k+1} &= f(k+1, a_k) && \text{porque vale la primera igualdad de (9)} \\ &= f(k+1, b_k) && \text{por la hipótesis inductiva} \\ &= b_{k+1} && \text{porque vale la segunda igualdad de (9).} \end{aligned}$$

  Vemos así que vale la afirmación $P(k+1)$

Esto completa la inducción y, por lo tanto, la prueba de la proposición. □

5.2.5. Nuestro siguiente resultado se ocupa de la cuestión de la existencia.

Proposición. *Sea A un conjunto, sea α un elemento de A y sea $f : \mathbb{N}_0 \times A \to A$ una función. Existe una sucesión $(a_n)_{n\geq 0}$ de elementos de A tal que*

$$a_0 = \alpha, \qquad a_n = f(n, a_{n-1})$$

para cada $n \in \mathbb{N}$.

Daremos dos demostraciones de esta proposición, basadas en ideas bastante diferentes. Las dos son de naturaleza técnica — se trata, por lejos, de los argumentos más difíciles que presentaremos en estas notas — así que el lector puede saltárselas sin mucha pérdida.

Primera demostración. Organizamos esta demostración en tres pasos.

Primer paso. Para cada $n \in \mathbb{N}_0$ sea $P(n)$ la afirmación

$$\begin{aligned}&\textit{existe una única función función } h_n : \{0, \dots, n\} \to A \textit{ tal que } h_n(0) = \alpha \textit{ y} \\ &h_n(i) = f(i, h_n(i-1)) \textit{ para cada } i \in \{1, \dots, n\}.\end{aligned} \tag{10}$$

Nuestro primer objetivo es probar por inducción en n que esta afirmación vale cualquiera sea el elemento n de $\mathbb{N}_0$.

- Hay una función $h_0 : \{0\} \to A$ tal que $h_0(0) = \alpha$. Esta función satisface las condiciones y claramente es la única función $\{0\} \to A$ que las satisface: esto significa que vale la afirmación $P(0)$.
- Sea $k \in \mathbb{N}_0$ y supongamos que vale la afirmación $P(k)$, de manera que existe una única función $h_k : \{0, \dots, k\} \to A$ tal que

  $$h_k(0) = \alpha$$

  y

  $$h_k(i) = f(i, h_k(i-1)) \text{ para cada } i \in \{1, \dots, k\}.$$

  Definimos una función $g : \{0, \dots, k+1\} \to A$ de la siguiente manera: si $i \in \{0, \dots, k+1\}$, ponemos

  $$g(i) \coloneqq \begin{cases} h_k(i), & \text{si } 0 \le i \le k; \\ f(k+1, h_k(k)), & \text{si } i = k+1. \end{cases} \tag{11}$$

  Afirmamos que g satisface las condiciones de que

  $$g(0) = \alpha \tag{12}$$

  y

  $$g(i) = f(i, g(i-1)) \text{ para cada } i \in \{1, \dots, k+1\}. \tag{13}$$

  Que la primera se cumple es evidente, ya que $g(0) = h_k(0) = \alpha$. Por otro lado, si i es un elemento de $\{1, \dots, k+1\}$, entonces hay dos casos: o bien $i \le k$, y entonces

  $$g(i) = h_k(i) = f(i, h_k(i-1)) = f(i, g(i-1)),$$

  o bien $i = k+1$, y en ese caso

  $$g(i) = g(k+1) = f(k+1, h_k(k)) = f(k+1, g(k)) = f(i, g(i-1))$$

  por la forma en que definimos a g.

  Veamos ahora que la función $g : \{0, \dots, k+1\} \to A$ que definimos en (11) es, de hecho, la *única* función $\{0, \dots, k+1\} \to A$ que satisface las condiciones (12) y (13). Para

verlo, supongamos que $g' : \{0, \dots, k+1\} \to A$ es otra función con $g'(0) = \alpha$ y tal que $g'(i) = f(i, g'(i-1))$ para cada $i \in \{1, \dots, k+1\}$, y mostremos que, de hecho, g y g' son la misma función. Si no lo son, entonces el conjunto

$$X \coloneqq \{i \in \{0, \dots, k+1\} : g(i) \neq g'(i)\}$$

es no vacío y tiene, por lo tanto, un menor elemento $j \coloneqq \min X$. No puede ser que j sea igual a 0, ya que $g(0) = \alpha = g'(0)$, así que j es un elemento positivo de $\{0, \dots, k+1\}$. Se sigue de eso que $j-1$ es un elemento de $\{0, \dots, k+1\}$ que *no* pertenece al conjunto X, es decir, tal que $g(j-1) = g'(j-1)$: pero esto es absurdo, porque en ese caso tenemos que

$$g(j) = f(j, g(j-1)) = f(j, g'(j-1)) = g'(j),$$

contradiciendo el hecho de que j pertenece a X.

Hemos probado que la función g que definimos en (11) satisface las condiciones (12) y (13), y que es la única que las satisface: esto significa que podemos poner $h_{k+1} \coloneqq g$ para concluir que la afirmación $P(k+1)$ se cumple.

Esto completa la inducción y, por lo tanto, la prueba de que la afirmación $P(n)$ de (10) vale cualquiera sea para todo $n \in \mathbb{N}$.

Segundo paso. El segundo paso de la demostración consiste en mostrar que

$$\text{*si } n \in \mathbb{N}_0\text{, entonces la restricción de la función } h_{n+1} \text{ al conjunto } \{0, \dots, n\} \text{ es } h_{n+1}|_{\{0,\dots,n\}} = h_n \text{ y, en particular, se tiene que } h_{n+1}(n) = h_n(n).* \tag{14}$$

Antes de eso, observemos que esta afirmación tiene sentido: el conjunto $\{0, \dots, n\}$ está contenido en el dominio de la función h_{n+1} y podemos entonces considerar la restricción $h_{n+1}|_{\{0,\dots,n\}}$, y esa restricción tiene el mismo dominio y codominio que h_n.

Para verificar (14), fijemos $n \in \mathbb{N}_0$ y llamemos q a la restricción $h_{n+1}|_{\{0,\dots,n\}}$, que es una función $\{0, \dots, n\} \to A$. Se tiene que

$$q(0) = h_{n+1}(0) = \alpha.$$

Por otro lado, si $k \in \{1, \dots, n\}$, entonces

$$q(k) = h_{n+1}(k) = f(k, h_{n+1}(k-1)) = f(k, q(k-1)).$$

Esto significa que q tiene las mismas propiedades que, de acuerdo a la afirmación $P(n)$, caracterizan unívocamente a la función h_n: se sigue de eso, entonces, que $q = h_n$, como queremos.

Tercer paso. Estamos por fin en condiciones de definir una sucesión $(a_n)_{n \geq 0}$ en A poniendo, para cada $n \in \mathbb{N}_0$,

$$a_n \coloneqq h_n(n).$$

Esto tiene sentido precisamente porque a esta altura tenemos determinada para cada $n \in \mathbb{N}_0$ una función h_n que tiene al número n en su dominio. Para concluir la prueba de la proposición es suficiente que mostremos que la sucesión $(a_n)_{n\geq 0}$ satisface las condiciones del enunciado. Procedemos, como siempre, por inducción.

Observemos primero que claramente $a_0 = h_0(0) = \alpha$, porque h_0 hace que valga la afirmación $P(0)$. Por otro lado, supongamos que $k \in \mathbb{N}_0$ es tal que vale que $a_k = f(k, a_{k-1})$ y observemos que entonces

$$\begin{aligned} a_{k+1} &= h_{k+1}(k+1) \\ &= f(k+1, h_{k+1}(k)) && \text{porque vale } P(k+1) \\ &= f(k+1, h_k(k)) && \text{gracias a (14)} \\ &= f(k+1, a_k). \end{aligned}$$

De acuerdo al principio de inducción, entonces, la sucesión a satisface las condiciones del enunciado. Esto completa la prueba de la proposición. □

Segunda demostración de la Proposición 5.2.5. Digamos que un subconjunto F de $\mathbb{N}_0 \times A$ es *bueno* si $(0, \alpha) \in F$ y cada todo elemento (n, a) de $\mathbb{N}_0$ vale que

$$(n, a) \in F) \implies (n+1, f(n+1, a)) \in F.$$

Hay subconjuntos buenos de $\mathbb{N}_0 \times A$, ya que $\mathbb{N}_0 \times A$ mismo es uno de ellos, así que podemos considerar la intersección de todos ellos: escribámosla $\mathscr{F}$. Mostremos que $\mathscr{F}$ es un subconjunto bueno de $\mathbb{N}_0 \times A$.

- El par $(0, \alpha)$ pertenece a cada subconjunto bueno de $\mathbb{N}_0 \times A$, así que pertenece a la intersección de todos los subconjuntos buenos de $\mathbb{N}_0 \times A$, es decir, a $\mathscr{F}$.
- Supongamos, por otro lado, que (n, a) es un elemento de $\mathscr{F}$. Si F es un subconjunto bueno de $\mathbb{N}_0 \times A$, entonces F contiene a $\mathscr{F}$ y, por lo tanto, tenemos que $(n, a) \in F$: como F es bueno, esto nos dice que también $(n+1, f(n+1, a)) \in F$. Vemos así que el par $(n+1, f(n+1, a))$ pertenece a cada subconjunto bueno de $\mathbb{N}_0 \times A$, así que también pertenece a la intersección $\mathscr{F}$ de todos ellos.

Más aún, el conjunto $\mathscr{F}$ tiene la siguiente propiedad:

ningún subconjunto propio *de $\mathscr{F}$ es bueno.* (15)

En efecto, si por el contrario hubiera un subconjunto propio F de $\mathscr{F}$ que es bueno, tendríamos al mismo tiempo que $\mathscr{F} \subseteq F$, ya que $\mathscr{F}$ está contenido en todo subconjunto bueno de $\mathbb{N}_0 \times A$, y que $F \subsetneq \mathscr{F}$, lo que es absurdo.

El conjunto $\mathscr{F}$ es un subconjunto de $\mathbb{N}_0 \times A$ y, por lo tanto, es una relación de $\mathbb{N}_0$ a A. Queremos probar que se trata, de hecho, de una *función* de $\mathbb{N}_0$ a A. Lo primero que tenemos que probar para ello es que para todo $n \in \mathbb{N}_0$ existe $a \in A$ tal que $(n, a) \in \mathscr{F}$ o, equivalentemente, que el conjunto

$$S \coloneqq \{m \in \mathbb{N}_0 : \text{existe } a \in A \text{ tal que } (n, a) \in \mathscr{F}\}$$

coincide con $\mathbb{N}_0$. Es suficiente para ello que probemos que este conjunto S es inductivo.

- Como $\mathscr{F}$ es un subconjunto bueno de $\mathbb{N}_0 \times A$ sabemos que el par $(0, \alpha)$ pertenece a $\mathscr{F}$ y, por lo tanto, que 0 pertenece al conjunto S.
- Sea ahora k un elemento de $\mathbb{N}_0$ tal que $k \in S$, de manera que hay un elemento a en A tal que $(k, a) \in \mathscr{F}$. Como $\mathscr{F}$ es un subconjunto bueno de $\mathbb{N}_0 \times A$, esto implica que el par $(k+1, f(k+1, a))$ pertenece también a $\mathscr{F}$ y, en consecuencia, que $k+1$ es un elemento de S.

La segunda verificación que tenemos que hacer para establecer que $\mathscr{F}$ es una función de $\mathbb{N}_0$ a A es la de que vale

si $m \in \mathbb{N}_0$ y $y, y' \in A$ son tales que (m, y) y (m, y') pertenecen a $\mathscr{F}$, entonces $y = y'$.

Para ello consideraremos el conjunto

$$T \coloneqq \{m \in \mathbb{N}_0 : \text{siempre que } y, y' \in A \text{ son tales que } (m, y) \text{ y } (m, y') \in \mathscr{F} \text{ es } y = y'\}$$

y mostraremos que coincide con $\mathbb{N}$ probando que es inductivo.

- Primero veamos que 0 pertenece a T. Supongamos que y e y' son dos elementos de A tales que los pares $(0, y)$ y $(0, y')$ están en $\mathscr{F}$ y, para llegar a un absurdo, que $y \neq y'$. Claramente al menos uno de y e y' tiene que ser distinto de α, y sin pérdida de generalidad podemos suponer que es $y' \neq \alpha$.

  Consideremos el conjunto $F \coloneqq \mathscr{F} \setminus \{(0, y')\}$, que es un subconjunto propio de $\mathscr{F}$. Mostraremos que F es un subconjunto bueno de $\mathbb{N}_0 \times A$, y esto es imposible en vista de (15): esta contradicción proviene de haber supuesto que y e y' son distintos, así que deben ser iguales y, por lo tanto, 0 pertenece al conjunto T.

  Como $(0, \alpha)$ está en $\mathscr{F}$ y $(0, \alpha) \neq (0, y')$ porque $\alpha \neq y'$, es claro que $(0, \alpha)$ está en F. Por otro lado, si (n, a) es un elemento cualquiera de F, entonces también es un elemento de $\mathscr{F}$ y, como $\mathscr{F}$ es un conjunto bueno, tenemos que $(n+1, f(n+1, a)) \in \mathscr{F}$: como $n+1 \neq 0$, claramente es $(n+1, f(n+1, a)) \in \mathscr{F} \setminus \{(0, y')\} = F$. Esto prueba que F es un subconjunto bueno, como dijimos.
- Supongamos ahora que m es un elemento de T y mostremos que $m+1$ también lo es. Sean y e y' dos elementos de A tales que los pares $(m+1, y)$ y $(m+1, y')$ pertenecen a $\mathscr{F}$ y para

llegar a una contradicción supongamos que estos dos elementos y e y' son distintos. Por lo que ya probamos, sabemos que hay un elemento z de A tal que $(m, z) \in \mathscr{F}$ y esto implica, ya que $\mathscr{F}$ es un subconjunto bueno de $\mathbb{N}_0 \times A$, que $(m+1, f(m+1, z))$ pertenece a $\mathscr{F}$. Como y e y' son distintos, alguno de los dos tiene que ser distinto de $f(m+1, z)$, y sin pérdida de generalidad podemos suponer que $y' \neq f(m+1, z)$.

Consideremos el subconjunto $F \coloneqq \mathscr{F} \setminus \{(m+1, y')\}$ de $\mathscr{F}$, que es propio, y mostremos que es un subconjunto bueno de $\mathbb{N}_0 \times A$: de la misma forma que antes, esto contradice a nuestra observación (15), y esta contradicción prueba que $m+1$ pertenece al conjunto T.

Como el par $(0, \alpha)$ pertenece a $\mathscr{F}$ y es distinto de $(m+1, y)$, ya que $0 \neq m+1$, es claro que $(0, \alpha)$ pertenece a F. Sea, por otro lado, (n, a) un elemento cualquiera de F. Como (n, a) pertenece a $\mathscr{F}$, sabemos que $(n+1, f(n+1, a))$ es un elemento de $\mathscr{F}$. Este par ordenado es distinto de $(m+1, y')$:

- Si $n \neq m$, entonces $n+1 \neq m+1$, por supuesto, así que $(n+1, f(n+1, a)) \neq (m+1, y')$.
- Si en cambio $n = m$, entonces $(m, a) = (n, a) \in \mathscr{F}$ y $(m, z) \in F$, y como m pertenece a T tenemos que $a = z$ y, por lo tanto que

$$(n+1, f(n+1, a)) = (m+1, f(m+1, z)) \neq (m+1, y'),$$

  ya que $f(m+1, z) \neq y'$.

En cualquier caso, entonces, tenemos que $(n+1, f(n, a)) \in F$. Esto prueba que F es bueno.

Juntando todo lo que hemos hecho, podemos concluir que el subconjunto $\mathscr{F}$ de $\mathbb{N}_0 \times A$ es una función $\mathbb{N}_0 \to A$. Veámosla como una sucesión $(a_n)_{n \geq 1}$, de manera que para cada $n \in \mathbb{N}$ el elemento a_n de A es el único tal que (n, a_n) pertenece a $\mathscr{F}$. Para terminar la prueba de la proposición mostraremos que esta sucesión satisfaces las condiciones descriptas en el enunciado. Como $\mathscr{F}$ es un subconjunto bueno de $\mathbb{N}_0 \times A$, sabemos que $(0, \alpha)$ pertenece a $\mathscr{F}$ y, por lo tanto, que $a_0 = \alpha$. Por otro lado, si n es un elemento cualquiera de $\mathbb{N}$, entonces $n-1$ es uno de $\mathbb{N}_0$, y $(n-1, a_{n-1})$ es un elemento de $\mathscr{F}$: como $\mathscr{F}$ es un subconjunto bueno, esto implica que $(n, f(n, a_{n-1}))$ también lo es y, por lo tanto, que $a_n = f(n, a_{n-1})$. La proposición queda así probada. □

5.2.6. Observación. Una de las razones por las que demostrar en detalle la Proposición 5.2.5 es importante es que exactamente las mismas ideas permiten probar algo mucho menos intuitivo, el llamado *principio de recursión transfinita*, que extiende el resultado de esa proposición a las llamadas «sucesiones transfinitas». El primer uso de este principio de recursión transfinita fue hecho por Georg Cantor en 1872 en su estudio [Can1872] del problema de la descripción de los posibles conjuntos de convergencia de las series de Fourier. Cantor se dio cuenta inmediatamente que su uso de ese principio era *demasiado* informal, y con la intención de hacerlo preciso estudió

con mayor generalidad la idea de recursión transfinita en [Can1897] y, de hecho, este trabajo es una de las motivaciones originales del desarrollo de la teoría formal de conjuntos.

La demostración del principio de recursión transfinita puede hacerse de exactamente la misma forma en que probamos la Proposición 5.2.5. La dificultad más grande reside en encontrar el reemplazo apropiado para el conjunto $\mathbb{N}_0$ que sirva para indexar las componentes de una «sucesión transfinita».

§5.3. Variaciones sobre la recursión

5.3.1. En la sección anterior vimos que es posible determinar una sucesión $(a_n)_{n\geq 0}$ de elementos de un conjunto A dando la componente inicial a_0 y describiendo cómo cada una de las demás componentes puede obtenerse a partir de la inmediatamente anterior. El punto clave que hace que esta idea funcione es que a pesar de que no damos una fórmula explícita para cada componente de la sucesión, la información que damos es de todas formas suficiente como para determinar unívocamente cada una de esas componentes.

Este idea admite muchas variaciones. Consideraremos en esta sección algunas.

Recurrencias de orden superior

5.3.2. Existe exactamente una sucesión $(F_n)_{n\geq 0}$ de elementos de $\mathbb{Z}$ tal que

$$F_0 = 0,$$
$$F_1 = 1$$

y

$$F_n = F_{n-1} + F_{n-2}$$

para cada entero $n \geq 2$. En efecto, F_0 y F_1 quedan completamente determinados por las dos primeras condiciones y sus valores son 0 y 1, respectivamente. La tercera condición, por su parte, nos dice que $F_2 = F_1 + F_0$, así que la componente F_2 también está completamente determinada: su valor es $F_2 = 1 + 0 = 1$. Esa misma tercera condición nos dice que $F_3 = F_2 + F_1$ y, de acuerdo a lo que ya sabemos, es entonces $F_3 = 1 + 1 = 2$. Claramente podemos continuar de esta forma: cada una de las componentes de la sucesión $(F_n)_{n\geq 0}$ empezando por la segunda está determinada por las dos anteriores: es su suma. Así, las primeras componentes de la sucesión son

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ 610,\ 987,\ 1597,\ \ldots$$

Llamamos a esta sucesión la ***sucesión de números de Fibonacci***, por Fibonacci, nombre por el que es conocido[1] Leonardo de Pisa. Durante su infancia, Fibonacci acompañó a su padre, que era comerciante, en sus viajes por la costa del Mediterráneo, y allí aprendió los métodos de los árabes para hacer cálculos aritméticos. Años mas tarde, en 1202, escribió un libro titulado *Liber Abaci* («El libro del cálculo» en latín) en el que explica el sistema de numeración que hoy llamamos arábigo: esta obra tuvo un rol fundamental en convencer a los europeos — tanto a los comerciantes como a los matemáticos — de abandonar el sistema de numeración romano, que usaban hasta ese momento, y adoptar el arábigo, que seguimos usando hasta hoy. En ese libro, Fibonacci plantea y resuelve un problema sobre el crecimiento de una población de conejos, y es en ese contexto que estudia la sucesión de números que hoy lleva su nombre.

5.3.3. Decimos que la definición de la sucesión de los números de Fibonacci es por una recurrencia ***de orden dos***, porque cada una de las componentes de la sucesión — a partir de la segunda — depende del valor de las *dos* anteriores. Es fácil dar muchos ejemplos de sucesiones de esa forma.

Un ejemplo importante y estrechamente relacionado con el de los números de Fibonacci es la sucesión $(L_n)_{n\geq 0}$ de enteros que está determinada por las condiciones de que

$$L_0 = 2,$$
$$L_1 = 1$$

y

$$L_n = L_{n-1} + L_{n-2}$$

para cada entero $n \geq 2$. Las primeras componentes de esta sucesión son

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ 76,\ 123,\ 199,\ 322,\ 521,\ 843,\ 1364,\ 2207,\ \ldots$$

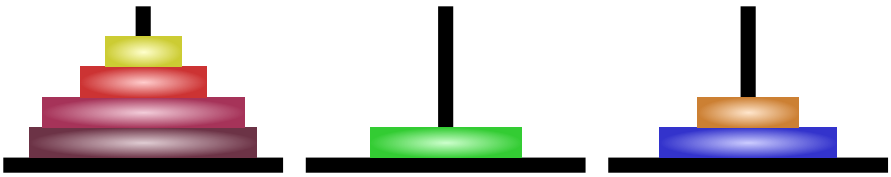
Notemos que la relación de recurrencia que define a esta sucesión es exactamente la misma que la que usamos para construir la sucesión de los números de Fibonacci: cada componente, desde la segunda en adelante, es suma de las dos que la preceden. La única diferencia entre las dos definiciones radica en los valores iniciales de la recursión.

Esta sucesión $(L_n)_{n\geq 0}$ es la de los ***números de Lucas***. El nombre recuerda a François Édouard Anatole Lucas, que estudió con gran detalle a los números de Fibonacci. Uno de sus intereses era el desarrollo de métodos para verificar si un número es primo o no: en 1857, a la edad de 15 años, empezó a probar un algoritmo — llamado hoy el «método de las secuencias de Lucas» — para decidir si el número

$$2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

[1] El apellido de su padre era Bonacci: Fibonacci es una contracción de la frase latina *filius Bonacci*, que significa «hijo de Bonacci». Es de notar que este sobrenombre le fue puesto recién en 1838 por el historiador francés Guillaume Libri.

es primo y en 1879, 19 años después, concluyó que sí lo es. Él inventó el juego conocido como *La Torre de Hanoi*, con el que el autor de estas notas se entretenía cuando era niño durante los largos viajes en auto que hacía con sus padres por la Patagonia.



5.3.4. Podemos también dar definiciones por recursión de órdenes más altos. Así, hay exactamente una sucesión $(T_n)_{n\geq 0}$ tal que

$$T_0 = T_1 = 0,$$
$$T_2 = 1$$

y

$$T_n = T_{n-1} + T_{n-2} + T_{n-3}$$

para cada $n \geq 3$. Calculando en orden, vemos que las primeras componentes de esta sucesión son

$$0,\ 0,\ 1,\ 1,\ 2,\ 4,\ 7,\ 13,\ 24,\ 44,\ 81,\ 149,\ 274,\ 504,\ 927,\ 1705,\ 3136,\ \ldots$$

La recursión que define esta sucesión — a la que llamamos, un poco en broma, ***sucesión de numeros de tribonacci*** — es de orden *tres*: cada uno de las componentes, a partir de la tercera, se calcula a partir de las tres anteriores.

5.3.5. De manera similar, hay exactamente una sucesión $(a_n)_{n\geq 0}$ tal que

$$a_0 = 0, \qquad a_1 = 1, \qquad a_2 = 2, \qquad a_3 = 3$$

y

$$a_n = a_{n-1}a_{n-4} + (-1)^n$$

para cada $n \geq 4$, y sus primeras componentes son, empezando por la 0-ésima,

$$0,\ 1,\ 2,\ 3,\ 1,\ 0,\ 1,\ 2,\ 3,\ -1,\ 0,\ -1,\ -2,\ 1,\ 1,\ -2,\ 5,\ 4,\ 5,\ -11,\ -54,\ \ldots$$

Esta es una sucesión dada por una recursión de orden cuatro: para calcular cada componente necesitamos conocer las cuatro anteriores — aunque en realidad solo usemos dos de esas cuatro.

5.3.6. En general, para cada $k \in \mathbb{N}$ podemos considerar sucesiones dadas por relaciones de recursión de orden k: el siguiente resultado es el análogo de las Proposiciones 5.2.5 y 5.2.4 para esta situación:

Proposición. *Sea A un conjunto, sea $k \in \mathbb{N}$, sean $\alpha_0, \ldots, \alpha_{k-1}$ elementos de A y sea*

$$f : \mathbb{N} \times \underbrace{A \times \cdots \times A}_{k \text{ factores}} \to A$$

una función. Existe una y una única sucesión $(a_n)_{n\geq 0}$ de elementos de A que para cada $n \in \mathbb{N}$ tiene

$$a_n = \alpha_i \text{ si } 0 \leq n < k$$

y

$$a_n = f(n, a_{n-k}, a_{n-k+1}, \ldots, a_{n-2}, a_{n-1}) \text{ si } n \geq k.$$

Demostración. Consideremos el conjunto $B \coloneqq A \times \cdots \times A$, producto cartesiano de k factores iguales a A, y la función $F : \mathbb{N} \times B \to B$ tal que para cada $n \in \mathbb{N}$ y cada elemento $b = (x_0, \ldots, x_{k-1})$ de B tiene

$$F(n, b) = (x_1, \ldots, x_{k-1}, f(n + k - 1, x_0, x_1, \ldots, x_{k-1})).$$

De acuerdo a la Proposición 5.2.5 hay exactamente una sucesión $(b_n)_{n\geq 0}$ de elementos de B tal que

$$b_0 = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \tag{16}$$

y

$$b_n = F(n, b_{n-1}) \tag{17}$$

para cada $n \in \mathbb{N}$. Ahora bien, para cada $n \in \mathbb{N}_0$ la componente n-ésima b_n de esta sucesión es un elemento del conjunto B, así que la podemos escribir en la forma

$$b_n = (b_{n,0}, b_{n,1}, \ldots, b_{n,k-1})$$

con $b_{n,0}$, $b_{n,1}$, …, $b_{n,k-1}$ elementos de A bien determinados. Usando esta notación, la ecuaciones (16) dice que

$$b_{0,i} = \alpha_i \qquad \text{para cada } i \in \{0, \ldots, k-1\},$$

mientras que la ecuación (17) nos dice que para todo $n \in \mathbb{N}$ es

$$\begin{aligned}(b_{n,0}, b_{n,1}, \ldots, b_{n,k-1}) &= b_n \\ &= F(n, b_{n-1}) \\ &= F(n, (b_{n-1,0}, b_{n-1,1}, \ldots, b_{n-1,k-1})) \\ &= (b_{n-1,1}, b_{n-2,2}, \ldots, b_{n-1,k-1}, f(n + k - 1, b_{n-1,0}, b_{n-1,1}, \ldots, b_{n-1,k-1})).\end{aligned}$$

Mirando componente a componente esta igualdad podemos concluir que para todo $n \in \mathbb{N}$ vale que

$$b_{n,i} = b_{n-1,i+1} \text{ para cada } i \in \{0, \dots, k-2\},$$
$$b_{n,k-1} = f(n+k-1, b_{n-1,0}, b_{n-1,1}, \dots, b_{n-1,k-1}).$$

De la primera de estas igualdades se deduce que si $n \in \mathbb{N}$ y $i \in \mathbb{N}_0$ son tales que $0 \leq i < k$ es

$$b_{n,i} = b_{n+i,0}.$$

Consideremos la sucesión $(a_n)_{n\geq 0}$ de elementos de A que para todo $n \in \mathbb{N}$ tiene componente n-ésima dada por

$$a_n \coloneqq b_{n,0}.$$

Sea n un elemento cualquiera de $\mathbb{N}$. Si $0 \leq n < k$, entonces $a_n = b_{n,0} = b_{0,n} = \alpha_n$. Si en cambio $n \geq k$, entonces $a_n = b_{n,0} = b_{n-k+1,k-1}$ y esto es la última componente de

$$\begin{aligned} b_{n-k+1} &= F(n-k+1, b_{n-k}) \\ &= F(n-k+1, (b_{n-k,0}, b_{n-k,1}, \dots, b_{n-k,k-1})) \\ &= (b_{n-k,1}, \dots, b_{n-k,k-1}, f(n, b_{n-k,0}, b_{n-k,1}, \dots, b_{n-k,k-1})) \\ &= (b_{n-k,1}, \dots, b_{n-k,k-1}, f(n, b_{n-k,0}, b_{n-k+1,0}, \dots, b_{n-1,0})) \\ &= (b_{n-k,1}, \dots, b_{n-k,k-1}, f(n, a_{n-k}, a_{n-k+1}, \dots, a_{n-1})) \end{aligned}$$

así que $a_n = f(n, a_{n-k}, a_{n-k+1}, \dots, a_{n-1})$. Vemos así que la sucesión $(a_n)_{n\geq 1}$ satisface las condiciones descriptas en la proposición.

Para terminar la prueba de la proposición, supongamos que $(a'_n)_{n\geq 1}$ es otra sucesión de elementos de A que satisface esas condiciones. Claramente tenemos que $a'_i = a_i$ para todo $i \in \{0, \dots, k-1\}$. Por otro lado, si n es un elemento de $\mathbb{N}_0$ tal que $n \geq k$ y vale que $a'_i = a_i$ para todo $i \in \{n-k, n-k+1, \dots, n-1\}$, entonces

$$a'_n = f(n, a'_{n-k}, a'_{n-k+1}, \dots, a'_{n-1}) = f(n, a_{n-k}, a_{n-k+1}, \dots, a_{n-1}) = a_n.$$

Podemos así concluir que las sucesiones $(a_n)_{n\geq 1}$ y $(a'_n)_{n\geq 1}$ coinciden, y esto prueba la afirmación de unicidad de la proposición. □

Omitimos la demostración, porque es enteramente similar a las de aquellas dos proposiciones. Esta proposición nos permite justificar la buena definición de los ejemplos que consideramos arriba:

- La sucesión $(F_n)_{n\geq 0}$ de los números de Fibonacci se obtiene tomando $A = \mathbb{N}_0$, $k = 2$,

$\alpha_0 = 0$, $\alpha_1 = 1$ y como $f : \mathbb{N} \times A \times A \to A$ a la función tal que $f(n, x, y) = x + y$ para cada $(n, x, y) \in \mathbb{N} \times A \times A$.

- La sucesión $(L_n)_{n\geq 0}$ de los números de Lucas, por su parte, se obtiene con esa misma elección de A, k y f, pero con $\alpha_0 = 2$ y $\alpha_1 = 1$.
- La sucesión $(T_n)_{n\geq 0}$ de los números de tribonacci se obtiene tomando $A = \mathbb{N}$, $k = 3$, $\alpha_0 = \alpha_1 = 0$, $\alpha_2 = 1$ y como $f : \mathbb{N} \times A \times A \times A \to A$ a la función tal que $f(n, x, y, z) = x + y + z$ cada vez que $n \in \mathbb{N}$ y $x, y, z \in A$.
- Finalmente, la sucesión del ejemplo 5.3.5 se obtiene tomando $A = \mathbb{Z}$, $k = 4$, $\alpha_i = i$ para cada $i \in \{0, 1, 2, 3\}$ y $f : \mathbb{N} \times A \times A \times A \times A \to A$ a la función tal que

  $$f(n, x, y, z, w) = xw + (-1)^n$$

  cada vez que $n \in \mathbb{N}$ y $x, y, z, w \in A$.

5.3.7. Es posible definir sucesiones por recursiones más complicadas que las que se consideran en la Proposición 5.3.6. Veamos dos ejemplos

(*a*) Hay una sucesión $(t_n)_{n\geq 1}$ que tiene $t_1 = 1$ y que es tal que, para cada entero $n \geq 2$, satisface la relación

$$t_n = \begin{cases} 1 + t_{n/2}, & \text{si } n \text{ es par;} \\ t_{n-1}, & \text{si } n \text{ es impar.} \end{cases}$$

Las primeras componentes de esta sucesión son

$$1,\ 2,\ 2,\ 3,\ 3,\ 3,\ 3,\ 4,\ 4,\ 4,\ 4,\ 4,\ 4,\ \ldots$$

(*b*) Hay una sucesión $(u_n)_{n\geq 0}$ tal que $u_1 = 0$ y

$$u_n = \sum_{m=0}^{n-1} m^2 u_m$$

para cada entero $n \geq 1$. Las primeras componentes de esta sucesión son

$$1,\ 5,\ 50,\ 850,\ 22100,\ 817700,\ 40885000,\ 2657525000,\ \ldots$$

En cada uno de estos dos ejemplos, la relación de recursión que determina cada componente de la sucesión no depende de un número fijo de componentes anteriores: en el primer ejemplo, t_n depende, cuando n es par, de $t_{n/2}$, mientras que en el segundo ejemplo para calcular u_n usando la relación de recurrencia necesitamos conocer *todas* las componentes anteriores, $u_0, \ldots, u_{n-1}$. De todas formas, es claro que en ambos casos las sucesiones consideradas están bien determinadas. Esto puede formalizarse en una proposición del mismo estilo que la Proposición 5.3.6, pero no lo haremos. Nos tomaremos, de todas formas, la libertad de usar estos y otros tipos de recursiones para definir sucesiones

5.3.8. Ejercicio. Sea A un conjunto y para cada $n \in \mathbb{N}_0$ escribamos $I_n \coloneqq \{0, \dots, n\}$ y $\mathscr{F}_n$ al conjunto de todas las funciones $I_n \to A$. Supongamos que tenemos

- un elemento α de A y
- para cada $n \in \mathbb{N}$ una función $F_n : \mathscr{F}_{n-1} \to A$.

Muestre que existe exactamente una función $f : \mathbb{N}_0 \to A$ tal que

- $f(0) = \alpha$ y
- para todo $n \in \mathbb{N}$ es $f(n) = F_n(f|_{I_{n-1}})$.

Esto nos da una generalización del principio de recursión de las Proposiciones 5.2.5 y 5.3.6. Por ejemplo, si A es $\mathbb{Z}$, α es 1 y para todo $n \in \mathbb{N}$ la función $F_n : \mathscr{F}_{n-1} \to \mathbb{N}_0$ es tal que

$$F_n(h) = \sum_{i=0}^{n-1} h(i) \qquad \text{para toda función } h : I_{n-1} \to \mathbb{Z},$$

entonces este resultado nos dice que hay una función $f : \mathbb{N}_0 \to \mathbb{Z}$, esto es, una sucesión $(f_n)_{n\geq 0}$ tal que

$$f_0 = 1, \qquad f_n = f_0 + f_1 + \cdots + f_{n-1} \text{ para cada } n \in \mathbb{N}.$$

§5.4. Manipulación de sucesiones definidas recursivamente

5.4.1. El principio de inducción es una herramienta natural para probar cosas sobre sucesiones que están definidas por recurrencia. El objetivo de esta sección es usar las sucesiones de los números de Fibonacci y de Catalan para ejemplificar esto.

Números de Fibonacci

5.4.2. Sea $(F_n)_{n\geq 0}$ la sucesión de números de Fibonacci, de manera que

$$F_0 = 0,$$
$$F_1 = 1$$

y

$$F_n = F_{n-1} + F_{n-2} \tag{18}$$

para cada entero n tal que $n \geq 2$.

5.4.3. Si calculamos los primeros números de Fibonacci vemos que crecen con bastante rapidez. Nuestro primero resultado es que, de todas formas, podemos acotarlos por una exponencial.

Lema. *Para todo $n \in \mathbb{N}_0$ se tiene que $F_n \leq 2^n$.*

Demostración. Procedemos por inducción, llamando $P(n)$ a la afirmación «$F_n \leq 2^n$». Es claro que $F_0 = 0 \leq 2^0$ y que $F_1 = 1 \leq 2^1$, así que $P(0)$ y $P(1)$ valen.

Supongamos, para establecer el paso inductivo, que $k \in \mathbb{N}$ es tal que $k \geq 2$ y que las afirmaciones $P(k-1)$ y $P(k-2)$ valen. Entonces

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} && \text{por (18)} \\ &\leq 2^{k-1} + 2^{k-2} && \text{por } P(k-1) \text{ y } P(k-2) \\ &\leq 2^{k-1} + 2^{k-1} && \text{ya que } 2^{k-2} \leq 2^2 \\ &= 2 \cdot 2^{k-1} = 2^k. \end{aligned}$$

Esto nos dice que, bajo la hipótesis inductiva, vale la afirmación $P(k)$ y, por lo tanto, completa la inducción. □

5.4.4. La suma de los primeros números de Fibonacci difiere ella misma de un número de Fibonacci en una unidad:

Lema. *Si $n \in \mathbb{N}$, entonces $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.*

Demostración. Procedemos por inducción con respecto a n. Si $n = 1$, el lado izquierdo de la igualdad que queremos probar es $F_1 = 1$ y el derecho es $F_3 - 1 = 2 - 1 = 1$: vemos así que en ese caso la igualdad vale.

Supongamos ahora que $k \in \mathbb{N}$ es tal que $k \geq 2$ y que la igualdad del enunciado vale cuando n es $k-1$, esto es, que

$$F_1 + F_2 + \cdots + F_{k-1} = F_{k+1} - 1.$$

Usando esto, vemos que

$$F_1 + F_2 + \cdots + F_{k-1} + F_k = F_{k+1} - 1 + F_k = F_{k+2} - 1,$$

así que la igualdad del enunciado también vale cuando n es k. Esto completa la inducción y prueba el lema. □

5.4.5. La siguiente identidad es conocida como ***identidad de Cassini***, por Giovanni Domenico

Cassini — cuyo nombre no solo usamos para nombrar una identidad sino también una nave espacial que fue enviada en 1997 a fotografiar los anillos de Saturno.

Lema. *Para cada $n \in \mathbb{N}$ se tiene que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.*

Demostración. Cuando $n = 1$, el lado izquierdo de la igualdad que queremos probar tiene valor $F_2F_0 - F_1^2 = 0 \cdot 1 - 1 = -1$ y el derecho $(-1)^1 = -1$, así que la igualdad vale en ese caso.

Supongamos ahora que k es un elemento de $\mathbb{N}$ tal que la igualdad del enunciado vale cuando n es k, es decir, tal que

$$F_{k+1}F_{k-1} - F_k^2 = (-1)^k, \tag{19}$$

y calculemos, usando la relación de recurrencia que define a los números de Fibonacci:

$$\begin{aligned} F_{k+2}F_k - F_{k+1}^2 &= (F_k + F_{k+1})F_k - F_{k+1}(F_{k-1} + F_k) \\ &= F_k^2 + F_{k+1}F_k - F_{k+1}F_{k-1} - F_{k+1}F_k \\ &= F_k^2 - F_{k+1}F_k \end{aligned}$$

y esto es, de acuerdo a la hipótesis inductiva (19),

$$= (-1)^{k+1}.$$

Vemos así que bajo esa hipótesis la igualdad del enunciado también vale cuando n es $k+1$. El lema es consecuencia de esto y del principio de inducción. □

5.4.6. Las sumas de los productos de números de Fibonacci consecutivos tienen también una descripción directa en términos de números de Fibonacci:

Lema. *Para cada entero $n \geq 2$ se tiene que*

$$F_1F_2 + F_2F_3 + \cdots + F_{n-1}F_n = \begin{cases} F_n^2, & \text{si } n \text{ es par;} \\ F_n^2 - 1, & \text{si } n \text{ es impar.} \end{cases}$$

Demostración. Sea $P(n)$ la afirmación de que vale la igualdad del enunciado. Cuando $n = 2$, a izquierda y a derecha en la igualdad del enunciado tenemos $F_1F_2 = 1 \cdot 1 = 1$ y $F_2^2 = 1^2 = 1$, respectivamente, así que esa igualdad vale en ese caso: en otras palabras, vale $P(2)$.

Supongamos ahora que k es un entero tal que $k \geq 2$ y que vale que

$$F_1F_2 + F_2F_2 + \cdots + F_{k-1}F_k = \begin{cases} F_k^2, & \text{si } k \text{ es par;} \\ F_k^2 - 1, & \text{si } k \text{ es impar.} \end{cases}$$

Tenemos entonces que

$$F_1F_2 + F_2F_2 + \cdots + F_kF_{k+1} = \begin{cases} F_k^2 + F_kF_{k+1}, & \text{si } k \text{ es par;} \\ F_k^2 - 1 + F_kF_{k+1}, & \text{si } k \text{ es impar.} \end{cases}$$

Ahora bien, es

$$F_k^2 + F_kF_{k+1} = F_k(F_k + F_{k+1}) = F_kF_{k+2} = F_{k+1}^2 + (-1)^{k+1}$$

de acuerdo a la identidad de Cassini 5.4.5, así que

$$F_1F_2 + F_2F_2 + \cdots + F_kF_{k+1} = \begin{cases} F_{k+1}^2 + (-1)^{k+1}, & \text{si } k \text{ es par;} \\ F_{k+1}^2 + (-1)^{k+1} - 1, & \text{si } k \text{ es impar;} \end{cases}$$

y esto es lo mismo que

$$\begin{cases} F_{k+1}^2 - 1, & \text{si } k+1 \text{ es impar;} \\ F_{k+1}^2, & \text{si } k+1 \text{ es par.} \end{cases}$$

Hemos mostrado así que si $k \geq 2$, entonces la afirmación $P(k)$ implica la afirmación $P(k+1)$. El lema sigue de esto, gracias al principio de inducción. □

5.4.7. Hasta ahora describimos relaciones entre componentes *cercanas* de la sucesión de Fibonacci. La siguiente, por el contrario, establece una relación sencilla entre componentes alejadas:

Lema. *Si $n \in \mathbb{N}$ y $m \in \mathbb{N}_0$, entonces*

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}.$$

Notemos que esta afirmación involucra *dos* números natural m y n.

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

para todo $m \in \mathbb{N}_0$ se tiene que $F_{n+m} = F_{n-1}F_m + F_nF_{m+1}$.

Observemos que es evidente que $P(1)$ vale: es simplemente la afirmación de que para todo $m \in \mathbb{N}_0$ se tiene que $F_{m+1} = F_{m+1}$, ya que $F_0 = 0$ y $F_1 = 1$.

Supongamos entonces, para hacer inducción, que $k \in \mathbb{N}$ y que vale la afirmación $P(k)$, de manera que para todo $m \in \mathbb{N}_0$ se tiene que $F_{k+m} = F_{k-1}F_m + F_kF_{m+1}$. Ahora bien, para todo $m \in \mathbb{N}_0$ tenemos que

$$F_{(k+1)+m} = F_{k+(m+1)}$$

y, usando la hipótesis inductiva, vemos que esto es

$$\begin{aligned} &= F_{k-1}F_{m+1} + F_kF_{m+2} \\ &= F_{k-1}F_{m+1} + F_k(F_m + F_{m+1}) \\ &= F_kF_m + (F_{k-1} + F_k)F_{m+1} \\ &= F_kF_m + F_{k+1}F_{m+1}. \end{aligned}$$

Esto nos dice, precisamente, que vale la afirmación $P(k+1)$, y completa la prueba del lema, gracias al principio de inducción. □

5.4.8. Este lema tiene el siguiente corolario: las fórmulas que aparecen en él se llaman ***fórmulas de duplicación***, ya que permiten duplicar el índice.

Corolario. *Para todo $n \in \mathbb{N}$ se tiene que*

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2 = F_n(2F_{n+1} - F_n)$$

y

$$F_{2n+1} = F_{n+1}^2 + F_n^2.$$

Demostración. Si en la identidad del Lema 5.4.7 ponemos $m = n$, vemos que

$$\begin{aligned} F_{2n} &= F_{n-1}F_n + F_nF_{n+1} \\ &= F_n(F_{n-1} + F_{n+1}) \\ &= (F_{n+1} - F_{n-1})(F_{n-1} + F_{n+1}) \\ &= F_{n+1}^2 - F_{n-1}^2, \end{aligned} \tag{20}$$

y esta es la primera de las igualdades del corolario. Volviendo a la igualdad (20), tenemos también que

$$F_{2n} = F_n(F_{n-1} + F_{n+1}) = F_n(2F_{n+1} - F_n),$$

ya que $F_{n-1} = F_{n+1} - F_n$, y esta es la segunda igualdad del enunciado. Finalmente, si ponemos $m = n + 1$ en el Lema 5.4.7, este nos dice que

$$\begin{aligned} F_{2n+1} &= F_{n-1}F_{n+1} + F_nF_{n+2} \\ &= F_{n-1}F_{n+1} + F_n(F_n + F_{n+1}) \\ &= (F_{n-1} + F_n)F_{n+1} + F_n^2 \\ &= F_{n+1}^2 + F_n^2, \end{aligned}$$

que es la tercera de las igualdades del corolario. □

5.4.9. La siguiente identidad, a la que llamamos ***identidad de Catalan***, generaliza a la de Cassini:

Lema. *Si* $0 \leq r \leq n$*, entonces*

$$F_{n-r}F_{n+r} - F_n^2 = (-1)^{n-r+1}F_r^2.$$

En efecto, la identidad de Cassini es el caso particular de esta en el que $r = 1$. La prueba de esta proposición es un poco más complicada que las de las anteriores: procederemos por inducción y para probar el paso inductivo haremos una inducción.

Demostración. Para cada $r \in \mathbb{N}_0$ sea $P(r)$ la afirmación

para cada entero $n \geq r$ *se tiene que* $F_{n-r}F_{n+r} - F_n^2 = (-1)^{n-r+1}F_r^2$.

Probaremos que para todo $r \in \mathbb{N}_0$ la afirmación $P(r)$ vale, procediendo por inducción con respecto a r: esto demostrará la proposición. Observemos que la validez de la afirmación $P(0)$ es evidente, así que bastará que nos ocupemos del paso inductivo.

Sea entonces $s \in \mathbb{N}_0$ y mostremos que $P(s) \implies P(s+1)$. Para ello, supongamos que $P(s)$ vale, es decir, que

$$\text{si } n \geq s, \text{ entonces } F_{n-s}F_{n+s} - F_n^2 = (-1)^{n-s+1}F_s^2, \tag{21}$$

y mostremos que entonces también vale $P(s+1)$, es decir, que se tiene que

$$\text{si } n \geq s+1, \text{ entonces } F_{n-s-1}F_{n+s+1} - F_n^2 = (-1)^{n-s+2}F_{s+1}^2. \tag{22}$$

Para hacer esto, procederemos por inducción: para cada entero $n \geq s+1$, llamemos $Q_s(n)$ a la afirmación

$$F_{n-s-1}F_{n+s+1} - F_n^2 = (-1)^{n-s+2}F_{s+1}^2$$

y mostremos que $Q_s(n)$ vale para todo entero $n \geq s+1$. Esto probará (22).

La afirmación $Q_s(s+1)$ vale, ya que lo que afirma es que

$$F_0F_{2(s+1)} - F_{s+1}^2 = (-1)^{s+1-s+2}F_{s+1}^2,$$

que es evidente. Supongamos entonces que $k \in \mathbb{N}$ es tal que $k \geq s+1$ y que $Q_s(k)$ vale. Sumando y restando $F_{k+1+s}F_{k+1-s}$, vemos que

$$\begin{aligned} &F_{k+1-s-1}F_{k+1+s+1} - F_{k+1}^2 \\ &\quad = F_{k+1-s-1}F_{k+1+s+1} - F_{k+1+s}F_{k+1-s} + \underbrace{F_{k+1+s}F_{k+1-s} - F_{k+1}^2}. \end{aligned} \tag{23}$$

Como $k+1 \geq s$ y estamos suponiendo que $P(s)$ vale —es decir, que vale (21)— podemos reemplazar la parte marcada, y ver que esto es

$$= F_{k+1-s-1}F_{k+1+s+1} - F_{k+1+s}F_{k+1-s} + (-1)^{k+1-s+1}F_s^2$$

y esto, reescribiendo $F_{k+1+s+1}$ usando la relación de recurrencia de los números de Fibonacci y simplificando un poco, es, a su vez,

$$\begin{aligned} &= F_{k-s}(F_{k+1+s} + F_{k+s}) - F_{k+1+s}F_{k+1-s} + (-1)^{k-s}F_s^2 \\ &= (F_{k-s} - F_{k+1-s})F_{k+1+s} + F_{k-s}F_{k+s} + (-1)^{k-s}F_s^2 \\ &= -F_{k-s-1}F_{k+1+s} + \underbrace{F_{k-s}F_{k+s} + (-1)^{k-s}F_s^2}. \end{aligned}$$

Como estamos suponiendo que $P(s)$ vale y $k \geq s$, reemplazando la parte marcada, vemos que esta última expresión es

$$= -F_{k-s-1}F_{k+1+s} + F_k^2$$

y, finalmente, como estamos suponiendo que $Q_s(k)$ vale, esto es

$$= (-1)^{k-s+1}F_{s+1}^2. \tag{24}$$

Con toda esta cadena de igualdades —que va de (23) a (24)— hemos probado que

$$F_{k+1-s-1}F_{k+1+s+1} - F_{k+1}^2 = (-1)^{(k+1)-(s+1)+1}F_{s+1}^2,$$

es decir, que vale $Q_s(k+1)$. Esto completa la prueba de la proposición. □

5.4.10. Todo lo que hemos probado hasta ahora sobre los números de Fibonacci estuvo basado pura y exclusivamente en el hecho de que satisfacen la relación de recurrencia que los define. En particular, hasta ahora no tenemos ninguna fórmula cerrada para calcular los números de Fibonacci, sino solamente un algoritmo para calcularlos. El siguiente resultado, conocido como la ***fórmula de Binet***, por Jacques Philippe Marie Binet, nos da una fórmula explícita:

Lema. *Sean* $\alpha = \dfrac{1+\sqrt{5}}{2}$ *y* $\beta = \dfrac{1-\sqrt{5}}{2}$ *las dos raíces del polinomio* $X^2 - X - 1$. *Para cada* $n \in \mathbb{N}_0$ *se tiene que*

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Demostración. Para cada $n \in \mathbb{N}_0$ sea $G_n = (\alpha^n - \beta^n)/\sqrt{5}$. Lo que tenemos que probar es que para cada $n \in \mathbb{N}_0$ es

$$F_n = G_n \tag{25}$$

y, como siempre, procedemos por inducción con respecto a n.

Como $G_0 = (1-1)/\sqrt{5} = 0$ y $G_1 = (\alpha - \beta)/\sqrt{5} = 1$, la igualdad (25) vale si n es 0 o 1. Para ver que vale el paso inductivo, supongamos que $k \in \mathbb{N}_0$ y que la igualdad (25) vale si n es k o $k+1$. En ese caso, tenemos que

$$\sqrt{5} \cdot F_{k+2} = \sqrt{5} \cdot F_{k+1} + \sqrt{5} \cdot F_k = \sqrt{5} \cdot G_{k+1} + \sqrt{5} \cdot G_k = (\alpha^{k+1} - \beta^{k+1}) + (\alpha^k - \beta^k).$$

Calculando, vemos que $\alpha^2 = \alpha + 1$ y $\beta^2 = \beta + 1$, así que $\alpha^{k+2} = \alpha^{k+1} + \alpha^k$ y $\beta^{k+2} = \beta^{k+1} + \beta^k$, y entonces lo que tenemos es que

$$\sqrt{5} \cdot F_{k+2} = \alpha^{k+2} - \beta^{k+2},$$

es decir, que $F_{k+2} = G_{k+2}$ y, por lo tanto, la igualdad (25) vale si n es $k+2$. Esto prueba el lema. □

5.4.11. Un corolario bonito de este lema es el siguiente:

Corolario. *Para todo $n \in \mathbb{N}$ el n-ésimo número de Fibonacci F_n es el entero más cercano a*

$$\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n.$$

Demostración. Sea n un elemento de $\mathbb{N}_0$. El lema nos dice que si ponemos $\alpha = (1+\sqrt{5})/2$ y $\beta = (1-\sqrt{5})/2$, entonces $F_n = (\alpha^n - \beta^2)/\sqrt{5}$, así que $\alpha^n/\sqrt{5} - F_n = \beta^n/\sqrt{5}$. Ahora bien, como $\beta = -1/\alpha$ y $\alpha = 1 + \sqrt{5} > 1$, tenemos que $|\beta^n| = 1/|\alpha|^n \leq 1$ y, por lo tanto, $|\beta^n/\sqrt{5}| < 1/2$, ya que $\sqrt{5} > 2$. Esto nos dice que F_n y $\alpha^n/\sqrt{5}$ están a distancia menor que $1/2$ y, por lo tanto, que el entero F_n es el más cercano al número $\alpha^n/\sqrt{5}$. □

5.4.12. Ejercicio. Pruebe que, de hecho, para todo $n \in \mathbb{N}$ vale que

$$F_n = \left\lfloor \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n + \frac{1}{2} \right\rfloor.$$

Números de Catalan

5.4.13. Recordemos de 5.2.2 que la sucesión $(C_n)_{n\geq 0}$ de los números de Catalan es tal que

$$C_0 = 1$$

y

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1} \tag{26}$$

para cada entero positivo n. Calculando, vemos que sus primeras componentes son

$$1,\ 1,\ 2,\ 5,\ 14,\ 42,\ 132,\ 429,\ 1430,\ 4862,\ 16796,\ \ldots \tag{27}$$

5.4.14. Una primera observación que podemos hacer es que la sucesión de números de Catalan está, como la de Fibonacci, acotada por una sucesión de crecimiento exponencial:

Lema. *Para cada $n \in \mathbb{N}_0$ se tiene que*

$$C_n \leq \frac{4^n}{n+1}.$$

Demostración. Sea $P(n)$ la afirmación de que vale la desigualdad del enunciado. Como $C_0 = 1$ y $4^0/(0+1) = 1$, es claro que $P(0)$ vale. Por otro lado, si $k \in \mathbb{N}$ y suponemos que vale $P(k-1)$, entonces

$$C_n = \frac{2(2n-1)}{n+1} C_n \leq \frac{2(2n-1)}{n+1} \frac{4^{n-1}}{n} = \frac{2n-1}{2n} \frac{4^n}{n+1} \leq \frac{4^n}{n+1},$$

es decir, vale $P(k)$. El lema es consecuencia de esto y del principio de inducción. □

5.4.15. A partir de la definición por recursión de los números de Catalan es fácil obtener una fórmula explícita:

Lema. *Para todo $n \in \mathbb{N}_0$ es*

$$C_n = \frac{1}{n+1} \frac{(2n)!}{n!n!}.$$

Demostración. Es inmediato que la igualdad del enunciado vale cuando $n = 0$. Veamos que si $k \in \mathbb{N}_0$ es tal que esa igualdad vale cuando n es k, entonces ella también vale cuando n es $k+1$: el lema seguirá entonces por inducción.

Sea entonces $k \in \mathbb{N}_0$ y supongamos que

$$C_k = \frac{1}{k+2} \frac{(2k)!}{k!k!}.$$

En ese caso, en vista de la relación de recurrencia que define a los números de Catalan, tenemos que

$$C_{k+1} = \frac{2(2(k+1)-1)}{(k+1)+1} C_k$$

y esto, gracias a nuestra hipótesis inductiva, es

$$= \frac{2(2k+1)}{k+2} \frac{1}{k+1} \frac{(2k)!}{k!k!}.$$

Multiplicando el numerador y el denominador de este cociente por $k+1$, vemos que es

$$\begin{aligned} &= \frac{2(2k+1)}{k+2} \frac{1}{k+1} \frac{(2k)!}{k!k!} \frac{k+1}{k+1} \\ &= \frac{1}{k+2} \frac{(2k+2)!}{(k+1)!(k+1)!}, \end{aligned}$$

y esto completa la inducción. □

5.4.16. Del cálculo directo de los números de Catalan, como en (27), vemos que parecen ser todos enteros: esto no es obvio ni a partir de la relación de recurrencia (26) que los define ni a partir de la fórmula explícita para ellos que nos da el Lema 5.4.15. Un primer paso para probar que se trata efectivamente de números enteros es el siguiente resultado, que es fundamental en el estudio de los números de Catalan:

Lema. *Para cada $n \in \mathbb{N}_0$ se tiene que*

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}.$$

Demostración. Para cada $n \in \mathbb{N}_0$, llamemos $P(n)$ a la afirmación de que vale la igualdad del enunciado. Es claro que $P(0)$ vale: el miembro izquierdo de la igualdad es $C_1 = 1$ y el derecho $\sum_{i=0}^{n} C_i C_{0-i} = C_0 C_0 = 1$.

Sea ahora $k \in \mathbb{N}_0$ y supongamos inductivamente que $P(k)$ vale. Tenemos que

$$\begin{aligned} (k+2) \sum_{i=0}^{k} C_i C_{k-i} &= \sum_{i=0}^{k} (k+2) C_i C_{k-i} = \sum_{i=0}^{k} (i+1+k-i+1) C_i C_{k-i} \\ &= \sum_{i=0}^{k} (i+1) C_i C_{k-i} + \sum_{i=0}^{k} (k-i+1) C_i C_{k-i} \\ &= C_0 C_k + \sum_{i=1}^{k} (i+1) C_i C_{k-i} + \sum_{i=0}^{k-1} (k-i+1) C_i C_{k-i} + C_k C_0 \end{aligned}$$

y, usando la relación (26), vemos que esto es

$$= C_0C_k + \sum_{i=1}^{k} 2(2i-1)C_{i-1}C_{k-i} + \sum_{i=0}^{k-1} 2(2(k-i)-1)C_iC_{k-i-1} + C_kC_0.$$

Si cambiamos el índice i por $i-1$ en la primera de las dos sumas, podemos reescribir esto en la forma

$$C_0C_k + \sum_{i=0}^{k-1} 2(2(i+1)-1)C_iC_{k-1-i} + \sum_{i=0}^{k-1} 2(2(k-i)-1)C_iC_{k-i-1} + C_kC_0$$

y, una vez hecho eso, juntar las dos sumas en una para obtener

$$2C_0C_k + \sum_{i=0}^{k-1} 2\Big((2(i+1)-1) + (2(k-i)-1)\Big)C_iC_{k-1-i}.$$

Esto es lo mismo que

$$2C_k + \sum_{i=0}^{k-1} 2\cdot 2k\cdot C_iC_{k-1-i} = 2C_k + 2\cdot 2k\sum_{i=0}^{k-1} C_iC_{k-1-i}$$

y, de acuerdo a la hipótesis inductiva, esto es igual a

$$2C_k + 2\cdot 2kC_k = 2(2(k+1)-1)C_k = (k+2)C_{k+1}.$$

Hemos probado de esta manera que

$$(k+2)\sum_{i=0}^{k} C_iC_{k-i} = (k+2)C_{k+1}$$

y, por lo tanto, que la afirmación $P(k+1)$ vale. El lema sigue por inducción. □

5.4.17. Una primera consecuencia del Lema 5.4.16 es que podríamos haber definido la sucesión $(C_n)_{n\geq 0}$ de los números de Catalan diciendo que

$$C_0 = 1$$

y que

$$C_{n+1} = \sum_{i=0}^{n} C_iC_{n-i}$$

para cada $n \in \mathbb{N}_0$. De hecho, esta definición es la más frecuente en la literatura.

5.4.18. Una segunda consecuencia de ese lema es que podemos ahora fácilmente verificar que todos los números de Catalan son enteros:

Lema. *Para todo $n \in \mathbb{N}_0$ el n-ésimo número de Catalan C_n es un entero.*

Demostración. Esto sigue inductivamente del lema anterior. En efecto, C_0 es un entero y si $k \in \mathbb{N}_0$ y suponemos inductivamente que cada uno de los números $C_0, \ldots, C_k$ es un entero, entonces el Lema 5.4.16 nos dice que

$$C_{k+1} = \sum_{i_0}^{k} C_i C_{k-i}$$

y claramente esto implica que C_{k+1} también es un entero. □

Un método rápido para calcular potencias

5.4.19. Fijemos un número real α no nulo y consideremos la sucesión $(a_n)_{n\geq 0}$ tal que

$$a_0 = 1$$

y

$$a_n = \alpha a_{n-1}$$

para cada $n \in \mathbb{N}$. Es inmediato que

para todo $n \in \mathbb{N}_0$ se tiene que $a_n = \alpha^n$.

En efecto, sigue inmediatamente de la definición de la sucesión que $a_0 = \alpha^0$, y si $k \in \mathbb{N}$ es tal que $a_{k-1} = \alpha^{k-1}$, entonces claramente se tiene que $a_k = \alpha a_{k-1} = \alpha\alpha^{k-1} = \alpha^k$. Esto nos da un procedimiento — el obvio — para calcular las potencias de α: para calcular α^n empezamos con 1 y lo multiplicamos n veces por α. Es evidente que cuando llevamos a cabo esto hacemos $n-1$ multiplicaciones (sin contar la primera, en la que un factor es 1). Hay una forma mucho más eficiente para determinar α^n, basada en el siguiente resultado:

5.4.20. Lema. *Hay una única sucesión $(b_n)_{n\geq 0}$ con $b_0 = 1$ y tal que para cada $n \in \mathbb{N}$ se tiene que*

$$b_n = \begin{cases} (b_{n/2})^2, & \text{si } n \text{ es par;} \\ \alpha(b_{(n-1)/2})^2, & \text{si } n \text{ es impar.} \end{cases}$$

De hecho, si $(b_n)_{n\geq 0}$ es una sucesión que satisface estas dos condiciones entonces $b_n = \alpha^n$ para todo $n \in \mathbb{N}_0$.

Demostración. Veamos por inducción que si $(b_n)_{n\geq 0}$ es una sucesión que satisface las dos condiciones del enunciado entonces $b_n = \alpha^n$ para todo $n \in \mathbb{N}_0$. Es claro que $b_0 = \alpha^0$. Sea, por otro lado, $k \in \mathbb{N}$ y supongamos que $b_i = \alpha^i$ para todo entero i tal que $0 \leq i < k$. Consideramos ahora dos casos, de acuerdo a la paridad de k.

- Si k es par, entonces $k/2$ es un entero no negativo menor que k, la hipótesis inductiva nos dice que $b_{k/2} = \alpha^{k/2}$ y, por lo tanto,

$$b_k = (b_{k/2})^2 = (\alpha^{k/2})^2 = \alpha^k.$$

- Si en cambio k es impar, entonces $(k-1)/2$ es un entero no negativo menor que k y otra vez la hipótesis inductiva nos dice que $b_{(k-1)/2} = \alpha^{(k-1)/2}$. Usando esto, vemos que

$$b_k = \alpha(b_{(k-1)/2})^2 = \alpha(\alpha^{(k-1)/2})^2 = \alpha^k.$$

Así, en cualquier caso tenemos que $b_k = \alpha^k$ y esto completa la inducción.

Esto nos dice que a lo sumo hay una sucesión que satisface las dos condiciones del enunciado, a saber, la sucesión $(\alpha^n)_{n\geq 0}$ de las potencias de α. Para completar la prueba del lema, entonces, es suficiente con mostrar que esta última sucesión satisface efectivamente aquellas dos condiciones: esto es inmediato. □

5.4.21. Este lema nos dice, por ejemplo, que

$$\alpha^{10} = b_{10} = b_5^2 = (\alpha b_2^2)^2 = (\alpha(b_1^2)^2)^2 = (\alpha(\alpha^2)^2)^2.$$

Esta expresión muestra que podemos calcular α^{10} haciendo cuatro productos: calculamos primero α^2, luego lo elevamos al cuadrado, multiplicamos por α el resultado y elevamos lo que obtenemos al cuadrado. Esto es menos que la mitad de las multiplicaciones que hacemos si calculamos α^{10} de la manera evidente. De manera similar, usando el lema vemos que

$$\alpha^{154} = (a((a(a(((a^2)^2)^2)^2)^2)^2)^2)^2$$

y la expresión que aparece a la derecha en esta igualdad puede calcularse usando 10 productos: esto es considerablemente mejor que hacerlo con 154 productos! En general, el lema nos provee una forma rápida de calcular las potencias de α — en las Figuras 5.1 y 5.2 en la página siguiente damos una implementación de esto en Haskell y en Python.

Queremos ahora estimar la cantidad de trabajo que este algoritmo realiza. Para cada $n \in \mathbb{N}$ sea M_n la cantidad de multiplicaciones que realizamos cuando usamos el Lema 5.4.20 para calcular α^n. De acuerdo a las fórmulas que aparecen en el enunciado de ese lema, tenemos que

$$M_1 = 0$$

```haskell
potencia :: Num a => a -> Integer -> a
potencia a 0          = 1
potencia a n | even n = potencia a (n `div` 2) ^ 2
             | odd n  = a * potencia a ((n - 1) `div` 2) ^ 2
```

Figura 5.1. Un algoritmo rápido en HASKELL para calcular las potencias de un número. La expresión `potencia a n` se evalúa a `a ^ n`, asumiendo que `n` es un entero no negativo.

```python
def potencia(a, n):
    if n == 0:
        return 1
    elif n % 2 == 0:
        return potencia(a, n // 2) ** 2
    else:
        return a * potencia(a, (n - 1) // 2) ** 2
```

Figura 5.2. Un algoritmo rápido en PYTHON para calcular las potencias de un número. La expresión `potencia(a, n)` se evalúa a `a ** n`, asumiendo que `n` es un entero no negativo.

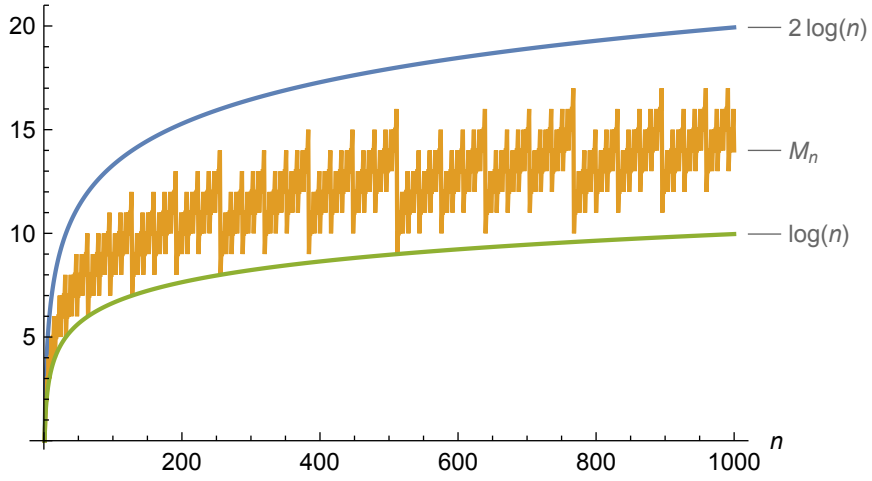


Figura 5.3. Un gráfico de la cantidad de multiplicaciones M_n que el algoritmo del Lema 5.4.20 hace al calcular α^n.

y para cada entero $n \geq 2$ que

$$M_n = \begin{cases} 1 + M_{n/2}, & \text{si } n \text{ es par;} \\ 2 + M_{(n-1)/2}, & \text{si } n \text{ es impar.} \end{cases}$$

Las primeras componentes de la sucesión $(M_n)_{n\geq 1}$ son

$$0,\ 0,\ 1,\ 2,\ 2,\ 3,\ 3,\ 4,\ 3,\ 4,\ 4,\ 5,\ 4,\ 5,\ 5,\ 6,\ 4,\ 5,\ 5,\ 6,\ 5,\ 6,\ 6,\ 7,\ 5,\ 6,\ 6,\ 7,\ 6,\ 7,\ 7,\ \ldots$$

Esta sucesión es bastante irregular —como puede verse en la Figura 5.3— pero podemos acotarla sin mucha dificultad.

5.4.22. Lema. *Para todo $n \in \mathbb{N}$ se tiene que $\log_2 n \leq M_n \leq 2 \log_2 n$.*

De acuerdo a esto, el algoritmo que se deduce del Lema 5.4.20 calcula $\alpha^{1\,000\,000}$ usando entre 20 y 40 multiplicaciones —ya que $\log_2 1\,000\,000 = 19{,}931\ldots$

Demostración. Cuando $n = 1$ la desigualdad es inmediata. Sea, por otro lado, $k \in \mathbb{N}$ tal que $k \geq 2$ y supongamos inductivamente que para todo entero i tal que $1 \leq i < k$ se tiene que $\log_2 n \leq M_n \leq 2 \log_2 n$. Dependiendo de la paridad de k tenemos dos casos.

Si k es par, entonces

$$M_k = 1 + M_{k/2} \leq 1 + 2 \log_2 \frac{k}{2} = 1 + 2 \log_2 k - 2 \log_2 2 \leq 2 \log_2 k,$$

ya que $1 - 2\log_2 2 = -1 \leq 0$, y

$$M_k = 1 + M_{k/2} \geq 1 + \log_2 \frac{k}{2} = 1 + \log_2 k - \log_2 2 = \log_2 k.$$

Si en cambio k es impar, tenemos que

$$\begin{aligned} M_k &= 2 + M_{(k-1)/2} \leq 2 + 2\log_2 \frac{k-1}{2} = 2 + 2\log_2(k-1) - 2\log_2 2 \\ &= 2\log_2(k-1) \leq 2\log_2 k \end{aligned}$$

y que

$$\begin{aligned} M_k &= 2 + M_{(k-1)/2} \geq 2 + \log_2 \frac{k-1}{2} = 2 + \log_2(k-1) - \log_2 2 \\ &= 1 + \log_2(k-1) \geq \log_2 k, \end{aligned}$$

ya que para todo número real $x \geq 2$ se tiene que $1 + \log_2(x-1) \geq \log_2 x$.

Vemos así que en cualquier caso se tiene que $\log_2 k \leq M_k \leq 2\log_2 k$, y el lema sigue por inducción. □

§5.5. Ejercicios

Una cota inferior exponencial para los números de Fibonacci

5.5.1. El Lema 5.4.3 nos dice que la sucesión de números de Fibonacci está acotada componente a componente superiormente por la sucesión $(2^n)_{n\geq 1}$, que crece exponencialmente. También podemos acotarla inferiormente:

Ejercicio. Muestre que existe un número real $a > 1$ tal que para todo entero $n \geq 3$ se tiene que $F_n \geq a^n$.

Subsucesiones de la sucesión de los números de Fibonacci

5.5.2. Ejercicio.

(*a*) Para cada entero $n \geq 2$ se tiene que

$$F_{2n} = 3F_{2(n-1)} - F_{2(n-2)}$$

y

$$F_{2n+1} = 3F_{2(n-1)+1} - F_{2(n-2)+1}.$$

(*b*) Sea $d \in \{0, 1, 2\}$. Para cada entero $n \geq 2$ se tiene que

$$F_{3n+d} = 4F_{3(n-1)+d} + F_{3(n-2)+d}.$$

5.5.3. Ejercicio.

(*a*) Existe $u \in \mathbb{Z}$ tal que para cada $d \in \{0, 1, 2, 3\}$ y cada entero $n \geq 2$ se tiene que

$$F_{4n+d} = uF_{4(n-1)+d} - F_{4(n-2)+d}.$$

(*b*) Existen $u, v \in \mathbb{Z}$ tal que para cada $d \in \{0, 1, 2, 3, 4\}$ y cada entero $n \geq 2$ se tiene que

$$F_{5n+d} = uF_{5(n-1)+d} + vF_{5(n-2)+d}.$$

Sumas de números de Fibonacci

5.5.4. El Lema 5.4.4 nos da el valor de la suma de los primeros números de Fibonacci. También podemos considerar la suma de los de índice par o impar:

Ejercicio. Si $n \in \mathbb{N}$, entonces

(*a*) $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$.

(*b*) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

5.5.5. Ejercicio. Para cada $n \in \mathbb{N}_0$ sean

$$A_n = F_0 + F_3 + \cdots + F_{3n},$$
$$B_n = F_1 + F_4 + \cdots + F_{3n+1},$$
$$C_n = F_2 + F_5 + \cdots + F_{3n+2}.$$

Para cada entero $n \geq 3$ se tiene que

$$A_n = 5A_{n-1} - 3A_{n-2} - A_{n-3},$$

$$C_n = 5C_{n-1} - 3C_{n-2} - C_{n-3}$$

y para cada entero $n \geq 2$ se tiene que

$$B_n = 4B_{n-1} + B_{n-2}.$$

La sumas de los cuadrados de los números de Fibonacci

5.5.6. El Lema 5.4.6 nos dice que la suma de los productos de los primeros pares de números de Fibonacci consecutivos es esencialmente el cuadrado de un número de Fibonacci. El siguiente resultado nos da el valor de una suma de cuadrados de números de Fibonacci:

Ejercicio. Para cada $n \in \mathbb{N}$ se tiene que $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$

Cocientes de números de Fibonacci

5.5.7. Ejercicio. Usando la identidad de Cassini 5.4.5 muestre que para todo $n \in \mathbb{N}$ es

$$\frac{F_{n+1}}{F_n} - \frac{F_n}{F_{n-1}} = \frac{(-1)^n}{F_{n-1}F_n}.$$

Deduzca de ello que la sucesión $(F_{2n}/F_{2n-1})_{n\geq 1}$ es creciente, que la sucesión $(F_{2n+1}/F_{2n})_{n\geq 1}$ es decreciente, que ambas tienen el mismo límite y que ese límite es el número $(1+\sqrt{5})/2$.

5.5.8. Ejercicio. Muestre que

$$\frac{F_3}{F_2} = 1+1, \qquad \frac{F_4}{F_3} = 1 + \frac{1}{1+1} \qquad \frac{F_5}{F_4} = 1 + \cfrac{1}{1+\cfrac{1}{1+1}} \qquad \frac{F_6}{F_5} = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+1}}}$$

y que, más generalmente, para cada entero $n \geq 2$ se tiene que

$$\frac{F_{n+1}}{F_n} = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}$$

con $n-2$ fracciones anidadas.

5.5.9. Ejercicio. Usando ahora la identidad de Catalan 5.4.9 estudie la sucesión de cocientes $(F_{n+r}/F_n)_{n\geq 1}$ para cada $r \in \mathbb{N}$.

Números de Lucas

5.5.10. Recordemos que la sucesión $(L_n)_{n\geq 0}$ de números de Lucas es la sucesión tal que

$$L_0 = 2,$$
$$L_1 = 1$$

y

$$L_n = L_{n-1} + L_{n-2}$$

para cada entero $n \geq 2$.

5.5.11. Ejercicio.

(a) $L_n = F_{n-1} + F_{n+1}$.
(b) $L_{2n} = L_n^2 + 2(-1)^n$.
(c) $F_{2n} = L_n F_n$.
(d) $F_{3n} = F_n(L_{2n} + (-1)^n)$.
(e) $F_{m+n} = \frac{1}{2}(F_m L_n + F_n L_m)$ y $F_{m-n} = \frac{1}{2}(-1)^n(F_m L_n - F_n L_m)$.
(f) $L_n^2 - 5F_n^2 = 4(-1)^n$.
(g) $\sum_{j=1}^{n} 2^{j-1} L_j = 2^n F_{n+1} - 1$.

5.5.12. Ejercicio. Si $n, m \in \mathbb{N}_0$ son tales que $m \leq n$, entonces

$$F_{n+m} = L_m F_n - (-1)^m F_{n-m}.$$

Observe que esto da una relación de recurrencia de orden dos para la sucesión

$$F_d,\ F_{m+d},\ F_{2m+d},\ F_{3m+d},\ F_{4m+d},\ \ldots$$

cada vez que $0 \leq d < m$. Esto generaliza los resultados de los ejercicios 5.5.4 y 5.5.5.

La razón áurea

5.5.13. Ejercicio. Sea $\alpha = (1+\sqrt{5})/2$.

(*a*) Para todo $n \in \mathbb{N}$ es $\alpha^n = \alpha F_n + F_{n-1}$ y $\alpha^n = \dfrac{L_n + F_n\sqrt{5}}{2}$.

(*b*) Para cada $n \in \mathbb{N}_0$ se tiene que

$$F_n = \left\lfloor \frac{\alpha^n}{\sqrt{5}} + \frac{1}{2} \right\rfloor.$$

Esto significa que F_n es el entero más cercano a $\alpha^n/\sqrt{5}$.

Cálculo rápido de los números de Fibonacci

5.5.14. La razón por la que las fórmulas de duplicación del Corolario 5.4.8 son importantes es que nos permiten calcular números de Fibonacci muy rápidamente. Así, por ejemplo, nos dice que

$$F_{100} = F_{50}(2F_{51} - F_{50})$$

y entonces para calcular F_{100} es suficiente que determinemos primero F_{50} y F_{51}. También tenemos que

$$F_{51} = F_{26}^2 - F_{25}^2, \qquad F_{50} = F_{25}(2F_{26} - F_{25}),$$

así que basta que encontremos F_{25} y F_{26}. Por supuesto, podemos iterar este proceso y usando el corolario encontrar las siguientes igualdades:

$$\begin{aligned}
&F_{26} = F_{13}(2F_{14} - F_{13}), && F_{25} = F_{13}^2 - F_{12}^2, && F_{14} = F_7(2F_8 - F_7),\\
&F_{13} = F_7^2 - F_6^2, && F_{12} = F_6(2F_7 - F_6), && F_8 = F_4(2F_5 - F_4),\\
&F_7 = F_4^2 - F_3^2, && F_6 = F_3(2F_4 - F_3), && F_5 = F_3^2 - F_2^2,\\
&F_4 = F_2(2F_3 - F_2), && F_3 = F_2^2 - F_1^2, && F_2 = F_1(2F_2 - F_1),\\
&F_1 = F_1^2 - F_0^2.
\end{aligned}$$

Esto significa que para calcular F_{100} podemos ir calculando en orden cada uno de los números

$$F_1,\ F_2,\ F_3,\ F_4,\ F_5,\ F_6,\ F_7,\ F_8,\ F_{12},\ F_{13},\ F_{14},\ F_{25},\ F_{26},\ F_{50},\ F_{51},\ F_{100}.$$

usando las igualdades que obtuvimos. De esta forma, vemos que podemos calcular F_{100} determinando solamente 15 otros números de Fibonacci y realizando unas 40 operaciones aritméticas. Esta idea puede extenderse a un algoritmo general. Veamos cómo.

Para cada $n \in \mathbb{N}_0$ sea P_n el par ordenado (F_n, F_{n+1}). La sucesiones de pares ordenados

$$P_0, P_1, P_2, \ldots$$

está determinada por una relación de recurrencia que permite calcular cada P_n en términos de $P_{\lfloor n/2 \rfloor}$:

Ejercicio. Muestre que $P_0 = (0,1)$ y que si $n \geq 1$, el par $P_{\lfloor n/2 \rfloor}$ es (a,b) y ponemos $c = a(2b-a)$ y $d = a^2 + b^2$, entonces

$$P_n = \begin{cases} (c,d), & \text{si } n \text{ es par;} \\ (d, c+d), & \text{si } n \text{ es impar.} \end{cases}$$

5.5.15. Ejercicio. Para cada $n \in \mathbb{N}_0$ llamemos $T(n)$ al número de sumas, diferencias y multiplicaciones que hacemos usando esta relación de recurrencia para calcular el par ordenado P_n usando esta relación de recurrencia. Mirando las fórmulas, claramente tenemos que

$$T(0) = 0$$

y

$$T(n) = \begin{cases} 6 + T(\tfrac{1}{2}n), & \text{si } n \text{ es par;} \\ 7 + T(\tfrac{1}{2}(n-1)), & \text{si } n \text{ es impar.} \end{cases}$$

Muestre que $T(n) \leq 10 \log_2 n$ para todo $n \geq 3$.

Esto implica, por ejemplo, que si calculamos $F_{1\,000\,000}$ determinando primero el par ordenado $P_{1\,000\,000}$ y nos quedamos luego con su primera componente, hacemos como mucho 200 operaciones aritméticas. Observemos que $F_{1\,000\,000}$ es un número de 208 988 cifras decimales.

$$F_{1\,000\,000} = \underbrace{19532821287077577316\cdots\cdots68996526838242546875}_{\text{208 988 dígitos}}$$

Si lo calculamos usando la recurrencia de orden dos que usamos para definir originalmente a los números de Fibonacci realizaremos un millón de sumas.

Hay que notar que muchas de esas 200 operaciones aritméticas son multiplicaciones y, más aún, multiplicaciones de números de muchos dígitos, así que hay que tener cuidado al comparar con el millón de sumas: multiplicar lleva bastante más tiempo que sumar. Hay, de todas formas, algoritmos muy rápidos para multiplicar números enteros — mucho más rápidos que el algoritmo que aprendemos de niños — y que entonces la determinación de un número como $F_{1\,000\,000}$ es factible. Los más conocido son el algoritmo de Karatsuba, descubierto por Anatoly Karatsuba en 1960 [KO1962], y el algoritmo de Schönhage–Strassen, de Arnold Schönhage y Volker Strassen, publicado en 1971 [SS1971]. Una extraodinariamente buena discusión sobre estps algoritmos puede encontrarse en el libro [Knu1969] de Donald Knuth.

Usando la implementación dada en la Figura 5.4 en la página siguiente, que es una transcripción directa a Haskell de la recurrencia del Ejercicio 5.5.14, podemos calcular $F_{1\,000\,000}$ en todo su

```
fibonacci :: Integer -> Integer
fibonacci n | n >= 0 = fst (fib n)

fib :: Integer -> (Integer, Integer)
fib 0         = (0, 1)
fib n
  | even n    = (c, d)
  | otherwise = (d, c + f)
  where (a, b) = fib (n `div` 2)
        c = a * (2 * b - a)
        d = a * a + b * b
```

Figura 5.4. Un algoritmo rápido en HASKELL para calcular números de Fibonacci, basado en la recurrencia del Ejercicio 5.5.14. La expresión `fib n` calcula el par ordenado P_n mientras que `fibonacci n` es la primera componente de ese par.

esplendor en 43 milisegundos.

Una cota inferior exponencial para los números de Catalan

5.5.16. Ejercicio. Para todo $n \in \mathbb{N}$ se tiene que $C_n \geq \dfrac{4^{n-1}}{n^2}$.

Un teorema de Zeckendorf

5.5.17. Ejercicio. Todo número natural puede escribirse como suma de números de Fibonacci distintos y no consecutivos. Por ejemplo,

$$278 = 1 + 2 + 8 + 34 + 233 = F_1 + F_3 + F_6 + F_9 + F_{13}.$$

Esta resultado —junto con la afirmación adicional de que esa escritura es única— es conocido como Teorema de Zeckendorf, por Edouard Zeckendorf, ya que este publicó ese resultado en su trabajo [Zec1972], aunque había sido encontrado antes por Cornelis Gerrit Lekkerkerker en 1952.

Capítulo 6

Divisibilidad

§6.1. La relación de divisibilidad

6.1.1. Si a y b son enteros, decimos que b ***divide*** a a, que b es un ***divisor*** de a y que a es un ***múltiplo*** de b, si existe un tercer entero c tal que $a = bc$ y en ese caso escribimos $b \mid a$. Obtenemos de esta forma una relación $\mid$ en el conjunto $\mathbb{Z}$ de los números enteros.

6.1.2. Una primera observación que podemos hacer es la siguiente.

Proposición.
(*i*) *Para todo* $a \in \mathbb{Z}$ *se tiene que* $1 \mid a$ *y que* $a \mid 0$.
(*ii*) *Si* a *y* b *son dos enteros tales que* $b \mid a$, *entonces también* $(-b) \mid a$, $b \mid (-a)$ *y* $(-b) \mid (-a)$.

En vista de esta segunda afirmación normalmente nos concentramos en estudiar la divisibilidad entre enteros no negativos.

Demostración. (*i*) Si a es un elemento de $\mathbb{Z}$, entonces $a = 1 \cdot a$ y $0 = a \cdot 0$ y, por lo tanto, $a \mid a$ y $a \mid 0$, como queremos.

(*ii*) Sean a y b dos elementos de $\mathbb{Z}$ tales que $b \mid a$, de manera que existe $c \in \mathbb{Z}$ tal que $a = bc$. Se sigue inmediatamente de eso que $a = (-b)c$, $(-a) = b(-c)$ y $(-a) = (-b)c$ y, por lo tanto, que $(-b) \mid a$, que $b \mid (-a)$ y que $(-b) \mid (-a)$. □

6.1.3. La relación de divisibilidad en $\mathbb{Z}$ no es una relación de orden porque no es anti-simétrica — por ejemplo, los números 3 y −3 se dividen mutuamente y son distintos. De todas formas, no está muy lejos de serlo y si la restringimos al conjunto $\mathbb{N}$ o $\mathbb{N}_0$, entonces ese problema desaparece.

Proposición.

(*i*) *La relación* $\mid$ *de divisibilidad en* $\mathbb{Z}$ *es reflexiva, transitiva y para cada* $a, b \in \mathbb{Z}$ *se tiene que*

$$a \mid b,\ b \mid a \implies a = b \text{ o } a = -b. \tag{1}$$

(*ii*) *La restricción de la relación* $\mid$ *de divisibilidad a* $\mathbb{N}$ *o a* $\mathbb{N}_0$ *es una relación de orden, es decir, es reflexiva, transitiva y anti-simétrica.*

Como se trata de una relación de orden en $\mathbb{N}$, podemos restringirla a cualquier subconjunto de $\mathbb{N}$ y obtener una relación de orden. En la Figura 6.1 en la página siguiente dibujamos el diagrama de Hasse de su restricción al conjunto de todos los divisores de 360.

Demostración. (*i*) Si a es un elemento de $\mathbb{Z}$, entonces $a = a \cdot 1$ y, por lo tanto, $a \mid a$: esto nos dice que la relación de divisibilidad es reflexiva. Por otro lado, si a, b y c son enteros y se tiene que $a \mid b$ y $b \mid c$, de manera que existen enteros x e y tales que $b = ax$ y $c = by$, entonces claramente $c = axy$ y esto nos dice que $a \mid c$: vemos así que la relación $\mid$ es transitiva.

Sean ahora a y b dos elementos de $\mathbb{Z}$ y supongamos que $a \mid b$ y que $b \mid a$, de manera que existen enteros c y d tales que $b = ac$ y $a = bd$. Tenemos entonces que $a = acd$, es decir, que

$$a(1 - cd) = 0. \tag{2}$$

Si $a = 0$, entonces $b = ac = 0c = 0$ y a y b son iguales. Si en cambio $a \neq 0$, entonces de la igualdad (2) se deduce que $1 - cd = 0$, esto es, que $cd = 1$ y, por lo tanto, que $c = 1$ o $c = -1$. Correspondiendo a esas dos posibilidades tenemos que $b = a \cdot 1 = a$ o que $b = a \cdot (-1) = -a$. Esto prueba la implicación (1).

(*ii*) La restricción de la relación $\mid$ a $\mathbb{N}$ o a $\mathbb{N}_0$ es reflexiva y transitiva porque la relación original en $\mathbb{Z}$ lo es, como acabamos de mostrar. Nos queda entonces probar que es anti-simétrica. Sean a y b dos elementos de $\mathbb{N}_0$ tales que $a \mid b$ y $b \mid a$. Como en $\mathbb{Z}$ vale la implicación (1), tenemos que $a = b$ o $a = -b$. Como a y b no negativo, esto solo puede ocurrir si son, de hecho, los dos nulos y, en particular, iguales. Esto prueba que la relación de divisibilidad en $\mathbb{N}_0$ es anti-simétrica, y esto implica inmediatamente que también lo es en $\mathbb{N}$. □

6.1.4. Usaremos muchas veces la siguiente observación, que establece una relación entre la relación de divisibilidad y la del orden usual de los números enteros:

Proposición. *Sean* a *y* b *dos enteros. Si* $b \mid a$ *y* $a \neq 0$*, entonces* $|b| \leq |a|$.

Notemos que la hipótesis de que el entero a no sea nulo es necesaria para alcanzar la conclusión de la proposición: por ejemplo, es $1 \mid 0$ pero ciertamente no vale que $1 \leq 0$.

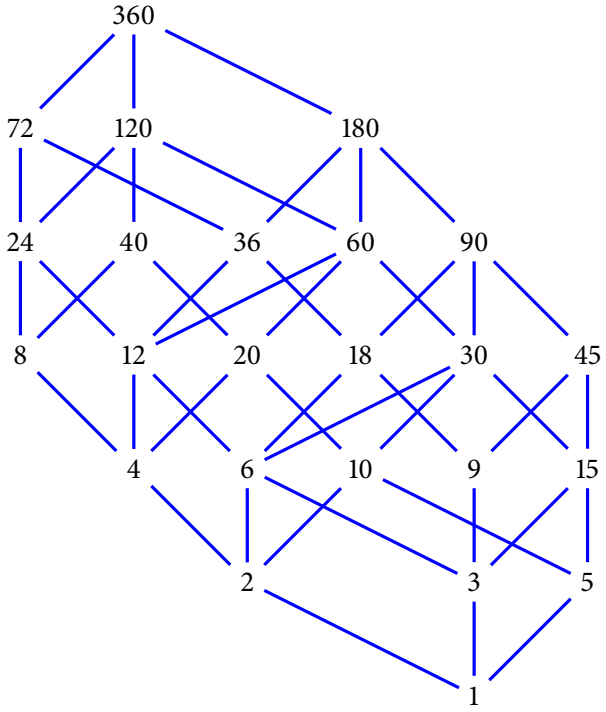


Figura 6.1. El diagrama de Hasse de la relación de divisibilidad restringida al conjunto de los divisores positivos de 360.

Demostración. Supongamos que b divide a a, de manera que hay un entero c tal que $a = bc$. De esto se sigue que $|a| = |b||c|$. Si $a \neq 0$, entonces tiene que ser $c \neq 0$ y, por lo tanto, como c es un entero, $|c| \geq 1$: tenemos entonces que $|a| = |b||c| \geq |b|$, como afirma la proposición. □

6.1.5. Otra propiedad básica de la divisibilidad es su compatibilidad con las operaciones aritméticas:

Proposición. *Sean a, b y c tres enteros.*
(*i*) *Si c divide a a y b, entonces también divide a $a + b$ y a $a - b$.*
(*ii*) *Si c divide a a, entonces también divide a ab.*

Las recíprocas de estas dos afirmaciones son falsas. Por ejemplo, 2 divide a $5 + 3$ y a $5 + 3$ pero no divide ni a 5 ni a 2. De manera similar, 6 divide a $4 \cdot 3$ pero no divide a ninguno de los dos factores. Hay, de todas formas, una situación importante en la que sí podemos garantizar que la implicación recíproca de la de (*ii*) vale: nos ocuparemos de eso en la Proposición 9.2.2 más adelante.

Demostración. (i) Supongamos que c divide a a y a b, de manera que hay enteros x e y tales que $a = cx$ y $b = cy$. En ese caso tenemos que $a + b = cx + cy = c(x + y)$ y $a - b = cx - cy = c(x - y)$: como claramente $x + y$ y $x - y$ son enteros, esto nos dice que c divide a $a + b$ y a $a - b$. La primera afirmación de la proposición queda así probada.

(i) Supongamos ahora que c divide a a, de manera que hay un entero x tal que $a = cx$. Por supuesto, esto implica que $ab = cbx$ y, por lo tanto, que c divide a ab. □

6.1.6. Muchas veces usaremos la Proposición 6.1.5 vía el siguiente corolario:

Corolario. *Sean a, b y c tres enteros. Si c divide a a y a $a + b$, entonces también divide a b.*

Demostración. En efecto, en ese caso de la proposición se sigue que c divide a $(a + b) - a = b$. □

§6.2. El algoritmo de la división

6.2.1. Si a y b son enteros y b divide a a, entonces hay otro entero c tal que $a = bc$. Cuando b *no* divide a a, esto no es cierto, por supuesto. La Proposición 6.2.3 que probaremos más abajo nos permite describir exactamente qué sucede en el caso general.

6.2.2. Antes de eso, hagamos una observación que nos será útil varias veces:

Lema. *Sea $b \in \mathbb{N}$ y sean $i, j \in \mathbb{Z}$. Si $0 \leq i, j < b$ y $b \mid i - j$, entonces $i = j$.*

Demostración. Supongamos que $0 \leq i, j < b$ y $b \mid i - j$. Tenemos entonces que

$$-b < 0 - j \leq i - j < b - j \leq b,$$

así que $|i - j| < b$. Por otro lado, como b divide a $i - j$, de la Proposición 6.1.4 sabemos que o bien $i - j = 0$ o bien $|b| \leq |i - j|$. La segunda de estas dos posibilidades no puede ocurrir, así que debe ocurrir la primera: esto nos dice que $i = j$, como afirma el lema. □

6.2.3. La siguiente proposición establece una propiedad fundamental de los números enteros:

Proposición. *Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Hay enteros q y r tales que $a = qb + r$ y $0 \leq r < b$ y, más aún, estos enteros q y r están unívocamente determinados por a y b.*

Llamamos a q y a r el ***cociente*** y el ***resto*** de la ***división*** de a por b, respectivamente.

Demostración. Consideremos el conjunto

$$S \coloneqq \{a - kb : k \in \mathbb{Z}, a - kb \geq 0\}.$$

Este conjunto no es vacío: si $a \geq 0$, entonces $a - 0 \cdot b = a \geq 0$, así que $a \in S$, y si en cambio $a < 0$, entonces $a - (2a)b = (1 - 2b)a \geq 0$, así que $a - (2a)b \in S$. Como S está claramente contenido en $\mathbb{N}_0$, podemos considerar su mínimo $r \coloneqq \min S$.

Como r pertenece a S, es $r \geq 0$ y existe $q \in \mathbb{Z}$ tal que $r = a - qb$, es decir, tal que $a = qb + r$. Mostremos que $r < b$. Supongamos por un momento que esto no es así, de manera que $r \geq b$ y, por lo tanto, $a - (q+1)b = r - b \geq 0$. Como consecuencia de esto, tenemos que $r - b \in S$: esto es absurdo, ya que $r - b$ es estrictamente menor que r, porque b es positivo, y r es el menor elemento de S. Vemos así que $a = qb + r$ y que $0 \leq r < b$, y esto prueba la afirmación de existencia del enunciado. Veamos la de unicidad.

Supongamos que q, r, q' y r' son enteros tales que

$$a = qb + r, \qquad 0 \leq r < b, \tag{3}$$

y

$$a = q'b + r, \qquad 0 \leq r' < b. \tag{4}$$

Observemos que

$$qb + r = q'b + r' \tag{5}$$

y, por lo tanto, que $r - r' = (q' - q)b$. En particular, b divide a $r - r'$: como $0 \leq r, r' < b$, de acuerdo al Lema 6.2.2 tenemos entonces que $r = r'$. Usando esto en (5), concluimos que $qb = q'b$ y, en consecuencia, que $(q - q')b = 0$. Como $b \neq 0$, esto nos dice que $q - q' = 0$, esto es, que $q = q'$. Así, si se cumplen las condiciones (3) y (4) se tiene necesariamente que $q = q'$ y que $r = r'$: esto prueba la afirmación de unicidad de la proposición. □

6.2.4. El siguiente corolario de la proposición es casi inmediato y muestra que podemos ver al resto de la división de un número por otro, en cierta forma, como la única "obstrucción" a la divisibilidad.

Corolario. *Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. El resto de la división de a por b es 0 si y solamente si b divide a a.*

Demostración. Sean q y r el cociente y el resto, respectivamente, de la división de a por b, de manera que $a = qb + r$ y $0 \leq r < b$. Observemos que es $|r| < b$.

Si $r = 0$, entonces tenemos que $a = qb$ y, por lo tanto, que b divide a a. Supongamos, para probar la implicación recíproca, que b divide a a. Hay entonces un entero c tal que $a = bc$ y, por lo

tanto, $bc = qb + r$. De esta igualdad vemos que $r = (c - q)b$, así que, en particular, b divide a r y, de acuerdo a la Proposición 6.1.4, o bien $r = 0$ o bien $|b| \leq |r|$. Esta segunda posibilidad no ocurre — en efecto, sabemos que $|r| < b = |b|$ — así que necesariamente $r = 0$. Esto prueba el corolario. □

6.2.5. Una observación importante que debemos hacer es que si $a \in \mathbb{Z}$ y $b \in \mathbb{N}$ siempre podemos encontrar de manera efectiva al cociente q y al resto r de la división de a por b. En la base de esto esta la siguiente descripción alternativa de ese cociente:

Lema. *Sea a un entero no negativo. El conjunto $T \coloneqq \{k \in \mathbb{N}_0 : a - kb \geq 0\}$ es no vacío y finito, y su elemento máximo es el cociente de la división de a por b.*

Demostración. El conjunto T no es vacío, ya que contiene a 0. Por otro lado, si $k \in T$, entonces $a - kb \geq 0$ y, por lo tanto, $k \leq a/b$: esto nos dice que el conjunto T está contenido en $\{0, \ldots, \lfloor a/b \rfloor\}$ y, en particular, que es finito. Tiene entonces sentido considerar su elemento máximo $q \coloneqq \max T$. Pongamos además $r \coloneqq a - qb$.

Como $q \in T$, es $r \geq 0$. Tiene que ser $r < b$: si no fuese ese el caso, tendríamos que

$$a - (q + 1)b = a - qb - b = r - b \geq 0$$

y, por lo tanto, que $q + 1 \in T$: esto es absurdo, ya que elegimos a q como el mayor elemento de T. Concluimos de esta manera que $a = qb + r$ y que $0 \leq r < b$. De acuerdo a la Proposición 6.2.3, se sigue de esto que q y r son el cociente y el resto de la división de a por b y esto prueba el lema. □

6.2.6. Este lema nos dice cómo encontrar el cociente y el resto de la división de un entero cualquiera a por un entero positivo b.

- Si a es positivo, este lema nos dice que para buscar el cociente y el resto de la división de a por b podemos proceder de la siguiente manera: para cada número $i \in \mathbb{N}_0$ desde 0 en adelante, en orden, calculamos $a - (i + 1)b$ y paramos la primera vez que esa diferencia sea negativa: el cociente entonces es i y el resto es $a - ib$.
- Si en cambio a es negativo, podemos usar este procedimiento para encontrar el cociente q y el resto r de la división de $-a$ por b, de manera que $-a = qb + r$ y $0 \leq r < b$. Si $r = 0$, entonces tenemos que $a = (-q)b$, así que $-q$ y 0 son el resto y el cociente de dividir a a por b; si en cambio $r \neq 0$, entonces es $a = (-q - 1)b + (b - r)$ y $0 \leq b - r < b$, así que $-q - 1$ y $b - r$ son el resto y el cociente de esa división.

En la Figuras 6.1 y 6.2 damos implementaciones de este algoritmo en Haskell y en Python. Es de notar que virtualmente todos los lenguajes de programación proveen herramientas para calcular el cociente y el resto de la división entre dos enteros, usando algoritmos mucho más eficientes que este. Así, en Haskell, por ejemplo, tenemos las funciones `div` y `mod` que hacen precisamente

eso: las expresiones `div a b` y `mod a b` denotan, respectivamente, el cociente y el resto de dividir a `a` por `b` cuando `b` es positivo.

```haskell
division :: Integer -> Integer -> (Integer, Integer)
division a b
  | a >= 0   = buscar 0
  | a < 0    = let (q, r) = division (-a) b
               in if r == 0 then (-q, 0) else (-1 - q, b - r)
  where buscar i
          | a - (i + 1) * b >= 0   = buscar (i + 1)
          | otherwise              = (i, a - i * b)
```

Programa 6.1. Un implementación del algoritmo de la división en Haskell. La expresión `division a b` se evalúa a un par ordenado `(q, r)` en el que `q` y `r` son, respectivamente, el cociente y el resto de la división de `a` por `b`.

```python
def division(a, b):
    if a >= 0:
        i = 0
        while a - (i + 1) * b >= 0:
            i = i + 1
        return (i, a - i * b)
    else:
        q, r = division(-a, b)
        if r == 0:
            return (-q, 0)
        else:
            return (-1 - q, b - r)
```

Programa 6.2. Un implementación del algoritmo de la división en Python. La expresión `division(a, b)` se evalúa a un par ordenado `(q, r)` en el que `q` y `r` son, respectivamente, el cociente y el resto de la división de `a` por `b`.

§6.3. La notación posicional

6.3.1. Una aplicación simple pero importante de la Proposición 6.2.3 de la sección anterior es el siguiente resultado, que está en base de la forma en que escribimos normalmente los números.

Proposición. *Sea b un entero tal que $b \geq 2$. Si a es un entero positivo, entonces existen $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ tales que*

$$a = d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k$$

y $d_k \neq 0$.

Demostración. Para cada entero positivo a sea $P(a)$ la afirmación

$$\text{existen } k \in \mathbb{N}_0 \text{ y } d_0, \ldots, d_k \in \{0, \ldots, b-1\} \text{ tales que } a = \textstyle\sum_{i=0}^{k} d_i b^i \text{ y } d_k \neq 0.$$

Probaremos haciendo inducción con respecto a a que $P(a)$ vale cualquiera sea $a \in \mathbb{N}$.

- Si $a = 1$, claramente podemos elegir $k = 0$ y $d_0 = 1$ para tener $a = \sum_{i=0}^{k} d_i b^i$, y esto prueba que vale la afirmación $P(1)$.
- Sea ahora a un elemento cualquiera de $\mathbb{N}$ y supongamos que cada una de las afirmaciones $P(1), P(2), \ldots, P(a)$ vale. De acuerdo a la Proposición 6.2.3, existen enteros q y r tales que $a+1 = qb + r$ y $0 \leq r < b$. Como $q = (a+1-r)/b \leq (a+1)/b$ y $b \geq 2$, tenemos que $q < a+1$.

  Si $q = 0$, entonces $a = r$ y podemos elegir $k = 0$ y $d_0 = r$ para ver que $P(a+1)$ vale. Supongamos entonces que $q > 0$. En ese caso, nuestra hipótesis inductiva nos dice que $P(q)$ vale, es decir, que existen $l \in \mathbb{N}_0$ y $e_0, \ldots, e_l \in \{0, \ldots, b-1\}$ tales que $q = \sum_{i=0}^{l} e_i b^i$ y $e_l \neq 0$. Como consecuencia de esto tenemos que

  $$a + 1 = r + qb = r + \left(\sum_{i=0}^{l} e_i b^i \right) b = r + \sum_{i=0}^{l} e_i b^{i+1} = r + \sum_{i=1}^{l+1} e_{i-1} b^i.$$

  Podemos entonces elegir $k = l+1$, $d_0 = r$ y $d_i = e_{i-1}$ para cada $i \in \{1, \ldots, k\}$ para tener $a + 1 = \sum_{i=0}^{k} d_i b^i$ y $d_k \neq 0$, y esto muestra que vale la afirmación $P(a+1)$ también en este caso.

La inducción queda así completa y eso prueba la proposición. □

6.3.2. Queremos probar ahora que los números k y $d_0, \ldots, d_k$ de la Proposición 6.3.1 están bien determinados por los números b y a con los que empezamos.

Proposición. *Sea b es un entero tal que $b \geq 2$. Si a es un entero positivo, entonces hay exactamente* una *forma de elegir $k \in \mathbb{N}$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que se cumplan las dos condiciones de la Proposición 6.3.1.*

Demostración. Sean $k, l \in \mathbb{N}_0$ y $d_0, \ldots, d_k, e_0, \ldots, e_l \in \{0, \ldots, b-1\}$ tales que

$$d_0 + d_1 b + \cdots + d_k b^k = a = e_0 + e_1 b + \cdots + e_l b^l, \tag{6}$$

$d_k \neq 0$ y $e_l \neq 0$. Probaremos que en esta situación necesariamente se tiene que $k = l$ y que $d_i = e_i$ para todo $i \in \{0, \ldots, k\}$: la proposición es consecuencia inmediata de esto. Observemos que sin pérdida de generalidad podemos suponer que $k \leq l$.

De la igualdad (6) se deduce que

$$d_0 - e_0 = \sum_{i=1}^{l} e_i b^i - \sum_{i=1}^{k} d_i b^i = \left(\sum_{i=1}^{l} e_i b^{i-1} - \sum_{i=1}^{k} d_i b^{i-1} k \right) b,$$

así que $b \mid d_0 - e_0$. Como $0 \leq d_0, e_0 < b$, el Lema 6.2.2 nos permite concluir que $d_0 = e_0$.

Vemos así que el conjunto

$$S \coloneqq \left\{ i \in \{0, \ldots, k\} : d_j = e_j \text{ para cada } j \in \{0, \ldots, i\} \right\}$$

no es vacío y podemos, por lo tanto, considerar su máximo $m \coloneqq \max S$. Tenemos entonces que $m \in S$, de manera que

$$d_j = e_j \text{ para cada } j \in \{0, \ldots, m\},$$

y que o bien $m = k$ o bien $m < k$ y $d_{m+1} \neq e_{m+1}$.

Supongamos que estamos en el segundo de estos dos casos. De la igualdad (6), tenemos que

$$\begin{aligned} 0 &= \sum_{i=0}^{l} e_i b^i - \sum_{i=0}^{k} d_i b^i = \sum_{i=m+1}^{l} e_i b^i - \sum_{i=m+1}^{k} d_i b^i \\ &= e_{m+1} - d_{m+1} + b \left(\sum_{i=m+1}^{l} e_i b^{i-1} - \sum_{i=m+1}^{k} d_i b^{i-1} \right). \end{aligned}$$

Como la expresión entre paréntesis es un entero, esto nos dice que b divide a $d_{m+1} - e_{m+1}$. Como además $0 \leq d_{m+1}, e_{m+1} < b$, el Lema 6.2.2 nos dice que $d_{m+1} = e_{m+1}$: esto es absurdo, ya que contradice nuestra hipótesis.

Debe ser entonces necesariamente $m = k$. Así, todos los sumandos que aparecen a la izquierda de la igualdad (6) también aparecen a la derecha y, por lo tanto, esa igualdad implica que

$$0 = \sum_{i=k+1}^{l} e_i b^i.$$

Si $k < l$, en esta suma cada uno de los términos de esta última suma es no negativo y el último, $e_l b^l$, positivo: esto es imposible. Podemos concluir entonces que $k = l$. Ahora bien, que los tres números m, l y k sean iguales significa precisamente que vale lo que queremos, y esto completa la prueba de la proposición. □

6.3.3. Si b es un entero tal que $n \geq 2$ y a un entero positivo, las Proposiciones 6.3.1 y 6.3.2 nos dicen que hay exactamente una forma de elegir $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que $a = \sum_{i=0}^{k} d_i b^i$ y $d_k \neq 0$. Escribimos en ese caso

$$a = (d_k, d_{k-1}, \ldots, d_1, d_0)_b.$$

Llamamos a esto la ***representación en base b*** del número a y a los números $d_k, \ldots, d_0$ los ***dígitos*** de a en base b. Cuando b es 10, 2, 8 o 16, decimos ***representación decimal***, ***binaria***, ***octal*** o ***hexadecimal*** en lugar de representación en base b. Así, por ejemplo, es fácil verificar que

$$1234 = (5, 4, 1, 4)_6 = (1, 6, 2, 1)_9 = (1, 18, 19)_{27} = (1, 0)_{1234} = (1234)_{10\,000}.$$

6.3.4. Notemos que solo hablamos de los dígitos en base b de un número cuando la base b es al menos 2. No tiene sentido hablar de los dígitos en base 1 de un número positivo a: de acuerdo a la definición, deberíamos podemos escribir a a en la forma

$$d_0 + d_1 \cdot 1 + \cdots + d_k \cdot 1^k$$

con $d_0, \ldots, d_k \in \{0\}$, pero esto es claramente imposible.

De todas formas, en varios contextos — como la teoría de la computabilidad — es usual hablar de la «escritura en base 1» de un número». Por esto nos referimos a lo siguiente: si a es un entero positivo, entonces la escritura en base 1 de a es la expresión

$$\underbrace{111\cdots111}_{a \text{ veces}}$$

con a unos. Así, por ejemplo,

11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

es la escritura en base 1 de 85. No es evidente que esto pueda llegar a tener alguna utilidad, ciertamente! Varios sistemas de escritura originalmente usaron ideas parecidas. Por ejemplo, los siguientes son los símbolos usados para escribir los números 1, 2 y 3 en chino, inclusive hoy en día, y en notación romana:

I II III

Es importante tener en cuenta, de todas formas, que esto no es un caso particular de la noción de «escritura en base b» que describimos arriba.

```haskell
digitos :: Integer -> Integer -> [Integer]
digitos a b
  | q == 0    = [r]
  | otherwise = r : digitos q b
  where q = a `div` b
        r = a `mod` b
```

Programa 6.3. Una implementación en HASKELL del algoritmo para obtener los dígitos de un entero positivo `a` en base `b`. El resultado es una lista de los dígitos, desde el menos significativo en adelante. Por ejemplo, `digitos 123 10` denota `[3, 2, 1]`.

6.3.5. Estudiando la demostración que dimos para la Proposición 6.3.1 se hace aparente que nos da método efectivo para encontrar los dígitos de un número entero positivo con respecto a una base. En efecto, supongamos que a y b son enteros positivos y que $b \geq 2$. Sean q y r el cociente y el resto de dividir a a por b. Si el cociente q es nulo, entonces $r \neq 0$ porque $a \neq 0$ y, por lo tanto, claramente es

$$a = (r)_b.$$

Si en cambio el cociente q no es nulo, y conocemos los dígitos de q en base b, de manera que conocemos $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que $d_k \neq 0$ y

$$q = (d_k, d_{k-1}, \ldots, d_1, d_0)_b, \tag{7}$$

entonces

$$a = (d_k, d_{k-1}, \ldots, d_1, d_0, r)_b. \tag{8}$$

En efecto, la igualdad (7) nos dice que $q = d_0 + d_1 b + \cdots + d_k b^k$, así que

$$a = r + qb = r + (d_0 + d_1 b + \cdots + d_k b^k)b = r + d_0 b + d_1 b^2 + \cdots + d_k b^{k+1}$$

y, como $d_k \neq 0$, esto significa que la igualdad (8) vale.

En las Figuras 6.3 y 6.4 damos implementaciones de esta idea en HASKELL y en PYTHON, respectivamente. Todos los lenguajes de programación proveen alguna forma de imprimir números y todos usan exactamente este algoritmo para encontrar sus dígitos.

```
def digitos(a, b):
    q = a // b
    r = a % b
    if q == 0:
        return [r]
    else:
        return [r] + digitos(q, b)
```

Programa 6.4. Una implementación en PYTHON del algoritmo para obtener los dígitos de un entero positivo `a` en base `b`. Como antes, el resultado es una lista de los dígitos, desde el menos significativo en adelante.

§6.4. Máximo común divisor

6.4.1. Sean a y b dos enteros y supongamos que no son los dos nulos. Un ***divisor común*** de a y b es simplemente un entero d que es tanto un divisor de a como de b. Escribimos $D(a,b)$ al conjunto de todos los divisores comunes *positivos* de a y b.

Este conjunto $D(a,b)$ no es vacío: en efecto, el número 1 pertenece a $D(a,b)$. Por otro lado, si $d \in D(a,b)$, entonces de la Proposición 6.1.4 tenemos que o bien $a = 0$ o bien $d \leq |a|$, y que o bien $b = 0$ o bien $d \leq |b|$. Como a y b no son los dos nulos, se sigue de esto que $d \leq \max\{|a|,|b|\}$. En otras palabras, si ponemos $N \coloneqq \max\{|a|,|b|\}$, entonces $D(a,b) \subseteq \{1,\dots,N\}$. Vemos así que el conjunto $D(a,b)$ es finito y, en particular, que podemos considerar su elemento máximo: lo llamamos ***máximo común divisor*** de a y b y lo escribimos $\mathsf{mcd}(a,b)$.

Esto define el máximo común divisor de dos números que no son simultáneamente nulos. Si, por el contrario, es $a = b = 0$, entonces todo elemento de $\mathbb{N}$ es un divisor común positivo de a y b y, por lo tanto, no tiene sentido hablar en este caso del elemento máximo de $D(a,b)$. En este caso especial definimos $\mathsf{mcd}(0,0) \coloneqq 0$.

6.4.2. Decimos que dos enteros a y b son ***coprimos*** cuando $\mathsf{mcd}(a,b) = 1$. Esta condición significa, precisamente, que no son ambos nulos y que el único divisor común positivo que tienen es 1. Así, por ejemplo, 2 y 3 son números coprimos, mientras que 6 y 15 no lo son.

6.4.3. El máximo común divisor de dos enteros es un elemento de $\mathbb{N}_0$ y es nulo si y solamente si esos dos enteros son nulos: esto es consecuencia inmediata de la definición. Otras observaciones sencillas que podemos hacer son las siguientes:

Proposición. *Sean a y b dos enteros.*

(*i*) *Es* $\mathsf{mcd}(a,b) = \mathsf{mcd}(b,a)$.

(*ii*) *Es* $\mathsf{mcd}(a,b) = |a|$ *si y solamente si a divide a b.*

(*iii*) *En particular, cualquiera sea a se tiene que* $\mathsf{mcd}(a, 0) = |a|$.
(*iv*) *Se tiene que* $\mathsf{mcd}(a, b) = \mathsf{mcd}(-a, b) = \mathsf{mcd}(a, -b) = \mathsf{mcd}(-a, -b)$.

Demostración. (*i*) Si $a = b = 0$, entonces es evidente que $\mathsf{mcd}(a, b) = \mathsf{mcd}(b, a)$. Si en cambio alguno de a o b es no nulo, entonces los conjuntos $D(a, b)$ y $D(b, a)$ coinciden, así que tienen el mismo elemento máximo: esto significa, precisamente, que $\mathsf{mcd}(a, b) = \mathsf{mcd}(b, a)$ también en este caso.

(*ii*) Supongamos primero que a divide a b. Si $a = 0$, entonces también $b = 0$ y la igualdad $\mathsf{mcd}(a, b) = |a|$ es evidente. Supongamos entonces que $a \neq 0$. Si $d \in D(a, b)$, entonces d divide a a y, de acuerdo a la Proposición **6.1.4**, se tiene que $d \leq |a|$. Como además $|a| \in D(a, b)$, vemos que $|a|$ es el elemento máximo del conjunto $D(a, b)$, es decir, que $|a| = \mathsf{mcd}(a, b)$. Esto muestra que la condición del enunciado es suficiente.

Veamos que es necesaria. Supongamos que $\mathsf{mcd}(a, b) = |a|$. Si $b = 0$, entonces a divide a b independientemente de nuestra hipótesis, así que supongamos que $b \neq 0$. En ese caso, $\mathsf{mcd}(a, b)$ es el elemento máximo del conjunto $D(a, b)$, y esto significa que, en particular, $|a|$ divide a b, así que a divide a b.

(*iii*) Como $a \mid 0$, esto es consecuencia de (*ii*).

(*iv*) Si $a = b = 0$, lo que afirma el enunciado es evidente. Si en cambio alguno de a o b es no nulo, entonces los conjuntos $D(a, b)$, $D(-a, b)$, $D(a, -b)$ y $D(-a, -b)$ coinciden y, por lo tanto, tienen el mismo elemento máximo. □

6.4.4. La siguiente propiedad es fundamental:

Proposición. *Si a, b y c son tres enteros, entonces*

$$\mathsf{mcd}(a - cb, b) = \mathsf{mcd}(a, b), \qquad \mathsf{mcd}(a, b - ca) = \mathsf{mcd}(a, b).$$

Demostración. En vista de la Proposición **6.4.3**(*i*) es suficiente que mostremos la primera de las igualdades del enunciado. Sean a, b y c tres enteros. Si b es cero, entonces esa igualdad evidente. Supongamos entonces que $b \neq 0$. Afirmamos que

$$D(a, b) = D(a - cb, b). \tag{9}$$

En efecto, si $d \in D(a, b)$, entonces d es un entero positivo que divide a a y a b y, por lo tanto, divide a $a - bc$ y a b: esto significa que $d \in D(a - cb, b)$. Recíprocamente, si $d \in D(a - cb, b)$, entonces d es un entero positivo que divide a $a - cb$ y a b, y por lo tanto divide a $a = (a - cb) + cb$ y a b, así que pertenece a $D(a, b)$.

De la igualdad (9) se deduce que

$$\mathsf{mcd}(a, b) = \mathsf{máx}\, D(a, b) = \mathsf{máx}\, D(a - cb, b) = \mathsf{mcd}(a - cb, b)$$

y esto prueba la proposición. □

6.4.5. Una de las razones por las que la Proposición 6.4.4 es importante es que está en la base de un algoritmo para calcular el máximo común divisor de dos enteros.

En vista de la Proposición 6.4.3(*iv*), es suficiente que veamos cómo hacer esto cuando los dos enteros son no negativos. Supongamos entonces que a y b son dos enteros no negativos y que, por ejemplo, $a \geq b$. Si $b = 0$, entonces sabemos que $\mathsf{mcd}(a, b) = a$ y no es necesario hacer más nada. Si en cambio $b > 0$, entonces podemos dividir a a por b. Sean q y r el cociente y el resto, respectivamente. Como $a = qb + r$, la Proposición 6.4.4 nos dice que

$$\mathsf{mcd}(a, b) = \mathsf{mcd}(a - qb, b) = \mathsf{mcd}(r, b).$$

Notemos que r y b son dos enteros no negativos y que $a + b > r + b$, ya que $a \geq b > r$. De esta forma redujimos el cálculo del máximo común divisor de dos números no negativos al del máximo común divisor de otros dos cuya suma es menor que la de los originales. Podemos repetir este procedimiento: cada vez que lo hacemos la suma de los dos números decrece y es positiva, así que el proceso tiene que terminar.

Veamos un ejemplo. Para calcular $\mathsf{mcd}(385, 150)$, observamos que el cociente y el resto de la división de 385 por 150 son 2 y 85, respectivamente, de manera que $385 = 2 \cdot 150 + 85$ y entonces

$$\mathsf{mcd}(385, 150) = \mathsf{mcd}(385 - 2 \cdot 150, 150) = \mathsf{mcd}(85, 150).$$

Tenemos que calcular ahora $\mathsf{mcd}(85, 150)$. Es $150 = 1 \cdot 85 + 65$, así que

$$\mathsf{mcd}(85, 150) = \mathsf{mcd}(85, 150 - 1 \cdot 85) = \mathsf{mcd}(85, 65).$$

Otra vez, dividiendo vemos que $85 = 1 \cdot 65 + 20$ y, por lo tanto, que

$$\mathsf{mcd}(85, 65) = \mathsf{mcd}(85 - 1 \cdot 65, 65) = \mathsf{mcd}(20, 65).$$

Finalmente, como $65 = 3 \cdot 20 + 5$,

$$\mathsf{mcd}(20, 65) = \mathsf{mcd}(20, 65 - 3 \cdot 20) = \mathsf{mcd}(20, 5)$$

y, como 5 divide a 20, este último máximo común divisor es 5. Concluimos así que

$$\mathsf{mcd}(385, 150) = 5.$$

Este procedimiento funciona en todos los casos, como veremos más abajo. Se lo conoce como el *algoritmo de Euclides*, porque Euclides lo describe en el Libro 7 de sus *Elementos*, publicados aproximadamente 300 años a.e.c. — aunque es probable que el algoritmo haya sido conocido desde mucho tiempo antes. En la Figura 6.2 reproducimos el pasaje relevante.

Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν. Ἔστωσαν οἱ δοθέντες δύο ἀριθμοὶ μὴ πρῶτοι πρὸς ἀλλήλους οἱ ΑΒ, ΓΔ. δεῖ δὴ τῶν ΑΒ, ΓΔ τὸ μέγιστον κοινὸν μέτρον εὑρεῖν. Εἰ μὲν οὖν ὁ ΓΔ τὸν ΑΒ μετρεῖ, μετρεῖ δὲ καὶ ἑαυτόν, ὁ ΓΔ ἄρα τῶν ΓΔ, ΑΒ κοινὸν μέτρον ἐστίν. καὶ φανερόν, ὅτι καὶ μέγιστον: οὐδεὶς γὰρ μείζων τοῦ ΓΔ τὸν ΓΔ μετρήσει. Εἰ δὲ οὐ μετρεῖ ὁ ΓΔ τὸν ΑΒ, τῶν ΑΒ, ΓΔ ἀνθυφαιρουμένου ἀεὶ τοῦ ἐλάσσονος ἀπὸ τοῦ μείζονος λειφθήσεταί τις ἀριθμός, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. μονὰς μὲν γὰρ οὐ λειφθήσεται: εἰ δὲ μή, ἔσονται οἱ ΑΒ, ΓΔ πρῶτοι πρὸς ἀλλήλους: ὅπερ οὐχ ὑπόκειται. λειφθήσεταί τις ἄρα ἀριθμός, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. καὶ ὁ μὲν ΓΔ τὸν ΒΕ μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν ΕΑ, ὁ δὲ ΕΑ τὸν ΔΖ μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν ΖΓ, ὁ δὲ ΓΖ τὸν ΑΕ μετρείτω. ἐπεὶ οὖν ὁ ΓΖ τὸν ΑΕ μετρεῖ, ὁ δὲ ΑΕ τὸν ΔΖ μετρεῖ, καὶ ὁ ΓΖ ἄρα τὸν ΔΖ μετρήσει: μετρεῖ δὲ καὶ ἑαυτόν: καὶ ὅλον ἄρα τὸν ΓΔ μετρήσει. ὁ δὲ ΓΔ τὸν ΒΕ μετρεῖ: καὶ ὁ ΓΖ ἄρα τὸν ΒΕ μετρεῖ: μετρεῖ δὲ καὶ τὸν ΕΑ: καὶ ὅλον ἄρα τὸν ΒΑ μετρήσει: μετρεῖ δὲ καὶ τὸν ΓΔ: ὁ ΓΖ ἄρα τοὺς ΑΒ, ΓΔ μετρεῖ. ὁ ΓΖ ἄρα τῶν ΑΒ, ΓΔ κοινὸν μέτρον ἐστίν. λέγω δή, ὅτι καὶ μέγιστον. εἰ γὰρ μή ἐστιν ὁ ΓΖ τῶν ΑΒ, ΓΔ μέγιστον κοινὸν μέτρον, μετρήσει τις τοὺς ΑΒ, ΓΔ ἀριθμοὺς ἀριθμὸς μείζων ὢν τοῦ ΓΖ. μετρείτω, καὶ ἔστω ὁ Η. καὶ ἐπεὶ ὁ Η τὸν ΓΔ μετρεῖ, ὁ δὲ ΓΔ τὸν ΒΕ μετρεῖ, καὶ ὁ Η ἄρα τὸν ΒΕ μετρεῖ: μετρεῖ δὲ καὶ ὅλον τὸν ΒΑ: καὶ λοιπὸν ἄρα τὸν ΑΕ μετρήσει. ὁ δὲ ΑΕ τὸν ΔΖ μετρεῖ: καὶ ὁ Η ἄρα τὸν ΔΖ μετρήσει: μετρεῖ δὲ καὶ ὅλον τὸν ΔΓ: καὶ λοιπὸν ἄρα τὸν ΓΖ μετρήσει ὁ μείζων τὸν ἐλάσσονα: ὅπερ ἐστὶν ἀδύνατον: οὐκ ἄρα τοὺς ΑΒ, ΓΔ ἀριθμοὺς ἀριθμός τις μετρήσει μείζων ὢν τοῦ ΓΖ: ὁ ΓΖ ἄρα τῶν ΑΒ, ΓΔ μέγιστόν ἐστι κοινὸν μέτρον: [ὅπερ ἔδει δεῖξαι].

Figura 6.2. La proposición 2 del Libro 7 de los Elementos de Euclides, en el que enuncia el problema de encontrar el máximo común divisor de dos números y lo resuelve, presentando el algoritmo que lleva su nombre. Empieza con «Dados dos números no primos uno al otro, encontrar su medida más grande. Sean AB y CD los dos números dados no primos uno al otro. Si CD mide a AB, y también se mide a sí mismo, entonces CD es una medida común de AB, CD. Y es manifiesto que es la más grande. Pero si CD no mide a AB, entonces, el menos de los números AB, CD se puede restar varias veces del más grande, y algún número sera el resto, que medirá al que está antes de él. Etc».

6.4.6. Describamos precisamente el algoritmo de Euclides en una forma conveniente para probar que funciona. Empezamos como arriba con dos números enteros no negativos a y b, suponemos que $a \geq b$ y definimos una sucesión

$$r_0, r_1, r_2, r_3, \ldots$$

de enteros no negativos de la siguiente manera. Ponemos $r_0 \coloneqq a$, $r_1 \coloneqq b$ y, para cada $i \geq 2$,

$$r_i \coloneqq \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases} \tag{10}$$

El algoritmo de Euclides para determinar el máximo común divisor de a y de b consiste en calcular las componentes de esta sucesión y quedarse con la última no nula. Por ejemplo, si $a = 385$ y $b = 150$, entonces la sucesión $(r_i)_{i\geq 0}$ es

$$385,\ 150,\ 85,\ 65,\ 20,\ 5,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ \ldots$$

y, por lo tanto, $\mathsf{mcd}(385, 150) = 5$.

6.4.7. Proposición. *Sean a y b dos enteros no negativos tales que $a \geq b$ y sea $(r_i)_{i\geq 0}$ la sucesión que acabamos de describir.*

(*i*) *Existe $N \in \mathbb{N}_0$ tal que $r_i \neq 0$ para todo $i \leq N$ y $r_i = 0$ para todo $i > N$.*

(*ii*) *Para todo $i \in \mathbb{N}$ tal que $i \leq N + 1$ se tiene que $\mathsf{mcd}(a, b) = \mathsf{mcd}(r_{i-1}, r_i)$.*

(*iii*) *Es $\mathsf{mcd}(a, b) = r_N$.*

Este resultado nos dice que el algoritmo de Euclides, cuando empezamos con dos enteros no negativos a y b, se detiene después de un número finito de pasos — el número N — y el último número que produce es precisamente el máximo común divisor de a y b. En otros palabras, nos dice que el algoritmo funciona, como queríamos.

Demostración. Observemos que

$$r_i \geq 0 \text{ para todo } i \in \mathbb{N}. \tag{11}$$

En efecto, se tiene que $r_1 = b \geq 0$ y para todo $i \geq 2$ se tiene que $r_i \geq 0$ ya que r_i es, de acuerdo a la definición (10), o bien el resto de una división, que es siempre un número no negativo, o bien 0.

Por otro lado, se tiene que

$$\text{para todo } i \in \mathbb{N} \text{ o bien } r_i = 0 \text{ o bien } r_i > r_{i+1}. \tag{12}$$

Para verlo, basta notar que si $i \in \mathbb{N}$ y $r_i \neq 0$, entonces r_{i+1} es el resto de dividir a un número por r_i, que es necesariamente menor que r_i.

Supongamos por un momento que $r_i \neq 0$ para todo $i \in \mathbb{N}$. De acuerdo a (11), el conjunto $R \coloneqq \{r_i : i \in \mathbb{N}\}$ está contenido en $\mathbb{N}_0$, así que tiene un menor elemento: esto es, existe $i \in \mathbb{N}$ tal que $r_i \leq r_j$ para todo $j \in \mathbb{N}$. Esto es absurdo, ya que como $r_i \neq 0$ por nuestra hipótesis, de (12) sabemos que $r_i > r_{i+1}$.

Esta contradicción implica que tiene que existir $i \in \mathbb{N}$ tal que $r_i = 0$ y, por lo tanto, que el conjunto $S \coloneqq \{i \in \mathbb{N} : r_{i+1} = 0\}$ no es vacío. Como está contenido en $\mathbb{N}$, sabemos que él también tiene tiene un menor elemento. Llamémoslo N. Se tiene, claro, que $r_i \neq 0$ si $i \leq N$ y $r_{N+1} = 0$. Más aún, en vista de la forma en que está definida la sucesión $(r_i)_{i\geq 0}$, es claro que como $r_{N+1} = 0$ se tiene que $r_i = 0$ para todo entero $i > N$. Esto prueba que vale la parte (i) de la proposición.

Para cada $i \in \mathbb{N}$ sea $P(i)$ la afirmación

$$i > N+1 \;\; o \;\; \mathsf{mcd}(a,b) = \mathsf{mcd}(r_{i-1}, r_i)$$

y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}$: esto probará la parte (ii) de la proposición.

Que $P(1)$ vale es evidente, ya que $r_0 = a$ y $r_1 = b$. Supongamos que $j \in \mathbb{N}$ y que la afirmación $P(j)$ vale, es decir, que $j > N+1$ o

$$\mathsf{mcd}(a,b) = \mathsf{mcd}(r_{j-1}, r_j). \tag{13}$$

Si $j > N+1$, entonces por supuesto es $j+1 > N+1$ y, por lo tanto, la afirmación $P(j+1)$ vale. Consideremos el caso en que $j \leq N$, de manera que vale la igualdad (13). La forma en que elegimos el número N implica que $r_j \neq 0$, así que la definición de la sucesión $(r_i)_{i\geq 0}$ nos dice que r_{j+1} es el resto de dividir a r_{j-1} por r_j. Si q es el cociente de esa división, entonces que $r_{j+1} = r_{j-1} - qr_j$ y, por lo tanto,

$$\mathsf{mcd}(r_{j-1}, r_j) = \mathsf{mcd}(r_{j-1} - qr_k, r_j) = \mathsf{mcd}(r_{j+1}, r_j) = \mathsf{mcd}(r_j, r_{j+1}).$$

Junto con (13) esto nos dice que $\mathsf{mcd}(a,b) = \mathsf{mcd}(r_j, r_{j+1})$ y, en definitiva, que $P(j+1)$ también vale en este caso. La inducción queda así completa.

Finalmente, tomando $i = N+1$ en la igualdad de la parte (ii), vemos que

$$\mathsf{mcd}(a,b) = \mathsf{mcd}(r_N, r_{N+1}) = \mathsf{mcd}(r_N, 0) = r_N,$$

como se afirma en la parte (iii) de la proposición. □

6.4.8. Es inmediato implementar este algoritmo en Haskell y en Python. En las Figuras 6.3 y 6.4 damos una forma de hacerlo. Este algoritmo es extremadamente importante en las aplicaciones, así que hay toda una literatura dedicada a su estudio y mejora — el código que presentamos es la implementación más sencilla posible. El libro [Knu1969] de Donald Knuth tiene una discusión detallada de este algoritmo.

```haskell
module MCD where

mcd :: Integer -> Integer -> Integer
mcd a 0 = abs a
mcd a b = mcd b (a `mod` b)
```

Figura 6.3. Un implementación en Haskell del algoritmo de la Euclides. Esto es casi exactamente el algoritmo que describimos en 6.4.6, salvo que esta modificado para que cualquiera de `a` o `b` pueda ser negativo en la expresión `mcd a b`.

```python
def mcd(a, b):
    if b == 0:
        return abs(a)
    else:
        return mcd(b, a % b)
```

Figura 6.4. Un implementación en Python del algoritmo de la Euclides.

Casi todos los lenguajes de programación cuentan con muy buenas implementaciones de este algoritmo — Haskell tiene la función `gcd` en su preludio y Python a la función `gcd` en el módulo `math` de la librería estándar — y en general uno debería usarlas.

6.4.9. El máximo común divisor de dos números que no son los dos nulos es, por definición, el máximo de un conjunto. Nuestro siguiente resultado da una descripción alternativa de él como el *mínimo* de otro conjunto.

Proposición. *Sean a y b dos enteros no simultáneamente nulos. El conjunto*

$$S(a,b) \coloneqq \{xa + yb : x, y \in \mathbb{Z},\ xa + yb > 0\}$$

es un subconjunto no vacío de $\mathbb{N}$ y su elemento mínimo es $\mathsf{mcd}(a,b)$.

Demostración. Alguno de los cuatro números a, $-a$, b o $-b$ es positivo y, por lo tanto, pertenece a $S(a,b)$: esto muestra que este conjunto no es vacío. Como está contenido en $\mathbb{N}$, podemos considerar su elemento mínimo $d \coloneqq \mathsf{mín}\, S$. Como d pertenece a $S(a,b)$, es claro que $d \geq 1$ y que existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.

Sean q y r el cociente y el resto de la división de a por d, de manera que $a = qd + r$ y $0 \leq r < d$.

Si $r > 0$, entonces como

$$(1 - qu)a - qvb = r$$

y $1 - qu$ y $-qv$ son enteros, se tiene que $r \in S(a, b)$: esto es imposible ya que $r < d$. Vemos así que tiene que ser $r = 0$ y, por lo tanto, d divide a a. Un argumento similar muestra que d divide a b y, por lo tanto, d es un divisor común de a y b.

Sea ahora e un elemento de $D(a, b)$, de manera que e divide a a y a b. Como $d = ua + vb$, es claro que e divide también a d y, como $d \neq 0$, la Proposición 6.1.4 nos dice que $e \leq d$. Esto muestra que d es el mayor elemento de $D(a, b)$ y, por lo tanto, que $d = \mathsf{mcd}(a, b)$, como afirma la proposición. □

6.4.10. Una consecuencia inmediata e importante de esta proposición es el siguiente corolario:

Corolario. *Si a y b son dos enteros y $d = \mathsf{mcd}(a, b)$, entonces hay enteros x e y tales que $d = xa + yb$.*

Llamamos a esta igualdad la ***identidad de Bézout***, por Étienne Bézout, que probó un análogo de este resultado para polinomios.

Demostración. Si $a = b = 0$, entonces $d = 0$ y eligiendo $x = y = 0$ es evidente que vale la igualdad del enunciado. Si en cambio a y b no son simultáneamente nulos, la Proposición 6.4.9 nos dice que el número d pertenece al conjunto $S(a, b)$ allí descripto y, por lo tanto, existen enteros x e y tales que $d = xa + yb$. □

6.4.11. Para muchas aplicaciones, necesitamos no solamente poder calcular el máximo común divisor de dos enteros sino que también queremos encontrar números x e y para los que valga la identidad de Bézout. Veamos cómo podemos hacer esto.

Supongamos como en 6.4.6 que tenemos dos enteros no negativos a y b tales que $a \geq b$, sea $d \coloneqq \mathsf{mcd}(a, b)$ y definamos la sucesión $(r_i)_{i \geq 0}$ como allí, esto es, poniendo $r_0 \coloneqq a$, $r_1 \coloneqq b$ y, para cada $i \geq 2$,

$$r_i \coloneqq \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases}$$

Sea N el número que nos provee la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ si $i > N$ y $r_N = d$. Estamos buscando enteros x e y tales que $xa + yb = r_N$. Busquemos, más generalmente, pares de enteros $x_0, y_0, x_1, y_1, \ldots, x_N, y_N$ tales que para cada $i \in \{0, \ldots, N\}$ se tenga $x_i a + y_i b = r_i$.

Observemos que cuando $i = 0$ o $i = 1$ esto es fácil: basta poner $x_0 \coloneqq 1$, $y_0 \coloneqq 0$, $x_1 \coloneqq 0$, $y_1 \coloneqq 1$, ya que $r_0 = a$ y $r_1 = b$. Ahora bien, supongamos que $2 \leq i \leq N$ y que ya encontramos enteros $x_{i-1}, y_{i-1}, x_i, y_i$ de manera tal que $x_{i-1}a + y_{i-1}b = r_{i-1}$ y $x_i a + y_i b = r_i$. Si llamamos q_{i+1} al cociente

de la división de r_{i-1} por r_i, de manera que $r_{i-1} = q_{i+1}r_i + r_{i+1}$, tenemos entonces que

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1}r_i = (x_{i-1}a + y_{i-1}b) - q_{i+1}(x_i a + y_i b) \\ &= (x_{i-1} - q_{i+1}x_i)a + (y_{i-1} - q_{i+1}y_i)b \end{aligned}$$

y, por lo tanto, basta que pongamos

$$x_{i+1} \coloneqq x_{i-1} - q_{i+1}x_i \tag{14}$$

e

$$y_{i+1} \coloneqq y_{i-1} - q_{i+1}y_i \tag{15}$$

para que se tenga que $x_{i+1}a + y_{i+1}b = r_{i+1}$.

De esta manera vamos determinando enteros x_i e y_i para cada i de 0 hasta N, hasta finalmente encontrar x_N e y_N: estos satisfacen la condición de que $x_N a + y_N b = r_N = d$, que es la identidad de Bézout.

Veamos un ejemplo de cómo funciona este proceso. Determinemos los coeficientes de la identidad de Bézout para $a = 385$ y $b = 150$. Como en **6.4.6**, calculamos las componentes de la sucesión $(r_i)_{i\geq 0}$ pero en cada paso a partir del segundo no solamente calculamos el resto r_i de dividir r_{i-2} por r_{i-1} sino también el cociente q_i. La primera componente nula de la sucesión de restos es r_6, así que sabemos que $r_5 = \mathsf{mcd}(a, b)$.

i	0	1	2	3	4	5	6
r_i	385	150	85	65	20	5	0
q_i			2	1	1	3	
x_i	1	0	1	−1	2	−7	
y_i	0	1	−2	3	−5	18	

(16)

Ahora calculamos en orden los números x_i e y_i: empezamos poniendo $x_0 = 1$, $y_0 = 0$, $x_1 = 0$ e $y_1 = 1$, y a todos los otros los determinamos usando las fórmulas (14) y (15). Encontramos de esta forma que

$$(-7) \cdot 385 + 18 \cdot 150 = 5,$$

que es la identidad de Bézout para 385 y 150, como queríamos.

Este procedimiento es conocido como el *algoritmo de Euclides extendido* y es la forma en que se determinan los coeficientes de la identidad de Bézout en la práctica. Todos los programas de álgebra computacional tienen implementaciones de este algoritmo. En la Figura 6.5 en la página siguiente damos una posible implementación en Haskell.

```
module EMCD where

emcd :: Integer -> Integer -> (Integer, Integer, Integer)
emcd a b = (d, signum a * x, signum b * y)
  where (d, x, y) = paso 1 0 0 1 (abs a) (abs b)

paso x y x' y' a 0 = (a, x, y)
paso x y x' y' a b = paso x' y' x'' y'' b (a `mod` b)
  where q = a `div` b
        x'' = x - q * x'
        y'' = y - q * y'
```

Programa 6.5. Un implementación en HASKELL del algoritmo de Euclides extendido. Con estas definiciones. `emcd a b` es una terna `(d, x, y)` tal que `d` es el máximo común divisor de `a` y `b`, y `x` e `y` son tales que $ax + by = 1$. Este algoritmo difiere del que describimos en 6.4.11. La función `paso` se ocupa de hacer cada paso del algoritmo: la vez i-ésima que es llamada recibe como argumentos a los números x_{i-1}, y_{i-1}, x_i, y_i, r_{i-1} y r_i, en ese orden.

```
module EMCD where

emcd :: Integer -> Integer -> (Integer, Integer, Integer)
emcd a 0 = (abs a, signum a, 0)
emcd a b = (d, y, x - (a `div` b) * y)
  where (d, x, y) = emcd b (a `mod` b)
```

Programa 6.6. Una implementación de la versión del algoritmo de Euclides extendido descripta en 6.4.13. Otra vez, el valor de `emcd a b` es una terna `(d, x, y)` tal que `d` es el máximo común divisor de `a` y `b`, y `x` e `y` son tales que $ax + by = 1$. Esta versión difiere de la anterior en que los coeficientes `x` e `y` se obtienen «hacia atrás». Este código es bastante más sencillo que el de la Figura 6.5 pero aquel tiene la ventaja de que usa lo que se llama *recursión de cola* y es, por lo tanto, más eficiente.

6.4.12. Probemos que este algoritmo funciona en todos los casos:

Proposición. *Sean a y b dos enteros no negativos y supongamos que $a \geq b$. Sea $(r_i)_{i\geq 0}$ la sucesión construida en 6.4.6 a partir de a y b, y sea $N \in \mathbb{N}_0$ como en la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ para todo $i > N$ y $r_N = \mathsf{mcd}(a, b)$. Sean $x_0, x_1, \ldots, x_N$ y $y_0, y_1, \ldots, y_N$ las secuencias de enteros tales que*

$$x_0 = 1, \qquad y_0 = 0, \tag{17}$$

$$x_1 = 0, \qquad y_1 = 1, \tag{18}$$

y, para cada $i \in \{2, \ldots, N\}$,

$$x_i = x_{i-2} - q_i x_{i-1}, \qquad y_i = y_{i-2} - q_i y_{i-1} \tag{19}$$

con q_i el cociente de dividir a r_{i-2} por r_{i-1}. Se tiene entonces que

$$r_i = x_i a + y_i b \tag{20}$$

para cada $i \in \{0, \ldots, N\}$ y, en particular, que

$$\mathsf{mcd}(a, b) = x_N a + y_N b.$$

Demostración. Es suficiente que mostremos que para cada $i \in \{0, \ldots, N\}$ vale la igualdad (20), ya que cuando i es N ésta nos dice que $x_N a + y_N b = r_N = \mathsf{mcd}(a, b)$.

Sea $P(i)$, para cada $i \in \mathbb{N}_0$, la afirmación «o bien $i > N$ o bien $r_i = x_i a + y_i b$» y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}_0$ haciendo inducción. Las afirmaciones $P(0)$ y $P(1)$ valen: esto es consecuencia inmediata de las igualdades (17) y (18). En efecto, $x_0 a + y_0 b = a = r_0$ y $x_1 a + y_1 b = b = r_1$.

Veamos ahora el paso inductivo. Sea j un entero tal que $j \geq 2$ y supongamos que las afirmaciones $P(j-1)$ y $P(j-2)$ valen. Si $j > N$, entonces claramente la afirmación $P(j)$ vale. Consideremos el caso en que $j \leq N$. Que $P(j-1)$ y $P(j-2)$ valgan, entonces, nos dice que $r_{j-1} = x_{j-1} a + y_{j-1} b$ y que $r_{j-2} = x_{j-2} a + y_{j-2} b$. Si q_j es el resto de dividir a r_{j-2} por r_{j-1}, tenemos que

$$\begin{aligned} r_j &= r_{j-2} - q_i r_{j-1} \\ &= (x_{j-2} a + y_{j-2} b) - q_i (x_{j-1} a + y_{j-1} b) \\ &= (x_{j-2} - q_i x_{j-1}) a + (y_{j-2} - q_i y_{j-1}) b \end{aligned}$$

y, de acuerdo a las ecuaciones (19), esto es

$$= x_j a + y_j b.$$

Vemos así que $P(j)$ vale también en este caso y esto completa la inducción. □

6.4.13. Hay una forma alternativa de obtener los coeficientes de la identidad de Bézout que es a veces más conveniente y que los encuentra «hacia atrás». Supongamos que empezamos con dos enteros positivos a y b tales que $a \geq b$, construyamos como en **6.4.6** la sucesión $(r_i)_{i\geq 0}$, y sea N el número cuya existencia asegura la Proposición 6.4.7, de manera que, en particular, $r_N = \mathsf{mcd}(a,b)$ y $r_{N+1} = 0$. Construimos ahora una secuencia de enteros $z_0, z_1, \ldots, z_N$ poniendo $z_0 \coloneqq 0$, $z_1 \coloneqq 1$ y, para cada i desde 2 hasta N,

$$z_i \coloneqq z_{i-2} - q_{N+2-i} z_{i-1},$$

con q_i el cociente de dividir a r_{i-2} por r_{i-1}. Al terminar, ponemos $x \coloneqq z_{N-1}$ e $y \coloneqq z_N$ y vale que $xa + yb = \mathsf{mcd}(a,b)$, así que encontramos la identidad de Bézout.

Por ejemplo, si $a = 385$ y $b = 150$ en primer lugar construimos la tabla

i	0	1	2	3	4	5	6
r_i	385	150	85	65	20	5	0
q_i			2	1	1	3	

(21)

de manera que aquí $N = 5$, y usando esa información una segunda tabla

i	0	1	2	3	4	5
z_i	0	1	−3	4	−7	18

En este caso es $x = -7$ e $y = 18$ y $385x + 150y = 5$ es el máximo común divisor de 385 y 150.

Proposición. *Sean a y b dos enteros positivos a y b tales que $a \geq b$ y sean N y $r_0, r_1, \ldots, r_N$ los números construidos en la Proposición 6.4.7. Si $z_0, z_1, \ldots, z_N$ es la secuencia de números construida arriba, entonces*

$$z_{N-1}a + z_N b = \mathsf{mcd}(a,b).$$

Esta proposición nos dice que el algoritmo descripto en **6.4.13** funciona, esto es, que los da coeficientes que hacen cierta la identidad de Bézout. En la Figura 6.6 damos una implementación en Haskell. La diferencia fundamental entre este y el anterior es que cuando llevamos a cabo el de **6.4.11** es suficiente que en todo momento tengamos las últimas dos columnas de la tabla (16), mientras que cuando llevamos a cabo el procedimiento de **6.4.13** es necesario guardar completa la tabla de (21) para poder empezar a calcular los enteros z_i.

Demostración. Supongamos que el conjunto

$$S \coloneqq \{i \in \{0, \ldots, N-1\} : z_i r_{N-i-1} + z_{i+1} r_{N-i} \neq \mathsf{mcd}(a,b)\}$$

no es vacío, y sea j su mínimo. Notemos que cuando $i = 0$ es

$$z_i r_{N-i-1} + z_{i+1} r_{N-i} = z_0 r_{N-1} + z_1 r_N = r_N = \mathsf{mcd}(a, b)$$

y esto nos dice que 0 no pertenece al conjunto S y, por lo tanto, que $j > 0$. Ahora bien, como j es es el menor elemento de S y $0 \leq j - 1 \leq N - 1$, la diferencia $j - 1$ tiene que pertenecer a S, y esto significa que

$$\begin{aligned} \mathsf{mcd}(a, b) &= z_{j-1} r_{N-j} + z_j r_{N-j+1} \\ &= (z_{j+1} + q_{N+1-j} z_j) r_{N-j} + z_j r_{N-j+1} \qquad \text{porque } z_{j+1} = z_{j-1} - q_{N+1-j} z_j \\ &= z_{j+1} r_{N-j} + z_j (q_{N+1-j} r_{N-j} + r_{N+1-j}) \\ &= z_{j+1} r_{N-j} + z_j r_{N-1-j} \end{aligned}$$

porque $r_{N+1-j} = q_{N-1-j} r_{N+1-j} + r_{N+2-j}$, de acuerdo a la definición de la sucesión $(r_i)_{i \geq 0}$. Esto es absurdo porque j no pertenece al conjunto S, y esta contradicción provino de haber supuesto que S no es vacío. Esto significa que sí lo es y, en particular, que $N - 1$ no pertenece a S, esto es, que

$$\mathsf{mcd}(a, b) = z_{N-1} r_0 + z_N r_1 = z_{N-1} a + z_N b.$$

Esto es lo que queríamos probar. □

§6.5. Algunas aplicaciones de la identidad de Bézout

6.5.1. Vamos a usar la identidad de Bézout varias veces en todo lo que sigue. La primera aplicación es la siguiente caracterización del máximo común divisor de dos enteros que es extremadamente útil:

Proposición. *Sean a y b dos enteros. El máximo común divisor de a y b es el único elemento d de $\mathbb{N}_0$ que tiene las siguientes dos propiedades:*

- *d es un divisor común de a y b, y*
- *todo elemento de $\mathbb{N}_0$ que es un divisor común de a y b también divide a d.*

Demostración. Sea $d \coloneqq \mathsf{mcd}(a, b)$ y sean x e y enteros tales que $d = xa + yb$. Si e es un divisor positivo común de a y b, entonces e también divide a $d = xa + yb$. Como d es un divisor común de a y b, vemos así que d tiene las dos propiedades del enunciado.

Supongamos ahora que tenemos otro entero no negativo d' que tiene esas dos propiedades. Como d' es un divisor común de a y b y d tiene la segunda propiedad del enunciado, tenemos que $d \mid d'$. Por otro lado, como d es un divisor común de a y de b y d' tiene la segunda propiedad del enunciado, tenemos que $d' \mid d$. Podemos concluir entonces que $d = d'$, ya que tanto d como d' son enteros no negativos. Esto prueba la proposición. □

6.5.2. La caracterización del máximo común divisor de dos enteros que nos da la Proposición 6.5.1 es extremadamente útil. Veamos algunos ejemplos de cómo podemos usarla.

Corolario. *Si a, a', b y b' son enteros tales que $a \mid a'$ y $b \mid b'$, entonces*

$$\mathsf{mcd}(a, b) \mid \mathsf{mcd}(a', b').$$

Demostración. Sean a, a', b y b' enteros y supongamos que $a \mid a'$ y que $b \mid b'$. Sea además $d \coloneqq \mathsf{mcd}(a, b)$. Como d divide a a y a divide a a', vemos que d divide a a'. De manera similar, d divide a b': como d es entonces un divisor común de a' y b', la Proposición 6.5.1 nos dice que d divide a $\mathsf{mcd}(a', b')$. Esto es lo que afirma el corolario. □

6.5.3. Otra aplicación sencilla y útil de la proposición es el siguiente resultado que nos permite simplificar expresiones que involucran la función mcd.

Proposición. *Si a, b y c son enteros, entonces*

$$\mathsf{mcd}(ac, bc) = \mathsf{mcd}(a, b) \cdot c.$$

Demostración. Escribamos $d \coloneqq \mathsf{mcd}(a, b)$ y $e \coloneqq \mathsf{mcd}(ac, bc)$. De acuerdo a la identidad de Bézout 6.4.10, hay enteros x e y tales que $d = xa + yb$. Como $dc = xac + ybc$ y e divide a ac y a bc, vemos entonces que e divide a dc.

Por otro lado, como d divide a a y a b, es claro que dc divide a bc y a bd, así que la Proposición 6.5.1 nos dice que dc divide a e. Como d y e son enteros no negativos, podemos concluir de todo esto que $d = e$, que es lo que afirma la proposición. □

6.5.4. Usando la Proposición 6.5.3 podemos dar una nueva caracterización del máximo común divisor de dos números:

Corolario. *Sean a y b dos enteros y sea $d \coloneqq \mathsf{mcd}(a, b)$.*

(*i*) *Los enteros a' y b' tales que $a = da'$ y $b = db'$ son coprimos.*

(*ii*) *Si e es un entero no negativo tal que existen dos enteros coprimos u y v para los que se tiene que $a = eu$ y $a = ev$, entonces $e = d$.*

Demostración. (*i*) En la situación del enunciado, tenemos que

$$d = \mathsf{mcd}(a, b) = \mathsf{mcd}(da', db') = d \cdot \mathsf{mcd}(a', b'),$$

así que necesariamente $\mathsf{mcd}(a', b') = 1$.

(*ii*) Si $e \in \mathbb{N}_0$ y $u, v \in \mathbb{Z}$ son tales que $a = eu$, $b = ev$ y $\mathsf{mcd}(u, v) = 1$, entonces

$$\mathsf{mcd}(a, b) = \mathsf{mcd}(eu, ev) = e \cdot \mathsf{mcd}(u, v) = e$$

y esto es lo que queremos. □

6.5.5. Nuestro siguiente resultado nos da mas posibilidades de manipulación de expresiones que contienen la función mcd.

Proposición. *Sean a, b y c tres enteros y supongamos que a y b son coprimos.*

(*i*) *Si* $a \mid bc$, *entonces* $a \mid c$.
(*ii*) *Si* $a \mid c$ *y* $b \mid c$, *entonces* $ab \mid c$.
(*iii*) *Es* $\mathsf{mcd}(a, bc) = \mathsf{mcd}(a, c)$.
(*iv*) *Es* $\mathsf{mcd}(ab, c) = \mathsf{mcd}(a, c) \cdot \mathsf{mcd}(b, c)$.

Demostración. Como a y b son coprimos, existen enteros x e y tales que $xa + yb = 1$.

(*i*) Supongamos primero que a divide a bc. Como $xac + ybc = c$ y a divide a los dos sumandos del lado izquierdo, también divide al lado derecho.

(*ii*) Supongamos ahora que $a \mid c$ y que $b \mid c$. De eso se sigue que ab divide a bc y a ac, así que también divide a c, porque este número es igual a $xac + ybc$.

(*iii*) Sean $d \coloneqq \mathsf{mcd}(a, c)$ y $e \coloneqq \mathsf{mcd}(a, bc)$. Como d divide a a y a c, divide a a y a bc: de acuerdo a la Proposición 6.5.1, tenemos entonces que d divide a e. Por otro lado, como e divide a a y a bc, vemos que e divide a $c = (xa + yb)c = xac + ybc$. Esto nos dice que e es un divisor común positivo de a y c, así que e divide a d. Como d y e se dividen mutuamente y son no negativos, concluimos de esta forma que $d = e$, que es lo que queremos.

(*iv*) Pongamos $d \coloneqq \mathsf{mcd}(a, c)$, $e \coloneqq \mathsf{mcd}(b, c)$ y $f \coloneqq \mathsf{mcd}(ab, c)$. Como $d \mid a$ y $e \mid b$, se tiene que $de \mid ab$. Por otro lado, como $d \mid a$ y $e \mid c$, tenemos que $de \mid ac$, y como $d \mid c$ y $e \mid b$ que $de \mid bc$: usando esto y la igualdad $c = xac + ybc$, podemos concluir que $de \mid c$. Vemos así que de es un divisor común de ab y de c, así que $de \mid f$.

Por otro lado, existen enteros u, v, r y s tales que $d = ua + vc$ y $e = rb + sc$, así que

$$de = (ua + vc)(rb + sc) = urab + (usa + vrb + vsc)c.$$

Como f divide a ab y a c, vemos entonces que también divide a de. Como f y de son enteros no

negativos que se dividen mutuamente, tenemos en definitiva que $de = f$, que es lo que queríamos probar. □

6.5.6. La última parte de la proposición que acabamos de probar tiene la siguiente generalización:

Corolario. *Sea $r \in \mathbb{N}$. Si $a_1, \ldots, a_r$ son enteros coprimos dos a dos y $b \in \mathbb{Z}$, entonces*

$$\mathsf{mcd}(a_1 \cdots a_r, b) = \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b).$$

Demostración. Procedamos por inducción con respecto a r, notando que cuando r es 1 la afirmación es evidente. Sea entonces $s \in \mathbb{N}$, supongamos que la afirmación del enunciado vale cuando r es s y mostremos que entonces vale también cuando r es $s+1$.

Sean entonces $a_1, \ldots, a_{s+1}$ enteros coprimos dos a dos y sea b otro entero. Como los s enteros $a_1, \ldots, a_s$ son coprimos dos a dos, la hipótesis inductiva nos dice que

$$\mathsf{mcd}(a_1 \cdots a_s, a_{s+1}) = \mathsf{mcd}(a_1, a_{s+1}) \cdots \mathsf{mcd}(a_s, a_{s+1}) = 1,$$

así que los números $a_1 \cdots a_s$ y a_{s+1} son coprimos. La Proposición **6.5.5**(*iv*) nos dice entonces que

$$\mathsf{mcd}(a_1 \cdots a_{s+1}, b) = \mathsf{mcd}(a_1 \cdots a_s \cdot a_{s+1}, b) = \mathsf{mcd}(a_1 \cdots a_s, b) \cdot \mathsf{mcd}(a_{s+1}, b)$$

y usando otra vez la hipótesis inductiva vemos que esto es igual a

$$\mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_s, b) \cdot \mathsf{mcd}(a_{s+1}, b).$$

Esto completa la inducción. □

6.5.7. El resultado del siguiente ejercicio describe qué ocurre en la situación del Corolario 6.5.6 si la hipótesis no se cumple.

Ejercicio. Sea $r \in \mathbb{N}$. Muestre que si $a_1, \ldots, a_r$ y b son enteros arbitrarios, entonces

$$\mathsf{mcd}(a_1 \cdots a_r, b) \mid \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b).$$

y, dando un ejemplo, muestre que estos dos números no son necesariamente iguales.

6.5.8. De manera similar, podemos generalizar la parte (*ii*) de la Proposición **6.5.5** al caso en que tenemos varios divisores:

Corolario. *Sea $r \in \mathbb{N}$. Si $a_1, \ldots, a_r$ son enteros coprimos dos a dos y cada uno de ellos divide a un entero b, entonces el producto $a_1 \cdots a_r$ también divide a b.*

Si los r enteros $a_1, \ldots, a_r$ no son dos a dos coprimos la concluimos en general no vale. Por ejemplo, 6 y 15 dividen a 30 pero su producto no lo hace.

Demostración. De acuerdo al Corolario 6.5.6, tenemos que

$$\mathsf{mcd}(a_1 \cdots a_r, b) = \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b)$$

y, de acuerdo a la Proposición 6.4.3(*ii*) y la hipótesis de que cada uno de los enteros $a_1, \ldots, a_r$ divide a b, tenemos que $\mathsf{mcd}(a_i, b) = |a_i|$ para cada $i \in \{1, \ldots, r\}$ y, por lo tanto, tenemos que

$$\mathsf{mcd}(a_1 \cdots a_r, b) = |a_1 \cdots a_r|.$$

Esa misma Proposición 6.4.3(*ii*) nos dice entonces que $a_1 \cdots a_r$ divide a b. □

6.5.9. Nuestro siguiente resultado afirma que si dos enteros son coprimos entonces dos potencias de ellos también lo son.

Proposición. *Sean a y b dos enteros y sean k, $l \in \mathbb{N}$. Si $\mathsf{mcd}(a, b) = 1$, entonces $\mathsf{mcd}(a^k, b^l) = 1$.*

Demostración. Supongamos que $\mathsf{mcd}(a, b) = 1$, de manera que existen enteros x e y tales que $1 = xa + yb$. Se sigue de esto y de la fórmula de Newton que

$$\begin{aligned} 1 = 1^{k+l} = (xa + yb)^{k+l} &= \sum_{i=0}^{k+l} \binom{k+l}{i} x^{k+l-1} y^i a^{k+l-i} b^i \\ &= \left(\sum_{i=0}^{l} \binom{k+l}{i} x^{k+l-i} y^i a^{l-i} b^i \right) a^k + \left(\sum_{i=l+1}^{k+l} \binom{k+l}{i} x^{k+l-i} y^i a^{k+l-i} b^{i-l} \right) b^l, \end{aligned}$$

y las dos expresiones encerradas entre paréntesis son enteros. Sea $d \coloneqq \mathsf{mcd}(a^k, b^l)$. Como d divide a a^k y a b^l, esa igualdad implica que d divide a 1. Por supuesto, esto nos dice que $d = 1$, como queremos. □

6.5.10. Otra propiedad útil al calcular máximos comunes divisores es la siguiente:

6.5.11. Corolario. *Si a y b son enteros y $k \in \mathbb{N}$, entonces $\mathsf{mcd}(a^k, b^k) = \mathsf{mcd}(a, b)^k$.*

Demostración. Sea $d \coloneqq \mathsf{mcd}(a, b)$. Como d divide a a y a b, hay enteros u y v tales que $a = du$ y $b = dv$. De acuerdo a la Proposición 6.5.3, tenemos que

$$d \cdot \mathsf{mcd}(u, v) = \mathsf{mcd}(du, dv) = \mathsf{mcd}(a, b) = d,$$

de manera que $\mathsf{mcd}(u, v) = 1$. La Proposición 6.5.9 nos dice entonces que también $\mathsf{mcd}(u^k, v^k) = 1$

y usando esto podemos concluir que

$$\mathsf{mcd}(a^k, b^k) = \mathsf{mcd}(d^k u^k, d^k v^k) = d^k \cdot \mathsf{mcd}(u^k, v^k) = d^k,$$

que es lo que afirma el corolario. □

§6.6. Ejercicios

Fracciones reducidas

6.6.1. Ejercicio. Muestre que todo número racional puede escribirse de una única forma como un cociente a/b con $a \in \mathbb{Z}$, $b \in \mathbb{N}$ y $\mathsf{mcd}(a, b) = 1$. Decimos que esta es la ***forma reducida*** de ese número.

Una definición uniforme para el máximo común divisor

6.6.2. Ejercicio. Si a y b son dos enteros cualesquiera, entonces $\mathsf{mcd}(a, b)$ es el único elemento d de $\mathbb{N}_0$ tal que el conjunto $\{xa + yb : x, y \in \mathbb{Z}\}$ coincide con $\{zd : z \in \mathbb{Z}\}$.

Podríamos haber usado esta caracterización del máximo común divisor de dos números para definirlo: tiene la ventaja de que no nos fuerza a considerar por separado en caso en el que los dos números a y b son nulos.

El máximo común divisor de un conjunto finito de números

6.6.3. Ejercicio. Sean $k \in \mathbb{N}$ y $a_1, \ldots, a_k \in \mathbb{Z}$.

(*a*) Si los enteros $a_1, \ldots, a_k$ no todos simultáneamente nulos, el conjunto $D(a_1, \ldots, a_k)$ de los enteros positivos que dividen a cada uno de ellos es finito y no vacío. Tiene sentido entonces considerar su elemento máximo, al que llamamos el ***máximo común divisor*** de los enteros $a_1, \ldots, a_k$ y escribimos $\mathsf{mcd}(a_1, \ldots, a_k)$. Si en cambio todos los enteros $a_1, \ldots, a_k$ son nulos, definimos $\mathsf{mcd}(0, \ldots, 0) = 0$.

(*b*) Si $k \geq 3$, entonces

$$\mathsf{mcd}(a_1, \ldots, a_k) = \mathsf{mcd}(\mathsf{mcd}(a_1, a_2), a_3, \ldots, a_k). \tag{22}$$

(*c*) Existen enteros $x_1, \ldots, x_k$ tales que

$$x_1 a_1 + \cdots + x_k a_k = \mathsf{mcd}(a_1, \ldots, a_k). \tag{23}$$

(*d*) El entero $\mathsf{mcd}(a_1, \ldots, a_k)$ es el único que tiene las siguientes dos propiedades:

- es un divisor común positivo de los números $a_1, \ldots, a_k$, y
- divide a cada divisor común de los números $a_1, \ldots, a_k$.

(*e*) El entero $\mathsf{mcd}(a_1, \ldots, a_k)$ es el único entero no negativo d tal que el conjunto

$$\{x_1 a_1 + x_2 a_2 + \cdots + x_k a_k : x_1, x_2, \ldots, x_k \in \mathbb{Z}\}$$

coincide con $\{yd : y \in \mathbb{Z}\}$.

(*f*) Describa un algoritmo basado en la igualdad (22) y el algoritmo de Euclides para encontrar tanto a $\mathsf{mcd}(a_1, \ldots, a_k)$ como a enteros $x_1, \ldots, x_k$ para los que vale la igualdad (23).

El mínimo común múltiplo de dos enteros

6.6.4. Ejercicio. Sean a y b dos enteros.

(*a*) Sea $M(a, b)$ el conjunto de los múltiplos positivos comunes de a y de b, es decir, de los números enteros positivos m tales que $a \mid m$ y $b \mid m$. Si a y b no son simultáneamente nulos, entonces el conjunto $M(a, b)$ no es vacío y podemos entonces considerar su mínimo elemento: lo llamamos el ***mínimo común múltiplo*** de a y b, y lo escribimos $\mathsf{mcm}(a, b)$. Si en cambio alguno de a o b es nulo definimos $\mathsf{mcm}(a, b) = 0$.

(*b*) El entero no negativo $\mathsf{mcm}(a, b)$ es el único que tiene las siguientes dos propiedades:

- es un múltiplo común de a y de b, y
- divide a todo múltiplo común de a y de b.

(*c*) Si a y b son no negativos, entonces $ab = \mathsf{mcd}(a, b) \cdot \mathsf{mcm}(a, b)$. En particular, es $\mathsf{mcm}(a, b) = ab$ si y solamente si $\mathsf{mcd}(a, b) = 1$.

(*d*) Si a, b y c son enteros, entonces

$$\mathsf{mcm}(ac, bc) = \mathsf{mcm}(a, b) \cdot c.$$

Si además a y b son coprimos, entonces

$$\mathsf{mcm}(ab, c) \cdot c = \mathsf{mcd}(a, c) \cdot \mathsf{mcd}(b, c).$$

(*e*) Dé una definición del mínimo común múltiplo de un conjunto finito de enteros, en el espíritu del Ejercicio 6.6.3, y pruebe sus propiedades básicas. En particular, muestre que si

$n \in \mathbb{N}$ es al menos 3 y $a_1, \ldots, a_n$ son enteros, entonces

$$\mathsf{mcm}(\mathsf{mcm}(a_1, a_2), a_3, \ldots, a_n) = \mathsf{mcm}(a_1, a_2, a_3, \ldots, a_n).$$

Algunas propiedades del máximo común divisor y del mínimo común múltiplo

6.6.5. Ejercicio.

(*a*) Si a, b y c son enteros, entonces

$$\mathsf{mcd}(\mathsf{mcd}(a, b), c) = \mathsf{mcd}(a, \mathsf{mcd}(b, c))$$

y

$$\mathsf{mcm}(\mathsf{mcm}(a, b), c) = \mathsf{mcm}(a, \mathsf{mcm}(b, c)).$$

En otras palabras, las operaciones $\mathsf{mcd}(\cdot, \cdot)$ y $\mathsf{mcm}(\cdot, \cdot)$ son asociativas.

(*b*) Si a, b, c son enteros, entonces

$$\mathsf{mcd}(a, \mathsf{mcm}(b, c)) = \mathsf{mcm}(\mathsf{mcd}(a, b), \mathsf{mcd}(a, c))$$

y

$$\mathsf{mcm}(a, \mathsf{mcd}(b, c)) = \mathsf{mcd}(\mathsf{mcm}(a, b), \mathsf{mcm}(a, c)).$$

(*c*) Si a y b no son simultáneamente nulos, entonces

$$\mathsf{mcd}\left(\frac{a}{\mathsf{mcd}(a, b)}, \frac{b}{\mathsf{mcd}(a, b)}\right) = 1.$$

(*d*) Si a, b y c son enteros, entonces

$$\mathsf{mcm}(a, b, c) \cdot \mathsf{mcd}(a, b) \cdot \mathsf{mcd}(b, c) \cdot \mathsf{mcd}(c, a) = abc \cdot \mathsf{mcd}(a, b, c).$$

Este ejercicio fue uno de los tomados en la primera Olimpíada de Matemáticas de Moscú en 1935.

La sucesión $(a^n - 1)_{n\geq 0}$

6.6.6. Ejercicio. Sea a un entero distinto de 0 y de 1.

(*a*) Si x e y son enteros y $n \in \mathbb{N}$, entonces

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

y, en particular, $x - y$ divide a $x^n - y^n$.

(*b*) Si $n, m \in \mathbb{N}$ y n divide a m, entonces $a^n - 1$ divide a $a^m - 1$.

(*c*) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m, entonces

$$\mathsf{mcd}(a^n - 1, a^m - 1) = \mathsf{mcd}(a^r - 1, a^m - 1).$$

(*d*) Si $n, m \in \mathbb{N}$, entonces $\mathsf{mcd}(a^n - 1, a^m - 1) = a^{\mathsf{mcd}(n,m)} - 1$.

Los números de Fibonacci

6.6.7. Ejercicio. Sea $(F_n)_{n\geq 0}$ la sucesión de los números de Fibonacci.

(*a*) Muestre que para todo $n \in \mathbb{N}$ se tiene que $\mathsf{mcd}(F_n, F_{n+1}) = 1$ y encuentre enteros x e y tales que $xF_n + yF_{n+1} = 1$.

(*b*) Si $n, m \in \mathbb{N}$ y n divide a m, entonces F_n divide a F_m.

(*c*) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m, entonces

$$\mathsf{mcd}(F_n, F_m) = \mathsf{mcd}(F_r, F_m).$$

(*d*) Si $n, m \in \mathbb{N}_0$, entonces

$$\mathsf{mcd}(F_n, F_m) = F_{\mathsf{mcd}(n,m)}.$$

Sugerencia: Para probar la parte (*b*) es útil recordar el Lema 5.4.7 del Capítulo 5.

6.6.8. Ejercicio. Sea $n \in \mathbb{N}$.

(*a*) El algoritmo de Euclides necesita $n + 1$ pasos para calcular $\mathsf{mcd}(F_{n+3}, F_{n+2})$.

(*b*) Si a y b son dos enteros positivos tales $a > b$ y para los cuales el algoritmo de Euclides necesita $n + 1$ pasos para calcular $\mathsf{mcd}(a, b)$, entonces $a \geq F_{n+3}$ y $b \geq F_{n+2}$.

Observemos que la conjunción de estas dos afirmaciones nos dice que el peor caso — en el sentido de que tarda la máxima cantidad de pasos — para el algoritmo de Euclides es aquél en el que sus datos de partida son dos números de Fibonacci consecutivos.

(*c*) Si a y b son enteros tales que $1 < b, a < N$, entonces el número de pasos que algoritmo de Eu-

clides requiere para calcular $\mathsf{mcd}(a,b)$ no excede a $\lceil \log_\varphi(\sqrt{5}N)\rceil - 2$. Aquí $\varphi = (1+\sqrt{5})/2$, $\log_\varphi$ denota el logaritmo en base φ y para cada número real u escribimos $\lceil u\rceil$ el menor entero mayor que u.

Este resultado es conocido como *Teorema de Lamé*, por Gabriel Lamé, quien lo obtuvo en 1844. Puede encontrarse una discusión detallada del algoritmo de Euclides desde el punto de vista de la complejidad en el libro [Knu1969].

Los números de la forma $2^{2^n}+1$

6.6.9. Ejercicio. Para cada $n \in \mathbb{N}_0$ sea $F_n := 2^{2^n}+1$.

(*a*) Muestre que para todo $n \in \mathbb{N}_0$ y todo $k \in \mathbb{N}$ vale $F_n \mid F_{n+k} - 2$.

(*b*) Deduzca de eso que los números $F_0, F_1, F_2, \ldots$ son coprimos dos a dos.

El desarrollo en fracción continua finita de un número racional

6.6.10. Ejercicio. Sea a/b un número racional positivo escrito de manera irreducible, de manera que a y b son enteros positivos y $\mathsf{mcd}(a,b) = 1$. Sea $(r_i)_{i\geq 0}$ la sucesión construida por el algoritmo de Euclides para calcular el máximo común divisor de a y b, como en 6.4.6, y sea N el número que nos da la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_N = \mathsf{mcd}(a,b) = 1$ y $r_i = 0$ si $i > N$. Sean, finalmente, $q_2, \ldots, q_{N+1}$ la sucesión de los cocientes que encontramos al llevar a cabo el algoritmo: esto es, tales que $r_{i-2} = q_i r_{i-1} + r_i$ para cada $i \in \{2, \ldots, N+1\}$.

Muestre que

$$\frac{a}{b} = q_2 + \frac{r_2}{r_1} = q_2 + \cfrac{1}{q_3 + \cfrac{r_3}{r2}} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{r_4}{r_3}}} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{q_5 + \cfrac{r_5}{r_4}}}} = \cdots$$

y que se puede continuar así hasta obtener la expresión

$$\frac{a}{b} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots + \cfrac{1}{q_{N+1}}}}}.$$

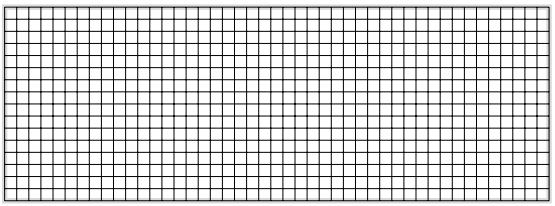
Esta escritura para el número a/b se llama su expresión como ***fracción continua finita***. Así, por

ejemplo, tenemos que

$$\frac{77}{30} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}}},$$

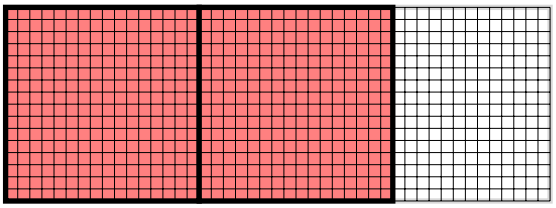
$$\frac{81\,201}{56\,660} = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{6 + \cfrac{1}{7 + \cfrac{1}{8}}}}}}}.$$

6.6.11. Sean a y b dos enteros positivo tales que $a \geq b$ y supongamos que tenemos una cuadrícula de a por b. Por ejemplo, si $a = 45$ y $b = 16$, tenemos el siguiente diagrama



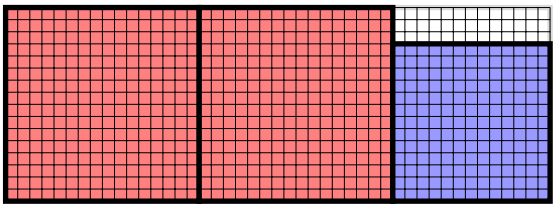
Nuestro objetivo es cubrir esta cuadrilla con cuadrados de tamaños enteros. Es claro que esto es posible: basta usar $45 \cdot 16 = 720$ cuadrados de 1 por 1. Lo que queremos, sin embargo, es usar la menor cantidad posible de cuadrados. Una estrategia posible que podemos probar es la de usar la mayor cantidad posible de cuadrados lo más grandes que podamos.

En este ejemplo concreto, es claro que el tamaño máximo de un cuadrado de lados enteros que entra en el diagrama es 16. Además, como el cociente de dividir 45 por 16 es 2, el número máximo de cuadrados de lado 16 que podemos poner es 2.

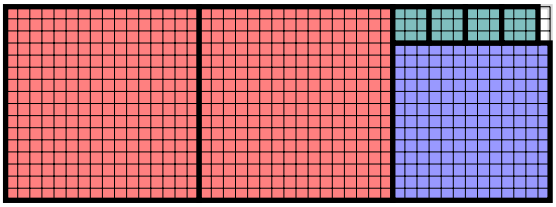


Después de poner esos dos rectángulos, nos queda sin cubrir una región de 13 por 16. El lado del

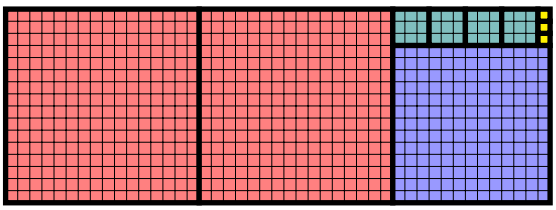
cuadrado más grande que entra en ella es 13 y claramente entra uno solo: si lo ponemos, queda



Quedó libre una región de 13 por 3: el cuadrado más grande que entra ahí es de 3 por 3 y entran 4 de ellos.



Finalmente, es claro que la región que nos queda sólo la podemos cubrir con 3 cuadrados de 1 por 1. Al terminar, entonces, tenemos la siguiente situación:

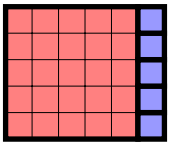


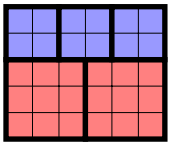
6.6.12. Ejercicio. Sean a y b dos enteros positivos tales que $a \geq b$ y sean $(r_i)_{i\geq 0}$, N y $q_2, \ldots, q_{N+1}$ como en el Ejercicio 6.6.10. Se tiene que

$$ab = q_2 r_1^2 + q_3 r_3^2 + \cdots + q_{N+1} r_N^2$$

y es posible cubrir un rectángulo de a por b con $q_2 + q_3 + \cdots + q_{N+1}$ cuadrados de lados de longitud entera.

Observemos que no es claro que la estrategia que describimos arriba para hacer cubrir el rectángulo sea una que minimice el número de cuadrados y, de hecho, esto no es cierto. El menor ejemplo de esto aparece cuando consideramos un rectángulo de 6 por 5: de los siguientes dos diagramas el de la izquierda fue construido usando la estrategia anterior y usa en total 6 cuadrados, mientras que el de la derecha usa solamente 5.





Si a y b son enteros positivos tales que $a \geq b$ y $\mathsf{mcd}(a, b)$, escribamos $\sigma(a, b)$ al menor número de cuadrados de lados enteros con los que es posible cubrir un rectángulo de a por b. Richard Kenyon mostró en su trabajo [Ken1996] que hay una constante positiva C tal que

$$\mathsf{máx}\left\{\frac{a}{b}, \log_2 a\right\} \leq \sigma(a, b) \leq \frac{a}{b} + C \log_2 b$$

cada vez que a y b son enteros coprimos y $a \geq b > 0$.

En el contexto de este problema, es interesante recordar el siguiente teorema clásico de Max Dehn [Deh1903] y Roland Sprague [Spr1940], que tiene una demostración sorprendentemente difícil: un rectángulo puede ser cubierto con finitos cuadrados sin que estos se superpongan si y solamente si el cociente de las longitudes de sus lados es un número racional. Una demostración muy simplificada y más conceptual de este resultado — en el que el problema se reduce a un problema sobre el flujo de electricidad en un circuito eléctrico que es luego resuelto usando la Ley de Kirchoff — puede encontrarse en [BSST1940].

Capítulo 7

Congruencias

§7.1. La relación de congruencia

7.1.1. Sea $m_0 \in \mathbb{N}$. Decimos que dos enteros a y b son ***congruentes módulo*** m si $m \mid a - b$ y en ese caso escribimos

$$a \equiv b \mod m.$$

Esto define una relación en el conjunto $\mathbb{Z}$, la relación de ***congruencia módulo*** m.

Proposición. *Sea $m \in \mathbb{N}_0$. La relación de congruencia módulo m en $\mathbb{Z}$ es una relación de equivalencia.*

Demostración. Verifiquemos que esa relación tiene las tres propiedades necesarias.

- Si a es un elemento de $\mathbb{Z}$, entonces sabemos que $m \mid 0 = a - a$, así que $a \equiv a \mod m$.
- Sean a y b dos elementos de $\mathbb{Z}$ tales que $a \equiv b \mod m$, de manera que $m \mid a - b$. De acuerdo a la Proposición 6.1.2(*ii*) tenemos que $m \mid -(a - b) = b - a$ y, por lo tanto, que $b \equiv a \mod m$.
- Sean a, b y c tres elementos de $\mathbb{Z}$ tales que $a \equiv b \mod m$ y $b \equiv c \mod m$, de manera que $m \mid a - b$ y $m \mid b - c$. La Proposición 6.1.5 nos dice que entonces

  $$m \mid (a - b) + (b - c) = a - c$$

  y, en consecuencia, que $a \equiv c \mod m$.

Así, la congruencia módulo m es reflexiva, simétrica y transitiva: esto prueba que es una relación de equivalencia. □

7.1.2. El único entero divisible por 0 es 0 mismo, y esto implica inmediatamente que dos enteros son congruentes módulo 0 exactamente cuando son iguales. En otras palabras, la relación de congruencia módulo 0 es la relación identidad sobre el conjunto $\mathbb{Z}$. Por otro lado, todo entero es divisible por 1, y entonces dos enteros cualesquiera son congruentes módulo 1. La relación de congruencia módulo 1 es, por lo tanto, la relación total en el conjunto $\mathbb{Z}$. En vista de esto, la congruencia módulo uno de estos dos números no es particularmente interesante y nos restringimos en general a considerar módulos mayores que 1.

Por otro lado, es inmediato verificar que si m es un entero negativo la relación de congruencia módulo m coincide con al relación de congruencia módulo $-m$. Es por esta razón que normalmente pedimos que el módulo con el que trabajamos sea no negativo.

7.1.3. La relación de congruencia está estrechamente conectada con el algoritmo de la división:

Proposición. *Sea $m \in \mathbb{N}$. Dos enteros son congruentes módulo m si y solamente si tienen el mismo resto en la división por m.*

Demostración. Sean a y b dos enteros y sean q y r, por un lado, y q' y r', por otro, el cociente y el resto de la división de a y de b por m, de manera que $a = qm + r$, $0 \leq r < m$, $b = q'm + r'$ y $0 \leq r' < m$.

Supongamos primero que $a \equiv b \mod m$, es decir, que $m \mid a - b$. Como m divide a $(q - q')m$ y

$$a - b = (qm + r) - (q'm - r') = (q - q')m + r' - r,$$

vemos que m divide a $r - r'$. Usando el Lema **6.2.2** podemos concluir de esto que $r = r'$ y, por lo tanto, que la condición que da la proposición es necesaria para que a y b sean congruentes módulo m.

Supongamos ahora, para probar que esa condición también es suficiente, que $r = r'$. En ese caso tenemos que

$$a - b = (qm + r) - (q'm + r') = (q - q')m + (r - r') = (q - q')m$$

y es claro que m divide a $a - b$, es decir, que $a \equiv b \mod m$. La proposición queda así probada. □

7.1.4. Usando congruencias, es fácil caracterizar al resto de la división de un número por otro:

Proposición. *Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$.*

(*i*) *Si r es el resto de dividir a a por m, entonces $a \equiv r \mod m$.*

(*ii*) *Recíprocamente, si s es un elemento de $\{0, \ldots, m-1\}$ tal que $a \equiv s \mod m$, entonces s es el resto de dividir a a por m.*

Estas dos afirmaciones juntas nos dicen que el resto de dividir a a por m es el único elemento

de $\{0, \ldots, m-1\}$ que es congruente con a módulo m.

Demostración. Sea a un entero y sean q y r, respectivamente, el cociente y el resto de dividir a a por m, de manera que, en particular, $a = qm + r$. Se sigue de esta igualdad que $a - r = qm$, así que claramente $m \mid a - r$, esto es, $a \equiv r \mod m$. Esto prueba la primera parte de la proposición.

Para ver la segunda, supongamos que $s \in \{0, \ldots, m-1\}$ es tal que $a \equiv s \mod m$. Como además $a \equiv r \mod m$, como acabamos de probar, vemos que $r \equiv s \mod m$, es decir, que m divide a $r - s$: de acuerdo al Lema 6.2.2, esto implica que $r = s$, esto es, que s es el resto de dividir a a por m. □

7.1.5. La relación de congruencia es compatible con las operaciones aritméticas en el siguiente sentido:

Proposición. *Sea $m \in \mathbb{N}$. Si a, a', b y b' son enteros tales que $a \equiv a' \mod m$ y $b \equiv b' \mod m$, entonces*

$$-a \equiv -a' \mod m,$$
$$a + b \equiv a' + b' \mod m$$

y

$$ab \equiv a'b' \mod m.$$

Demostración. Sean a, a', b, b' enteros tales que $a \equiv a' \mod m$ y $b \equiv b' \mod m$, de manera que m divide a $a - a'$ y a $b - b'$, y hay, por lo tanto, enteros c y d tales que $a - a' = cm$ y $b - b' = dm$. Por un lado, tenemos que

$$(-a) - (-a') = -(a - a') = (-c)m$$

así que m divide a $(-a) - (-a')$ y, en consecuencia, $-a \equiv -a' \mod m$. Por otro,

$$(a + b) - (a' + b') = (a - a') + (b - b') = cm + dm = (c + d)m$$

y

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \\ &= cmb + a'dm = (cb + a'd)m. \end{aligned}$$

Esto nos dice que m divide a $(a + b) - (a' + b')$ y a $ab - a'b'$, es decir, que $a + b \equiv a' + b' \mod m$ y que $ab \equiv a'b' \mod m$, como afirma la proposición. □

7.1.6. La Proposición 7.1.5 nos dice que la relación de congruencia es compatible con la suma y el producto de pares de enteros, pero una inducción más o menos evidente muestra que esto se

extiende a sumas y productos de cualquier número finito de enteros:

Corolario. *Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ son tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$, entonces*

$$a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \mod m$$

y

$$a_1 \cdots a_n \equiv b_1 \cdots b_n \mod m.$$

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

> *si $a_1, \ldots, a_n, b_1, \ldots, b_n$ son enteros tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$, entonces $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \mod m$ y $a_1 \cdots a_n \equiv b_1 \cdots b_n \mod m$.*

Mostraremos que $P(n)$ vale para todo $n \in \mathbb{N}$ y esto claramente probará el corolario. Observemos que la afirmación $P(1)$ vale trivialmente, así que bastará que establezcamos el paso inductivo.

Sea entonces n un elemento cualquiera de $\mathbb{N}$ tal que $n \geq 2$, supongamos que la afirmación $P(n-1)$ vale, y sean $a_1, \ldots, a_n, b_1, \ldots, b_n$ enteros tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$. En particular, tenemos que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n-1\}$ y, por lo tanto, la hipótesis inductiva nos dice que

$$a_1 + \cdots + a_{n-1} \equiv b_1 + \cdots + b_{n-1} \mod m$$

y

$$a_1 \cdots a_{n-1} \equiv b_1 \cdots b_{n-1} \mod m.$$

Como además $a_n \equiv b_n \mod m$, usando la Proposición 7.1.5, tenemos que

$$\begin{aligned} a_1 + \cdots + a_n &= (a_1 + \cdots + a_{n-1}) + a_n \\ &\equiv (b_1 + \cdots + b_{n-1}) + b_n \mod m \\ &= b_1 + \cdots + b_n \end{aligned}$$

y, de manera similar, que

$$\begin{aligned} a_1 \cdots a_n &= (a_1 \cdots a_{n-1}) a_n \\ &\equiv (b_1 \cdots b_{n-1}) b_n \mod m \\ &= b_1 \cdots b_n. \end{aligned}$$

Esto significa que la afirmación $P(n)$ vale y completa la inducción. □

7.1.7. Un caso particular útil del corolario que acabamos de probar es aquel en que consideramos

productos en que todos los factores son iguales:

Corolario. *Sea $m \in \mathbb{N}$. Si a y b son dos enteros tales que $a \equiv b \mod m$ y k es un entero no negativo, entonces $a^k \equiv b^k \mod m$.*

Demostración. Si k es 0 esto es evidente, y si k es positivo esto es un caso particular de la segunda afirmación del Corolario 7.1.6 en el que $a_1 = \cdots = a_k = a$ y $b_1 = \cdots = b_k = b$. □

7.1.8. Como consecuencia de la Proposición 7.1.5 y sus corolarios, cuando tenemos una expresión aritmética construida a partir de enteros usando sumas, productos y potencias y estamos trabajando módulo algún entero positivo m podemos reemplazar esos enteros por otros congruentes. Así, por ejemplo, trabajando módulo 7 es

$$222 + 210^{23} - 297 \cdot 91 \equiv 5 + 0^{23} - 3 \cdot 0 = 5,$$

ya que $222 \equiv 5$, $210 \equiv 91 \equiv 0$ y $297 \equiv 3$. De manera similar, podemos ver que para todo $n \in \mathbb{N}$ el número $10^{3n} + 1$ es divisible por 7 si y solamente si n es impar. En efecto, trabajando módulo 7 tenemos que $10^3 \equiv -1$, así que

$$10^{3n} + 1 = (10^3)^n + 1 \equiv (-1)^n + 1,$$

y esto es 0 si y solamente si n es impar. Observemos que esto nos dice además que cuando n es par el resto de dividir a $10^{3n} + 1$ por 7 es 2.

7.1.9. Veremos muchas aplicaciones de esto en todo lo que sigue, pero mostremos cómo podemos usar los resultados de esta sección para resolver una parte del Ejercicio 6.6.6:

Proposición. *Si a es un entero distinto de 1 y n un entero positivo, entonces $a - 1$ divide a $a^n - 1$.*

Demostración. Sea a un entero distinto de 1 y sea n un entero positivo. Como $|a - 1|$ divide a $a - 1$, trabajando módulo $|a - 1|$ es claro que $a \equiv 1$. De acuerdo al Corolario 7.1.7, entonces, tenemos que $a^n \equiv 1^1 = 1$ y esto significa, precisamente, que $|a - 1|$ divide a $a^n - 1$. La afirmación de la proposición sigue inmediatamente de esto. □

Es importante notar cuál es la diferencia entre esta forma de proceder y la sugerida por el ejercicio 6.6.6. Allí, para ver que $a - 1$ divide a $a^n - 1$ mostramos explícitamente cuál es el cociente — a saber, la suma geométrica $1 + a + \cdots + a^{n-1}$ — mientras que aquí llegamos a la misma conclusión sin necesidad de hacer eso. Es más: el argumento que acabamos de usar no nos da ninguna idea sobre cuál es ese cociente. En la sección siguiente haremos uso de esta misma idea para obtener varios criterios de divisibilidad.

7.1.10. Una última propiedad extremadamente importante y que nos será muy útil más adelante es la siguiente aplicación de la identidad de Bézout.

Proposición. *Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Existe un entero $b \in \mathbb{Z}$ tal que $ab \equiv 1 \mod m$ si y solamente si a es coprimo con m.*

Demostración. Supongamos primero que a y m son coprimos, de manera que existen enteros b y c tales que $ab + mc = 1$. Tenemos entonces que $ab = 1 - mc \equiv 1 \mod m$ y esto muestra que la condición del enunciado es suficiente.

Por otro lado, supongamos que existe un entero b tal que $ab \equiv 1 \mod m$, de manera que m divide a $ab - 1$, esto es, existe $x \in \mathbb{Z}$ tal que $ab - 1 = mx$. Si d un divisor común positivo de a y m, entonces d divide también a $ab - mx = 1$: esto sólo es posible si $d = 1$ y muestra que $\mathsf{mcd}(a, m) = 1$. □

7.1.11. Por ejemplo, como 7 es coprimo con 152, esta proposición nos dice que hay un entero b tal que $7b \cong 1 \mod 152$. Para encontrarlo, usamos el algoritmo de Euclides extendido para encontrar los coeficientes de la identidad de Bézout entre 152 y 7: encontramos fácilmente que $3 \cdot 152 + (-65) \cdot 7 = 1$ y entonces podemos elegir b igual a -65.

Notemos que -65 no es el único entero b con la propiedad de que $7b \equiv 1 \mod 152$. De hecho, si b' es otro entero cualquiera que es congruente con b módulo 152, entonces sabemos que $7b' \equiv 7b \equiv 1 \mod 152$. Nuestro siguiente resultado dice que de esta manera obtenemos todos los enteros con esta propiedad.

Proposición. *Sea $m \in \mathbb{N}$ y sean a y b dos enteros tales que $ab \equiv 1 \mod m$. Un entero c tiene la propiedad de que $ac \equiv 1 \mod m$ si y solamente si es congruente con b módulo m.*

Demostración. Sea c un entero. Si $c \equiv b \mod m$, entonces sabemos que $ac \cong ab \cong 1 \mod m$ y, por lo tanto, la condición que da la proposición es necesaria. Por otro lado, si es $ac \equiv 1 \mod m$, entonces $c = 1c \equiv bac \equiv b1 = 1 \mod m$, así que esa condición también es suficiente. □

7.1.12. Si $m \in \mathbb{N}$ y a es un entero coprimo con m, entonces la Proposición 7.1.10 nos dice que hay enteros b tales que $ab \equiv 1 \mod m$: los llamamos ***inversos módulo m*** de a. Hay, de hecho, muchos, pero la Proposición 7.1.11 nos dice que el conjunto de ellos es una clase de congruencia módulo m: decimos que es «único módulo m».

§7.2. Algunos criterios de divisibilidad

7.2.1. Como $10 \equiv 1 \mod 9$, el Corolario 7.1.7 nos dice que $10^n \equiv 1^n = 1 \mod 9$ para todo $n \in \mathbb{N}$. De esto obtenemos fácilmente el siguiente criterio de divisibilidad por 9:

Proposición. *Sea a un entero positivo. Si $a = (d_k, \ldots, d_0)_{10}$ es la escritura de a en base 10, entonces a es divisible por 9 si y solamente si la suma $d_0 + \cdots + d_k$ de sus dígitos decimales lo es y, de hecho, ambos números tienen el mismo en la división por 9.*

Así, por ejemplo, la suma de los dígitos decimales de 45 261 189 es 36, y la suma de los dígitos decimales de este último número es 9: vemos así que 9 divide a 45 261 189. Esta proposición es el primer ejemplo que da Gauss en su *Disquisitiones Arithmeticae* de una aplicación de la relación de congruencia, y la prueba de damos es exactamente la misma que él da —que reproducimos en la Figura 7.1 en la página siguiente.

Demostración. Sea $(d_k, \cdots, d_0)_{10}$ la escritura decimal de a, de manera que

$$a = d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k.$$

Como observamos arriba, es $10^n \equiv 1 \mod 9$ para todo $n \in \mathbb{N}$, así que gracias a la Proposición 7.1.5 tenemos que $d_i \cdot 10^i \equiv d_1 \cdot 1 = d_1 \mod 9$ para cada $i \in \{0, \ldots, k\}$ y entonces, usando el Corolario 7.1.6, que

$$a = d_0 + d_1 + \cdot 10 + \cdots + d_k \cdot 10^k \equiv d_0 + d_1 + \cdots + d_k \mod 9.$$

Sabemos que a es divisible por 9 si y solamente si $a \equiv 0 \mod 9$ y, de acuerdo a lo que acabamos de probar, esto sucede si y solamente si $d_p + \cdots + d_k \equiv 0 \mod 9$, es decir, si la suma $d_0 + \cdots + d_k$ es divisible por 9. Esto prueba la proposición. □

7.2.2. De manera similar podemos obtener un criterio de divisibilidad por 11:

Proposición. *Sea a un entero positivo y sea $(d_k, \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 11 si y solamente si 11 divide a la suma alternada de sus dígitos decimales,*

$$d_0 - d_1 + d_2 - d_2 + \cdots + (-1)^k d_k.$$

Por ejemplo, el número 64 320 883 es divisible por 11: en efecto, la suma alternada de sus dígitos decimales es $3 - 8 + 8 - 0 + 2 - 3 + 4 - 6 = 0$, que es divisible por 11.

12.

Theorematibus in hoc capite traditis complura quae in arithmeticis doceri solent innituntur, e. g. regulae ad explorandam divisibilitatem numeri propositi per 9, 11 aut alios numeros. *Secundum modulum* 9 omnes numeri 10 potestates unitati sunt congruae: quare si numerus propositus habet formam $a+10b+100c$ + etc., idem residuum minimum secundum modulum 9 dabit, quod $a+b+c$ + etc. Hinc manifestum est, si figurae singulae numeri decadice expressi sine respectu loci quem occupant addantur, summam hanc numerumque propositum eadem residua minima praebere, adeoque hunc per 9 dividi posse, si illa per 9 sit divisibilis, et contra. Idem etiam de divisore 3 tenendum. Quoniam *secundum modulum* 11, $100 \equiv 1$ erit generaliter $10^{2k} \equiv 1$. $10^{2k+1} \equiv 10 \equiv -1$, et numerus formae $a+10b+100c+$ etc. secundum modulum 11 idem residuum minimum dabit quod $a-b+c$ etc.; unde regula nota protinus derivatur. Ex eodem principio omnia similia praecepta facile deducuntur.

Figura 7.1. El párrafo 12 de las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss, en el que enuncia y prueba nuestra Proposición 7.2.1.

Demostración. Como $10 \equiv -1 \mod 11$, para todo $n \in \mathbb{N}_0$ es $10^n \equiv (-1)^n \mod 11$, así que, como en la prueba de la proposición anterior, tenemos que

$$a = \sum_{i=0}^{k} d_i \cdot 10^n \equiv \sum_{i=0}^{k} d_i \cdot (-1)^n \mod 11.$$

De esto se deduce que 11 divide a a si y solamente si divide a $\sum_{i=0}^{k} d_i \cdot (-1)^n$, que es lo que afirma la proposición. □

7.2.3. El siguiente resultado es similar al de la Proposición 7.2.1, pero ahora tomando los dígitos en bloques de a tres:

Proposición. *Sea $a \in \mathbb{N}$ y sean $(d_k \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 27 si y solamente si la suma de los números que se obtienen agrupando sus dígitos de a tres desde la derecha,*

$$(d_2, d_1, d_0)_{10} + (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \cdots,$$

es divisible por 27.

Así, el número 12 492 342 315 es divisible por 27 porque 315 + 342 + 492 + 12 = 1 161 lo es, y esto es así porque 161 + 1 = 162 = 27 · 6 lo es.

Demostración. Sea $l = \lfloor k/3 \rfloor$ y, para cada $i \in \{0, \dots, l\}$, sea $e_i = (d_{3i+2}, d_{3i+1}, d_{3i})_{10}$. Sabemos que $a = (e_l, \dots, e_0)_{1000}$ y la proposición es consecuencia de que

$$a = \sum_{i=0}^{l} e_i \cdot 1000^i \equiv \sum_{i=0}^{l} e_i \mod 27,$$

ya que $1000 \equiv 1 \mod 27$. □

7.2.4. Hay muchos criterios de divisibilidad que miran solamente los últimos dígitos del número. Algunos de ellos son los siguientes:

Proposición. *Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a.*

(*i*) *El número a es divisible por 2 si y solamente si d_0 es par, y es divisible por 5 si y solamente si $d_0 \in \{0, 5\}$.*

(*ii*) *El número a es divisible por 4 o por 25 si y solamente si el número $(d_1, d_0)_{10}$ lo es.*

Usando esta proposición vemos inmediatamente que 12 326 es divisible por 2, que 101 436 no es divisible por 5, que 874 917 no es divisible por 4 y que 1 927 225 es divisible por 25.

Demostración. Como $10 \equiv 0 \mod 2$ y $10 \equiv 0 \mod 5$, para todo $n \in \mathbb{N}$ se tiene que $10^n \equiv 0 \mod 2$ y $10^n \equiv 0 \mod 5$. Esto implica que

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \equiv d_0$$

tanto módulo 2 como módulo 5. La primera afirmación de la proposición es consecuencia de esto. Por otro lado, como $10^2 \equiv 0$ módulo 4 y módulo 25, tenemos que para cada entero $n \geq 2$ es $10^n = 10^2 \cdot 10^{n-2} \equiv 0 \cdot 10^{n-2} = 0$ tanto módulo 4 como módulo 25 y, por lo tanto,

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \equiv d_0 + d_1 \cdot 10 = (d_1, d_0)_{10}$$

módulo 4 o módulo 25. De esta congruencia se deduce la segunda afirmación de la proposición. □

7.2.5. Un tercer tipo de criterio de divisibilidad puede deducirse usando las mismas ideas.

Proposición. *Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 7 si $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ lo es.*

El interés de esto es que el número $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ es más chico que a y, por lo tanto, que podemos usar el criterio recursivamente. Por ejemplo, para ver que 96 502 es divisible por 7 basta observar que $2 \cdot 965 + 2 = 1\,932$ lo es, y para esto que $2 \cdot 19 + 32 = 70$ lo es.

Demostración. Si $b = (d_k, \dots, d_2)_{10}$ y $c = (d_1, d_0)_{10}$, entonces

$$a = 100b + c \equiv 2b + c \mod 7,$$

ya que $100 \equiv 2 \mod 7$. La proposición es consecuencia de esta congruencia. □

7.2.6. Es natural preguntarse si para todo entero m hay un criterio de divisibilidad por m del estilo de los que vimos.

7.2.7. Proposición. *Sea m un entero positivo. Hay dos enteros positivos N y M tales que para todo $n \in \mathbb{N}$ vale*

$$n \geq N \implies 10^n \equiv 10^{n+M} \mod m.$$

Demostración. Consideremos la sucesión de números

$$r_m(10^0), \quad r_m(10^1), \quad r_m(10^2), \quad r_m(10^3), \quad \dots$$

Todos estos números pertenecen al conjunto $\{0, \dots, m-1\}$ así que no pueden ser distintos: esto nos dice que existen dos enteros u_0 y v_0 tales que $u_0 < v_0$ y $r_m(10^{u_0}) = r_m(10^{v_0})$.

Como consecuencia de esto, el conjunto S de los enteros positivos u tales que existe otro entero v tal que $u < v$ y $r_m(10^u) = r_m(10^v)$ no es vacío, ya que contiene a u_0. Podemos entonces considerar el número $N \coloneqq \min S$. Ahora bien, como N pertenece a S, el conjunto

$$T \coloneqq \{v \in \mathbb{N} : r_m(10^N) = r_m(10^{N+v})\}$$

no es vacío y, otra vez, podemos considerar su elemento mínimo $M \coloneqq \min T$.

Sea ahora n un entero positivo tal que $n \geq N$ y sean q y r el cociente y el resto de dividir a $n - N$ por M, de manera que $n - N = qM + r$ y $0 \leq r < M$. Si $q = 0$, de manera que $n = N + r$, entonces

$$10^{n+M} = 10^{N+M+r} = 10^{N+M}10^r \equiv 10^N 10^r = 10^{N+r} = 10^n \mod m.$$

□

§7.3. Los enteros módulo m

7.3.1. Si $m \in \mathbb{N}$, escribimos $\mathbb{Z}_m$ al conjunto cociente de $\mathbb{Z}$ por la relación de congruencia módulo m y lo llamamos el conjunto de los ***enteros módulo*** m. Es importante recordar que a pesar de este nombre, los elementos de $\mathbb{Z}_m$ no son enteros sino clases de equivalencia, es decir, *conjuntos* de enteros.

7.3.2. Una consecuencia importante de la Proposición 7.1.3 es la determinación de la cantidad de elementos de $\mathbb{Z}_m$:

Proposición. *Sea $m \in \mathbb{N}$. La relación de congruencia módulo m parte a $\mathbb{Z}$ en m clases de equivalencia, que son*

$$[0],\ [1],\ \ldots,\ [m-1].$$

Demostración. Sea $a \in \mathbb{Z}$ y sean $q \in \mathbb{Z}$ y $r \in \{0, \ldots, m-1\}$ el cociente y el resto de la división de a por m. Como $a - r = qm$, tenemos que $a \equiv r \mod m$ y, por lo tanto, que $[a] = [r]$. Esto nos dice que todas las clases de congruencia módulo m aparecen en la lista del enunciado. Para terminar, entonces, bastará que probemos que las m clases allí listadas son distintas dos a dos.

Sean $i, j \in \{0, \ldots, m-1\}$ y supongamos que $[i] = [j]$, de manera que $i \equiv j \mod m$. La Proposición 7.1.3 nos dice entonces que i y j dan el mismo resto al ser divididos por m: como $0 \leq i, j < m$, esto implica que $i = j$ y prueba lo que queríamos. □

7.3.3. La compatibilidad entre la relación de congruencia y las operaciones aritmética que afirma la Proposición 7.1.5 se ve reflejada en el siguiente resultado:

Proposición. *Sea $m \in \mathbb{N}$. Hay funciones $S, P : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ tales que cada vez que a y b está en $\mathbb{Z}$ se tiene que*

$$S([a],[b]) = [a+b]$$

y

$$P([a],[b]) = [ab].$$

Demostración. Consideremos el subconjunto

$$S = \{(([a],[b]),[a+b]) \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

del conjunto $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$. Se trata, por supuesto, de una relación de $\mathbb{Z}_m \times \mathbb{Z}_m$ a $\mathbb{Z}_m$. Mostremos que se trata, de hecho, de una función.

- Sea $x \in \mathbb{Z}_m \times \mathbb{Z}_m$, de manera que existen α y $\beta \in \mathbb{Z}_m$ tales que $x = (\alpha, \beta)$. Como $\mathbb{Z}_m$ es

el cociente de $\mathbb{Z}$ por la relación de congruencia módulo m, existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, de acuerdo a la definición del conjunto S, el par ordenado $(x, [a+b]) = (([a], [b]), [a+b])$ pertenece a S.

- Supongamos, por otro lado, que $x \in \mathbb{Z}_m \times \mathbb{Z}_m$ e y, $y' \in \mathbb{Z}_m$ son tales que los pares ordenados(x, y) y (x, y') están en S. Como recién, existen enteros a, b, c y c' tales que $x = ([a], [b])$, $y = [c]$ e $y' = [c']$.

  Ahora bien, como $(x, y) = (([a], [b]), [c])$ está en S, existen a_1, $b_1 \in \mathbb{Z}$ tales que $[a] = [a_1]$, $[b] = [b_1]$ y $[c] = [a_1 + b_1]$. Esto nos dice que modulo m se tiene que $a \equiv a_1$, $b \equiv b_1$ y $c \equiv a_1 + b_1$ y, por lo tanto, $c \equiv a + b$.

  De manera similar, como $(x, y') = (([a], [b]), [c'])$ está en S, existen a_2, $b_2 \in \mathbb{Z}$ tales que $[a] = [a_2]$, $[b] = [b_2]$ y $[c'] = [a_2 + b_2]$, de manera que $a \equiv a_2$, $b \equiv b_2$ y $c' \equiv a_2 + b_2$: esto implica que $c \equiv a + b$.

  Juntando estas dos cosas, concluimos que $c \equiv c'$ y, como consecuencia de ello, que $y = [c] = [c'] = y'$.

Si a y b son enteros, entonces es claro que $(([a], [b]), [a+b])$ está en S y esto significa, precisamente, que $S([a], [b]) = [a+b]$. Esto muestra que la función S satisface la condición que aparece en el enunciado.

Para ver el resto de la proposición, basta considerar el subconjunto

$$P = \{(([a], [b]), [ab]) \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

de $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$ y mostrar que es también una función $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ y que satisface la condición del enunciado. Esto puede hacerse de exactamente la misma forma a lo que acabamos de hacer: dejamos los detalles al lector. □

7.3.4. Normalmente escribimos a las funciones S y P que nos da la proposición que acabamos de probar usando los símbolos + y · de suma y producto: si α y β son dos elementos de $\mathbb{Z}_m$, escribimos $\alpha + \beta$ y $\alpha \cdot \beta$ en lugar de $S(\alpha, \beta)$ y $P(\alpha, \beta)$.

Así, si a y b son dos enteros, usando esta notación tenemos que

$$[a] + [b] = [a + b] \tag{1}$$

y

$$[a] \cdot [b] = [a \cdot b].$$

Es importante observar que los símbolos + y · en estas igualdades denotan cosas distintas a la izquierda y a la derecha del signo de igualdad: a la derecha + y · denotan las operaciones usuales entre enteros, mientras que a la izquierda denotan las operaciones que acabamos de definir entre elementos de $\mathbb{Z}_m$. Esto introduce, por supuesto, una ambigüedad en lo que escribimos, pero el contexto es siempre suficiente para resolverla.

7.3.5. Las operaciones de suma y producto que hemos definido en el conjunto $\mathbb{Z}_m$ tienen muchas de las mismas propiedades formales que las usuales de $\mathbb{Z}$:

Proposición. *Sea $m \in \mathbb{N}$.*

(*i*) *Si α, β y γ son elementos de $\mathbb{Z}_n$, entonces*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma), \tag{2}$$

$$\alpha + \beta = \beta + \alpha, \qquad \alpha \cdot \beta = \beta \cdot \alpha, \tag{3}$$

$$\alpha + [0] = \alpha = [0] + \alpha, \qquad \alpha \cdot [1] = \alpha = [1] \cdot \alpha,$$

y

$$(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma. \tag{4}$$

(*ii*) *Para cada $\alpha \in \mathbb{Z}_m$, existe $\beta \in \mathbb{Z}_m$ tal que $\alpha + \beta = \beta + \alpha = [0]$. Más aún, si a es un entero tal que $\alpha = [a]$, entonces podemos elegir $\beta = [-a]$.*

Las identidades de (2) nos dicen que las operaciones + y · son asociativa, las de (3) que son conmutativas, las de (3) que las clases $[0]$ y $[1]$ son elementos neutros para ellas, y la de (4) que el producto · se distribuye sobre sumas +. Por otro lado, la segunda parte de la proposición nos dice que todo elemento de $\mathbb{Z}_m$ posee un *opuesto* con respecto a la suma +.

Demostración. Cada una de estas afirmaciones es consecuencia de la correspondiente afirmación sobre las operaciones entre enteros y de la observación de que todo elemento de $\mathbb{Z}_m$ es de la forma $[a]$ para algún $a \in \mathbb{Z}$.

Por ejemplo, si α y β son dos elementos de $\mathbb{Z}_m$, entonces existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, por lo tanto,

$$\alpha + \beta = [a] + [b] = [a + b] = [b + a] = [b] + [a] = \beta + \alpha,$$

de manera que la suma en $\mathbb{Z}_m$ es conmutativa. La segunda y la cuarta de estas igualdades son consecuencia directa de la relación (1) y la tercera de la conmutatividad de la suma de enteros. Dejamos al lector la verificación de las demás afirmaciones de la proposición. □

7.3.6. A pesar de esta proposición, que nos dice que las operaciones de suma y producto en $\mathbb{Z}_m$ funcionan en muchos aspectos como las de $\mathbb{Z}$, hay diferencias importantes. Mencionemos las dos que son probablemente las principales:

- En $\mathbb{Z}$ el producto de dos enteros no nulo es siempre no nulo. En $\mathbb{Z}_m$, por otro lado, esto no es siempre cierto. Por ejemplo, si $m = 6$ sabemos que las clase $[2]$ y $[3]$ no son la clase nula $[0]$, pero su producto es $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$.
- En $\mathbb{Z}$ los dos únicos elementos inversibles son 1 y −1. En $\mathbb{Z}_m$ esto puede no ser cierto. Si

$m = 11$, por ejemplo, la clase $[4]$ es inversible, ya que el producto $[4] \cdot [3] = [12] = [1]$ es la clase unidad $[1]$: esto nos dice que $[4]$ es inversible en $\mathbb{Z}_{11}$ y, sin embargo, $[4]$ no es ni $[1]$ ni $[-1]$.

Con la información que tenemos disponible en este punto podemos caracterizar qué clases de $\mathbb{Z}_m$ son inversibles:

7.3.7. Proposición. *Sea m un entero positivo y sea a un entero. La clase de congruencia $[a]$ es inversible en $\mathbb{Z}_m$ si y solamente si el entero a es coprimo con m.*

Demostración. Si el entero a es coprimo con m, la Proposición 7.1.10 nos dice que hay un entero b tal que $ab \equiv 1 \mod m$ y, por lo tanto, tal que $[a] \cdot [b] = [ab] = [1]$. Recíprocamente, si la clase $[a]$ es inversible en $\mathbb{Z}_m$, entonces hay otra clase β en ese conjunto tal que $[a] \cdot \beta = [1]$. Si b es un entero tal que $\beta = [b]$, esto nos dice que $[ab] = [a] \cdot [b] = [a] \cdot \beta = [1]$, de manera que $ab \equiv 1 \mod m$ y, de acuerdo a la Proposición 7.1.10, entonces a es coprimo con m. □

§7.4. Ejercicios

Algunos criterios de divisibilidad

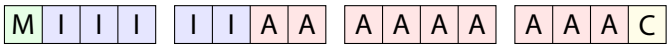
7.4.1. Ejercicio. Sea $a \in \mathbb{N}$ y sean $(d_k \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 7 si y solamente si la suma alternada de los números que se obtienen agrupando sus dígitos de a tres desde la derecha,

$$(d_2, d_1, d_0)_{10} - (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \cdots,$$

es divisible por 7. Así, por ejemplo, para ver que 13 476 066 723 es divisible por 7 observamos que $723 - 66 + 476 - 13 = 1\,120$ y que $120 - 1 = 119 = 7 \cdot 17$.

El algoritmo de Luhn

7.4.2. Por lo general, el número de una tarjeta de crédito tiene 16 dígitos y, de acuerdo al estándar ISO/IEC 7812, tiene a siguiente estructura:



- El primer dígito identifica la categoría de entidad que emitió la tarjeta. Por ejemplo, si es un 1 la tarjeta fue emitida por una aerolínea, y si es un 4 o un 5 por un banco.
- Los siguientes cinco dígitos forman un número que identifica al emisor de la tarjeta.
- Los siguientes nueve forman el número de cuenta.
- El último es el llamado ***dígito de control***.

Este último dígito queda determinado por los demás de acuerdo al llamado ***algoritmo de Luhn*** de la siguiente manera. Supongamos que $d_{15} \dots d_2 d_1$ son los quince primeros dígitos del número. Definimos una función $p : \{0, \dots, 9\} \to \{0, \dots, 9\}$ poniendo, para cada $i \in \{0, \dots, 9\}$,

$$p(i) \coloneqq \begin{cases} 0 & \text{si } i = 0; \\ r_9(2i) & \text{si } 0 < i < 9; \\ 9 & \text{si } i = 9. \end{cases}$$

Es fácil tabular los valores de p:

i	0	1	2	3	4	5	6	7	8	9
$p(i)$	0	2	4	6	8	1	3	5	7	9

Si ahora

$$s \coloneqq p(d_1) + d_2 + p(d_3) + d_3 + \cdots + p(d_{13}) + d_{14} + p(d_{15}),$$

entonces el dígito de control d_0 es el resto de dividir por 10 a $-s$. El número completo de la tarjeta es, entonces, $d_{15} \dots, d_2 d_1 d_0$. Por ejemplo, en el número de tarjeta de crédito

```
5204 7400 0990 0014
```
(5)

el número s es

$$p(5) + 2 + p(0) + 4 + p(7) + 4 + p(0) + 0 + p(0) + 9 + p(9) + 0 + p(0) + 0 + p(1) = 36$$

y el resto de dividir a -36 por 10 es 4, que es precisamente el último dígito de (5).

7.4.3. Ejercicio.

(*a*) Muestre que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito con d_0 calculado a partir del algoritmo de Luhn, entonces

$$d_0 + p(d_1) + d_2 + p(d_3) + d_3 + \cdots + p(d_{13}) + d_{14} + p(d_{15}) \equiv 0 \mod 10.$$

Cuando esta condición se cumple decimos que el número es ***válido***.

(*b*) Pruebe que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito, entonces un número $d'_{15}d'_{14}\dots d'_1d'_0$ se obtiene de él cambiando cualquier dígito no es válido.

Por ejemplo, como `5204 7400 0990 0014` es un número válido, ninguno de los siguientes números lo es

`1204 7400 0990 0014`, `5604 7400 0990 0014`,
`5294 7400 0990 0014`, `5203 7400 0990 0014`,
`5204 6400 0990 0014`, `5204 7401 0990 0014`.

(*c*) Pruebe que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito, entonces el número $d'_{15}d'_{14}\dots d'_1d'_0$ se obtiene de él intercambiando dos dígitos contiguos que son distintos entre sí y que no son 0 y 9 no es válido.

Por ejemplo, como `5204 7400 0990 0014` es un número válido, ninguno de los siguientes números lo es

`2504 7400 0990 0014`, `5024 7400 0990 0014`,
`5240 7400 0990 0014`, `5204 7040 0990 0014`,
`5204 7400 0990 0041`, `5207 4400 0990 0014`.

De todas formas, los números

`5204 7400 9090 0014`, `5204 7400 0909 0014`,

que se obtiene intercambiando en el número original un 0 y un 9 contiguos sí son válidos.

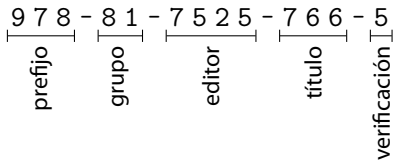
Estos resultados nos dicen que si copiamos mal un número de tarjeta de crédito porque copiamos un dígito mal o porque intercambiamos (casi) cualquier par de dígitos contiguos, podemos darnos cuenta. Esto nos permite reconocer cuándo hubo un error de esos dos tipos, aunque no arreglarlo.

Esta idea es debida a Hans Peter Luhn, que la patentó en 1960 en Estados Unidos [Luh1960]. Hoy pasó al dominio público y está especificada formalmente en el estándar ISO/IEC 7812-1 [IOfS-IEC2017].

Figura 7.2. El código ISBN de un libro y un código de barras que lo representa.

El código ISBN

7.4.4. Normalmente, cuando un libro es publicado el editor contacta a una agencia llamada *International ISBN Agency* y solicita que le asignen un número que lo identifique de manera única, llamado en número ISBN de libro, por las iniciales de *International Standard Book Number*. El formato de estos números fue cambiando desde que fueron creados en 1970. Hoy en día consiste de una tira de 13 dígitos, con el siguiente formato:



Los primeros tres dígitos forman el llamado *prefijo*, que hoy puede ser solamente 978 o 979. Los siguientes dos dígitos dan información sobre el *grupo de registro*, que normalmente está determinado por el país de origen de la publicación o su idioma. Después hay dígitos que identifican el editor de la publicación y al título registrado. Finalmente, el último dígito es el llamado *dígito de verificación*. Frecuentemente las distintas partes del número ISBN se escriben separadas por guiones, como en el ejemplo de arriba, pero no tienen longitudes fijas.

Decimos que un número ISBN $d_{13}d_{12}\cdots d_2d_1$, de manera que cada dígito d_i es un elemento de $\{0,1,\ldots,9\}$, es ***valido*** si

$$d_{12} + 3d_{11} + d_{10} + 3d_9 + d_8 + 3d_7 + d_6 + 3d_5 + d_4 + 3d_3 + d_2 + 3d_1 \equiv 0 \mod 10.$$

Los coeficientes que aparecen aquí son alternadamente 1 y 3.

Ejercicio.

(*a*) Muestre que si $d_{13}\cdots d_2$ los doce dígitos determinados por el prefijo, el grupo de registro, el editor y el título, entonces hay exactamente una forma de elegir un dígito más $d_1 \in \{0,\ldots,9\}$ de manera que $d_{13}\cdots d_2d_1$ sea un número ISBN válido.

(*b*) Pruebe que si $d_{13}\cdots d_2d_1$ es un número ISBN válido, entonces cambiar cualquiera de sus

dígitos por uno distinto, o intercambiar cualquiera de sus pares de dígitos adyacentes que no difieran en 5 resulta en un número que no es válido.

7.4.5. Hasta 2007 se usaba un formato distinto de números ISBN con solamente 10 «dígitos», en el que los nueve primeros son dígitos decimales, es decir, elementos de $\{0, \ldots, 9\}$ y el décimo es un elemento de $\{0, \ldots, 9, 10\}$. Cuando este último dígito es diez, lo escribimos con una letra `X`. Por ejemplo, los siguientes son números ISBN de 10 dígitos:

```
0-8044-2957-X    1-84356-028-3    93-86954-21-4  0-9752298-0-X
```

Como antes, en uno de estos números $d_{10}d_9 \cdots d_2 d_1$ los primeros 9 dígitos $d_{10} \cdots d_2$ se determinan a partir de información como el editor de la publicación y su proveniencia, y el último dígito d_1, llamado *de control*, se determina a partir de los demás, pero en este caso se elige de manera que

$$\sum_{i=1}^{10} (11 - i) d_i \equiv 0 \mod 11.$$

Cuando esta condición se cumple decimos que el número $d_{10}d_9 \cdots d_2 d_1$ es válido.

Ejercicio.

(*a*) Muestre que si $d_{10}d_9 \cdots d_2$ es un número de 9 dígitos decimales hay una única forma de elegir d_1 en $\{0, 1, \ldots, 9, 10\}$ de manera que el número $d_{10}d_9 \cdots d_2 d_1$ sea válido.

(*b*) Muestre que si en un número de estos que es válido cambiamos cualquiera de los dígitos por otro distinto o intercambiamos dos dígitos distintos adyacentes cualesquiera obtenemos un número que no es válido.

Notemos que la segunda parte de este ejercicio nos dice que este método de verificación es mejor que el que describimos arriba para los números ISBN de trece dígitos, ya que permite detectar *cualquier* transposición de dígitos. La razón por que la que este sistema fue abandonado y remplazado por el actual es la necesidad de usar códigos de barra para simplificar la lectura automática de estos números: los códigos de barra normalmente usados solo permiten codificar dígitos decimales.

Capítulo 8

Ecuaciones diofánticas

§8.1. Ecuaciones diofánticas

8.1.1. En el sentido más general, una ***ecuación diofántica*** es una ecuación en la que buscamos soluciones con valores enteros. El nombre de estas ecuaciones recuerda a Diofanto de Alejandría, conocido como "el padre del álgebra" y autor de una serie de libros, la *Arithmetica*, sobre la solución de ecuaciones algebraicas.

8.1.2. Vamos algunos ejemplos.

(*a*) *Ecuaciones diofánticas lineales.* Si $r \in \mathbb{N}$ y $a_1, \ldots, a_r, b \in \mathbb{Z}$, la ***ecuación diofánticas lineal*** consiste en decidir si existen r-uplas $(x_1, \ldots, x_r)$ de enteros tales que

$$a_1x_1 + \cdots + a_rx_r = b$$

y, cuando ese es el caso, encontrarlos.

(*b*) *La ecuación de Pitágoras.* En este caso, buscamos las ternas (x, y, z) de enteros tales que

$$x^2 + y^2 = z^2,$$

a las que llamamos ternas pitagóricas.

(*c*) *La ecuación de Pell.* Fijamos $n \in \mathbb{N}$. El problema de encontrar enteros x e y tales que

$$x^2 - ny^2 = 1$$

es una ecuación diofántica, la *ecuación de Pell*, por John Pell, aunque esta ecuación fue estudiada mucho tiempo antes — de hecho, la ecuación se conoce con el nombre de Pell porque Leonhard Euler equivocadamente atribuyó a este un método para su solución que fue en realidad fue desarrollado por William Brouncker.

(*d*) *La ecuación de Fermat.* Fijemos un entero positivo n. La ***ecuación de Fermat de exponente n*** es el problema de encontrar enteros x, y y z tales que

$$x^n + y^n = z^n. \tag{1}$$

Famosamente Fermat hizo la siguiente anotación en un margen de su copia del libro de Diofanto, al lado de donde está enunciado el Problema VIII, que es precisamente el de la ecuación de Pitágoras, que mencionamos recién:

> *Es imposible separar un cubo en dos cubos, o una potencia cuarta en dos potencias cuartas, o en general cualquier potencia más alta que la segunda en dos potencias similares. He descubierto una demostración verdaderamente maravillosa de esto, pero este margen es demaciado angosto para contenerla.*

Lo que ahí afirma Fermat es que la ecuación (1) no tiene soluciones (salvo las "triviales") cuando $n \geq 3$. Hoy hay acuerdo en que Fermat no tenía ninguna prueba de esto y fue recién en 1993 que Andrew Wiles pudo probar que la afirmación de Fermat es cierta —aunque hubo muchos resultados parciales antes.

(*e*) *La ecuación Ramanujan–Nagell.* Así es conocido el problema de encontrar enteros x y n tales que

$$2^n - 7 = x^2.$$

Notemos que en esta ecuación, a diferencia de todas las anteriores, hay una incógnita que aparece como un exponente. El problema fue planteado originalmente por Srinivasa Ramanujan en 1913, quien además conjeturó que hay exactamente diez soluciones, y esta conjetura fue probada por Trygve Nagell en 1948. Las diez soluciones (x, n) de la ecuación son los pares

$$(\pm 1, 3), \qquad (\pm 3, 4), \qquad (\pm 5, 5), \qquad (\pm 11, 7), \qquad (\pm 181, 15).$$

La ecuación de Ramanujan–Nagell parece a primera vista bastante exótica y antojadiza, pero aparece en realidad en varios contextos. Por ejemplo, es equivalente al problema de encontrar los números de Mersenne, es decir, de la forma $2^a - 1$ con $a \in \mathbb{N}_0$, que son triangulares, esto es, de la forma $b(b+1)/2$ con $b \in \mathbb{N}_0$. En efecto,

$$\begin{aligned} 2^a - 1 = \frac{b(b+1)}{2} &\iff 8(2^a - 1) = 4b(b+1) \\ &\iff 2^{a+3} - 8 = 4b^2 + 4b \\ &\iff 2^{a+3} - 7 = 4b^2 + 4b + 1 \\ &\iff 2^{a+3} - 7 = (2b+1)^2. \end{aligned}$$

Esto nos dice que el número de Mersenne $2^a - 1$ es igual al número triangular $b(b+1)/2$ si y solamente si el par $(x, n) = (2b+1, a+3)$ es una solución de la ecuación de Ramanujan–Nagell. Por supuesto, el problema de encontrar números de Mersenne que son triangulares no parece mucho menos antojadizo que la ecuación de Ramanujan–Nagell! En el trabajo [BS1956] de Georges Browkin y André Schinzel hay un estudio de este problema.

De todas formas, la ecuación de Ramanujan–Nagell aparece de forma natural en el estudio de los códigos con corrección de errores [SS1959], en teoría de álgebra diferencial [Mea1973] y en computación cuántica [PR2013]. No podemos aquí explicar cómo.

§8.2. Ecuaciones lineales con dos incógnitas

8.2.1. Como dijimos, una ***ecuación diofántica lineal*** es un problema de la siguiente forma: dados $r \in \mathbb{N}$ y $a_1, \ldots, a_r, b \in \mathbb{Z}$, decidir si hay r-uplas de enteros $(x_1, \ldots, x_r)$ tales que

$$a_1x_1 + \cdots a_rx_r = b$$

y, si ese es el caso, encontrarlas. Supondremos siempre que todos los coeficientes $a_1, \ldots, a_r$ son no nulos, ya que esto no nos restringe en nada. Nuestro objetivo en esta sección es resolver este problema completamente.

8.2.2. Empecemos por el caso más sencillo: aquel en que $r = 1$ y hay, por lo tanto, una sola incógnita. Así, tenemos dos enteros a y b y queremos determinar si existen enteros x tales que $ax = b$ y, cuando los hay, encontrarlos. Reconocemos inmediatamente aquí el problema de la división entera, que ya sabemos resolver:

Proposición. *Sean a y b dos enteros y supongamos que $a \neq 0$. Consideremos el problema de encontrar enteros x tales que*

$$ax = b.$$

Hay soluciones si y solamente si a divide a b. Si ese es el caso, entonces hay exactamente una solución, que es $x = b/a$.

Demostración. Si hay una solución al problema, esto es, si existe un entero x tal que $ax = b$, entonces a divide a b simplemente por definición: esto muestra que la condición del enunciado es necesaria para que exista una solución. Recíprocamente, si suponemos que esa condición se cumple, de manera que a divide a b y existe un entero c tal que $ac = b$, entonces claramente ese

entero c, que es b/a, es una solución a la ecuación. Esto muestra que la condición es también suficiente.

Supongamos ahora que x y x' son dos soluciones a la ecuación. En ese caso, tenemos que $ax = b = ax'$ y, por lo tanto, $a(x-x') = 0$. Como a no es nulo, esto es solo posible si $x-x' = 0$, esto es, si $x = x'$. Vemos así que cuando $a \neq 0$ y hay soluciones, hay de hecho una única solución. □

8.2.3. Consideremos ahora el caso en que hay dos variables, es decir, en que $r = 2$ en la situación de 8.2.1. Así, tenemos tres enteros a, b y c con $ab \neq 0$ y buscamos pares ordenados (x, y) de enteros tales que

$$ax + by = c.$$

Empezamos analizando el ***caso homogéneo***, es decir, aquel en el que $c = 0$.

Proposición. *Sean a y b dos enteros no nulos, sea $d \coloneqq \mathsf{mcd}(a, b)$, y sean a' y b' los enteros tales que $a = da'$ y $b = db'$. Las soluciones de la ecuación*

$$ax + by = 0, \tag{2}$$

son los pares de la forma $(tb', -ta')$ con $t \in \mathbb{Z}$.

Demostración. Supongamos que (x, y) es una solución de la ecuación (2), de manera que

$$0 = ax + by = da'x + db'y = d(a'x + b'y).$$

Como $d \neq 0$, esto nos dice que $a'x + b'y = 0$, así que $b'y = -a'x$. En particular, el entero b' divide a $-a'x$ y, como es coprimo con a', divide a x: existe entonces un entero t tal que $x = tb'$. Usando esto vemos que también $b'y = -a'x = -a'b't$, así que, como $b' \neq 0$, es $y = -a't$. Se sigue de esto que todas las soluciones de la ecuación son de la forma $(tb', -ta')$ con $t \in \mathbb{Z}$.

Por otro lado, si t es un entero, entonces $a \cdot (tb') + b \cdot (-ta') = 0$, así que el par $(tb', -ta')$ es una solución de la ecuación (2). Esto prueba la proposición. □

8.2.4. Podemos enunciar esta proposición de una forma equivalente que es a veces útil. Digamos que un par de enteros (x, y) es ***primitivo*** si $\mathsf{mcd}(x, y) = 1$. Notemos que si (x, y) es un par de enteros cualquiera no simultáneamente nulos y ponemos $d \coloneqq \mathsf{mcd}(x, y)$, entonces hay enteros x' e y' tales que $x = dx'$ e $y = dy'$ y es, por lo tanto, $(x, y) = (dx', dy')$ y el par (x', y') es primitivo: esto nos dice que todo par distinto de $(0, 0)$ es un múltiplo de un par primitivo.

Proposición. *Sean a y b dos enteros no nulos, y sean a' y b' los enteros tales que $a = da'$ y $b = db'$.*

(*i*) *La ecuación*

$$ax + by = 0, \tag{3}$$

tiene exactamente dos soluciones primitivas, $(b', -a')$ *y* $(-b', a')$.

(*ii*) *Si* (x_0, y_0) *es una solución primitiva de esa ecuación, entonces las soluciones de la ecuación son todos los pares de la forma* (tx_0, ty_0) *con* $t \in \mathbb{Z}$.

Demostración. Sabemos de la Proposición 8.2.3 que los pares $(b', -a')$ y $(-b', a')$ son soluciones de la ecuación y, como $\mathsf{mcd}(a', b') = 1$, se trata de soluciones primitivas. Más aún, como a' y b' son no nulos, ya que a y b son no nulos, estas dos soluciones son distintas. Por otro lado, si (x, y) es una solución primitiva de la ecuación (3), entonces esa proposición nos dice que $(x, y) = (tb', -ta')$ para exactamente un entero t, y es

$$1 = \mathsf{mcd}(x, y) = \mathsf{mcd}(tb', -ta') = |t|\,\mathsf{mcd}(b', -a') = |t|,$$

así que (x, y) es o $(b', -a')$ o $(-b', a')$. Esto prueba la primera afirmación de la proposición. La segunda afirmación, por su parte, es ahora consecuencia inmediata de la descripción de las soluciones de la ecuación dada por la Proposición 8.2.3. □

8.2.5. Nos ocupamos ahora del caso general de la ecuación diofántica lineal con dos incógnitas:

Proposición. *Sean* a, b *y* c *tres enteros tales que* $ab \neq 0$ *y consideremos el problema de encontrar pares de enteros* (x, y) *tales que*

$$ax + by = c. \tag{4}$$

(*i*) *Hay soluciones a este problema si y solamente si el entero* $d := \mathsf{mcd}(a, b)$ *divide a* c.

(*ii*) *Si ese es el caso y* a', b', c' *enteros tales que* $ax_0 + by_0 = d$, $a = da'$ *y* $b = db'$, *entonces el par* (x_0c', y_0c') *es una solución de* (4).

(*iii*) *Más aún, si* (x_0, y_0) *es una solución cualquiera de la ecuación* (4), *entonces toda solución esa ecuación es de la forma* $(x_0 + x_1, y_0 + y_1)$ *con* (x_1, y_1) *una y solo una solución de la ecuación homogénea*

$$ax + by = 0. \tag{5}$$

La primera parte de esta proposición nos permite decidir cuándo una ecuación diofánticas lineal no homogénea tiene soluciones. Por otro lado, la segunda nos permite encontrar una solución particular de la ecuación, y la tercera nos dice que si tenemos una solución cualquiera, entonces el problema de resolver la ecuación (4) se reduce al de resolver la ecuación homogénea (5) asociada

— y a este último problema sabemos resolverlo, de acuerdo a la Proposición 8.2.3.

Demostración. Supongamos primero que el problema (4) tiene soluciones y sea (x, y) una de ellas. En ese caso, como d divide a a y a b, tenemos que $d \mid ax + by = c$: esto muestra que la condición del enunciado es necesaria para que existan soluciones.

Supongamos ahora que d divide a c y sean x_0, y_0, a', b', c' enteros tales que $ax_0 + by_0 = d$, $a = da'$, $b = db'$ y $c = dc'$. Como

$$ax_0c' + by_0c' = (ax_0 + by_0)c' = dc' = c,$$

es claro que (x_0c', y_0c') es una solución al problema (4). Esto prueba que la condición del enunciado es también suficiente para la existencia de soluciones y, por lo tanto, completa la prueba de las partes (*i*) y (*ii*) de la proposición.

Probemos ahora la parte (*iii*). Sea (x_0, y_0) una solución cualquiera de la ecuación (4). Si (x, y) es otra solución de esa ecuación, entonces tenemos que

$$0 = c - c = (ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0),$$

y esto nos dice que $(x_1, y_1) \coloneqq (x - x_0, y - y_0)$ es una solución de la ecuación homogénea (5) tal que $(x, y) = (x_0 + x_1, y_0 + y_1)$.

Recíprocamente, si (x_1, y_1) es una solución cualquiera de la ecuación homogénea (5), de manera que $ax_1 + by_1 = 0$, entonces tenemos que

$$a(x_0 + x_1) + b(x_0 + x_1) = (ax_0 + by_0) + (ax_1 + by_1) = c + 0 = c,$$

así que el par $(x_0 + x_1, y_0 + y_1)$ es una solución de la ecuación (4). Esto prueba (*iii*). □

8.2.6. De acuerdo a esta proposición y su demostración, para resolver una ecuación de la forma

$$ax + by = c \tag{6}$$

con a, b y c tres enteros tales que $ab \neq 0$ podemos proceder de la siguiente manera.

- En primer lugar, calculamos $d \coloneqq \mathsf{mcd}(a, b)$. Si d no divide a c, entonces sabemos que no hay soluciones de la ecuación y no hay más nada que hacer.
- Supongamos entonces que d sí divide a c. Usando el algoritmo de Euclides extendido buscamos enteros u y v tales que $ua + vb = d$, y dividiendo buscamos el entero c' tal que $c = c'd$. El par $(c'u, c'v)$ es entonces una solución de la ecuación (6)
- Dos divisiones nos dan enteros a', b' tales que $a = a'd$, $b = b'd$, y sabemos que las soluciones de la ecuación homogénea $ax + by = 0$ son las de la forma $(b't, -a't)$ con $t \in \mathbb{Z}$.
- Con todo esto podemos concluir que todas las soluciones de la ecuación (6) son las de la

```haskell
import EMCD

resolverH :: Integer -> Integer -> (Integer,Integer)
resolverH a b = (b `div` d, - a `div` d)
  where (d, x, y) = emcd a b

resolverNH :: Integer -> Integer -> Integer -> Maybe (Integer, Integer)
resolverNH a b c
  | c `mod` d /= 0 = Nothing
  | otherwise      = Just (c * u, c * v)
  where (d, u, v) = emcd a b
        c'        = c `div` d
```

Programa 8.1. Un programa en Haskell para resolver ecuaciones diofánticas lineales con dos incógnitas. Cuando `a` y `b` son enteros no simultáneamente nulos, la expresión `resolverH a b` tiene como valor un par ordenado `(x, y)` que es una solución primitiva de la ecuaciones diofántica homogénea $ax + by = 0$. Por otro lado, cuando `a` y `b` son enteros no simultáneamente nulos, la expresión `resolverNH a b c` tiene o valor `Just (x, y)`, y en ese caso la ecuación $ax + by = c$ tiene soluciones y `(x, y)` es una de ellas, o valor `Nothing`, y en ese caso esa ecuación no tiene ninguna solución. Este código necesita alguna implementación del algoritmo de Euclides extendido.

forma $(c'u + b't, c'v - a't)$ con $t \in \mathbb{Z}$.

El programa 8.1 da una implementación de esto en Haskell.

§8.3. Ecuaciones lineales con un número arbitrario de incógnitas

8.3.1. Exactamente las mismas ideas nos permiten estudiar las ecuaciones diofánticas lineales en un número arbitrario de variables.

Proposición. *Sea $r \in \mathbb{N}$, sean $a_1, \ldots, a_r$ enteros todos distintos de 0, sea b un entero, y consideremos la ecuación*

$$a_1x_1 + \cdots + a_rx_r = b. \tag{7}$$

(*i*) *Hay soluciones a esta ecuación si y solamente si el entero* $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ *divide a* b.

(*ii*) *Si ese es el caso y* $a'_1, \ldots, a'_r$ *y* b' *son los enteros tales que* $a_i = da'_i$ *para cada* $i \in \{1, \ldots, d\}$ *y* $b = db'$, *y* $u_1, \ldots, u_r$ *son enteros tales que* $a_1u_1 + \cdots + a_ru_d = d$, *entonces* $(u_1b', \ldots, u_rb')$ *es una solución de la ecuación* (7).

(*iii*) *Más aún, si* $(x_1^0, x_2^0, \ldots, x_r^0)$ *es una solución cualquiera de la ecuación* (7), *entonces toda solución de esa ecuación es de la forma* $(x_1^0 + x_1^1, \ldots, x_r^0 + x_r^1)$ *con* $(x_1^1, \ldots, x_r^1)$ *una solución de la ecuación homogénea*

$$a_1x_1 + \cdots + a_rx_r = 0. \tag{8}$$

Demostración. Si hay una solución $(x_1, \ldots, x_r)$ a la ecuación (7), entonces claramente el entero $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ divide a $a_1x_1 + \cdots + a_rx_r = b$. Para ver que vale la implicación recíproca, supongamos que d divide a b y sea b' el entero tal que $b = db'$. La identidad de Bézout nos dice que existen enteros $u_1, \ldots, u_r$ tales que $a_1u_1 + \cdots + a_ru_r = d$ y entonces $a_1u_1b' + \cdots + a_ru_rb' = db' = b$, así que la r-upla $(u_1b', \ldots, u_rb')$ es una solución de la ecuación. Esto prueba las afirmaciones (*i*) y (*ii*) de la proposición.

Sea ahora $(x_1^0, x_2^0, \ldots, x_r^0)$ una solución cualquiera de la ecuación (7). Si $(x_1, \ldots, x_r)$ es otra solución, entonces la r-upla $(x_1^1, \ldots, x_r^1) \coloneqq (x_1 - x_1^0, \ldots, x_r - x_r^0)$ es una solución de la ecuación homogénea (8), ya que

$$a_1(x_1 - x_1^0) + \cdots + a_r(x_r - x_r^0) = (a_1x_1 + \cdots + a_rx_r) + (a_1x_1^0 + \cdots + a_rx_r^0) = b - b = 0,$$

y es $(x_1, \ldots, x_r) = (x_1^0 + x_1^1, \ldots, x_r^0 + x_r^1)$. Esto prueba la afirmación (*iii*) de la proposición. □

8.3.2. Una diferencia entre la situación de la que se ocupa esta última proposición y la de la Proposición **8.2.5** es que no tenemos una fórmula explícita para las soluciones de la ecuación homogénea como la que da la Proposición 8.2.3 en el caso en que solo hay dos incógnitas. Podemos describir, de todas formas, un *procedimiento* para resolverla. Veamos esto.

Supongamos que $r \geq 2$, que $a_1, \ldots, a_r$ son enteros no nulos, y que buscamos las soluciones de la ecuación diofántica lineal homogénea

$$a_1x_1 + \cdots + a_rx_r = 0. \tag{9}$$

Escribamos $\mathsf{Sol}(a_1, \ldots, a_r)$ al conjunto de todas las r-uplas $(x_1, \ldots, x_r)$ de enteros que son soluciones de esta ecuación. Nuestro objetivo, entonces, es describir este subconjunto de $\mathbb{Z}^r$.

Sin pérdida de generalidad podemos suponer que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$. En efecto, si ese no es el caso, podemos poner $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ y $a'_i \coloneqq a_i/d$ para cada $i \in \{1, \ldots, r\}$ y considerar en lugar de (9) la ecuación $a'_1x_1 + \cdots + a'_rx_r = 0$, que tiene exactamente las mismas soluciones que la ecuación original y cuyos coeficientes son tales que $\mathsf{mcd}(a'_1, \ldots, a'_r) = 1$.

Sea $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$ y supongamos que $(x_1, \ldots, x_r)$ es una solución de la ecuación (9). Como $\mathsf{mcd}(a_1, e) = \mathsf{mcd}(a_1, \ldots, a_r) = 1$ y

$$e \mid a_2x_2 + \cdots + a_rx_r = -a_1x_1,$$

el entero e divide a x_1 y existe un entero t tal que $x_1 = et$. Por otro lado, el algoritmo de Euclides extendido nos permite encontrar $r-1$ enteros $u_2, \ldots, u_r$ tales que

$$a_2u_2 + \cdots + a_ru_r = e.$$

Calculando vemos que

$$\begin{aligned} a_2(x_2 + a_1tu_2) + \cdots + a_r(x_r + a_1tu_r) &= (a_2x_2 + \cdots + a_rx_r) + a_1t\,(a_2u_2 + \cdots + a_ru_r) \\ &= -a_1x_1 + a_1te = 0, \end{aligned}$$

y esto nos dice que la $(r-1)$-upla $(x_2 + a_1tu_2, \ldots, x_r + a_1tu_r)$ es una solución de la ecuación

$$a_2y_2 + \cdots + a_ry_r = 0 \tag{10}$$

en $r-1$ incógnitas $y_2, \ldots, y_r$.

Recíprocamente, cada vez que $(y_2, \ldots, y_r)$ es una solución de esta última ecuación (10) e t es un entero cualquiera, tenemos que

$$\begin{aligned} a_1et + a_2(y_2 - a_1tu_2) + \cdots + a_r(y_r - a_1tu_r) & \\ = ea_1t - a_1t\,(a_2u_2 + \cdots + a_ru_r) + (a_2y_2 + \cdots + a_ry_r) &= 0, \end{aligned}$$

y esto nos dice que la r-upla $(et, y_2 - a_1tu_2, \ldots, y_r - a_1tu_r)$ es una solución de la ecuación (9), que es claramente equivalente a

$$\frac{a_2}{e}u_2 + \cdots + \frac{a_r}{e}u_r = e.$$

Hemos probado la siguiente proposición.

8.3.3. Proposición. *Supongamos que r y $a_1, \ldots, a_r$ son enteros tales que $r \geq 2$ y $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, sea $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$ y sean $u_2, \ldots, u_r$ enteros tales que $a_2u_2 + \cdots + a_ru_r = e$. El conjunto $\mathsf{Sol}(a_1, \ldots, a_r)$ de las soluciones de la ecuación $a_1x_1 + \cdots + a_rx_r = 0$ es*

$$\{(et, z_2 - a_1tu_2, \ldots, z_r - a_1tu_r) : t \in \mathbb{Z}, (z_2, \ldots, z_r) \in \mathsf{Sol}(a_2/e, \ldots, a_r/e)\}. \qquad \square$$

El punto de esto es que nos permite reduce el problema de encontrar todas las soluciones de una ecuación diofántica lineal homogénea con r incógnitas al de encontrar todas las soluciones de una ecuación del mismo tipo pero con una incógnita menos. Repitiendo esto podemos resolver completamente el problema.

8.3.4. Veamos un ejemplo de este procedimiento. Consideremos la ecuación

$$6 \cdot x_1 + 105 \cdot x_2 + 30 \cdot x_3 + 70 \cdot x_4 = 0. \tag{11}$$

Los coeficientes son coprimos, es $\mathsf{mcd}(105, 30, 70) = 5$, y usando el algoritmo de Euclides extendido encontramos que

$$1 \cdot 105 + 20 \cdot 30 + (-10) \cdot 70 = 5.$$

La proposición nos dice entonces que $\mathsf{Sol}(6, 105, 30, 70)$ es el conjunto de las 4-uplas de la forma

$$(5 \cdot t_1, y_2 - 6 \cdot t_1, y_3 - 120 \cdot t_1, y_4 + 60 \cdot t_1) \tag{12}$$

con $t_1 \in \mathbb{Z}$ y $(y_2, y_3, y_4) \in \mathsf{Sol}(21, 6, 14)$.

Tenemos ahora que resolver la ecuación

$$21 \cdot y_2 + 6 \cdot y_3 + 14 \cdot y_4 = 0, \tag{13}$$

que tiene coeficientes coprimos. Es $\mathsf{mcd}(6, 14) = 2$ y el algoritmo de Euclides extendido nos dice que

$$(-2) \cdot 6 + 1 \cdot 14 = 2.$$

Usando el resultado de la proposición, podemos concluir entonces que las soluciones de la ecuación (13) son las 3-uplas de la forma

$$(2 \cdot t_2, z_3 + 42 \cdot t_2, z_4 - 21 \cdot t_2) \tag{14}$$

con $t_2 \in \mathbb{Z}$ y (z_3, z_4) un elemento de $\mathsf{Sol}(3, 7)$.

Finalmente, tenemos que resolver la ecuación

$$3 \cdot z_3 + 7 \cdot z_4 = 0$$

en dos incógnitas: sus soluciones son los pares de la forma

$$(7 \cdot t_3, -3 \cdot t_3)$$

con $t_3 \in \mathbb{Z}$. Usando esto en (14) vemos que las soluciones de la ecuación (13) son las 3-uplas de la forma

$$(2 \cdot t_2, 7 \cdot t_3 + 42 \cdot t_2, -3 \cdot t_3 - 21 \cdot t_2)$$

con $t_2, t_3 \in \mathbb{Z}$. A su vez, usando esto en (12) vemos que las soluciones de la ecuación (11) con la que empezamos son las 4-uplas de la forma

$$(5 \cdot t_1, 2 \cdot t_2 - 6 \cdot t_1, 7 \cdot t_3 + 42 \cdot t_2 - 120 \cdot t_1, -3 \cdot t_3 - 21 \cdot t_2 + 60 \cdot t_1)$$

con t_1, t_2, $t_3 \in \mathbb{Z}$. En otras palabras, las soluciones de la ecuación (11) son todas las que 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo tres enteros t_1, t_2, y t_3 y poniendo

$$\begin{aligned} x_1 &\coloneqq \cdot t_1, \\ x_2 &\coloneqq -\cdot t_1 + \cdot t_2, \\ x_3 &\coloneqq -120\cdot t_1 + 42\cdot t_2 + 7\cdot t_3, \\ x_4 &\coloneqq 60\cdot t_1 - 21\cdot t_2 - 3\cdot t_3 \end{aligned} \tag{15}$$

8.3.5. Las soluciones de una ecuación homogénea siempre tienen una forma similar a la de las del ejemplo que acabamos de dar:

Proposición. *Sea $r \in \mathbb{N}$ tal que $r \geq 2$, y sean $a_1, \ldots, a_r$ enteros no nulos tales que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$. Hay $r-1$ elementos*

$$u_1 = (u_{1,1}, \ldots, u_{1,r}), \quad u_2 = (u_{2,1}, \ldots, u_{2,r}), \quad \ldots, \quad u_{r-1} = (u_{r-1,1}, \ldots, u_{r-1,r})$$

de $\mathbb{Z}^r$ tales que las soluciones de la ecuación homogénea

$$a_1x_1 + \cdots + a_rx_r = 0 \tag{16}$$

son todas las r-uplas $(x_1, \ldots, x_r)$ que se obtienen eligiendo $r-1$ enteros $t_1, \ldots, t_{r-1}$ y poniendo

$$\begin{aligned} x_1 &= t_1u_{1,1} + t_2u_{2,1} + \cdots + t_{r-1}u_{r-1,1}, \\ x_2 &= t_1u_{1,2} + t_2u_{2,2} + \cdots + t_{r-1}u_{r-1,2}, \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\ x_r &= t_1u_{1,r} + t_2u_{2,r} + \cdots + t_{r-1}u_{r-1,r}. \end{aligned}$$

En el ejemplo que hicimos arriba sobre la ecuación (11) es $r = 4$ y como los 3 elementos u_1, u_2 y u_3 a los que se refiere esta proposición podemos elegir a

$$(5, -30, 90, 6), \qquad (0, 2, 42, -21), \qquad (0, 0, 7, -3).$$

Demostración. Demostraremos esto procediendo por inducción con respecto al número r de incógnitas de la ecuación (16).

Supongamos primero que $r = 2$. Tenemos entonces dos enteros a_1 y a_2 que son nulos y tales que $\mathsf{mcd}(a_1, a_2) = 1$. De acuerdo a la Proposición 8.2.3, las soluciones de la ecuación $a_1x_1 + a_2x_2 = 0$ son todos los pares ordenados (x_1, x_2) de la forma $(t_1a_2, -t_1a_1)$ con t_1 un entero, y esto nos dice que si ponemos $u_1 \coloneqq (a_2, -a_1)$ entonces la afirmación de la proposición vale.

Supongamos ahora que es $r \geq 3$. Sean $a_1, \ldots, a_r$ enteros tales que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, y consideremos el número $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$. La ecuación

$$\frac{a_2}{e}y_2 + \cdots + \frac{a_r}{e}y_r = 0 \tag{17}$$

tiene $r-1$ incógnitas y sus coeficientes son coprimos, así que la hipótesis inductiva evidente implica que hay $r-2$ elementos

$$v_2 = (v_{2,2}, v_{2,3}, \ldots, v_{2,r}), \quad v_3 = (v_{3,2}, v_{3,3}, \ldots, v_{3,r}), \quad \ldots, \quad v_{r-1} = (v_{r-1,2}, v_{r-1,3}, \ldots, v_{r-1,r})$$

de $\mathbb{Z}^{t-1}$ tales que las soluciones de la ecuación (17) son las $(r-1)$-uplas $(y_2, \ldots, y_r)$ que se obtienen eligiendo $r-2$ enteros $t_2, \ldots, t_{r-1}$ y poniendo

$$\begin{aligned}
y_2 &= t_2 v_{2,2} + t_3 v_{3,2} + \cdots + t_{r-1} v_{r-1,2}, \\
y_3 &= t_2 v_{2,3} + t_3 v_{3,3} + \cdots + t_{r-1} v_{r-1,3}, \\
&\vdots \qquad \vdots \qquad \vdots \qquad\qquad \vdots \\
y_r &= t_2 v_{2,r} + t_3 v_{3,r} + \cdots + t_{r-1} v_{r-1,r}.
\end{aligned}$$

Por otro lado, como $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, hay enteros $w_1, \ldots, w_r$ tales que $w_1 a_1 + \cdots + w_r a_r = 1$ y la Proposición 8.3.3 nos dice que

> *las soluciones de la ecuación* (16) *del enunciado son las r-uplas de la forma* $(et, y_2 - a_1 t w_2, \ldots, y_r - a_1 t w_r)$ *con* $t \in \mathbb{Z}$ *e* $(y_2, \ldots, y_r)$ *una solución de la ecuación* (17). (18)

Consideremos ahora los $r-1$ elementos

$$\begin{aligned}
u_1 &\coloneqq (e, -a_1 w_2, -a_1 w_3, \ldots, -a_1 w_r), \\
u_2 &\coloneqq (0, \quad v_{2,2}, \quad v_{2,3}, \ldots, \quad v_{2,r}), \\
u_3 &\coloneqq (0, \quad v_{3,2}, \quad v_{3,3}, \ldots, \quad v_{3,r}), \\
&\vdots \qquad\qquad\qquad \vdots \\
u_{r-1} &\coloneqq (0, \quad v_{r-1,2}, \quad v_{r-1,3}, \ldots, \quad v_{r-1,r})
\end{aligned}$$

de $\mathbb{Z}^r$ y para cada $i \in \{1, \ldots, r-1\}$ y cada $j \in \{1, \ldots, r\}$ escribamos $u_{i,j}$ a la componente j-ésima de u_i. Unos momentos de reflexión deberían ser suficientes para convencer al lector que las r-uplas $(x_1, \ldots, x_r)$ que se obtienen eligiendo $r-1$ enteros $t_1, \ldots, t_r$ y poniendo

$$\begin{aligned}
x_1 &= t_1 u_{1,1} + t_2 u_{2,1} + \cdots + t_{r-1} u_{r-1,1}, \\
x_2 &= t_1 u_{1,2} + t_2 u_{2,2} + \cdots + t_{r-1} u_{r-1,2}, \\
&\vdots \qquad \vdots \qquad \vdots \qquad\qquad \vdots \\
x_r &= t_1 u_{1,r} + t_2 u_{2,r} + \cdots + t_{r-1} u_{r-1,r}.
\end{aligned}$$

son precisamente las soluciones de la ecuación (16), de acuerdo a (18). Esto completa la inducción y, por lo tanto, la prueba de la proposición. □

```
import EMCD

resolverH :: [Integer] -> [[Integer]]
resolverH [a]      = []
resolverH (a : as) = primera : [ 0 : s | s <- resolverH as]
  where (e,us)     = emcdN as
        (d,_,_)    = emcd a e
        primera    = e `div` d : [ - u * a `div` d | u <- us]

resolverNH :: [Integer] -> Integer -> Maybe [Integer]
resolverNH as b
  | r /= 0    = Nothing
  | otherwise = Just (map (q *) us)
  where (d, us) = emcdN as
        (q, r) = divMod b d

emcdN :: [Integer] -> (Integer, [Integer])
emcdN [a]    = (a, [1])
emcdN (a:as) = (d, x : [y * u | u <- us])
  where (e, us) = emcdN as
        (d, x, y) = emcd a e
```

Programa 8.2. Funciones en HASKELL que resuelven ecuaciones diofánticas lineales homogéneas y no homogéneas con una cantidad arbitraria de incógnitas. Ambas asumen que todos los coeficientes son distintos de 0. Usamos aquí el código del Programa 6.5 en la página 186 para calcular los coeficientes de la identidad de Bézout.

8.3.6. Ejercicio. Muestre que en la situación de la proposición que acabamos de probar los $r-1$ elementos $u_1, \ldots, u_{r-1}$ de $\mathbb{Z}^r$ pueden elegirse de manera que para toda elección de i en $\{1, \ldots, r-1\}$ y de j en $\{1, \ldots, r\}$ valga

$$1 \leq j < i \implies u_{j,i} = 0.$$

Esto es la generalización del hecho observado en nuestro ejemplo de 8.3.4 de que la solución final (15) de la ecuación allí considerada es «triangular»

8.3.7. El programa 8.2 da una implementación sencilla de este algoritmo para resolver ecuaciones diofánticas lineales homogéneas y la correspondiente aplicación para encontrar una solución particular de las no homogéneas. Por ejemplo, podemos evaluar

```
*Ecuaciones> resolverH [6, 105, 30, 70]
[[5,-6,-120,60],[0,2,42,-21],[0,0,7,-3]]
```

El resultado es la lista de las 4-uplas que encontramos en 8.3.4, de manera que las soluciones de la ecuación

$$6x_1 + 105x_2 + 30x_3 + 70x_4 = 0$$

que consideramos ahí son las 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo t_1, t_2 y t_3 en $\mathbb{Z}$ y poniendo

$$\begin{aligned} x_1 &:= \ 5 \cdot t_1, \\ x_2 &:= -\ 6 \cdot t_1 + \ 2 \cdot t_2, \\ x_3 &:= -\ 120 \cdot t_1 + 42 \cdot t_2 + 7 \cdot t_3, \\ x_4 &:= \ 60 \cdot t_1 - \ 21 \cdot t_2 - 3 \cdot t_3 \end{aligned}$$

Las tres listas del valor de `resolverH [6, 105, 30, 70]` son los coeficientes de t_1, t_2 y t_3 en estas fórmulas.

De manera similar, las soluciones de la ecuación

$$30x_1 + 14x_2 + 105x_3 + 231x_4 = 0$$

son las 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo t_1, t_2 y t_3 en $\mathbb{Z}$ y poniendo

$$\begin{aligned} x_1 &= \ 7t_1 \\ x_2 &= \ 30t_1 + 3t_2 \\ x_3 &= -\ 60t_1 + 4t_2 + 11t_3 \\ x_4 &= -\ 30t_1 - 2t_2 - \ 5t_3 \end{aligned}$$

ya que evaluando `resolverH [30,14,105,231]` obtenemos

```
Ecuaciones*> resolverH [30,14,105,231]
[[7,30,60,-30],[0,3,4,-2],[0,0,11,-5]]
```

Por otro lado, la función `resolverNH` nos da una solución de una ecuación no homogénea, si es que hay alguna: podemos evaluar

```
*Ecuaciones> resolverNH [90, 15, -78] 24
Just [24,360,72]
```

y esto nos dice que una solución de la ecuación

$$90x_1 + 15x_2 - 78x_3 = 24$$

es $(x_1, x_2, x_3) = (24, 306, 72)$. Por otro lado,

```
*Ecuaciones> resolverNH [30, 14, 106] 7
Nothing
```

y esto nos dice que la ecuación

$$30x_1 + 14x_2 + 106x_3 = 7$$

no tiene soluciones.

§8.4. Ecuaciones lineales en congruencias

8.4.1. En esta sección nos ocupamos de siguiente problema: dados $m \in \mathbb{N}$ y enteros a y b, queremos decidir si hay enteros x tales que

$$ax \equiv b \mod m$$

y, cuando los haya, encontrarlos.

Proposición. *Sea $m \in \mathbb{N}$, sean a y b dos enteros y sea $d := \mathsf{mcd}(a, m)$. Hay enteros x tales que*

$$ax \equiv b \mod m \tag{19}$$

si y solamente si d divide a b. Si ese es el caso y si u_0, v_0, a', m' y b' son enteros tales que $au_0 + mv_0 = d$, $a = da'$, $m = dm'$ y $b = db'$, entonces los d enteros

$$u_0b' + 0m', \quad u_0b' + 1m', \quad u_0b' + 2m', \quad \dots, \quad u_0b' + (d-1)m'.$$

son soluciones de la ecuación no congruentes módulo m dos a dos y toda otra solución es congruente a una de ellas.

Demostración. Si existe un entero x tal que $ax \equiv b \mod m$, entonces m divide a $ax - b$ y, por lo tanto, existe un entero y tal que $ax - b = my$. Se tiene entonces que

$$d \mid ax - my = b.$$

Supongamos, para ver la recíproca, que d divide a b. La Proposición 8.2.5 nos dice que hay dos enteros x e y tales que $ax + my = b$: como entonces se tiene que $ax \equiv b \mod m$, vemos que la ecuación (19) tiene soluciones. Esto prueba la primera afirmación del enunciado.

Sean u_0, v_0, a', m' y b' enteros tales que $au_0 + mv_0 = d$, $a = da'$, $m = dm'$ y $b = db'$. Para cada entero x tenemos que

$$\begin{aligned} ax \equiv b \mod m &\iff dx \equiv u_0 ax \equiv u_0 b \equiv u_0 db' \mod m \\ &\iff x \equiv u_0 b' \mod m'. \end{aligned}$$

Esto nos dice que toda solución de la ecuación (19) es de la forma

$$x = u_0 b' + m' t$$

para un t unívocamente determinado.

Más aún, las soluciones $u_0 b' + m' t$ y $u_0 b' + m' s$ correspondientes a dos enteros t y s son congruentes módulo m si y solamente si

$$m' d = m \mid (x_0 b' + m' t) - (x_0 b' + m' s) = m'(t - s),$$

lo que ocurre si y solamente si t y s son congruentes módulo d. Esto implica inmediatamente que las d soluciones

$$u_0 b' + 0m', \quad u_0 b' + 1m', \quad u_0 b' + 2m', \quad \ldots, \quad u_0 b' + (d-1)m'$$

son no congruentes módulo m dos a dos y que toda solución de la ecuación es congruente a una de ellas, □

8.4.2. Proposición. *Sean m_1, $m_2 \in \mathbb{N}$, sean b_1, $b_2 \in \mathbb{Z}$ y sea $d = \mathsf{mcd}(m_1, m_2)$. Existen enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ x \equiv b_2 \mod m_2 \end{cases} \tag{20}$$

si y solamente si $b_1 \equiv b_2 \mod d$. Más aún, si ese es el caso y n_1, n_2 son enteros tales que $n_1 m_1 + n_2 m_2 = d$ y $M = \mathsf{mcm}(m_1, m_2)$, entonces el número

$$u = \frac{n_2 m_2 b_1 + n_1 m_1 b_2}{d}$$

es entero y el conjunto de soluciones de (21) es precisamente la clase de congruencia de u módulo M.

Demostración. Supongamos primero que hay un entero x que satisface las dos ecuaciones (20). En ese caso, como d divide tanto a m_1 como a m_2 tenemos que también $x \equiv b_1 \mod d$ y $x \equiv b_2 \mod d$, de manera que $b_1 \equiv b_2 \mod d$.

Supongamos ahora que $b_1 \equiv b_2 \mod d$. Un entero x satisface la primera de las ecuaciones de (21) si y solamente si existe un entero t tal que $x = b_1 + m_1 t$, y entonces también satisface la segunda de esas ecuaciones si además $b_1 + m_1 t \equiv b_2 \mod m_2$, esto es, si

$$m_1 t \equiv b_2 - b_1 \mod m_2.$$

Como d divide a $b_2 - b_1$, esta ecuación tiene soluciones, en vista del criterio que nos da la Proposición 8.4.1, así que el sistema (20) también. □

8.4.3. La generalización del resultado de la Proposición 8.4.2 al caso de sistemas de un número arbitrario de congruencias es conocida usualmente como el *Teorema Chino del Resto*. El nombre con el que es conocido el teorema se debe a que la primera aparición registrada de este resultado es en el libro *Sunzi Suanjing*, escrito en China en algún momento entre el siglo III y el V de la era cristiana. En el libro se plantea y se resuelve el siguiente problema:

> *Hay ciertas cosas cuyo número se desconoce. Si las contamos de a tres, sobran dos; si de a cinco, sobran tres; y si de a siete, sobran dos. ¿Cuántas cosas hay?*

que es equivalente al de resolver el sistema de congruencias

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5, \\ x \equiv 2 \mod 7. \end{cases}$$

De todas maneras, no menciona ni el enunciado general ni una demostración. Brahmagupta, en el siglo VII en la India, también conocía casos particulares y en su libro *Brāhmasphuṭasiddhānta* plantea el siguiente problema:

> *Una anciana va al mercado y un caballo pisa su canasta y aplasta los huevos que llevaba. El jinete ofrece pagarle los huevos y le pregunta cuántos tenía. Ella no recuerda el número exacto, pero sí que cuando los había ordenado en filas de dos había sobrado uno, y que lo mismo había ocurrido cuando había intentado ordenarlos en filas de tres, de cuatro, de cinco y de seis, y que solo cuando había intentado ponerlos en filas de siete habían quedado parejos. ¿Cuál es la menor cantidad de huevos que pudo haber tenido?*

Por supuesto, lo que quiere Brahmagupta es la menor solución positiva del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod 2, \\ x \equiv 1 \mod 3, \\ x \equiv 1 \mod 4, \\ x \equiv 1 \mod 5, \\ x \equiv 1 \mod 6, \\ x \equiv 0 \mod 7. \end{cases}$$

Más tarde, Fibonacci da varios ejemplos en su libro *Liber Abaci* de 1202. Uno de ellos es el siguiente: se le pide a alguien que piense un número y que nos diga el resto de dividirlo por 5, por 7 y por 9 y el problema consiste en «adivinarlo».

El primero en enunciar el teorema con total generalidad y probarlo fue Gauss, en sus *Disquisitiones* de 1801. Gauss plantea, a partir del párrafo 33, el problema general de «encontrar los números que tienen residuos dados, con respecto a módulos cualesquiera» y después de explicar un método general para resolver ese tipo de problemas y dar varios ejemplos numéricos, plantea la siguiente aplicación práctica a un «problema de cronología»:

> *Encontrar el número de un año del que se conoce la indicción, el número áureo y el ciclo solar.*

La ***indicción*** de un año es el resto de dividir por 15 la suma de su número más 3 (por ejemplo, la indicción del año 2018 es 11) y es uno de los periodos del calendario bizantino, junto con el mes y el año, y que se usaba para la liquidación de impuestos. Por otro lado, el ***número áureo*** de un año (que no tiene nada que ver con el número $(1+\sqrt{5})/2$) es 1 más el resto de dividirlo por 19: este número se usó desde el año 432 a.C. para poder calcular los ciclos lunares con precisión, usando un amétodo debido al griego Metón. Finalmente, el ***ciclo solar*** de un año A es uno más el resto de dividir $A+1$ por 28. Así, el problema que plantea Gauss es el de determinar el año x con indicción i, número aureo a y ciclo solar s es equivalente al de resolver el sistema de congruencias

$$\begin{cases} x \equiv i-3 \mod 15, \\ x \equiv a-1 \mod 19, \\ x \equiv s-1 \mod 28. \end{cases}$$

El mínimo común múltiplo de 15, 19 y 28 es 7980: veremos más abajo que eso implica que cada año desde el primero hasta el 7979 está completamente determinado por su indicción, su número áureo y su ciclo solar.

El problema que plantea Gauss parece hoy bastante extraño, pero en su época era de gran interés. Gauss había tenido un gran éxito un año antes de la publicación de sus *Disquisitiones* al hacer conocer un método algorítmico —el primero en la historia— para el cálculo de la fecha de Pascua. Ese método tenía ciertas falencias y en 1816 publicó finalmente un algoritmo mejorado que permitía calcular exactamente la fecha de Pascua de todos los años a partir del año 1583 del calendario gregoriano.

8.4.4. Empecemos con un caso particular del Teorema Chino del Resto, aquel en el que lo módulos son coprimos dos a dos. La demostración de este caso es más sencilla que la del general y, a la vez, es el que más usamos en la práctica:

Proposición. *Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_r$ enteros. Hay enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{21}$$

y el conjunto de tales enteros es una clase de congruencia módulo $m_1 \cdots m_r$.

Demostración. Sea $M = m_1 \cdots m_r$. Veamos primero que si hay soluciones al sistema de congruencias (21), entonces el conjunto de esas soluciones es precisamente una clase de congruencia módulo M. Esto probará la segunda afirmación del enunciado.

Supongamos entonces que hay un entero x_0 tal que $x_0 \equiv b_i \mod m_i$ para cada $i \in \{1, \ldots, r\}$. Si x es otro entero que satisface las mismas congruencias, entonces tenemos que $x - x_0 \equiv b_i - b_i \mod m_i$ y, por lo tanto, la diferencia $x - x_0$ es divisible por cada uno de los números $m_1, \ldots, m_r$. Como estos r números son coprimos dos a dos, el Corolario 6.5.8 nos dice que su producto M también divide a $x - x_0$ y, por lo tanto que $x \equiv x_0 \mod M$.

Recíprocamente, si x es un entero que es congruente con x_0 módulo M, entonces para cada $i \in \{1, \ldots, r\}$ tenemos que $x \equiv x_0 \mod m_i$, porque m_i divide a M, y entonces que $x \equiv x_0 \equiv b_i \mod m_i$. Así, x es una solución del sistema de congruencias (21).

Concluimos de esta forma que si x_0 es una solución del sistema (21) entonces el conjunto de todas las soluciones es precisamente la clase de congruencia de x_0 módulo M, como queríamos.

Veamos ahora que existen soluciones. Procederemos por inducción. Para cada $r \in \mathbb{N}$ sea $P(r)$ la afirmación

> *si $m_1, \ldots, m_r$ son enteros positivos coprimos dos a dos y $b_1, \ldots, b_r$ son enteros, entonces existe un entero x tal que $x \equiv b_i \mod m_i$ para cada $i \in \{1, \ldots, r\}$.*

Que $P(1)$ vale es evidente y que $P(2)$ vale es un caso particular de la Proposición 8.4.2. Sea, para hacer inducción, s un entero tal que $s \geq 2$, supongamos que $P(s)$ vale y mostremos que entonces $P(s+1)$ también vale. Sean, para eso, $m_1, \ldots, m_{s+1}$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_{s+1}$ enteros.

Como m_s y m_{s+1} son coprimos, la Proposición 8.4.2 nos dice que hay un entero a tal que para cada $x \in \mathbb{Z}$ se tiene que

$$x \equiv a \mod m_1 m_2 \iff \begin{cases} x \equiv b_s \mod m_s, \\ x \equiv b_{s+1} \mod m_{s+1} \end{cases} \tag{22}$$

Por otro lado, la hipótesis inductiva implica que existe un entero x_0 que satisface el sistema de

s congruencias

$$\begin{cases} x_0 \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x_0 \equiv b_{s-1} & \text{mód } m_{s-1} \\ x_0 \equiv a & \text{mód } m_s m_s \end{cases}$$

ya que los enteros $m_1, \ldots, m_{s-1}, m_s m_{s+1}$ son coprimos dos a dos, y de esta última congruencia y de (22) deducimos que además $x_0 \equiv b_s \mod m_s$ y $x_0 \equiv b_{s+1} \equiv m_{s+1}$. Así, tenemos que

$$\begin{cases} x_0 \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x_0 \equiv b_{s+1} & \text{mód } m_{s+1} \end{cases}$$

si y solamente si satisface el sistema de s congruencias

$$\begin{cases} x \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv b_{s+1} & \text{mód } m_{s+1} \end{cases}$$

y, en definitiva, el entero x_0 es una solución al sistema de congruencias (21) del enunciado. Esto prueba que este sistema posee soluciones, por supuesto. □

8.4.5. La prueba de existencia que acabamos de hacer nos da un algoritmo que podemos usar en la práctica. Por ejemplo, supongamos que queremos encontrar un entero x que satisfaga las congruencias

$$\begin{cases} x \equiv 1 & \text{mód } 2, \\ x \equiv 2 & \text{mód } 3, \\ x \equiv 3 & \text{mód } 5, \\ x \equiv 4 & \text{mód } 7. \end{cases} \tag{23}$$

La identidad de Bézout para 2 y 3 es $2 \cdot (-1) + 3 \cdot 1 = 1$ y

$$3 \cdot 1 \cdot 1 + 2 \cdot (-1) \cdot 2 = -1 \equiv 5 \mod 6,$$

así que la Proposición 8.4.2 nos dice que para cada $x \in \mathbb{Z}$ es

$$x \equiv 5 \mod 6 \iff \begin{cases} x \equiv 1 & \text{mód } 2, \\ x \equiv 2 & \text{mód } 3. \end{cases}$$

El sistema (23) es por lo tanto equivalente a

$$\begin{cases} x \equiv 5 \mod 6, \\ x \equiv 3 \mod 5, \\ x \equiv 4 \mod 7. \end{cases} \tag{24}$$

Otra vez, la identidad de Bézout para 6 y 5 es $6 \cdot 1 + 5 \cdot (-1) = 1$, y

$$5 \cdot (-1) \cdot 5 + 6 \cdot 1 \cdot 3 = -7 \equiv 23 \mod 30.$$

De acuerdo a la Proposición 8.4.2, entonces,

$$x \equiv 23 \mod 30 \iff \begin{cases} x \equiv 5 \mod 6, \\ x \equiv 3 \mod 5 \end{cases}$$

y el sistema (24) es equivalente a

$$\begin{cases} x \equiv 23 \mod 30, \\ x \equiv 4 \mod 7. \end{cases} \tag{25}$$

Finalmente, la identidad de Bézout para 30 y 7 es $30 \cdot (-3) + 7 \cdot 13 = 1$ y

$$7 \cdot 13 \cdot 23 + 30 \cdot (-3) \cdot 4 = 1733 \equiv 53 \mod 210,$$

así que el sistema (25) es equivalente a la congruencia

$$x \equiv 53 \mod 210.$$

Ésta es entonces la solución del sistema (23) con el que empezamos.

8.4.6. El procedimiento para resolver un sistema de congruencias que se deduce de la prueba que dimos para la Proposición 8.4.4 es iterativo: vamos resolviendo parcialmente el sistema de a una congruencia por vez. También podemos construir una solución de una sola vez:

Proposición. *Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_r$ enteros. Pongamos $M = m_1 \cdots m_r$ y para cada $i \in \{1, \ldots, r\}$ sea $q_i = M/m_i$. Para cada $i \in \{1, \ldots, r\}$ existen enteros s_i y t_i tales que $s_i q_i + t_i m_i = 1$ y el entero*

$$x = s_1 q_1 b_1 + \cdots + s_r q_r b_r$$

es una solución del sistema de congruencias

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{26}$$

Demostración. Sea $i \in \{1, \dots, r\}$. Como $q_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_r$ y los $r-1$ factores en este producto son coprimos dos a dos, tenemos que

$$\begin{aligned} \mathsf{mcd}(m_i, q_i) &= \mathsf{mcd}(m_i, m_1) \cdots \mathsf{mcd}(m_i, m_{i-1}) \, \mathsf{mcd}(m_i, m_{i+1}) \cdots \mathsf{mcd}(m_i, m_r) \\ &= 1. \end{aligned}$$

De la identidad de Bézout, entonces, sabemos que existen enteros s_i y t_i tales que

$$s_i q_i + t_i m_i = 1.$$

Esto prueba la primera afirmación del enunciado.

Sea, por otro lado, $x = s_1 q_1 b_1 + \cdots + s_r q_r b_r$, como en el enunciado de la proposición, y sea $i \in \{1, \dots, r\}$. Si j es otro elemento de $\{1, \dots, r\}$ distinto de i, entonces m_j divide a q_i, así que

$$x = s_1 q_1 b_1 + \cdots + s_r q_r b_r \equiv s_i q_i b_i (1 - t_i m_i) b_i \equiv b_i \mod m_i.$$

Vemos así que x es una solución a cada una de las congruencias del sistema (26). □

8.4.7. Resolvamos el sistema de congruencias (23) de 8.4.5 usando esta vez el resultado que acabamos de probar. Tenemos $r = 4$ y

$$m_1 = 2, \quad m_2 = 3, \quad m_3 = 5, \quad m_4 = 7, \quad b_1 = 1, \quad b_2 = 2, \quad b_3 = 3, \quad b_4 = 4.$$

Ponemos $q_1 = 3 \cdot 5 \cdot 7 = 105$, $q_2 = 2 \cdot 5 \cdot 7 = 70$; $q_3 = 2 \cdot 3 \cdot 7 = 42$ y $q_4 = 2 \cdot 3 \cdot 5 = 30$ y, usando el algoritmo de Euclides extendido cuatro veces encontramos que

$$\begin{aligned} q_1 + (-52) m_1 &= 1, & q_2 + (-23) m_2 &= 1, \\ (-2) q_3 + 17 m_3 &= 1, & (-3) q_4 + 13 m_4 &= 1, \end{aligned}$$

así que podemos elegir $s_1 = s_2 = 1$, $s_3 = -2$ y $s_4 = -3$. La proposición nos dice entonces que el entero

$$x = 1 \cdot q_1 \cdot 1 + 1 \cdot q_2 \cdot 2 + (-2) \cdot q_3 \cdot 3 + (-3) \cdot q_4 \cdot 4 = -367$$

es una solución del sistema (23). Esto es consistente, por supuesto, con lo que hicimos antes, ya que $-367 \equiv 53 \mod 2 \cdot 3 \cdot 5 \cdot 7$.

En la práctica, el procedimiento iterativo para resolver sistemas de congruencias es más conveniente, ya que generalmente puede llevarse a cabo sin necesidad de considerar en el proceso enteros tan grandes como los que aparecen usando la idea de la Proposición 8.4.6.

8.4.8. Consideremos ahora la versión general del Teorema Chino del Resto. Cuando los módulos de las congruencias no son coprimos dos a dos, es necesario imponer una condición aritmética para que existan soluciones:

Proposición. *Sea $r \in \mathbb{N}$. Si $m_1, \ldots, m_r$ son enteros positivos y $b_1, \ldots, b_r \in \mathbb{Z}$, entonces hay enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{27}$$

si y solamente si se tiene que $b_i \equiv b_j \mod \mathsf{mcd}(m_i, m_j)$ para cada elección de i y j en $\{1, \ldots, r\}$. Cuando ese es el caso, el conjunto de los tales enteros es una clase de congruencia módulo $\mathsf{mcm}(m_1, \ldots, m_r)$.

Demostración. Sean $r \in \mathbb{N}$, $m_1, \ldots, m_r \in \mathbb{N}$ y $b_1, \ldots, b_r \in \mathbb{Z}$ y supongamos que existe un entero x tal que $x \equiv b_t \mod m_t$ para cada $t \in \{1, \ldots, r\}$. Si i y j son dos elementos de $\{1, \ldots, r\}$, tenemos en particular que

$$\begin{cases} x \equiv b_i \mod m_i, \\ x \equiv b_j \mod m_j \end{cases}$$

y la Proposición 8.4.2 nos dice que $b_i \equiv b_j \mod \mathsf{mcd}(m_i, m_j)$. Esto muestra que la condición del enunciado es necesaria para que existan soluciones del sistema de congruencias (27).

Probemos que también es suficiente y la última afirmación del enunciado haciendo inducción con respecto a r. Si r es 1, esto es evidente, y si r es 2 esto es parte de lo que afirma la Proposición 8.4.2.

Supongamos que s es un entero tal que $s \geq 2$ y que lo que afirma la proposición es cierto cuando r es s, y sean $m_1, \ldots, m_{s+1}$ enteros positivos y $b_1, \ldots, b_{s+1}$ enteros tales que $b_i \equiv b_j \mod \mathsf{gcd}(m_i, m_j)$ cada vez que i y j son elementos de $\{1, \ldots, r\}$.

La Proposición 8.4.2 nos dice que hay enteros x tales que

$$\begin{cases} x \equiv b_s \mod m_s, \\ x \equiv b_{s+1} \mod m_{s+1} \end{cases} \tag{28}$$

y, más aún, que el conjunto de tales enteros es una clase de congruencia módulo $\mathsf{mcm}(m_s, m_{s+1})$: así, existe $a \in \mathbb{Z}$ tal que un entero x satisface las congruencias (28) si y solamente si $x \equiv a$

$\mod \operatorname{mcm}(m_s, m_{s+1})$. Observemos que, en particular, tenemos que $a \equiv b_s \mod m_1$ y $a \equiv b_{s+1} \mod m_{s+1}$.

Como consecuencia de esto, es claro que un entero x satisface el sistema de $s+1$ congruencias

$$\begin{cases} x \equiv b_1 & \mod m_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv b_{s+1} & \mod m_{s+1} \end{cases}$$

si y solamente si satisface el sistema de s congruencias

$$\begin{cases} x \equiv \tilde{b}_1 & \mod \tilde{m}_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv \tilde{b}_{s-1} & \mod \tilde{m}_{s-1}, \\ x \equiv \tilde{b}_s & \mod \tilde{m}_s \end{cases}$$

en el que

$$\tilde{b}_1 = b_1, \quad \ldots, \quad \tilde{b}_{s-1} = b_{s-1}, \quad \tilde{b}_s = a,$$

y

$$\tilde{m}_1 = m_1, \quad \ldots, \quad \tilde{m}_{s-1} = m_{s-1}, \quad \tilde{m}_s = \operatorname{mcm}(m_s, m_{s+1}).$$

□

```
module TCR where

import EMCD

resolverTCR :: [(Integer, Integer)] -> Maybe (Integer, Integer)
resolverTCR [(a, m)]               = Just (a `mod` m, m)
resolverTCR ((a, m) : (b, n) : eqs)
  | (a - b) `mod` d == 0           = resolverTCR ((c, p) : eqs)
  | otherwise                      = Nothing
  where (d, x, y) = emcd m n
        c         = (x * m * b + y * n * a) `div` d
        p         = m * n `div` d
```

Programa 8.3. Con esta definición, si `eqs` es una lista de pares de enteros de la forma `[(a1,m1), ..., (ar,mr)]`, entonce s la expresión `resolverTCD eqs` se evalúa o bien a `Just (c,s)`, en caso de que el sistema de congruencias $x \equiv a_1 \mod m_1, \ldots, x \equiv a_r \mod m_r$ tenga como soluciones a los enteros congruentes con `c` módulo `s`, o bien a `Nothing`, en caso de que ese sistema de ecuaciones no posee ninguna solución. Este código depende del Programa 6.5 en la página 186.

§8.5. Ejercicios

Una demostración alternativa del Teorema Chino del Resto

8.5.1. Ejercicio. Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros coprimos dos a dos y pongamos $M = m_1 \cdots m_r$. Para cada $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ escribamos $[a]_m$ a la clase de congruencia de a módulo m, que es un elemento del conjunto $\mathbb{Z}_m$.

(*a*) La función $\varphi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ tal que

$$\varphi([a]_M) = ([a]_{m_1}, \ldots, [a]_{m_r})$$

para todo $a \in \mathbb{Z}$ es inyectiva.

(*b*) El dominio y el codominio de la función φ tienen el mismo cardinal, así que φ también es sobreyectiva.

(*c*) Si $b_1, \ldots, b_r$ son enteros, entonces existe un entero x tal que

$$\varphi([x]_M) = ([b_1]_{m_1}, \ldots, [b_r]_{m_r})$$

y si y es otro entero con la misma propiedad entonces $[x]_M = [y]_M$. Deduzca de esto que el Teorema Chino del Resto 8.4.4 vale.

Capítulo 9

Números primos

§9.1. Números primos

9.1.1. Si a es un entero, llamamos a todo número $b \in \mathbb{Z}$ tal que $b \mid a$ un ***divisor*** de a. De acuerdo a la Proposición 6.1.4, si a es distinto de 0 y b es un divisor de a, entonces $|b| \leq |a|$. Esto implica que si queremos buscar los divisores de un número a no nulo basta buscarlos entre los elementos del conjunto $\{i \in \mathbb{Z} : -a \leq i \leq a\}$. Esto es importante, ya que este conjunto es *finito*: para encontrar todos los divisores de a hay que hacer un número finito de cálculos.

Si a es positivo, entonces a tiene por lo menos a 1 y a a como divisores positivos. Una consecuencia inmediata de esto es que el único entero positivo que tiene exactamente *un* divisor positivo es 1: todos los otros enteros positivos tienen al menos dos. Decimos que un número entero positivo p es ***primo*** cuando tiene exactamente *dos* divisores positivos. Un entero positivo mayor que 1 que no es primo es ***compuesto***. Observemos que el entero 1 no es ni primo ni compuesto.

9.1.2. Una observación inmediata sobre los primos es la siguiente:

Proposición. *Sea p un número primo y sea a un entero cualquiera. El máximo común divisor $\mathsf{mcd}(p, a)$ es o 1 o p, y el segundo caso ocurre si y solamente si p divide a a.*

Demostración. En efecto, el número $\mathsf{mcd}(p, a)$ es un divisor de p, así que es o 1 o p, y es p exactamente cuando p divide a a. □

9.1.3. Para determinar si un entero $a > 1$ es primo, hay que verificar en principio que ningún entero b tal que $1 < b < a$ divide a a. El siguiente resultado implica que basta verificar que ningún *primo* p tal que $1 < p < a$ divide a a.

Proposición. *Un entero mayor que* 1 *es o primo o divisible por un número primo menor que él.*

Una forma equivalente de decir esto es que todo un número mayor que 1 que tiene por lo menos tres divisores tiene uno que es primo.

Demostración. Para cada entero n sea $P(n)$ la afirmación

n es primo o divisible por un número primo menor que él

y mostremos por inducción que $P(n)$ vale para todo entero $n \geq 2$. El número 2 es primo, ya que ningún entero b tal que $1 < b < 2$ lo divide: de hecho, no hay ningún entero que satisfaga ni siquiera la primera de esas condiciones. Vemos así que la afirmación $P(2)$ vale y esto nos da el paso inicial de la inducción.

Supongamos ahora que k es un entero tal que $k \geq 2$ y que las afirmaciones $P(2)$, $P(3)$, $\ldots$, $P(k-1)$ valen. Si k es primo, entonces $P(k)$ vale. Si en cambio k no es primo, como es mayor que 1 tiene más que dos divisores positivos: esto implica que tiene un divisor positivo l distinto de 1 y de k. Por supuesto, esto implica que $1 < l < k$ y entonces nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale.

Ahora bien, este número l puede ser primo o no. Si es primo, entonces es un divisor primo de k menor que k y vemos que $P(k)$ vale. Si en cambio l no es primo, la validez de $P(l)$ implica que existe un primo p menor que l tal que $p \mid l$. Como $l \mid k$, gracias a transitividad de la divisibilidad tenemos que $p \mid k$: vemos así que p es un primo que divide a k y, como es menor que l, que es menor que k. Esto muestra que en cualquiera de los dos casos la afirmación $P(k)$ vale y completa la inducción. □

9.1.4. Un corolario inmediato pero útil de la proposición que acabamos de probar es:

Corolario. *Todo entero mayor que* 1 *es divisible por un número primo.*

Muchas veces usamos esto para probar que un número positivo es igual a 1: mostramos que no es divisible por ningún número primo.

Demostración. De acuerdo a la proposición un número entero mayor que 1 es primo o tiene un divisor primo menor que él: en cualquiera de los dos casos tiene un divisor primo. □

9.1.5. Apoyándonos en la Proposición 9.1.3, podemos describir un algoritmo para obtener la lista de los números primos menores que un número entero positivo dado N. Empezamos escribiendo la lista en orden de los números enteros desde el 2 hasta N. A medida que vayamos avanzando, vamos a ir tachando alguno de estos números y marcando otros con un círculo. Llevaremos a cabo

el siguiente paso repetidas veces, mientras podamos:

> *encerramos con un círculo el primer número de la lista que no esté ni tachado ni encerrado con un círculo y a continuación tacharemos todos los números más grandes que él y que son sus multiplos.*

El procedimiento se detiene cuando no podamos realizar esto: cuando no quede ningún número que no esté ni tachado ni encerrado en un círculo.

Veamos cómo funciona esto cuando N es 59. Empezamos con la lista de los números de 2 al 59:

		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

El primer paso es localizar el primer número de la lista que no está ni tachado ni encerrado en un círculo: como no hay ninguno tachado ni marcado con un círculo, es claro que se trata del 2. Ahora encerramos al 2 con un círculo y tachamos todos sus múltiplos: nos queda

		(2)	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19
~~20~~	21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~	31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39
~~40~~	41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~	51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59

En este momento, el primer número que no está ni tachado ni encerrado en un círculo es el 3, así que lo encerramos en un círculo y tachamos sus múltiplos:

		(2)	(3)	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59

Observemos que al tachar los múltiplos de 3 volvimos a tachar algunos números que ya estaban tachados, como el 6 o el 12. Para el tercer paso, el primer entero libre es el 5 y lo que nos queda después de encerrarlo en un círculo y tachar sus múltiplos es

		(2)	(3)	~~4~~	(5)	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59

Continuamos de esta forma: en sucesivos pasos encerramos en círculos al 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, y al 59, tachando en cada paso los múltiplos de estos números. Al terminar de

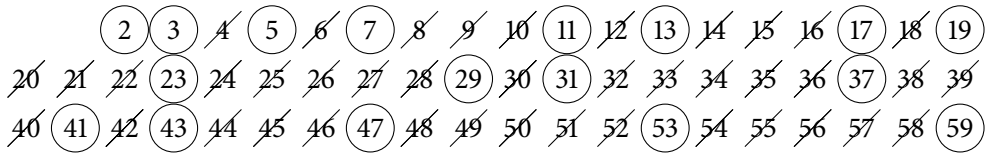
```
module Primos where

primos :: Integer -> [Integer]
primos n = cribar [2 .. n]

cribar :: [Integer] -> [Integer]
cribar []       = []
cribar (x : xs) = x : cribar [i | i <- xs, i `mod` x /= 0]
```

Programa 9.1. Una implementación de la criba de Eratóstenes en Haskell. El valor de la expresión `primos n` es la lista creciente de los primos menores o iguales que `n`. Es interesante observar que con estas definiciones, la expresión `cribar [2..]` se evalúa a la lista de *todos* los primo y entonces, por ejemplo, podemos calcular `takeWhile (<1000) (cribar [2..])` para determinar la lista de los primos menores que 1000 y `cribar [2..] !! 100` para determinar el centésimo primo.

hacer eso, lo que tenemos es:



Como ya no quedan números que no estén ni tachados ni encerrados en un círculo, el algoritmo termina. Los números que quedaron encerrados en círculos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59

y estos son precisamente los números primos menores o iguales a 59.

Este procedimiento se llama la ***criba*[1] *de Eratóstenes***, por Eratóstenes de Cirena, a quien se le atribuye desde principios de la era cristiana su invención. Eratóstenes llegó a ser el bibliotecario de la Biblioteca de Alejandría, en Egipto. Su más célebre logro es la determinación de la circunferencia de la Tierra "sin haber salido de su biblioteca". En la Figura 9.1 damos una posible implementación de este algoritmo en Haskell. En la computadora del autor, esta implementación determina la lista de los primos menores que 100 000, que son 9 592, en 20 segundos.

9.1.6. Imaginemos que empezamos con la lista infinita de *todos* los enteros mayores que 1 y realizamos el proceso de cribado tal cual como lo describimos arriba: al comenzar cada paso,

[1] La palabra *criba* designa el utensilio que se usa para cribar, es decir, para filtrar y seleccionar semillas o minerales.

identificamos el primer entero de la lista que no está ni tachado ni encerrado en un círculo, lo encerramos en un círculo y tachamos todos sus (¡infinitos!) múltiplos. Una cosa que podría ocurrir, *a priori*, es que lleguemos a un punto — después de realizar un cierto número de pasos — en el que no podamos continuar porque ya no quedan números que no estén ni tachados ni encerrados en círculos y, entonces, no podamos realizar el paso siguiente.

Si esto ocurriera, en ese momento tendríamos un número finito de números encerrados en círculos (ya que en cada uno de los pasos que sí pudimos hacer encerramos exactamente un número en un círculo) y todos los otros números estarían tachados. Claramente, esto nos diría que hay un número finito de números primos.

Una observación fundamental — debida a Euclides — es que esto no ocurre:

Proposición. *Existen infinitos números primos.*

Así, el proceso de cribado de la lista de todos los enteros mayores que 1 nunca se detiene. La demostración que daremos es de esta proposición es debida a Euclides mismo.

Demostración. Supongamos que, por el contrario, hay un número finito de números primos, sea

$$p_1,\ p_2,\ \ldots,\ p_m \tag{1}$$

la lista de todos ellos y consideremos el número $N = p_1 \cdots p_m + 1$. Como los números primos son todos positivos, es claro que $N > 1$ y la Proposición **9.1.3** nos dice entonces que N tiene un divisor primo. Ese divisor primo tiene que ser uno de los números de la lista (1), así que existe $i \in \{1, \ldots, m\}$ tal que $p_i \mid p_1 \cdots p_m + 1$. Como claramente p_i también divide al producto $p_1 \cdots p_m$, el Corolario **6.1.6** nos dice que p_i divide a 1: esto es, por supuesto, absurdo. Esta contradicción muestra que nuestra hipótesis es insostenible y, por lo tanto, que el conjunto de los números primos es infinito, como afirma la proposición. □

9.1.7. Otra consecuencia importante de la Proposición **9.1.3** es:

Proposición. *Todo entero positivo es igual a un producto de números primos.*

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

el número n es igual a un producto de números primos.

Mostremos que $P(n)$ vale para todo $n \in \mathbb{N}$ por inducción. Que $P(1)$ vale es claro, ya que 1 es igual al producto de cero factores primos, y esto establece el paso base.

Supongamos ahora que $k \in \mathbb{N}$ y que las afirmaciones $P(1), \ldots, P(k-1)$ valen, y mostremos que entonces también vale $P(k)$. Ahora bien, si k es primo, entonces es claro que $P(k)$ vale, ya que

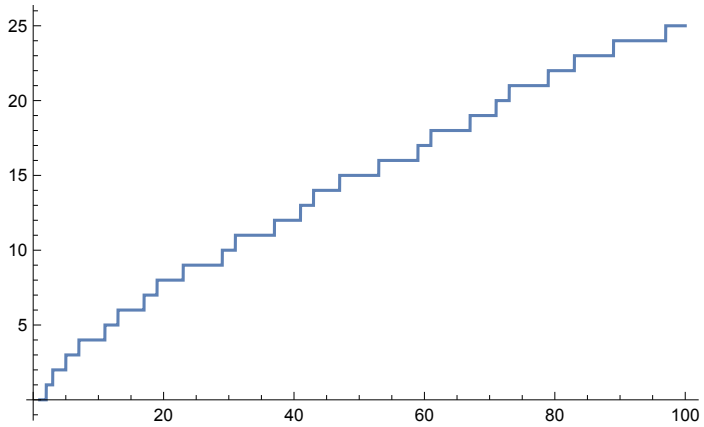


Figura 9.1. La función π en el intervalo $[0, 100]$.

k es igual a un producto de números primos con un sólo factor. Supongamos entonces que, por el contrario, k no es primo. La Proposición 9.1.3 nos dice que hay un número primo p menor k tal que $p \mid k$ y, en consecuencia, que hay entonces un entero positivo l tal que $k = pl$. Como $p \geq 2$ y, por lo tanto,

$$l = \frac{k}{p} \leq \frac{k}{2} < k,$$

tenemos que $1 \leq l < k$. En particular, nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale, es decir, que l es igual a un producto de números primos: existen $r \in \mathbb{N}_0$ y números primos $p_1, \ldots, p_r$ tales que $l = p_1 \cdots p_r$. Como entonces $k = pl = pp_1 \cdots p_r$, vemos que k es igual a un producto de números primos, es decir, que $P(k)$ vale. Esto completa la inducción. □

9.1.8. La Proposición 9.1.6 nos dice que hay infinitos números primos. Podemos ser más ambiciosos y hacernos la siguiente pregunta: si x es un número real positivo, ¿cuántos números primos que menores que x? En otras palabras, esta pregunta pide determinar el entero

$$\pi(x) \coloneqq |\{n \in \mathbb{N} : n \text{ es primo y } n \leq x\}|.$$

Notemos que de esta forma obtenemos una función $\pi : [0, +\infty) \to \mathbb{R}$. Si tenemos a nuestra disposición una tabla de números primos o, mejor, una computadora, podemos evaluar π fácilmente. En la Figura 9.1 podemos ver el gráfico de la función π en el intervalo $[0, 100]$.

La Proposición 9.1.6 nos dice que la función π no está acotada superiormente y si analizamos la forma en la que la probamos podemos obtener también una cota inferior para ella:

Proposición. *Para todo $n \geq 2$ vale que $\pi(n) \geq \ln \ln n$.*

Esta cota inferior crece de manera extremadamente lenta con n y resulta no ser particularmente buena. Nos dice, por ejemplo, que $\pi(10^{15}) \geq \ln\ln 10^{15} = 3{,}542\,082\ldots$, lo que es cierto, ya que $\pi(10^{15}) = 29\,844\,570\,422\,669$, pero claramente no es muy informativo!

Demostración. Sea $p_1, p_2, p_3, \ldots$, la lista en orden creciente de los números primos. Mostremos que para cada $n \in \mathbb{N}$ vale que

$$p_n \leq 2^{2^{n-1}}. \tag{2}$$

Esto ciertamente es cierto cuando n es 1, ya que $p_1 = 2 \leq 2^{2^{1-1}}$. Supongamos, por otro lado, que k es un elemento cualquiera de $\mathbb{N}$ mayor que 1 y que sabemos que la desigualdad (2) es cierta siempre que $1 \leq n < k$. El número $p_1 \cdots p_{k-1} + 1$ es mayor que 1, así que es divisible por algún primo: como no es divisible por ninguno de los primos $p_1, p_2, \ldots, p_{k-1}$, tiene que ser divisible por algún primo mayor o igual que p_k y, en particular,

$$p_k \leq p_1 p_2 \cdots p_{k-1} + 1 \leq 2^{2^{1-1}} 2^{2^{2-1}} \cdots 2^{2^{(k-1)-1}} + 1 = 2^{2^0 + 2^1 + \cdots + 2^{k-2}} + 1 = 2^{2^{k-1}-1} + 1.$$

Como $k \geq 2$, es $2^{k-1} - 1 \geq 2^1 - 1 = 1$, así que $2^{2^{k-1}-1} \geq 1 \geq 1$ y

$$2^{2^{k-1}-1} + 1 \leq 2^{2^{k-1}-1} + 2^{2^{k-1}-1} = 2 \cdot 2^{2^{k-1}-1} = 2^{2^{k-1}}.$$

Esto nos dice que la desigualdad (2) vale cuando n es k. Esa desigualdad es, por lo tanto, cierta para cualquier $n \in \mathbb{N}$. Notemos que esto nos dice que n es un elemento cualquiera de $\mathbb{N}$, entonces $p_n \leq 2^{2^{n-1}}$ y, por lo tanto, $\pi(2^{2^{n-1}}) \geq n$.

Sea ahora n un entero mayor que 2 y sea $m \coloneqq \lfloor \log_2 \log_2 n \rfloor$. Es $m \leq \log_2 \log_2 n < m + 1$, así que $2^m \leq \log_2 n$, $2^{2^m} \leq n <$ y, por lo tanto,

$$\log_2 \log_2 n < m + 1 \leq \pi(2^{2^m}) \leq \pi(n). \tag{3}$$

Es $0 < \ln 2 < 1$, ya que $2 < e$, así que para todo número real x mayor que 1 es $\log_2 x = \ln x / \ln 2 > \ln x$. Como la función $\log_2$ es creciente, esto implica a su vez que para todo número real x tal que $\ln x$ es mayor que 1 es

$$\log_2 \log_2 x \geq \log_2 \ln x > \ln\ln x.$$

Combinando esta desigualdad con la de (3) obtenemos la de la proposición. □

9.1.9. Un resultado fundamental de la teoría de números es el siguiente teorema, usualmente llamado el *teorema de los números primos*:

Teorema. *Si x es un número real suficientemente grande, entonces* $\pi(x) \sim \dfrac{x}{\ln x}$. □

Explícitamente, lo que queremos decir aquí es que cuando el número x es grande el cociente de $\pi(x)$ y de $x/\ln x$ se aproxima a 1, esto es, que

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

El primero en conjeturar que la función π puede aproximarse por una expresión como la que aparece en el teorema fue Adrien-Marie Legendre, en 1797, en base a la consideración de tablas de primos elaboradas por Anton Felkel y Jurij Bartolomej Vega[2]

El problema de aproximar π fue considerado desde entonces por muchos matemáticos — Carl Friedrich Gauss, Peter Gustav Lejeune Dirichlet, Pafnuty Chebyshev, Leonhard Euler, Bernhard Riemann, entre muchos otros — pero el teorema de los números primos fue probado por primera vez recién por Jacques Hadamard [Had1896]y Charles Jean de la Vallée Poussin [dLVP1896a, dLVP1896b, dLVP1896c, dLVP1897a, dLVP1897b] en trabajos independientes y casi simultáneos basados de manera esencial en ideas de Riemann. Hoy se conocen varias pruebas del teorema y todas son largas y complicadas. La más sencilla fue encontrada por Donald Joseph Newman en 1980 [New1980]; una versión de esta de Don Zagier puede encontrarse en [Zag1997].

Una consecuencia directa del teorema es la observación de que cuando n es un entero positivo grande podemos dar una aproximación para el n-ésimo primo p_n:

$$p_n \sim n \ln n. \tag{4}$$

Por ejemplo, el primo 10^{15}-avo es

$$p_{10^{15}} = 37\,124\,508\,045\,065\,437$$

mientras que

$$10^{15} \ln 10^{15} \sim 34\,538\,776\,394\,910\,685{,}260\,269\ldots$$

La diferencia entre $p_{10^{15}}$ y $10^{15}\ln 10^{15}$ es grande, del orden de 10^{15}, pero el error relativo de la aproximación es pequeño y menor que el 7 %:

$$\frac{p_{10^{15}} - 10^{15}\ln 10^{15}}{p_{10^{15}}} = 0{,}069\,650\,3\ldots$$

[2] Felkel había publicado entre 1776 y 1777 una tabla [Fel1776] que daba la factorización de todos los números coprimos con 30 entre 1 y 10 000 000. En la Figura 9.2 puede verse una página de este trabajo. El trabajo matemático más famoso de Vega, por su parte, es una serie de volúmenes con tablas de logaritmos decimales y funciones trigonométricas, en los que trabajó durante toda su vida. Además de eso, Vega se dedicó a la astronomía, a la física y a la balística. Hay un cráter en la luna que lleva su nombre, con coordenadas $45.4^\circ S\ 63.4^\circ E$.

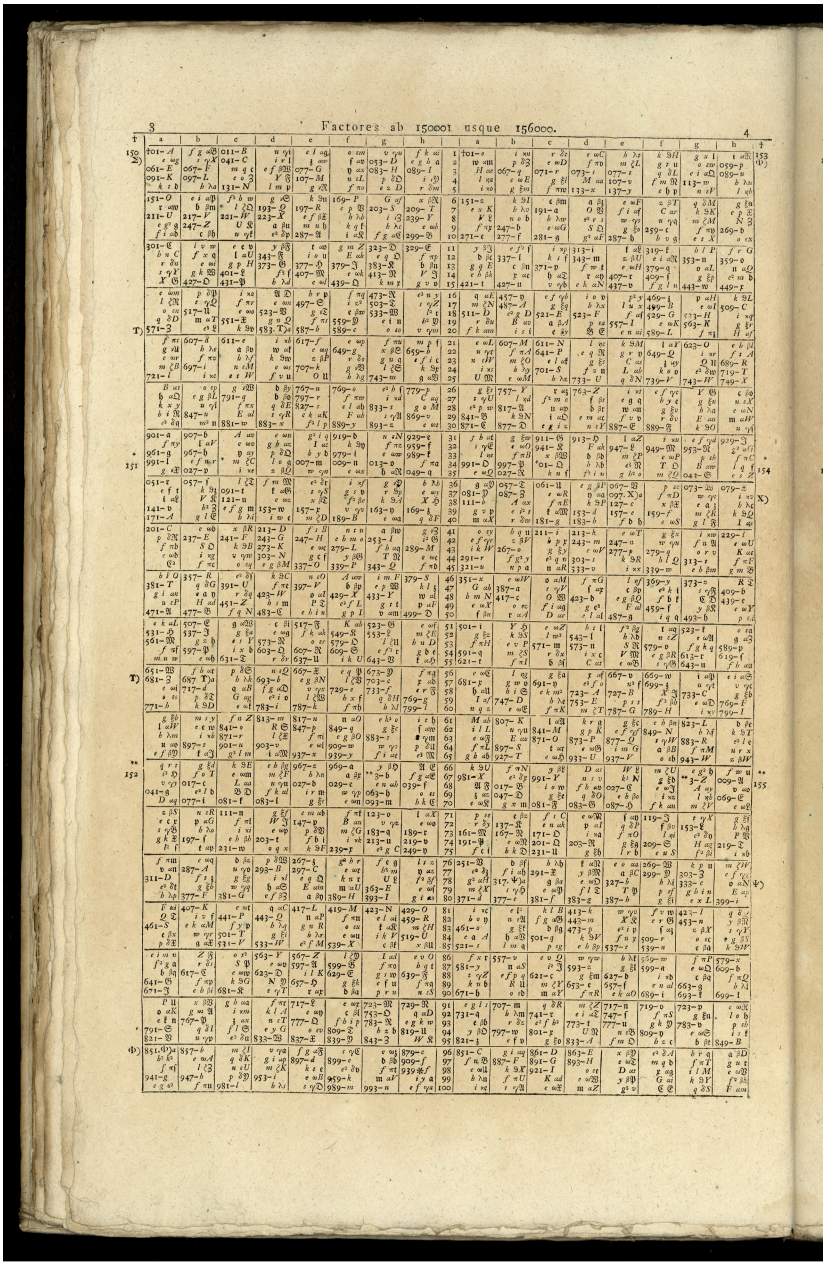


Figura 9.2. Una página de la tabla de Anton Felkel con la factorización de todos los enteros positivos coprimos con 30 y menores que 10 000 000. El libro puede encontrarse entero en versión electrónica en la URL incluida en la referencia [Fel1776]. La computadora del autor de estas notas puede generar esa tabla completa en 16 segundos.

Es en este sentido que debe entenderse la aproximación (4): el límite cuando n crece del error relativo de la aproximación es 0.

Es de notar que se conocen aproximaciones al n-ésimo primo mucho mejores que la de (4), que se deducen de resultados más precisos que el teorema de los números primos. Por ejemplo, Ernesto Cesàro probó en [Ces1894] que para cada entero positivo n es

$$\frac{p_n}{n} = \ln n + \ln\ln n - 1 + \frac{\ln\ln n - 2}{\ln n} - \frac{(\ln\ln n)^2 - 6\ln\ln n + 11}{2(\ln n)^2} + \varepsilon_n,$$

con ε_n un número tal que

$$\lim_{n\to\infty} \frac{\varepsilon_n}{1/(\ln n)^2} = 0.$$

Esto nos dice que 10^{15}-avo primo $p_{10^{15}}$ es aproximadamente igual a

$$37\,124\,545\,467\,703\,341{,}527\,861\ldots$$

Esta aproximación tiene un error relativo de 0,000 100 8 %, remarcablemente mejor que la anterior.

Una segunda consecuencia del teorema es que si N es un entero positivo grande, entonces la proporción de números primos en el conjunto $\{1,\ldots,N\}$ es aproximadamente

$$\frac{\pi(N)}{N} \sim \frac{N/\ln N}{N} = \frac{1}{\ln N}. \tag{5}$$

Esto nos dice que cuando N crece cada vez hay relativamente menos y menos primos en el conjunto $\{1,\ldots,N\}$, porque sabemos que $\lim_{N\to\infty} \ln N = +\infty$. De todas formas, como la función $\ln$ crece de manera muy lenta con su argumento, esta proporción decrece muy lentamente. Por ejemplo, hay $\pi(10^{15}) = 29\,844\,570\,422\,669$ y $\pi(10^{20}) = 2\,220\,819\,602\,560\,918\,840$ primos en los conjuntos $\{1,\ldots,10^{15}\}$ y $\{1,\ldots,10^{20}\}$, así que las proporciones de primos en esos conjuntos son

$$\frac{\pi(10^{15})}{10^{15}} = 0{,}029\,844\ldots \qquad \frac{\pi(10^{20})}{10^{20}} = 0{,}022\,208\ldots$$

mientras que las estimaciones dadas por (5) para esas proporciones son

$$\frac{1}{\ln 10^{15}} = 0{,}028\,953\ldots \qquad \frac{1}{\ln 10^{20}} = 0{,}021\,714\ldots$$

§9.2. El Teorema Fundamental de la Aritmética

9.2.1. En la sección anterior probamos la Proposición 9.1.7, que nos dice que todo entero positivo es igual a un producto de números primos. Nuestro objetivo en esta es mostrar que, de hecho, ese producto de primos es esencialmente único.

9.2.2. El primer paso para eso es establecer la siguiente caracterización de los números primos, usualmente conocida como el *Lema de Euclides* — es la Proposición 30 del libro VII de sus *Elementos*.

Proposición. *Un número p mayor que* 1 *es primo si y solamente si cada vez que divide al producto de dos enteros divide a alguno de ellos.*

Demostración. Veamos primero que la condición del enunciado es necesaria. Sea p un entero mayor que 1 que es primo, sean a y b dos enteros tales que p divide al producto ab, supongamos que p no divide a a y mostremos que entonces p necesariamente divide a b. El máximo común divisor de p y a es 1: en efecto, si d es un divisor común positivo de p y a, entonces en particular divide a p y, como p es primo, es o bien 1 o bien p, pero como estamos suponiendo que p no divide a a, esta segunda posibilidad no ocurre. Por otro lado, de acuerdo a la identidad de Bézout 6.4.10, existen entonces enteros x e y tales que $xp + ya = 1$. Si multiplicamos esta igualdad por b, vemos que $xpb + yab = b$. Como p divide tanto a xpb como a yab, deducimos de esto que p divide a b, como queríamos.

Probemos ahora que la condición del enunciado es suficiente para que p sea primo. Esto es, supongamos que p es un entero mayor que 1 tal que cada vez que divide a un producto de dos enteros divide a uno de los factores y mostremos que p debe ser entonces primo.

Supongamos para ello que, por el contrario, p no es primo. En ese caso, como es mayor que 1, posee un divisor d tal que $1 < d < p$. Si e es el cociente de la división de p por d, tenemos entonces que $p = de$. En particular, vemos que p divide al producto de y, de acuerdo a la hipótesis, divide entonces a alguno de los factores: esto es absurdo, ya que $1 < d < p$ y $1 < e < p$. Esta contradicción provino de haber supuesto que p no es primo, así que debe serlo. Esto completa la prueba de la proposición. □

9.2.3. La siguiente generalización de parte de la proposición anterior nos será útil:

Corolario. *Sea p un número primo, sea $r \in \mathbb{N}$ y sean $a_1, \ldots, a_r$ enteros. Si p divide al producto $a_1 \cdots a_r$, entonces existe $i \in \{1, \ldots, r\}$ tal que p divide a a_i.*

Demostración. Para cada $r \in \mathbb{N}$ sea $P(r)$ la afirmación

> *si p divide a un producto $a_1 \cdots a_r$ de r enteros $a_1, \ldots, a_r$, entonces existe $i \in \{1, \ldots, r\}$ tal que p divide a a_i.*

Que $P(1)$ vale es evidente. Supongamos, para hacer inducción, que k es un elemento cualquiera de $\mathbb{N}$ tal que $P(k)$ vale, y mostremos que entonces $P(k+1)$ también vale: esto probará el corolario.

Sean entonces $a_1, \ldots, a_{k+1}$ enteros, supongamos que p divide al producto $a_1 \cdots a_{k+1}$ y mostremos que p divide a alguno de los $k+1$ factores. Ahora bien, si llamamos b al producto $a_1 \cdots a_k$, entonces tenemos que p divide a ba_{k+1}: de acuerdo a la Proposición **9.2.2**, se sigue de esto que p divide a b o a a_{k+1}. Si la segunda de estas posibilidades ocurre, entonces claramente p divide a uno de los factores del producto $a_1 \cdots a_{k+1}$. Si en cambio p divide a $b = a_1 \cdots a_k$, entonces la hipótesis inductiva $P(k)$ nos dice que p divide a alguno de los factores $a_1, \ldots, a_k$ de b. En cualquier caso, vemos que la afirmación $P(k+1)$ vale, como queríamos. □

9.2.4. De acuerdo a la Proposición **9.1.7**, un entero positivo n es igual a un producto de números primos, esto es, existen $r \in \mathbb{N}_0$ y números primos $p_1, p_2, \ldots, p_r$ tales que

$$n = p_1 \cdots p_r. \tag{6}$$

Los números primos que aparecen en esta factorización no son necesariamente distintos. De todas formas, como la multiplicación de enteros es conmutativa, reindexándolos apropiadamente podemos suponer que $p_1 \leq p_2 \leq \cdots \leq p_r$. Mostraremos ahora que, bajo esta condición extra, hay exactamente *una* factorización de n como la de (6).

Proposición. *Si $r, s \in \mathbb{N}_0$ y $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son números primos tales que*

$$p_1 \leq \cdots \leq p_r, \qquad q_1 \leq \cdots \leq q_s \qquad y \qquad p_1 \cdots p_r = q_1 \cdots q_s,$$

entonces $r = s$ y $p_i = q_i$ para cada $i \in \{1, \ldots, r\}$.

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

> *si $r, s \in \mathbb{N}_0$ y $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son números primos tales que $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ y $n = p_1 \cdots p_r = q_1 \cdots q_s$, entonces $r = s$ y $p_i = q_i$ para cada $i \in \{1, \ldots, r\}$.*

Vamos a mostrar que $P(n)$ vale cualquiera sea $n \in \mathbb{N}$ haciendo inducción.

Empecemos por $P(1)$. Supongamos que $r, s \in \mathbb{N}_0$ y que $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son números primos tales que $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ y $1 = p_1 \cdots p_r = q_1 \cdots q_s$. Si $r > 0$, entonces el número primo p_1 divide al producto $p_1 \cdots p_r$, que es igual a 1: esto es absurdo y esta contradicción nos dice que debe ser $r = 0$. De manera similar podemos ver que $s = 0$ y, por lo tanto, tenemos que $r = s$ y, de manera tautológica, que $p_i = q_i$ para todo $i \in \{1, \ldots, r\}$. Concluimos de esta forma que la

afirmación $P(1)$ vale.

Sea ahora k un elemento cualquiera de $\mathbb{N}$, supongamos que para cada entero i tal que $1 \leq i < k$ la afirmación $P(i)$ vale, y mostremos que entonces la afirmación $P(k)$ también vale. Para ello, supongamos que $r, s \in \mathbb{N}_0$ y que $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son números primos tales que $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ y

$$k = p_1 \cdots p_r = q_1 \cdots q_s. \tag{7}$$

No puede ser que se tenga que $p_r < q_s$. En efecto, si fuera ese el caso, como q_s divide a $k = p_1 \cdots p_r$, el Corolario 9.2.3 nos diría que existe $i \in \{1, \ldots, r\}$ tal que q_s divide a p_i, y esto es imposible porque $p_i \leq p_r < q_s$. De manera similar podemos ver que no puede ser que se tenga que $p_r > q_s$, y concluir, en definitiva, que $p_r = q_s$. Si ponemos $l \coloneqq k/p_r$, de la igualdad (7) deducimos, dividiendo en cada miembro por p_r, que

$$l = p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}. \tag{8}$$

Ahora bien, este entero l es positivo y estrictamente menor que k (porque $p_r \geq 2$), así que nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale. Usándola en (8), vemos que $r - 1 = s - 1$, es decir, que $r = s$, y que $p_i = q_i$ para cada $i \in \{1, \ldots, r-1\}$. Junto con el hecho que ya establecimos antes de que $p_r = q_r$, esto muestra que vale la afirmación $P(k)$, como queríamos. □

9.2.5. Podemos ahora enunciar y probar el llamado *Teorema fundamental de la aritmética*:

Proposición. *Si n es un entero positivo, entonces existen*

- *un entero no negativo $s \in \mathbb{N}_0$,*
- *números primos $p_1, \ldots, p_s$ y*
- *enteros positivos $a_1, \ldots, a_s$*

tales que $p_1 < \cdots < p_s$ y $n = p_1^{a_1} \cdots p_s^{a_s}$ y, más aún, todos ellos están unívocamente determinados por n.

Demostración. Sea n un entero positivo. De la Proposición 9.1.7 sabemos que existen $r \in \mathbb{N}_0$ y números primos $q_1, \ldots, q_r$ tales que $n = p_1 \cdots p_r$. Más aún, como observamos en 9.2.4, podemos suponer sin pérdida de generalidad que $q_1 \leq \cdots \leq q_r$, ya que si no es ese el caso basta reindexar apropiadamente los primos $q_1, \ldots, q_r$.

Los primos $q_1, \ldots, q_r$ no son necesariamente distintos dos a dos. Sea s la cantidad de elementos del conjunto $\{q_1, \ldots, q_r\}$, sean $p_1, \ldots, p_s$ los elementos de este conjunto listados en orden estrictamente creciente y para cada $i \in \{1, \ldots, s\}$ sea a_i la cantidad de veces que el primo p_i aparece en la

lista $q_1, \ldots, q_r$, es decir, el cardinal del conjunto $\{j \in \{1, \ldots, r\} : q_j = p_i\}$. Es claro, entonces, que

$$n = q_1 \cdots q_r = \underbrace{p_1 \cdots p_1}_{a_1 \text{ factores}} \underbrace{p_2 \cdots p_2}_{a_2 \text{ factores}} \cdots\cdots \underbrace{p_s \cdots p_s}_{a_s \text{ factores}} = p_1^{a_1} \cdots p_s^{a_s}.$$

Esto prueba la afirmación de existencia de la proposición.

Para ver la de unicidad, supongamos que $r, s \in \mathbb{N}_0$, que $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son dos secuencias estrictamente crecientes de números primos, y que $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathbb{N}$ son tales que

$$n = p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}.$$

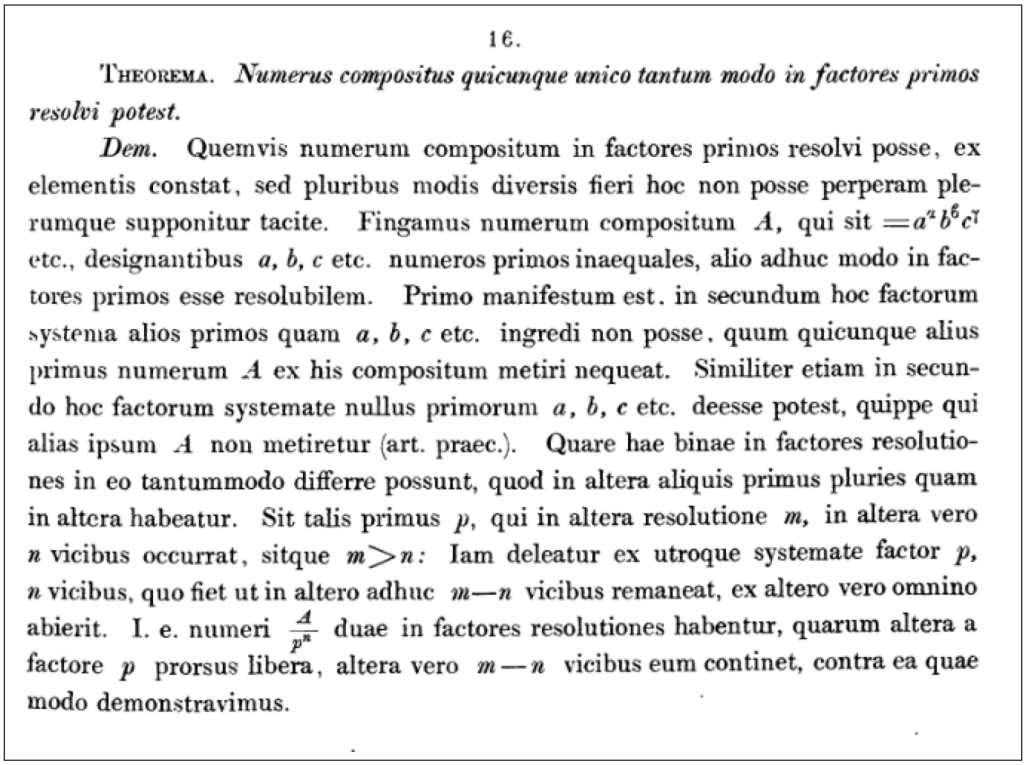
Podemos reescribir esta última igualdad en la forma

$$\underbrace{p_1 \cdots p_1}_{a_1 \text{ factores}} \cdots\cdots \underbrace{p_r \cdots p_r}_{a_r \text{ factores}} = \underbrace{q_1 \cdots q_1}_{b_1 \text{ factores}} \cdots\cdots \underbrace{q_s \cdots q_s}_{b_s \text{ factores}}.$$

A la izquierda tenemos un producto de $a_1 + \cdots + a_r$ números primos y los factores están en orden no decreciente, mientras que a la derecha tenemos un producto de $b_1 + \cdots + b_s$ números primos también listados en orden no decreciente. De acuerdo a la Proposición **9.1.7**, entonces, a ambos lados de la igualdad tenemos la misma cantidad de factores, así que $a_1 + \cdots + a_r = b_1 + \cdots + b_s$, y los factores son los mismos en el mismo orden. Es inmediato entonces que $r = s$ y que $p_i = q_i$ y $a_i = b_i$ para cada $i \in \{1, \ldots, r\}$. La proposición queda así probada. □

9.2.6. A pesar de que este *Teorema fundamental de la aritmética* es en efecto fundamental, fue recién Gauss en 1801, en sus *Disquisitiones Arithmeticae*, el primero en enunciarlo precisamente y probarlo. El teorema no aparece en los *Elementos* de Euclides: aunque ciertamente aparecen ahí nuestro Corolario **9.1.4**, que usamos para probar la existencia de una factorización en factores primos, y nuestra Proposición **9.2.2**, que está en la base de nuestro argumento para probar la unicidad, ninguna de las dos partes de la Proposición **9.2.5** puede leerse en los *Elementos*.

Luego de Euclides, el siguiente en ocuparse de la cuestión fue Kamāl al-Dīn al-Fārisī, un gran matemático, físico y astrónomo persa que murió hacia 1320. al-Fārisī escribió un libro sobre los "números amigos" en el que aparece el primer enunciado y la primera prueba de la afirmación de existencia de factorizaciones con factores primos de la que se tiene registro. Después de él, Jean Prestet en 1689, Leonhard Euler en 1770 y Adrien-Marie Legendre en 1798 hicieron ciertos avances en el estudio de estas factorizaciones pero no llegaron a enunciar ni probar la afirmación de unicidad, aunque la usaron implícitamente. Como dijimos, el teorema aparece en toda su gloria recién en 1801 en las *Disquisitiones Arithmeticae*, donde Gauss lo enuncia esencialmente igual que nosotros y lo prueba de una manera muy parecida a la nuestra, aunque con menos detalles. En la Figura 9.3 en la página siguiente reproducimos el pasaje relevante.



16.

THEOREMA. *Numerus compositus quicunque unico tantum modo in factores primos resolvi potest.*

Dem. Quemvis numerum compositum in factores primos resolvi posse, ex elementis constat, sed pluribus modis diversis fieri hoc non posse perperam plerumque supponitur tacite. Fingamus numerum compositum A, qui sit $= a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, alio adhuc modo in factores primos esse resolubilem. Primo manifestum est, in secundum hoc factorum systema alios primos quam a, b, c etc. ingredi non posse, quum quicunque alius primus numerum A ex his compositum metiri nequeat. Similiter etiam in secundo hoc factorum systemate nullus primorum a, b, c etc. deesse potest, quippe qui alias ipsum A non metiretur (art. praec.). Quare hae binae in factores resolutiones in eo tantummodo differre possunt, quod in altera aliquis primus pluries quam in altera habeatur. Sit talis primus p, qui in altera resolutione m, in altera vero n vicibus occurrat, sitque $m > n$: Iam deleatur ex utroque systemate factor p, n vicibus, quo fiet ut in altero adhuc $m-n$ vicibus remaneat, ex altero vero omnino abierit. I. e. numeri $\frac{A}{p^n}$ duae in factores resolutiones habentur, quarum altera a factore p prorsus libera, altera vero $m-n$ vicibus eum continet, contra ea quae modo demonstravimus.

Figura 9.3. El párrafo 16 de las *Disquisitiones Arithmeticae* de Gauss, en el que enuncia y prueba el Teorema Fundamental de la Aritmética. El enunciado dice: «Todo número compuesto puede resolverse en factores primos de una única manera».

En el trabajo [AÖ2001] puede encontrarse una descripción detallada de la historia de la Proposición 9.2.5 y en [AÖ1997] una revista de las muchas pruebas que han sido dadas de ella.

9.2.7. Si uno tiene acceso a la lista de los números primos menores que un entero positivo n, es fácil — aunque laborioso — encontrar la factorización de n como producto de números primos. Basta ir recorriendo la lista de los primos desde 2 en adelante y para cada uno de ellos determinar cuántas veces lo divide. Una simplificación de este proceso consiste en observar que cada vez que encontramos un primo que lo divide, es suficiente continuar buscando una factorización del correspondiente cociente.

Por ejemplo, supongamos que nos proponemos factorizar el entero 29 822 375. Los primeros primos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

Probamos dividir nuestro número por 2 y por 3, sin éxito. Es divisible por 5, y el cociente es 5 964 475; este es otra vez divisible por 5, con

29 822 375	5
5 964 475	5
1 192 895	5
238 579	11
21 689	23
943	23
41	41
1	

cociente 1 192 895, y este también, con cociente 238 579. Ya 5 no divide a este número: probamos entonces con 7, que no lo divide, y con 11, que sí funciona. El cociente es 21 689. Este número no es divisible por 11, así que continuamos probando con 13, 17 y 19, que no lo dividen, y con 23, que sí lo hace. El cociente es 943, que es otra vez divisible por 23, con cociente 41. Como 41 es primo, aquí termina el proceso. Concluimos así que la factorización que buscábamos es $29\,822\,375 = 5^3 \cdot 11 \cdot 23^2 \cdot 41$.

En la Figura 9.2 en la página siguiente damos una implementación en Haskell de este algoritmo. Con esas definiciones, podemos evaluar en un intérprete

```
*Main> factorizar 29822375
[5,5,5,11,23,23,41]
*Main> pares 29822375
[(5,3),(11,1),(23,2),(41,1)]
```

El primer resultado nos da la lista de primos con repeticiones que aparecen en la factorización de 29 822 375 mientras que el segundo nos da los pares (p, a) de primos y exponentes que aparecen en esa factorización.

9.2.8. Demos una aplicación sencilla y bonita del teorema fundamental de la aritmética:

Proposición. *Para todo $n \in \mathbb{N}$ el n-ésimo número primo p_n es menor que 4^n.*

Demostración. Sea n un entero positivo, sean $p_1, \ldots, p_n$ los primeros n números primos listados en orden creciente y sin repeticiones, y sea sea I el conjunto de todos los enteros de 1 a p_n.

Sea m un elemento cualquiera de I. Los primos que dividen a m pertenecen a I, porque son menores o iguales que p_n, así que hay enteros no negativos $a_1, \ldots, a_n$ tales que

$$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}.$$

Dividiendo estos enteros por 2 vemos que hay otros enteros no negativos $b_1, \ldots, b_n$ y elementos $c_1, \ldots, c_n$ del conjunto $\{0, 1\}$ tales que $a_i = 2b_i + c_i$ para cada $i \in \{1, \ldots, n\}$ y, por lo tanto, que

$$m = p_1^{2b_1+c_1} p_2^{2b_2+c_2} \cdots p_n^{2b_n+c_n} = \left(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}\right)^2 p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}.$$

Así, todo elemento de I es igual al producto de un cuadrado — necesariamente menor que p_n — y un elemento del conjunto

$$F \coloneqq \{p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} : 0 \leq c_1, c_2, \ldots, c_n \leq 1\}.$$

El número de cuadrados menores que p_n es, como mucho, $\sqrt{p_n}$, y el conjunto F tiene, de acuerdo al teorema fundamental de la aritmética, exactamente 2^n elementos. La cantidad de elementos de I es, por lo tanto,

$$p_n = |I| \leq \sqrt{p_n} \cdot 2^n.$$

```haskell
module Factorizar where

factorizar :: Integer -> [Integer]
factorizar n = reducir n (primos n)

reducir :: Integer -> [Integer] -> [Integer]
reducir 1 (p : ps) = []
reducir x (p : ps)
  | x `mod` p == 0 = p : reducir (x `div` p) (p : ps)
  | otherwise      = reducir x ps

pares :: Integer -> [(Integer, Integer)]
pares n = [(p, count p factores) | p <- nub factores]
  where factores = factorizar n
        count x ys = length [y | y <- ys, y == x]

sigma :: Integer -> Integer -> Integer
sigma 0 n = product [a + 1 | (p,a) <- pares n]
sigma k n = product [f (p, a) | (p, a) <- pares n]
  where f (p, a) = (p ^ (k * (a+1)) - 1) `div` (p ^ k - 1)
```

Programa 9.2. Una implementación en HASKELL del algoritmo trivial de factorización de un entero positivo como producto de números primos y de las funciones σ_k de la sección 9.4, usando las definiciones de la Figura 9.1 en la página 249.

Dividiendo por $\sqrt{p_n}$ a ambos lados de esta desigualdad y elevando luego al cuadrado vemos que $p_n \leq 4^n$, que es lo que la proposición afirma. □

9.2.9. Usando la misma idea que usamos para probar esta proposición encontrar una cota para la función π:

Corolario. *Para cada entero n es* $\pi(n) \geq \dfrac{\ln n}{2 \ln 2}$.

Esta cota es mejor que la que nos da la Proposición 9.1.8. Por ejemplo, es posible calcular que $\pi(10^{15}) = 29\,844\,570\,422\,669$: la cota que nos da aquella proposición es

$$\pi(10^{15}) \geq \ln \ln 10^{15} = 3{,}542\,082\ldots$$

mientras que el corolario nos dice que

$$\pi(10^{15}) \geq \frac{\ln 10^{15}}{2 \ln 2} = 24{,}914\,460\ldots$$

De todas formas, vemos con esto que se trata de una cota muy grosera. Sin embargo, cuando n crece la nueva cota es mucho mejor que la que teníamos, ya que

$$\lim_{n \to \infty} \frac{\ln \ln n}{\frac{\ln n}{2 \ln 2}} = 0.$$

Demostración. Sea n un entero tal que $n \geq 2$, sea $N \coloneqq \pi(n)$, y sean $p_1, \ldots, p_N$ los primos menores o iguales que n. En la demostración de la proposición vimos que todo elemento de $\{1, \ldots, n\}$ puede escribirse como un producto de un cuadrado menor o igual que n, de los cuales hay como mucho $\sqrt{n}$, y un número que es un producto de la forma $p_1^{c_1} \cdots p_N^{c_N}$ con $c_1, \ldots, c_N \in \{0, 1\}$, de los que hay 2^N. Esto implica, claro, que $n \leq \sqrt{n} \cdot 2^N$, así que $\sqrt{n} \leq 2^{\pi(n)}$: tomando logaritmos obtenemos la desigualdad del enunciado. □

Tanto la Proposición 9.2.8 como el Corolario 9.2.9 son debidos a Paul Erdős [Erd1938].

9.2.10. Es importante notar que para probar el Teorema fundamental de la aritmética 9.2.5 no usamos nunca el hecho de que hay infinitos números primos. Leonhard Euler aprovechó esto en su célebre artículo [Eul1744] para dar una prueba alternativa de que hay infinitos números primos.

Supongamos, siguiendo a Euler, que, por el contrario, hay un número finito de ellos, y sea $p_1, p_2, \ldots, p_N$ la lista de todos en orden creciente y sin repeticiones.

Sea m un entero positivo. Si distribuimos el producto de N factores

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots + \frac{1}{p_1^m}\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots + \frac{1}{p_2^m}\right) \cdots \left(1 + \frac{1}{p_N} + \frac{1}{p_N^2} + \cdots + \frac{1}{p_N^m}\right) \tag{9}$$

el resultado es la suma de $(m+1)^N$ fracciones de la forma

$$\frac{1}{p_1^{b_1} p_2^{b_2} \cdots p_N^{b_N}},$$

una para cada forma de elegir elementos $b_1, \ldots, b_N$ en el conjunto $\{0, \ldots, m\}$. Ahora bien, si n es un elemento de $\{1, \ldots, m\}$, entonces según el teorema fundamental de la aritmética hay exactamente una forma de elegir $a_1, \ldots, a_N$ en $\mathbb{N}_0$ tales que $n = p_1^{a_1} p_2^{a_2} \cdots p_N^{a_N}$, y es claro que todos ellos pertenecen a $\{0, \ldots, m\}$, ya que $n \leq m$: esto nos dice que exactamente una de las fracciones de la gran suma descripta arriba es igual a $1/n$. Esto prueba que el producto (9) es mayor o igual que la suma

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}.$$

Notando que cada uno de los factores de ese producto es una suma geométrica, concluimos así que

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} \leq \prod_{i=1}^{N} \frac{1 - 1/p_i^{m+1}}{1 - 1/p_i} \leq \prod_{i=1}^{N} \frac{1}{1 - 1/p_i}.$$

Esto es cierto cualquiera sea m en $\mathbb{N}$. Supongamos ahora que k es un entero positivo y pongamos $m = 2^k - 1$. Tenemos entonces que

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k - 1} \\ = 1 + \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \left(\frac{1}{8} + \cdots + \frac{1}{15}\right) + \cdots + \left(\frac{1}{2^{k-1}} + \cdots + \frac{1}{2^k - 1}\right). \end{aligned}$$

Para cada $i \in \{1, \ldots, k\}$ el i-ésimo sumando de esta última suma es él mismo una suma de 2^{i-1} términos todos mayores o iguales que $1/2^i$, así que es mayor o igual a $2^{i-1} \cdot 1/2^i = 1/2$. Como hay en total k de esos sumandos, esto nos dice que

$$\frac{k}{2} \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k - 1} \leq \prod_{i=1}^{N} \frac{1}{1 - 1/p_i}.$$

Esto no puede ser cierto para toda elección de k en $\mathbb{N}$, por supuesto. Esta contradicción provino de haber supuesto que hay un número finito de números primos: podemos concluir, entonces, que hay infinitos, y esto es lo que queríamos.

Esta demostración de la Proposición 9.1.6 es considerablemente más compleja que todas las que vimos antes! El argumento de Euler es importante, sin embargo, porque es el inicio de la llamada *teoría analítica de números*, que consiste en el uso de técnicas del análisis real y complejo para estudiar propiedades de los números enteros. La elaboración de esas ideas es lo que eventualmente llevó a la prueba del teorema de los números primos.

9.2.11. Ejercicio. Sea p_1, p_2, p_3, …la lista en orden creciente y sin repeticiones de los números primos. Muestre que si k un entero positivo, entonces existe un entero positivo N tal que

$$e^{2k} \leq \prod_{i=1}^{N} \frac{1}{1-1/p_i}.$$

Tomando logaritmos y recordando que $-\ln(1-x) \leq 2x$ para todo $x \in (0, \frac{1}{2}]$, concluya que

$$k \leq \sum_{i=1}^{N} \frac{1}{p_i}$$

Esto nos dice que el conjunto $\{\sum_{i=1}^{N} \frac{1}{p_i} : N \in \mathbb{N}\}$ no está acotado superiormente y, en el lenguaje del análisis, que

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = +\infty.$$

Este es un célebre teorema de Leonhard Euler publicado en [Eul1744].

9.2.12. Ejercicio. Sea p_1, p_2, p_3, …la lista en orden creciente y sin repeticiones de los números primos, y para cada $n \in \mathbb{N}$ sea

$$s_n \coloneqq \sum_{i=1}^{n} \frac{1}{p_i}.$$

Pruebe que para ningún $n \in \mathbb{N}$ el número s_n, que es ciertamente racional, es entero. Para hacerlo, muestre haciendo inducción que si a_n/b_n es la expresión de s_n como cociente de dos enteros coprimos, entonces uno de los números a_n y b_n es par y el otro impar.

§9.3. Valuaciones

9.3.1. Fijemos un número primo p y sea n un entero no nulo. Si $k \in \mathbb{N}_0$ es tal que p^k divide a n, entonces $p^k \leq |n|$ y, por lo tanto, $k \leq \log_p |n|$. Esto implica que el conjunto

$$V_p(n) = \{k \in \mathbb{N}_0 : p^k \mid n\}$$

está contenido en $\{0, \ldots, \lfloor \log_p |n| \rfloor\}$ y es, en consecuencia, finito. Como además no es vacío, tiene sentido entonces considerar su máximo elemento, al que escribimos $v_p(n)$ y llamamos la

valuación p-ádica de n. Se trata, de acuerdo a esta definiciones, del exponente más grande k tal que p^k divide a n. Así, por ejemplo, $v_2(168) = 3$ y $v_5(50) = 2$.

9.3.2. Una observación inmediata que podemos hacer es:

Lema. *Sea p un número primo. Si n es un entero no nulo, entonces*

$$V_p(n) = \{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\}.$$

En otras palabras, una potencia entera p^k de p divide a n si y solamente si $0 \leq k \leq v_p(n)$. En particular, p divide a n si y solamente si $v_p(n) > 0$.

Demostración. Sea n un entero no nulo. Si k es un entero tal que $0 \leq k \leq v_p(n)$, entonces $p^k \mid p^{v_p(n)}$ y, como $p^{v_p(n)} \mid n$, tenemos que $p^k \mid n$, es decir, que $k \in V_p(n)$. Esto muestra que $\{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\} \subseteq V_p(n)$. Por otro lado, como $v_p(n)$ es el máximo elemento de $V_p(n)$, es claro que $V_p(n)$ está contenido en $\{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\}$. Vale, en definitiva, la igualdad del enunciado. □

9.3.3. Podemos dar una caracterización alternativa sencilla de la valuación p-ádica:

Proposición. *Sea p un número primo y sea n un entero no nulo. La valuación p-ádica $v_p(n)$ de n es el único entero no negativo k tal que hay un entero m no divisible por p tal que $n = p^k m$.*

Demostración. Como $v_p(n)$ es un elemento del conjunto $V_p(n)$, tenemos que $p^{v_p(n)} \mid a$ y, por lo tanto, que existe hay un entero m tal que $n = p^{v_p(a)}m$. Supongamos por un momento que p divide a m, de manera que existe $u \in \mathbb{Z}$ tal que $m = pu$. En ese caso tenemos que $n = p^{v_p(a)+1}u$ y, por lo tanto, que $p^{v_p(n)+1}$ divide a n, es decir, que $v_p(n) + 1 \in V_p(n)$: esto es imposible, ya que $v_p(n)$ es el mayor elemento del conjunto $V_p(n)$. Vemos así que p no divide a m, y esto prueba que el número $v_p(n)$ tiene la propiedad descripta en el enunciado de la proposición.

Para ver que esa propiedad la caracteriza, supongamos ahora que $k \in \mathbb{N}_0$ es tal que existe $m \in \mathbb{Z}$ para el cual se tiene que $n = p^k m$ y $p \nmid m$. Esto nos dice, en particular, que p^k divide a n, así que $k \in V_p(n)$ y, por lo tanto, que

$$k \leq v_p(n), \tag{10}$$

ya que $v_p(n)$ es el mayor elemento de $V_p(n)$. Supongamos que la desigualdad (10) es estricta, de manera que $k + 1 \leq v_p(n)$. Tenemos entonces que $p^{k+1} \mid p^{v_p(n)} \mid n = p^k m$, así que existe $u \in \mathbb{Z}$ tal que $p^k m = p^{k+1}u$. Esto implica que $p^k(m - pu) = 0$ y, como $p \neq 0$, que $m = pu$, es decir, que p divide a m: esto contradice a nuestra hipótesis. Esta contradicción provino de suponer que la desigualdad (10) era estricta y podemos concluir entonces que $k = v_p(n)$, como afirma el enunciado. □

9.3.4. Si p es un número primo, entonces la valuación p-ádica es una función $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$. La siguiente proposición describe sus propiedades fundamentales.

Proposición. *Sea p un número primo.*

(*i*) *Si n es un entero no nulo, entonces $v_p(n) \in \mathbb{N}_0$ y*

$$v_p(-n) = v_p(n).$$

(*ii*) *Si n y m son dos enteros no nulos, entonces nm no es nulo y*

$$v_p(nm) = v_p(n) + v_p(m).$$

(*iii*) *Si n y m son dos enteros no nulos tales que $n + m \neq 0$, entonces*

$$v_p(n + m) \geq \mathsf{mín}\{v_p(n), v_p(m)\}.$$

Demostración. (*i*) Sea n un entero no nulo. Como $v_p(n)$ es el máximo elemento del conjunto finito $V_p(n)$ y este está contenido en $\mathbb{N}_0$, es evidente que $v_p(n) \geq 0$. Por otro lado, es evidente que $V_p(-n) = V_p(n)$, así que claramente $v_p(-n) = v_p(n)$.

(*ii*) Sean n y m dos enteros no nulos, de manera que en particular, $nm \neq 0$. La Proposición 9.3.3 nos dice que existen enteros n' y m' tales que $n = p^{v_p(n)}n'$, $m = p^{v_p(m)}m'$, $p \nmid n'$ y $p \nmid m'$. Se sigue de esto que

$$nm = p^{v_p(n)+v_p(m)}n'm'$$

y, gracias a la Proposición 9.2.2, que $p \nmid n'm'$. La Proposición 9.3.3 nos permite entonces concluir que $v_p(nm) = v_p(n) + v_p(m)$.

(*iii*) Sean n y m dos enteros no nulos tales que $n + m \neq 0$ y consideremos el entero no negativo $k = \mathsf{mín}\{v_p(n), v_p(m)\}$. Como $k \leq v_p(n)$ y $k \leq v_p(m)$, sabemos que p^k divide a n y a m, y se sigue de eso que p^k divide a $n + m$ y, por lo tanto, que $k \in V_p(n + m)$. Como $v_p(n + m)$ es el máximo elemento de $V_p(n + m)$, vemos así que $k \leq v_p(n + m)$: esto es precisamente lo que afirma el enunciado. □

9.3.5. Una de las razones por las que nos interesan las valuaciones de un número es que nos dicen exactamente cuáles son los exponentes en la factorización de este como producto de potencias de primos distintos dos a dos.

Proposición. *Sea n un número entero positivo. Si $p_1, \ldots, p_r$ son todos los números primos que dividen a n listados sin repeticiones, entonces*

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Demostración. Sean $p_1, \ldots, p_r$ los números primos que dividen a n listados sin repeticiones y sea i un elemento de $\{1, \ldots, r\}$. Sabemos que hay enteros positivos $a_1, \ldots, a_r$ tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Como p_i es distinto de todos los primos $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_r$, es coprimo con todos ellos, así que también es coprimo con los números $p_1^{a_1}, \ldots, p_{i-1}^{a_{i-1}}, p_{i+1}^{a_{i+1}}, \ldots, p_r^{a_r}$ y, finalmente, con el producto de todos estos,

$$m \coloneqq p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_r^{a_r}.$$

Tenemos entonces que $n = p_i^{a_i} m$ y que $p_i \nmid m$, así que la Proposición 9.3.3 nos permite concluir que $a_i = v_{p_i}(n)$. Como esto es cierto cualquiera sea el elemento i de $\{1, \ldots, n\}$, tenemos entonces que

$$n = p_1^{a_1} \cdots p_r^{a_r} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)},$$

como afirma la proposición. □

9.3.6. Más generalmente, tenemos lo siguiente:

Corolario. *Sea n un entero positivo. Si $p_1, \ldots, p_r$ es una lista de primos dos a dos distintos que incluye a todo primo que divide a n, entonces*

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

A diferencia de lo que ocurre en la Proposición 9.3.5, los exponentes que aparecen en esta factorización pueden ser nulos.

Demostración. Supongamos que $p_1, \ldots, p_r$ es una lista de primos dos a dos distintos que incluye a todo primo que divide a n. Reordenándola si es que es necesario, podemos suponer que hay un entero s con $0 \leq s \leq r$ y tal que los primos $p_1, \ldots, p_s$ dividen a n y los primos $p_{s+1}, \ldots, p_s$ no lo hacen. Como $p_1, \ldots, p_s$ son entonces todos los primos que dividen a n listados sin repeticiones, sabemos que

$$n = p_1^{v_{p_1}(n)} \cdots p_s^{v_{p_s}(n)}.$$

Por otro lado, como ninguno de $p_{s+1}, \ldots, p_r$ divide a n, sabemos que $v_{p_i}(n) = 0$ para cada $i \in \{s+1, \ldots, r\}$ y, por lo tanto, que

$$1 = p_{s+1}^{v_{p_{s+1}}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Juntando todo, vemos que

$$n = n \cdot 1 = p_1^{v_{p_1}(n)} \cdots p_s^{v_{p_s}(n)} \cdot p_{s+1}^{v_{p_{s+1}}(n)} \cdots p_r^{v_{p_r}(n)},$$

y este último producto es el mismo que aparece en el enunciado del corolario. □

9.3.7. Las valuaciones nos dan un criterio sencillo de divisibilidad:

Proposición. *Sean n y m dos enteros. Una condición necesaria y suficiente para que n divida a m es que para todo número primo p se tenga que $v_p(n) \leq v_p(m)$.*

Demostración. Sean $p_1, \dots p_r$ los primos que dividen a n listados sin repeticiones. De acuerdo a la Proposición 9.3.5 tenemos que

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Supongamos primero que se cumple la condición del enunciado, de manera que para cada elemento i de $\{1, \dots, r\}$ tenemos que $v_{p_i}(n) \leq v_{p_i}(m)$ y, por lo tanto, que $p_i^{v_{p_i}(n)} \mid m$. Como los números $p_1^{v_{p_1}(n)}, \dots, p_r^{v_{p_r}(n)}$ son coprimos dos a dos, el Corolario 6.5.8 nos permite deducir de eso que $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$ también divide a m. La condición es por lo tanto suficiente para que n divida a m.

Para probar la necesidad, supongamos que n divide a m y sea p un número primo. Como $p^{v_p(n)}$ divide a n, la transitividad de la divisibilidad implica que también divide a m y, por lo tanto, que $v_p(n) \leq v_p(m)$: vemos así que la condición se satisface. □

9.3.8. De manera muy similar, podemos usar valuaciones para dar expresiones para el máximo común divisor y el mínimo común múltiplo de dos enteros que son muchas veces útiles.

Proposición. *Sean n y m dos enteros positivos y sean $p_1, \dots, p_r$ los primos que dividen a nm listados sin repeticiones. Se tiene entonces que*

$$\mathsf{mcd}(n, m) = p_1^{a_1} \cdots p_r^{a_r}, \qquad \mathsf{mcm}(n, m) = p_1^{b_1} \cdots p_r^{b_r}$$

con

$$a_i = \mathsf{mín}\{v_{p_1}(n), v_{p_i}(m)\}, \qquad b_i = \mathsf{máx}\{v_{p_1}(n), v_{p_i}(m)\}$$

para cada $i \in \{1, \dots, r\}$.

Demostración. Sea $d \coloneqq p_1^{a_1} \cdots p_r^{a_r}$. Para cada $i \in \{1, \dots, r\}$ pongamos

$$s_i \coloneqq v_{p_i}(n) - a_i, \qquad t_i \coloneqq v_{p_i}(m) - a_i,$$

y observemos s_i y t_i son los dos no negativos y que alguno de los dos es nulo. Consideremos, finalmente, los números $x = p_1^{s_1} \cdots p_r^{s_r}$ e $y = p_1^{t_1} \cdots p_r^{t_r}$. Se tiene que

$$xd = p_1^{s_1} \cdots p_r^{s_r} \cdot p_1^{a_1} \cdots p_r^{a_r} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)} = n,$$

ya que $a_i + s_i = v_{p_i}(n)$ para todo $i \in \{1, \dots, r\}$. De manera similar, es $yd = m$.

Por otro lado, es $\mathsf{mcd}(x, y) = 1$. En efecto, sea f ese máximo común divisor. Si p es un primo y p divide a f, entonces p divide tanto a x como a y y, por lo tanto, existe $i \in \{1, \dots, r\}$ tal que $p = p_i$, $s_i > 0$ y $t_i > 0$: esto es imposible, ya que alguno de los dos números s_i o t_i es nulo. Vemos así que ningún primo divide a f y, como f es un entero positivo, que $f = 1$.

Juntando todo, vemos que tenemos dos enteros coprimos x e y tales que $n = xd$ y $m = yd$. De acuerdo al Corolario 6.5.4(*ii*), podemos concluir que $d = \mathsf{mcd}(n, m)$. Esto prueba la primera de las igualdades de la proposición.

Sea ahora $e \coloneqq p_1^{b_1} \cdots p_r^{b_r}$. Tenemos que

$$\begin{aligned} d \cdot e &= p_1^{a_1} \cdots p_r^{a_r} \cdot p_1^{b_1} \cdots p_r^{b_r} \\ &= p_1^{a_1+b_1} \cdots p_r^{a_r+b_r} \\ &= p_1^{v_{p_1}(n)+v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)+v_{p_r}(n)}, \end{aligned}$$

porque $a_i + b_i = v_{p_i}(n) + v_{p_i}(m)$ para todo $i \in \{1, \dots, r\}$, y esto es

$$\begin{aligned} &= p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_1}(n)} \cdot p_1^{v_{p_1}(m)} \cdots p_r^{v_{p_r}(m)} \\ &= n \cdot m. \end{aligned}$$

Así, tenemos que $\mathsf{mcd}(n, m) \cdot e = n \cdot m$ y, gracias al Ejercicio 6.6.4(*c*), podemos concluir que $e = \mathsf{mcm}(n, m)$. Esto prueba la segunda de las igualdades de la proposición. □

9.3.9. La descripción que nos da la última proposición del máximo común múltiplo nos permite probar fácilmente el siguiente resultado, que nos será útil más tarde.

Proposición. *Si n y m son dos enteros positivos, entonces existen enteros coprimos u y v tales que $\mathsf{mcm}(n, m) = uv$, $u \mid n$ y $u \mid m$.*

Demostración. Sean n y m dos enteros positivos y sean $p_1, \dots, p_r$ los primos que dividen al producto nm, listados sin repeticiones. Para cada $i \in \{1, \dots, r\}$ sean

$$a_i \coloneqq \begin{cases} v_{p_i}(n), & \text{si } v_{p_i}(n) \geq v_{p_i}(m); \\ 0, & \text{en caso contrario} \end{cases}$$

y

$$b_i \coloneqq \begin{cases} v_{p_i}(m), & \text{si } v_{p_i}(n) < v_{p_i}(m); \\ 0, & \text{en caso contrario.} \end{cases}$$

Consideremos finalmente los enteros $u \coloneqq p_1^{a_1} \cdots p_r^{a_r}$ y $v \coloneqq p_1^{b_1} \cdots p_r^{b_r}$. Para todo $i \in \{1, \dots, r\}$ tenemos que

- $v_{p_i}(u) = a_i \leq v_{p_i}(m)$ y $v_{p_i}(v) = b_i \leq v_{p_i}(m)$,
- $v_{p_i}(u) + v_{p_i}(v) = a_i + b_i = \max(v_{p_i}(n), v_{p_i}(m))$, y
- $\min\{v_{p_i}(u), v_{p_i}(v)\} = \min(a_i, b_i) = 0$.

De la primera de estas observaciones y la Proposición 9.3.7 vemos que $u \mid n$ y que $v \mid n$. De la segunda y de la tercera, usando la Proposición 9.3.8, que $\mathsf{mcd}(u, v) = 1$ y que $uv = \mathsf{mcm}(n, m)$. La proposición queda así probada. □

9.3.10. Antes de cambiar de tema, probemos un resultado bien conocido y útil de Adrien-Marie Legendre que determina las valuaciones de los factoriales. Se lo conoce habitualmente como ***fórmula de Legendre*** o ***de Polignac***, por Alphonse de Polignac.

Proposición. *Si n es un entero positivo y p un número primo, entonces*

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

En esta situación es fácil ver que hay un entero positivo l tal que $n < p^l$, así que para todo entero k tal que $k \geq l$ se tiene que $\lfloor n/p^k \rfloor = 0$. Esto nos dice que en la suma de esta proposición hay un número finito de sumandos no nulos: es por eso que tiene sentido.

Demostración. De acuerdo a la segunda parte de la Proposición 9.3.4, tenemos que

$$v_p(n!) = v_p(1 \cdot 2 \cdot \cdots n) = v_p(1) + v_p(2) + \cdots + v_p(n). \tag{11}$$

Sabemos que hay un entero positivo l tal que $n < p^l$, y esto implica inmediatamente que todos los n sumandos de esta suma son menores que l.

Para cada $k \in \mathbb{N}_0$ escribimos m_k a la cantidad de términos de la suma de (11) que son mayores o iguales a k. Para cada $k \in \mathbb{N}_0$, entonces, el número de términos de esa suma que son *iguales* a k es exactamente $m_k - m_{k+1}$ y, por lo tanto, tenemos que

$$\begin{aligned} v_p(n!) &= 0 \cdot (m_0 - m_1) + 1 \cdot (m_1 - m_2) + 2 \cdot (m_2 - m_2) + \cdots + l \cdot (m_l - m_{l+1}) \\ &= 0 \cdot m_0 + (1 - 0) \cdot m_1 + (2 - 1) \cdot m_2 + \cdots + (l - (l - 1)) \cdot m_l - l \cdot m_{l+1} \end{aligned}$$

y como $m_{l+1} = 0$ por la forma que elegimos a l, esto es

$$= m_1 + m_2 + \cdots + m_l. \tag{12}$$

Ahora bien, si $k \in \mathbb{N}_0$, entonces un elemento i de $\{1, \ldots, n\}$ tiene $v_p(i) \geq k$ si y solamente si i es divisible por p^k, y esto nos dice que m_k es el número de elementos del conjunto $\{1, \ldots, n\}$ divisibles por p^k, esto es, $\lfloor n/p^k \rfloor$. La igualdad (12) es, por lo tanto, la que afirma la proposición. □

9.3.11. Daremos una aplicación de la fórmula de Legendre. Para eso necesitamos la siguiente propiedad sencilla de la función «parte entera».

Ejercicio. Muestre que si x e y son dos números reales entonces

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

y que, en particular, $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

9.3.12. La fórmula de Legendre nos da una expresión para la valuación p-ádica de un número factorial y usándola podemos obtener información sobre los números binomiales, que se expresan de manera sencilla usando factoriales. El siguiente resultado se ocupa de los llamados ***números binomiales centrales***.

Corolario. *Sea p un número primo. Si n es un entero positivo y $N \coloneqq \binom{2n}{n}$, entonces*

$$p^{v_p(N)} \leq 2n.$$

Si escribimos $\log_p$ al logaritmo en base p, este corolario nos dice que $v_p(N) \leq \log_p 2n$.

Demostración. Sea n un entero positivo y sea $N \coloneqq \binom{2n}{n} = (2n)!/n!^2$. La multiplicatividad de la valuación p-ádica implica que

$$2v_p(n!) + v_p(N) = v_p(n!^2 N) = v_p((2n)!),$$

así que usando la fórmula de Legendre 9.3.10 vemos que

$$v_p(N) = v_p((2n)!) - 2v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \tag{13}$$

Si l es un entero tal que $l > \log_p 2n$, entonces $p^l > 2n$, así que $0 \leq n/p^l < 2n/p^l < 1$ y, por lo tanto, $\lfloor 2n/p^l \rfloor - 2\lfloor n/p^l \rfloor = 0$. Esto nos dice que en la suma de (13) todos los términos que tienen $k > \log_p 2n$ se anulan y que, por lo tanto,

$$v_p(N) = \sum_{k=1}^{\lfloor \log_p 2n \rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Por otro lado, el resultado del Ejercicio 9.3.11 nos dice cada uno de los $\lfloor \log_p 2n \rfloor$ términos de esta suma vale como mucho 1, así que $v_p(N) \leq \lfloor \log_p 2n \rfloor$ y, en definitiva,

$$p^{v_p(N)} \leq p^{\lfloor \log_p 2n \rfloor} \leq p^{\log_p 2n} = 2n,$$

como afirma el corolario. □

§9.4. Sumas de divisores

9.4.1. Si n es un entero positivo, escribimos $\sigma_0(n)$ al número de los divisores positivos de n. Por ejemplo, los divisores positivos de 300 son

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 25,\ 30,\ 50,\ 60,\ 75,\ 100,\ 150,\ 300$$

y, por lo tanto, $\sigma_0(300) = 18$.

Para calcular $\sigma_0(n)$, en principio, hay que determinar todos los divisores positivos de n, pero mostraremos más abajo en la Proposición 9.4.2 que es suficiente encontrar la factorización de n como producto de primos. Veamos antes un ejemplo.

La factorización de $n = 172\,772$ como producto de primos es $2^3 \cdot 3^2 \cdot 7^4$. Si d es un divisor positivo de n, entonces los primos que dividen a d necesariamente están entre 2, 3 y 7: esto significa que $d = 2^{a_1} \cdot 3^{a_2} \cdot 7^{a_3}$ para ciertos enteros no negativos a_1, a_2 y a_3. Más aún, como d divide a n, la Proposición 9.3.7 nos dice que

$$0 \le a_1 \le 3, \qquad 0 \le a_2 \le 2, \qquad 0 \le a_3 \le 4. \tag{14}$$

Por supuesto, el divisor d queda completamente determinado por estos tres exponentes y un momento de reflexión es suficiente para convencernos de que cualquier elección de tres enteros a_1, a_2 y a_3 que satisfagan las condiciones (14) produce un divisor de n. Como hay 4 formas de elegir a a_1, 3 de elegir a_2 y 5 de elegir a_3, y dos elecciones distintas de estos exponentes producen divisores de n distintos — esto es consecuencia del Teorema Fundamental de la Aritmética — podemos concluir que n tiene $4 \cdot 3 \cdot 5 = 60$ divisores. Probaremos el resultado general siguiendo exactamente esta misma idea.

9.4.2. Proposición. *Sea n un entero positivo, sean $p_1, \ldots, p_r$ los primos que dividen a n, de manera que se tiene $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$. La cantidad de divisores positivos de n es*

$$\sigma_0(n) = (v_{p_1}(n) + 1) \cdots (v_{p_r}(n) + 1).$$

Así, por ejemplo, como $300 = 2^2 \cdot 3 \cdot 5^2$, esta proposición nos dice que

$$\sigma_0(300) = (2+1)(1+1)(2+1) = 3 \cdot 2 \cdot 3 = 18.$$

Esto coincide con nuestro ejemplo de 9.4.1. De manera similar, como $172\,772 = 2^3 \cdot 3^2 \cdot 7^4$, la proposición nos dice que

$$\sigma_0(172\,772) = (3+1)(2+1)(4+1) = 60,$$

como dijimos.

Demostración. Consideremos para cada $i \in \{1, \ldots, r\}$ el conjunto

$$I_i \coloneqq \{t \in \mathbb{N}_0 : 0 \leq t \leq v_{p_i}(n)\}.$$

Si d es un divisor de n, entonces los primos que dividen a d son algunos de los primos $p_1, \ldots, p_r$ y, por lo tanto,

$$d = p_1^{v_{p_1}(d)} \cdots p_r^{v_{p_r}(d)}.$$

Más aún, como d divide a n la Proposición 9.3.7 nos dice que $0 \leq v_{p_i}(d) \leq v_{p_i}(n)$ para todo $i \in \{1, \ldots, r\}$, y entonces la r-upla $(v_{p_1}(d), \ldots, v_{p_r}(d))$ pertenece al producto cartesiano $I_1 \times \cdots \times I_r$.

Si escribimos $D(n)$ al conjunto de todos los divisores positivos de n, podemos definir entonces una función

$$\varphi : d \in D(n) \mapsto (v_{p_1}(d), \ldots, v_{p_r}(d)) \in I_1 \times \cdots \times I_r$$

Mostremos que esta función es una biyección.

- Sea $(a_1, \ldots, a_r)$ un elemento de $I_1 \times \cdots \times I_r$ y consideremos el entero $e \coloneqq p_1^{a_1} \cdots p_r^{a_r}$. Como los primos que dividen a e están entre $p_1, \ldots, p_r$ y para cada $i \in \{1, \ldots, r\}$ se tiene evidentemente que $v_{p_i}(e) = a_i \leq v_{p_i}(n)$, la Proposición 9.3.7 nos dice que $e \in D(n)$. Como $\varphi(d)$ es precisamente la r-upla $(a_1, \ldots, a_r)$ con la que empezamos, esto muestra que la función φ es sobreyectiva.
- Supongamos, por otro lado, que d y e son dos elementos de $D(n)$ tales que $\varphi(d) = \varphi(e)$. Esto significa precisamente que

  $$\textit{para cada } i \in \{1, \ldots, r\} \textit{ se tiene que } v_{p_i}(d) = v_{p_i}(e). \tag{15}$$

  Ahora bien, como d y e son divisores de n, los primos que los dividen están entre $p_1, \ldots, p_r$, así que la Proposición 9.3.5 nos dice que $d = p_1^{v_{p_1}(d)} \cdots p_r^{v_{p_r}(d)}$ y $e = p_1^{v_{p_1}(e)} \cdots p_r^{v_{p_r}(e)}$. En vista de (15) es claro que los miembros derechos de estas dos igualdades coinciden, así que $d = e$. Vemos así que la función φ es inyectiva.

Como φ es biyectiva, su dominio y su codominio tienen el mismo cardinal, así que

$$|D(n)| = |I_1 \times \cdots \times I_r| = |I_1| \cdots |I_r| = (v_{p_1}(n) + 1) \cdots (v_{p_r}(n) + 1),$$

y esto es lo que afirma la proposición. □

9.4.3. Decimos que un número $n \in \mathbb{N}$ es ***altamente compuesto*** si tiene más divisores que cualquier otro entero positivo menor que él. Usando la Proposición 9.4.2, es fácil ver (¡usando una

computadora!) que los primeros números altamente compuestos son

$$1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, 1260, 1680, 2520, 5040, \ldots$$

Esta definición fue dada por Srinivasa Ramanujan en 1915 pero es probable que ya los griegos hayan considerado estos números. Platón, por ejemplo, explica en *Las Leyes* — el último y el más largo de sus diálogos, en el que expone sus ideas sobre como deben organizarse las sociedades — que el número ideal de ciudadanos[3] de una ciudad es 5040, precisamente porque este número tiene muchos divisores.

9.4.4. Además de la función σ_0 que definimos arriba, se estudian otras funciones de tipo similar. Si $k \in \mathbb{R}$, para cada $n \in \mathbb{N}$ escribimos $\sigma_k(n)$ a la suma de las potencias k-ésimas de los divisores positivos de n. Por ejemplo,

$$\sigma_3(24) = 1^3 + 2^3 + 3^3 + 4^3 + 6^3 + 8^3 + 12^3 + 24^3 = 16\,380.$$

Observemos que $d^0 = 1$ para todo entero positivo d, y entonces $\sigma_0(n)$ es simplemente la suma de muchos unos, uno por cada divisor de n y esto es lo mismo que el número de divisores que n tiene: vemos así que esta definición para σ_0 coincide con la que dimos en 9.4.1. Nos proponemos obtener un resultado similar al de la Proposición 9.4.2 para σ_k. Como el argumento que usamos para probar esa proposición es bastante flexible, haremos antes algunas consideraciones generales que nos servirán también más adelante.

9.4.5. Decimos que una función $f : \mathbb{N} \to A$ con valores en un subconjunto A de $\mathbb{R}$ es ***multiplicativa*** si cada vez que n y m son enteros positivos coprimos se tiene que $f(nm) = f(n)f(m)$. Un ejemplo sencillo de esto es el siguiente: la función identidad $I_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ es multiplicativa. Obtenemos otro ejemplo, un poco más interesante, fijando un entero a y considerando la función $f_a : n \in \mathbb{N} \mapsto \mathsf{mcd}(n, a) \in \mathbb{N}_0$: que esta función es multiplicativa es precisamente lo que afirma la Proposición 6.5.5(*iv*).

9.4.6. Que una función sea multiplicativa nos da una forma de evaluarla en un producto de dos números coprimos. El siguiente resultado extiende esa propiedad a productos de un número arbitrario de factores.

Lema. *Sea $f : \mathbb{N} \to \mathbb{R}$ una función multiplicativa. Si $r \in \mathbb{N}$ y $n_1, \ldots, n_r$ son enteros positivos coprimos dos a dos, entonces $f(n_1 \cdots n_r) = f(n_1) \cdots f(n_r)$.*

Demostración. Procedemos por inducción con respecto a r. Si r es 1, entonces no hay nada que probar, y si es 2, lo que se afirma es cierto precisamente por la definición de multiplicatividad. Supongamos entonces que $r \geq 3$ y sean $n_1, \ldots, n_r$ enteros positivos coprimos dos a dos. De acuerdo

[3] Para Platón no todos los habitantes de una ciudad son ciudadanos.

al Corolario 6.5.6, tenemos que

$$\mathsf{mcd}(n_1 \cdots n_{r-1}, n_r) = \mathsf{mcd}(n_1, n_r) \cdots \mathsf{mcd}(n_{r-1}, n_r) = 1,$$

porque n_r es coprimo con cada uno de los números $n_1, \ldots, n_{r-1}$. Como la función f es multiplicativa, tenemos entonces que

$$f(n_1 \cdots n_r) = f(n_1 \cdots n_{r-1}) f(n_r).$$

Ahora bien, la hipótesis inductiva nos dice que $f(n_1 \cdots n_{r-1}) = f(n_1) \cdots f(n_{r-1})$ y si usamos esto en la igualdad que acabamos de obtener vemos que

$$f(n_1 \cdots n_r) = f(n_1) \cdots f(n_r),$$

y esto completa la inducción. □

9.4.7. El interés de que una función $f : \mathbb{N} \to \mathbb{R}$ sea multiplicativa reduce en que podemos calcular su valor $f(n)$ en un número $n \in \mathbb{N}$ usando la factorización de n como producto de potencias de números primos distintos dos a dos:

Proposición. *Sea $f : \mathbb{N} \to \mathbb{R}$ una función multiplicativa. Si $n \in \mathbb{N}$ y $p_1, \ldots, p_r$ son los primos que dividen a n, de manera que $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$, entonces*

$$f(n) = f\left(p_1^{v_{p_1}(n)}\right) \cdots f\left(p_r^{v_{p_r}(n)}\right).$$

Demostración. Sea $n \in \mathbb{N}$ y sean $p_1, \ldots, p_r$ los primos que dividen a n. Como los números $p_1, \ldots, p_r$ son coprimos dos a dos, la Proposición 6.5.9 nos dice que también los números $p_1^{v_{p_1}(n)}, \ldots, p_r^{v_{p_r}(n)}$ son coprimos dos a dos y, por lo tanto, gracias al Lema 9.4.6 tenemos que

$$f(n) = f(p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}) = f\left(p_1^{v_{p_1}(n)}\right) \cdots f\left(p_r^{v_{p_r}(n)}\right),$$

como afirma el enunciado. □

9.4.8. Vamos a necesitar un par de veces un resultado sencillo sobre divisores, que probamos ahora. Para cada entero positivo n escribamos, como antes, $D(n)$ al conjunto de todos los divisores positivos de n.

Supongamos que n y m son dos enteros y que $\mathsf{mcd}(n, m) = 1$. Si d y e son un divisor positivo de n y uno de m, respectivamente, entonces d y e son divisores coprimos de nm y, por lo tanto, su producto de es un divisor positivo de nm. Esto nos dice que hay una función

$$P : (d, e) \in D(n) \times D(m) \mapsto de \in D(nm).$$

Lema. *Si n y m son dos enteros coprimos, entonces la función*

$$P : (d, e) \in D(n) \times D(m) \mapsto de \in D(nm)$$

es una biyección y su función inversa es

$$Q : u \in D(nm) \mapsto (\mathsf{mcd}(u, n), \mathsf{mcd}(u, m)) \in D(n) \times D(m).$$

Demostración. Sean n y m dos enteros coprimos. Si $u \in D(nm)$, entonces $\mathsf{mcd}(u, n) \in D(n)$ y $\mathsf{mcd}(u, m) \in D(m)$, así que hay una función

$$Q : u \in D(nm) \mapsto (\mathsf{mcd}(n, u), \mathsf{mcd}(m, u)) \in D(n) \times D(m).$$

Mostremos que esta función Q es inversa de P.

- Si u es un elemento cualquiera de $D(nm)$, entonces

  $$P(Q(u)) = P(\mathsf{mcd}(n, u), \mathsf{mcd}(m, u)) = \mathsf{mcd}(n, u)\,\mathsf{mcd}(m, u)$$

  y, de acuerdo a la Proposición 6.5.5(*iv*) y gracias a que n y m son coprimos, esto es

  $$= \mathsf{mcd}(nm, u) = u,$$

  ya que u es un divisor positivo de nm. Esto significa que $P \circ Q$ es la función identidad de $D(nm)$.

- Sea, por otro lado, (d, e) un elemento de $D(n) \times D(m)$. Es

  $$Q(P(d, e)) = Q(de) = (\mathsf{mcd}(n, de), \mathsf{mcd}(m, de)). \tag{16}$$

  Como e divide a m, el Corolario 6.5.2 nos dice que $\mathsf{mcd}(n, e) \mid \mathsf{mcd}(n, m) = 1$, así que n y e son coprimos: usando ahora la Proposición 6.5.5(*iii*), vemos que

  $$\mathsf{mcd}(n, de) = \mathsf{mcd}(n, d) = d,$$

  ya que d divide a n. De manera similar, vemos que $\mathsf{mcd}(m, de) = e$ y, volviendo a (16), que

  $$Q(P(d, e)) = (d, e).$$

  Esto significa que $Q \circ P$ es la función identidad de $D(n) \times D(m)$.

Como P y Q son funciones inversas, la función P es biyectiva. □

9.4.9. Volvamos ahora a nuestro problema de calcular las funciones σ_k.

Proposición. *Sea $k \in \mathbb{R}$. La función $\sigma_k : \mathbb{N} \to \mathbb{R}$ es multiplicativa. Si k no es nulo, $n \in \mathbb{N}$ y $p_1, \ldots, p_r$ son los primos que dividen a n, entonces*

$$\sigma_k(n) = \frac{p_1^{k(v_{p_1}(n)+1)} - 1}{p_1^k - 1} \cdot \ldots \cdot \frac{p_r^{k(v_{p_r}(n)+1)} - 1}{p_r^k - 1}.$$

Observemos que es necesario excluir el caso en que $k = 0$ en la segunda afirmación de esta proposición: en ese caso los denominadores que aparecen en la fórmula se anulan, así que la fórmula no tiene sentido.

Demostración. Probemos primero que la función σ_k es multiplicativa. Sea n y m dos enteros positivos coprimos y recordemos las funciones P y Q del Lema 9.4.8. Tenemos que

$$\sigma_k(n) \cdot \sigma_k(m) = \sum_{d \in D(n)} d^k \cdot \sum_{e \in D(m)} e^k = \sum_{(d,e) \in D(n) \times D(m)} d^k e^k = \sum_{(d,e) \in D(n) \times D(m)} P(d,e)^k$$

y, usando el hecho de que P y Q son funciones inversas, podemos ver que esto es

$$= \sum_{u \in D(nm)} P(Q(u))^k = \sum_{u \in D(nm)} u^k = \sigma_k(nm).$$

Concluimos así que σ_k es una función multiplicativa, como queríamos.

Ocupemos ahora de la segunda afirmación de la proposición. Supongamos que $k \neq 0$, sea $n \in \mathbb{N}$ y sean $p_1, \ldots, p_r$ los primos que dividen a n. En vista de la Proposición 9.4.7, tenemos que

$$\sigma_k(n) = \sigma_k\left(p_1^{v_{p_1}(n)}\right) \cdots \sigma_k\left(p_r^{v_{p_r}(n)}\right). \tag{17}$$

Ahora bien, si p es un número primo y $a \in \mathbb{N}_0$, entonces de acuerdo a la Proposición 9.3.7 los divisores positivos de p^a son los $a+1$ enteros

$$1, p, p^2, \ldots, p^a,$$

así que la suma de las potencias k-ésimas de estos divisores es

$$\sigma_k(p^a) = 1^k + p^{2k} + \cdots + p^{ak}.$$

Esta suma es una suma geométrica de razón p^k, así que, como vimos en 4.2.1 en el Capítulo 4, es igual a

$$\frac{p^{k(a+1)} - 1}{p^k - 1}.$$

Si usamos esta observación con cada uno de los factores que aparecen a la derecha de la igualdad (17), vemos que

$$\sigma_k(n) = \frac{p_1^{k(v_{p_1}(n)+1)} - 1}{p_1^k - 1} \cdot \ldots \cdot \frac{p_r^{k(v_{p_r}(n)+1)} - 1}{p_r^k - 1}.$$

Esto completa la prueba de la proposición. □

9.4.10. Usando la Proposición 9.4.9 podemos calcular fácilmente las funciones σ_k. Por ejemplo, como $317\,765\,539 = 7^2 \cdot 13 \cdot 23^3 \cdot 41$, tenemos que

$$\begin{aligned}\sigma_3(317\,765\,539) &= \frac{7^{3(2+1)}-1}{7^3-1} \cdot \frac{13^{3(1+1)}-1}{13^3-1} \cdot \frac{23^{3(3+1)}-1}{23^3-1} \cdot \frac{41^{3(1+1)}-1}{41^3-1} \\ &= 117\,993 \cdot 2\,198 \cdot 1\,801\,300\,709\,520 \cdot 68\,922 \\ &= 32\,197\,935\,268\,666\,697\,933\,108\,160.\end{aligned}$$

§9.5. Números perfectos

9.5.1. Un número n es ***perfecto*** si $\sigma_1(n) = 2n$. Por ejemplo, 6 y 28 son números perfectos, ya que

$$\sigma_1(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$$

y

$$\sigma_1(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$$

Como n siempre es un divisor de n, la condición de que n sea perfecto es equivalente a que la suma de los divisores *propios* de n sea igual a n.

Esta definición aparece en el Libro VII de los *Elementos* de Euclides. Desde la época de Euclides hubo siempre una peculiar fascinación por estos números y un gran empeño en encontrarlos en los contextos más diversos. Así, por ejemplo, Philo de Alejandría explicaba, hacia el año 100 d.C., que el mundo había sido creado en 6 días y que la luna tarda 28 días en dar una revolución alrededor de la tierra precisamente porque 6 y 28 son números perfectos.

Los primeros diez números perfectos son

$$\begin{aligned}&6,\quad 28,\quad 496,\quad 8\,128,\quad 33\,550\,336,\quad 8\,589\,869\,056,\quad 137\,438\,691\,328,\\ &2\,305\,843\,008\,139\,952\,128,\quad 2\,658\,455\,991\,569\,831\,744\,654\,692\,615\,953\,842\,176,\\ &191\,561\,942\,608\,236\,107\,294\,793\,378\,084\,303\,638\,130\,997\,321\,548\,169\,216\end{aligned}$$

Sólo los primeros cuatro eran conocidos por los griegos clásicos: recién en el año 100 d.C. el matemático Nicómaco de Gerasa, que escribió un célebre tratado de aritmética, se dio cuenta que 8 128 es perfecto. Los siguientes tres fueron encontrados más de mil años después por el matemático Ismail ibn Fallūs, quien también listó varios más, que ahora sabemos que no son perfectos.

El 29 de septiembre de 2023 se conocían 51 números perfectos[4]. El más grande de ellos es el número

$$2^{82\,589\,932} \cdot (2^{82\,589\,933} - 1),$$

que tiene 49 724 095 dígitos. No sabemos si hay infinitos números perfectos o no, aunque se cree que sí los hay: esta afirmación es conocida como la conjetura de Lenstra, Pomerance y Wagstaff. Por otro lado, todos los números perfectos que conocemos son pares y no sabemos si existe alguno impar. Decidir si existen o no números perfectos impares es uno de los problemas más viejos de la aritmética — Euler afirmó que se trata de «un problema de la mayor dificultad» y viniendo de él esto es muy significativo!

9.5.2. La siguiente observación, que nos provee de una forma de construir números perfectos, aparece ya en el libro de Euclides:

Proposición. *Si $n \in \mathbb{N}$ es tal que $2^n - 1$ es primo, entonces el número $2^{n-1}(2^n - 1)$ es perfecto.*

La demostración que da Euclides de esto es bastante laboriosa. Nosotros podemos hacer otra mucho más sencilla usando los resultados que obtuvimos en esta sección.

Demostración. Si $2^n - 1$ es primo y ponemos

$$N = 2^{n-1}(2^n - 1),$$

entonces lo que aparece a la derecha de esta igualdad es la factorización de N como producto de primos. La Proposición 9.4.9 nos dice, en consecuencia, que

$$\sigma_1(N) = \frac{2^n - 1}{2 - 1} \cdot \frac{(2^n - 1)^2 - 1}{(2^n - 1) - 1} = (2^n - 1)2^n = 2N$$

Vemos así que N es perfecto, como queríamos. □

9.5.3. Observando que $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ y $127 = 2^7 - 1$ son primos, concluimos gracias a esta proposición que los números

$$2^1(2^2 - 1) = 6, \qquad 2^2(2^3 - 1) = 28, \qquad 2^4(2^5 - 1) = 496, \qquad 2^6(2^7 - 1) = 8\,128$$

son perfectos. Estos son los primeros cuatro números perfectos y los únicos que los antiguos griegos conocían. Los siguientes números perfectos provistos por esa proposición son

$$2^{12}(2^{13} - 1) = 33\,509\,381, \qquad 2^{16}(2^{17} - 1) = 8\,589\,869\,056$$

[4] En una versión anterior de este libro decíamos que el 10 de enero de 2018 se conocían 50 números perfectos: el 7 de diciembre de ese año se encontró uno más. Hasta ese momento el más grande conocido era $2^{77\,232\,916} \cdot (2^{77\,232\,917} - 1)$ que tiene 46 498 850 dígitos.

y

$$2^{18}(2^{19}-1) = 137\,438\,691\,328,$$

ya que $8\,191 = 2^{13}-1$, $131\,071 = 2^{17}-1$ y $524\,287 = 2^{19}-1$ son primos. Estos son los tres números perfectos encontrados por ibn Fallūs aproximadamente en el año 1200. El octavo es

$$2^{30}(2^{31}-1) = 2\,305\,843\,008\,139\,952\,128,$$

pero este no fue encontrado hasta el año 1772, cuando Euler pudo determinar que

$$2\,147\,483\,647 = 2^{31}-1$$

es primo.

9.5.4. La Proposición 9.5.2 nos da una manera de construir números perfectos, pero para usarla necesitamos números primos de la forma $2^n - 1$. Estos primos se llaman ***primos de Mersenne***, por Marin Mersenne.

Una observación sencilla que podemos hacer es que si un número de la forma $2^n - 1$ es primo, entonces n mismo tiene que ser primo. Esto es consecuencia de la afirmación del Ejercicio 6.6.6(b): si n no es primo y m es un divisor de n tal que $1 < m < n$, entonces $2^m - 1$ es un divisor propio de $2^n - 1$ distinto de 1. Gracias a esto, para encontrar primos de Mersenne tenemos que decidir, para cada primo p, si $2^p - 1$ es o no primo. El problema con esto es que cuando p crece el valor de $2^p - 1$ crece mucho más rápido y decidir si es primo es muy laborioso. Por lo pronto, no es cierto que sea siempre primo: el ejemplo más chico de esto es

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

De los números de la forma $2^n - 1$ el más grande que es compuesto y que sabemos factorizar es $2^{1\,193} - 1$ (que tiene 360 dígitos). Por otro lado, sabemos que el número $2^{1\,277} - 1$ (que tiene 385 dígitos) es compuesto pero no conocemos ninguno de sus divisores propios — esto es un poco sorprendente: se debe a que conocemos algoritmos que nos permiten decidir si uno de estos números es compuesto o no pero que no nos dan ninguno de sus factores en caso de que lo sea.

Desde 1996, un esfuerzo colaborativo y distribuido llamado *Great Internet Mersenne Prime Search* (GIMPS) busca primos de Mersenne y desde su fundación hasta septiembre de 2023 encontró 18 primos, el más grandes de los cuales es

$$2^{82\,589\,933} - 1,$$

que es, de hecho, el número primo más grande que conocemos — tiene 24 862 048 dígitos decimales.

9.5.5. Los números perfectos que nos permite construir la Proposición 9.5.2 son todos pares. Euler probó en 1899 que de esa forma obtenemos, de hecho, *todos* los números perfectos pares.

Figura 9.4. En el episodio *The Duh-Vinci Code*, el quinto de la sexta temporada de *Futurama*, el equipo de Planet Express viaja a Roma y encuentra la inscripción

$$\mathrm{II}^{\mathrm{XI}} - (\mathrm{XXIII} * \mathrm{LXXXIX})$$

grabada en una tumba.

Proposición. *Si n es un número perfecto par, hay un número primo p tal que $n = 2^{p-1}(2^p - 1)$.*

Demostración. Sea n un numero perfecto par y sea $k = v_2(n)$, que es un número positivo. Sabemos que hay un entero impar m tal que $n = 2^k m$. Como n es perfecto y la función σ_1 es multiplicativa, tenemos que

$$2^{k+1}m = 2n = \sigma_1(n) = \sigma_1(2^k m) = \sigma_1(2^k)\sigma_1(m) = (2^{k+1} - 1)\sigma_1(m).$$

Como $\mathsf{mcd}(2^{k+1}, 2^{k+1} - 1) = 1$, de esto se deduce que $2^{k+1} - 1$ divide a m y que, por lo tanto, el número $r = m/(2^{k+1} - 1)$ es entero y divide a m; observemos que como $k \geq 1$, se tiene que $r < m$.

Si dividimos a ambos lados de la igualdad $2^{k+1}m = (2^{k+1} - 1)\sigma_1(m)$ por $2^{k+1} - 1$, vemos que

$$2^{k+1}r = \sigma_1(m) = m + r + S$$

con S la suma de todos los divisores positivos de m distintos de m y de r, y esto es

$$= (2^{k+1} - 1)r + r + S = 2^{k+1}r + S.$$

Así, es $2^{k+1}r = 2^{k+1}r + S$: la única forma en que esto puede ocurrir es que sea $S = 0$. En otras palabras, los únicos divisores positivos de m son m mismo y r. Como $m \neq r$, m tiene exactamente dos divisores positivos, es primo y el menor de esos divisores es 1: esto nos dice que $1 = m/2^{k+1} - 1$

y, por lo tanto, que $m = 2^{k+1} - 1$. Como observamos arriba, que $2^{k+1} - 1$ sea primo implica que $p = k + 1$ es primo. Como nuestro número perfecto de partida es entonces $n = 2^k m = 2^{p-1}(2^p - 1)$, esto prueba la proposición. □

§9.6. Ejercicios

Números perfectos multiplicativos

9.6.1. Ejercicio. Muestre que un número a es igual al producto de sus divisores propios si y solamente si es de la forma p^3 para algún primo p, o de la forma pq para dos primos distintos p y q.

Esto nos dice que el análogo «multiplicativo» de la definición de números perfectos no es muy interesante.

La función de Möbius

9.6.2. Si n es un entero positivo y $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, con $r \in \mathbb{N}_0$, $p_1, p_2, \ldots, p_n$ primos distintos dos a dos y $a_1, \ldots, a_r$ enteros positivos, es su factorización usual, entonces escribimos

$$\mu(n) \coloneqq \begin{cases} 0 & \text{si alguno de los números } a_1, a_2, \ldots, a_r \text{ es mayor que 1;} \\ (-1)^r & \text{en caso contrario.} \end{cases}$$

Obtenemos de esta forma una función $\mu : \mathbb{N} \to \mathbb{Z}$ llamada la ***función de Möbius***, por August Ferdinand Möbius que la estudió en 1832.

9.6.3. Ejercicio.

(*a*) Muestre que $\mu(n) = 0$ si y solamente si n es divisible por un cuadrado mayor que 1.

(*b*) Prueba que la función μ es multiplicativa, esto es, que si n y m son dos enteros positivos coprimos entonces $\mu(nm) = \mu(n)\mu(m)$.

(*c*) Muestre que para todo entero positivo n vale que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } n > 1. \end{cases}$$

Notemos que esta suma tiene un término por cada divisor *positivo* de n.

(*d*) Sea $f : \mathbb{N} \to \mathbb{R}$ una función cualquiera. Si $g : \mathbb{N} \to \mathbb{R}$ es la función que en cada entero

positivo n toma el valor

$$g(n) \coloneqq \sum_{d|n} f(d),$$

entonces para todo entero positivo n vale que

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Esta es la llamada ***fórmula de inversión de Möbius***.

Capítulo 10

Potencias

§10.1. El pequeño teorema de Fermat

10.1.1. Nuestro primer objetivo en este capítulo es probar el llamado *pequeño teorema de Fermat*. Se conocen varias formas de llegar a ese resultado — aquí elegiremos una que es puramente algebraica. Empezamos con una observación puramente aritmética.

Proposición. *Sea p un número primo. Si i es un entero tal que $0 < i < p$, entonces p divide a $\binom{p}{i}$.*

Demostración. Sea i un entero tal que $0 < i < p$. Claramente p no divide a $i!$ ni a $(p-i)!$, ya que no divide a ninguno de los factores de esos dos factoriales y es primo. Por otro lado, es evidente que divide a $p!$. De esto se sigue, por supuesto, que divide al cociente

$$\frac{p!}{i!(p-i)!} = \binom{p}{i},$$

y esto es lo que afirma la proposición. □

10.1.2. Una consecuencia inmediata de esta proposición y de la fórmula de Newton es que esta última se simplifica considerablemente si trabajamos módulo un número primo:

Corolario. *Sea p un número primo. Si a y b son dos enteros, entonces*

$$(a+b)^p \equiv a^p + b^p \mod p.$$

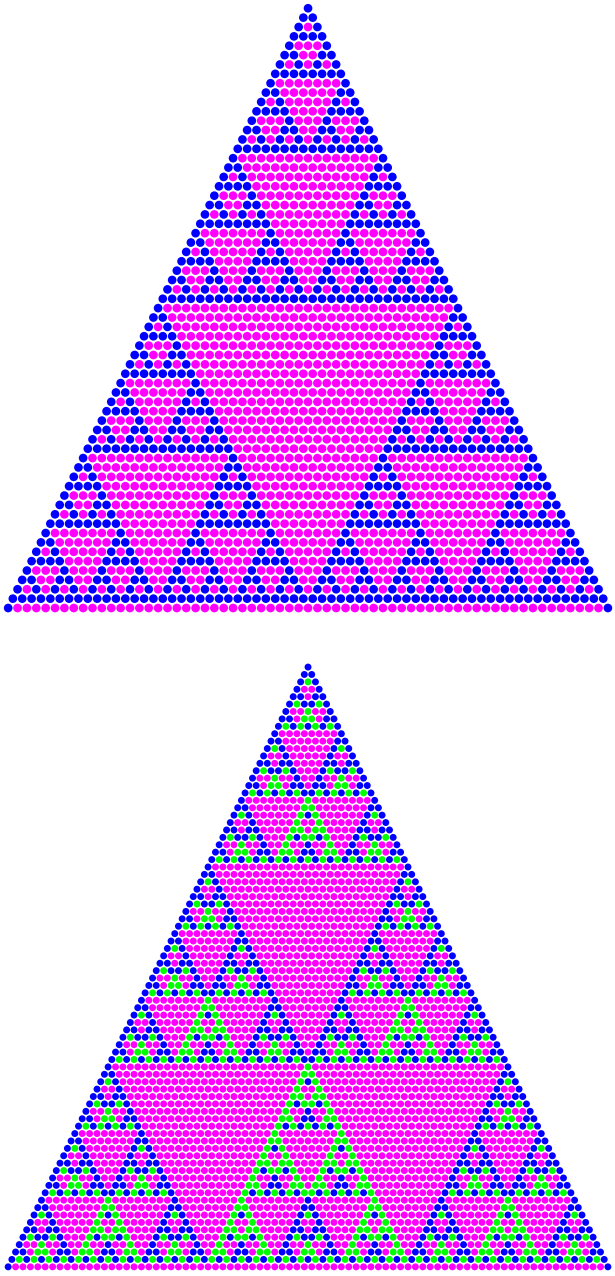


Figura 10.1. El triángulo de Pascal módulo 2 y módulo 3. Se trata de las primeras 64 y 81 filas del triángulo, respectivamente, y en los dos casos el magenta representa los números que tienen resto 0.

Demostración. Sean a y b dos enteros. La fórmula de Newton para las potencias de un binomio nos dice que

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Ahora bien, de acuerdo a la Proposición 10.1.1 el número p divide a los sumandos de esta suma que corresponden a valores del índice i tales que $0 < i < p$, y entonces la suma completa es congruente módulo p a la suma de los dos términos restantes:

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Esto es precisamente lo que afirma el corolario. □

10.1.3. Gracias a esta simplificación de la fórmula de Newton podemos probar lo que es casi el teorema que estamos buscando.

Proposición. *Sea p un número primo. Para todo entero a se tiene que $a^p \equiv a \mod p$.*

Demostración. Para cada $a \in \mathbb{Z}$ sea $P(a)$ la afirmación «$a^p \equiv a \mod p$». Mostremos primero que $P(a)$ vale para todo $a \in \mathbb{N}_0$ haciendo inducción con respecto a a. Notemos que $P(0)$ vale por razones triviales. Supongamos entonces que $a \in \mathbb{N}_0$ y que la afirmación $P(a)$ vale. De acuerdo al Corolario 10.1.2, tenemos que

$$(a+1)^p \equiv a^p + 1 \mod p$$

y la hipótesis inductiva nos dice que $a^p \equiv a \mod p$ así que, juntando todo, vemos que

$$(a+1)^p \equiv a + 1 \mod p,$$

es decir, que $P(a+1)$ vale. Esto completa la inducción.

Nos queda mostrar que $P(a)$ vale también cuando a es negativo. Ahora bien, si a es negativo, entonces $a - ap$ es positivo y congruente con a módulo p, así que

$$a^p \equiv (a-ap)^p \equiv a - ap \equiv a \mod p,$$

usando, en la segunda congruencia, que ya sabemos que $P(a-ap)$ vale. Esto termina la prueba de la proposición. □

10.1.4. La siguiente proposición es generalmente conocida como el *Pequeño Teorema de Fermat*, por Pierre de Fermat, quien lo enunció por primera vez en una carta a un amigo. El primero

en publicar una prueba, sin embargo, fue Euler en 1736. Gauss lo describe en sus *Disquisitiones* — donde lo demuestra de varias maneras— como un resultado «remarcable tanto por su elegancia como por su utilidad».

Proposición. *Sea p un número primo. Si a es un entero coprimo con p, entonces*

$$a^{p-1} \equiv 1 \mod p.$$

Demostración. De acuerdo a la Proposición 10.1.3 tenemos que $a^p \equiv a \mod p$, es decir, que p divide a $a^p - a = a(a^{p-1} - a)$. Como p no divide a a y sí a este producto, tiene que dividir a $a^{p-1} - 1$: esto significa, precisamente, que $a^{p-1} \equiv 1 \mod p$. □

10.1.5. Una aplicación muy sencilla del Teorema de Fermat 10.1.4 es al cálculo de potencias módulo un número primo: tenemos un número primo p, un entero a coprimo con p y un entero no negativo n, y queremos determinar a^n módulo p. Si llamamos q y r al cociente y al resto de la división de n por $p-1$, de manera que $n = q(p-1) + r$, tenemos que

$$a^n = (a^{p-1})^q a^r \equiv a^r \mod p,$$

ya que, de acuerdo al teorema de Fermat 10.1.4, es $a^{p-1} \equiv 1 \mod p$. Por ejemplo, 11 es primo y coprimo con 2, y es $100 = 9(11-1) + 4$, así que

$$2^{104} = (2^{11-1})^9 2^4 \equiv 2^4 = 16 \equiv 5 \mod 11,$$

De manera similar, el número 541 es primo y coprimo con 123, así que el teorema de Fermat nos dice que $132^{541-1} \equiv 1 \mod 541$ y, por lo tanto, que

$$132^{999\,548} \equiv 132^{1\,851\cdot(541-1)+8} \equiv 132^8 \equiv ((132)^2)^2)^2 \equiv (112^2)^2 \equiv 101^2 \equiv 463 \mod 541.$$

10.1.6. El teorema de Fermat solo se aplica cuando estamos trabajando módulo un número primo, pero junto con el teorema chino del resto podemos extender su aplicabilidad.

Por ejemplo, supongamos que queremos calcular el resto de dividir a 2^{123} por 15. Se trata del único entero r tal que $2^{123} \equiv r \mod 15$ y $0 \leq r < 15$, como sabemos, y esa congruencia implica que también es $2^{123} \equiv r \mod 3$ y $2^{123} \equiv r \mod 5$. El teorema de Fermat nos permite calcular que

$$2^{123} \equiv (2^{3-1})^{61} \cdot 2 \equiv 2 \mod 3, \qquad 2^{123} \equiv (2^{5-1})^{30} \cdot 2^3 \equiv 8 \equiv 3 \mod 5,$$

y entonces el número r es una solución del sistema de congruencias

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5. \end{cases}$$

Claramente 8 es una solución de este sistema, y esto implica que el conjunto de todas las soluciones es la clase de congruencia de 8 módulo 15. La única de esas soluciones que pertenece al conjunto $\{0, \ldots, 14\}$ es 8, y podemos concluir entonces que el resto que buscamos es $r = 8$.

De manera similar, podemos calcular el resto r de dividir a 5^{99} por $1178 = 2 \cdot 19 \cdot 31$. En efecto, es $r \equiv 5^{99} \mod 2 \cdot 19 \cdot 31$, así que

$$\begin{aligned} r &\equiv 5^{99} \equiv 1 \mod 2, \\ r &\equiv 5^{99} \equiv 5^{5\cdot(19-1)+9} \equiv 5^9 \equiv 1 \mod 19, \\ r &\equiv 5^{99} \equiv 5^{3\cdot(31-1)+9} \equiv 5^9 \equiv 1 \mod 31, \end{aligned}$$

y esto nos dice que r es una solución del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod 2, \\ x \equiv 1 \mod 19, \\ x \equiv 1 \mod 31. \end{cases}$$

Ahora bien, es evidente que 1 es una solución de este sistema de congruencias, y sabemos que todas sus soluciones son entonces congruentes a 1 módulo $2 \cdot 19 \cdot 31$. La única de esas soluciones que está en el conjunto $\{0, \ldots, 2 \cdot 19 \cdot 31 - 1\}$ es 1 y, por lo tanto, ese es el resto que buscamos.

10.1.7. Debería ser claro para el lector en este punto que esta idea funciona siempre que queremos calcular el resto de dividir una potencia por un número que es producto de primos distintos dos a dos. Usando la misma idea, por otro lado, podemos probar la siguiente generalización del teorema de Fermat:

Proposición. *Sean p y q dos primos distintos. Si a es un entero coprimo con pq, entonces*

$$a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Demostración. Sea a un entero coprimo con pq. Como a es a la vez coprimo con p y con q, el teorema de Fermat nos dice que $a^{p-1} \equiv 1 \mod p$ y que $a^{q-1} \equiv 1 \mod q$, así que tenemos que $a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod p$ y $a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1 \mod q$. Esto nos dice que el entero $a^{(p-1)(q-1)}$ es una solución del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod p, \\ x \equiv 1 \mod q. \end{cases}$$

Es claro que 1 es una solución de este sistema y, como p y q son primos distintos, sabemos que entonces todas las soluciones del sistema son congruentes entre sí módulo pq: podemos concluir entonces que $a^{(p-1)(q-1)} \equiv 1 \mod pq$, como afirma la proposición. □

10.1.8. Por supuesto, podemos generalizar esto a la situación en que tenemos más que dos primos:

Ejercicio. Sea r un entero positivo y sean $p_1, p_2, \dots, p_r$ números primos distintos dos a dos. Muestre que si a es un entero coprimo con el producto $p_1 p_2 \cdots p_r$, entonces

$$a^{(p_1-1)(p_2-1)\cdots(p_r-1)} \equiv 1 \mod p_1 \cdots p_r.$$

10.1.9. Veamos qué podemos decir cuando trabajamos módulo un número que no es producto de primos distintos dos a dos. Empecemos considerando un ejemplo.

Calculemos el resto de dividir a 7^{29} por 5^2, que es el único entero r tal que

$$r \equiv 7^{29} \mod 5^2, \qquad 0 \le r < 5^2. \tag{1}$$

Como vale esa congruencia, también es $r \equiv 7^{29} \mod 5$ y el teorema de Fermat nos permite calcular que $7^{29} \equiv 7^{7(5-1)+1} \equiv 7 \equiv 2 \mod 5$, así que es $r = 5s + 2$ para algún entero s. Volviendo a la congruencia de (1) vemos que $5s + 2 \equiv 7^{29} \mod 5^2$, así que $5s \equiv 7^{29} - 2 \mod 5^2$.

§10.2. La función de Euler

10.2.1. Si $n \in \mathbb{N}$, escribimos $\varphi(n)$ a la cantidad de elementos del conjunto $\{1, \dots, n\}$ que son coprimos con n, es decir, el cardinal del conjunto

$$C(n) := \{i \in \mathbb{N} : 1 \le i \le n, \mathsf{mcd}(i, n) = 1\}.$$

Esa cantidad es positiva, ya que $1 \in C(n)$. De esta manera obtenemos una función $\varphi : \mathbb{N} \to \mathbb{N}$, a la que llamamos ***función de Euler***. Por ejemplo, los enteros positivos que no superan a 20 son

$$\boxed{1}\ 2\ \boxed{3}\ 4\ 5\ 6\ \boxed{7}\ 8\ \boxed{9}\ 10\ \boxed{11}\ 12\ \boxed{13}\ 14\ 15\ 16\ \boxed{17}\ 18\ \boxed{19}\ 20$$

y los que son coprimos con 20 están marcados con un cuadrado: vemos que $\varphi(20) = 8$. Por otro lado, si p es un número primo entonces todo elemento de $\{1, \dots, p\}$, salvo p mismo, es coprimo con p y, por lo tanto, $\varphi(p) = p - 1$.

10.2.2. Veremos más abajo, en la Proposición 10.2.3, cómo calcular $\varphi(n)$ a partir de la factorización de n como producto de primos. Para llegar a eso necesitamos el siguiente resultado preliminar:

Proposición. *La función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ es* multiplicativa*: si n y m son dos enteros coprimos, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.*

Sin imponer la condición de coprimalidad entre n y m no podemos en general llegar a la conclusión de la proposición: por ejemplo, $\varphi(2 \cdot 10) = \varphi(20) = 8$, como vimos arriba, pero $\varphi(2)\varphi(10) = 1 \cdot 4 = 4$.

Demostración. Sean n y m dos enteros coprimos. Probaremos la afirmación de la proposición en varios pasos.

Primer paso. Empezamos construyendo dos funciones

$$f : C(n) \times C(m) \to C(nm), \qquad g : C(nm) \to C(n) \times C(m).$$

Sabemos que existen dos enteros x e y tales que $xn + ym = 1$.

- Sean $a \in C(n)$ y $b \in C(m)$, de manera que $1 \leq a < n$, $1 \leq b < m$, $\mathsf{mcd}(a, n) = 1$ y $\mathsf{mcd}(b, m) = 1$, y consideremos el entero $c = xnb + yma$. Se tiene que

  $$\mathsf{mcd}(c, n) = \mathsf{mcd}(xnb + yma, n) = \mathsf{mcd}(yma, n) = 1,$$

  ya que cada uno de los enteros y, m y a es coprimo con n. De manera similar, tenemos que $\mathsf{mcd}(c, m) = 1$ y, por lo tanto,

  $$\mathsf{mcd}(c, nm) = \mathsf{mcd}(c, n)\,\mathsf{mcd}(m) = 1.$$

  Si escribimos $r_{nm}(c)$ al resto de dividir a c por nm, tenemos entonces que también $r_{nm}(c)$ es coprimo con nm y que, además, $0 \leq r_{nm}(c) < nm$: esto nos dice que $r_{nm}(c)$ es un elemento de $C(nm)$. Hay por lo tanto una función $f : C(n) \times C(m) \to C(nm)$ tal que

  $$f(a, b) = r_{nm}(xnb + yma)$$

  para cada $(a, b) \in C(n) \times C(m)$.

- Sea $c \in C(nm)$ y sea $a = r_n(c)$ el resto de dividir a c por n. Si q es el correspondiente cociente, de manera que $r_n(c) = c - qn$, se tiene que

  $$\mathsf{mcd}(r_n(c), n) = \mathsf{mcd}(r_n(c) + qn, n) = \mathsf{mcd}(c, n) \mid \mathsf{mcd}(c, nm) = 1,$$

  así que $r_n(c) \in C(n)$. De manera similar podemos ver que $r_m(c) \in C(m)$ y, por lo tanto, que hay una función $g : C(nm) \to C(n) \times C(m)$ tal que para cada $c \in C(nm)$ se tiene que

  $$g(c) = (r_n(c), r_m(c)).$$

Segundo paso. En segundo lugar, probaremos que las funciones f y g que construimos son mutuamente inversas.

- Sea $(a, b) \in C(n) \times C(m)$ y sea $c = xnb + yma$, de manera que $f(a, b) = r_{nm}(c)$. Sea q el cociente de dividir a c por nm. Como $xnb + yma = c = qnm + r_{nm}(c)$, tenemos que

  $$r_{nm}(c) = (xb - qm)n + yma = (xb - qm)n - xna + a$$

  así que, como $0 \leq a < n$, es $r_n(r_{nm}(c)) = a$. De manera similar podemos ver que $r_m(r_{nm}(c)) = b$ y entonces que

  $$g(f(a, b)) = g(r_{nm}(c)) = (r_n(r_{nm}(c)), r_m(r_{nm}(c))) = (a, b).$$

  Esto nos dice que $g \circ f$ es la función identidad de $C(n) \times C(m)$.

- Sea ahora $c \in C(nm)$, de manera que $g(c) = (r_n(c), r_m(c))$, y pongamos

  $$d = xnr_m(c) + ymr_n(c).$$

  Sean q_n y q_m los cocientes de la división de c por n y por m, respectivamente. Tenemos que

  $$\begin{aligned} c &= xnc + ymc \\ &= xn(q_m m + r_m(c)) + ym(q_n n + r_n(c)) \\ &= (xq_m + yq_n)nm + xnr_m(c) + ymr_n(c) \\ &= (xq_m + yq_n)nm + d \end{aligned}$$

  así que $c = r_{nm}(c) = r_{nm}(d) = f(g(c))$. Vemos de esta forma que $f \circ g$ es la función identidad de $C(nm)$.

Tercer paso. Ahora que sabemos que f y g son funciones mutuamente inversas, sabemos en particular que f es biyectiva y, por lo tanto, que su dominio y su codominio tienen el mismo cardinal, esto es, que $|C(n) \times C(m)| = |C(nm)|$. Usando esto, vemos que

$$\varphi(n)\varphi(m) = |C(n)| \cdot |C(m)| = |C(n) \times C(m)| = |C(nm)| = \varphi(nm),$$

que es lo que queremos probar. □

10.2.3. Usando la multiplicatividad de la función de φ podemos, como con toda función multiplicativa, calcularla a partir de la factorización de su argumento como producto de primos:

Proposición. *Sea $n \in \mathbb{N}$, sean $p_1, \ldots, p_r$ los primos que dividen a n, listados sin repeticiones, y sean $a_1, \ldots, a_r \in \mathbb{N}$ tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Se tiene que*

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdot \ldots \cdot (p_r^{a_r} - p_r^{a_r - 1}), \qquad \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

La segunda expresión que nos da esta proposición para $\varphi(n)$ se llama el ***producto de Euler*** para φ.

Demostración. Sea p un número primo y sea $a \in \mathbb{N}$. Un número $k \in \{1, \ldots, p^a - 1\}$ tiene $\mathsf{mcd}(k, p^a) \neq 1$ si y solamente si es divisible por p, y esto ocurre si y solamente es de la forma pm con $m \in \{1, \ldots, p^{a-1}\}$. Esto nos dice que en $\{1, \ldots, p^a - 1\}$ hay p^{a-1} números que no son coprimos con p^a y, por lo tanto, que hay $p^a - p^{a-1}$ números que sí lo son. En otras palabras, tenemos que

$$\varphi(p^a) = p^a - p^{a-1}.$$

Sea ahora $n = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ como en el enunciado de la proposición. Como la función φ es multiplicativa, la Proposición 9.4.7 nos dice, en vista de lo que ya hicimos, que

$$\varphi(n) = \varphi(p_1^{a_1}) \cdot \ldots \cdot \varphi(p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1}) \cdot \ldots \cdot (p_r^{a_r} - r_r^{a_r-1}).$$

Esta es la primera igualdad que aparece en el enunciado. Para ver la segunda observamos simplemente que esta última expresión es igual a

$$p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_r^{a_r}\left(1 - \frac{1}{p_r}\right)$$

y reordenamos los factores, recordando que el producto $p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ es igual a n. □

10.2.4. Si n es un entero positivo y $p_1, \ldots, p_r$ son los primos que dividen a n listados sin repeticiones, la proposición que acabamos de probar nos dice que

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right). \tag{2}$$

La fracción que aparece a la izquierda en esta igualdad es el cociente entre el número de enteros coprimos con n de $\{1, \ldots, n\}$ sobre el número total de elementos de este conjunto: en otras palabras, es la proporción de números coprimos con n que hay en el conjunto $\{1, \ldots, n\}$. Podemos hacer algunas observaciones sencillas sobre esta proporción:

- Para cada $i \in \{1, \ldots, r\}$ el factor $1 - 1/p_i$ que aparece en (2) es menor que 1 pero mientras más grande es p_i mas cerca de 1 está. Esto nos dice que la proporción de números coprimos disminuye si aumenta el número de divisores primos de n y aumenta si esos divisores primos son más grandes.
- La proporción $\varphi(n)/n$ depende solamente de qué primos dividen a n y no de con qué potencias aparecen en la factorización de n. Así, por ejemplo, en proporción hay tantos números coprimos con $2 \cdot 5 \cdot 7$ como con $2^{23} \cdot 5^{12} \cdot 7^{201}$.

- Para n como en (2) se tiene que

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \leq \left(1 - \frac{1}{2}\right)^r = \frac{1}{2^r},$$

ya que todo primo es mayor o igual que 2. De esto se deduce que los números de la forma 2^a son los que más números coprimos tienen, en proporción: la mitad de los enteros positivos que no superan a 2^a son coprimos con él.

- Si ε es un número real positivo, sabemos, por un lado, que existe $r \in \mathbb{N}$ tal que $\varepsilon < 2^{-r}$ y, por otro, que hay r primos $p_1, \ldots, p_r$ distintos dos a dos —esto último porque sabemos que hay, de hecho, infinitos números primos. Se sigue de esto que si $n = p_1 \cdots p_r$ es el producto de esos r primos, entonces $\varphi(n)/n \leq 2^{-r} < \varepsilon$.

  Vemos así que hay números n para los que la proporción $\varphi(n)/n$ de números coprimos con n y menores que él es tan baja como queramos. Es posible cuantificar esto de manera muy precisa: para todo número positivo ε hay infinitos positivos n para los que

$$\frac{\varphi(n)}{n} \cdot \log\log n \geq \frac{1}{e^\gamma} - \varepsilon$$

y el número $1/e^\gamma$ es el mas chico con esta propiedad. Aquí $\gamma \approx 0{,}577\,216\ldots$ la llamada constante de Euler–Mascheroni, de manera que $e^\gamma \approx 1{,}781\,072\ldots$ Puede encontrarse una prueba de esto, junto con mucha más información sobre la función φ, en [HW2008, §18.4].

10.2.5. La siguiente observación es debida a Gauss, y describe una propiedad de la función de Euler que resulta ser fundamental.

Proposición. *Si $n \in \mathbb{N}$, entonces*

$$\sum_{d|n} \varphi(d) = n.$$

Los términos de la suma que aparece en el enunciado están indexados por los divisores positivos de n. Por ejemplo, los divisores de 30 son 1, 2, 3, 5, 6, 10, 15 y 30, y la proposición nos dice que $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 30$.

Demostración. Para cada $n \in \mathbb{N}$ escribamos

$$\psi(n) = \sum_{d|n} \varphi(d).$$

Obtenemos de esta forma una función $\psi : \mathbb{N} \to \mathbb{N}$. Mostremos que es multiplicativa.

Sean n y m dos enteros positivos coprimos. Es

$$\psi(n)\psi(m) = \sum_{d \in D(n)} \varphi(d) \cdot \sum_{e \in D(m)} \varphi(e) = \sum_{(d,e) \in D(n) \times D(m)} \varphi(d)\varphi(e).$$

Ahora bien, si (d,e) es un elemento del conjunto $D(n) \times D(m)$, entonces $d \mid n$ y $e \mid m$, así que $\mathsf{mcd}(d,e) \mid \mathsf{mcd}(n,m) = 1$ y, como la función φ es multiplicativa, tenemos que $\varphi(d)\varphi(e) = \varphi(de)$. Usando esto en cada uno de los términos de la última suma que obtuvimos, y recordando las funciones P y Q del Lema 9.4.8, vemos que

$$\begin{aligned}\psi(n)\psi(m) &= \sum_{(d,e)\in D(n)\times D(m)} \varphi(de) = \sum_{(d,e)\in D(n)\times D(m)} \varphi(P(d,e)) \\ &= \sum_{u\in D(nm)} \varphi(P(Q(u))) = \sum_{u\in D(nm)} \varphi(u) = \psi(nm).\end{aligned}$$

Esto muestra que ψ es multiplicativa, como queríamos.

Sea ahora p un número primo y sea $a \in \mathbb{N}$. Los divisores positivos de p^a son los números $1, p, p^2, \ldots, p^{a-1}, p^a$ así que

$$\begin{aligned}\psi(p^a) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^{a-1}) + \varphi(p^a) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^{a-1} - p^{a-2}) + (p^a - p^{a-1}) = p^a.\end{aligned}$$

Finalmente sea n un entero positivo cualquiera, sean $p_1, \ldots, p_r$ los primos que dividen a n listados sin repeticiones, y sean $a_1, \ldots, a_r$ los enteros tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Usando la multiplicatividad de la función ψ podemos calcular ahora que

$$\psi(n) = \psi(p_1^{a_1} \cdots p_r^{a_r}) = \psi(p_1^{a_1}) \cdots \psi(p_r^{a_r}) = p_1^{a_1} \cdots p_r^{a_r} = n.$$

Esto prueba la proposición. □

10.2.6. Una consecuencia importante de la proposición que acabamos de probar es la siguiente relación de la función φ de Euler y la función μ de Möbius que vimos en 9.6.2.

Corolario. *Para todo entero positivo n se tiene que*

$$\varphi(n) = \sum_{d\mid n} \mu(d) \cdot \frac{n}{d}.$$

Demostración. Consideremos la función $\mathrm{id} : n \in \mathbb{N} \mapsto n \in \mathbb{N}$. La Proposición 10.2.5 nos dice que para todo $n \in \mathbb{N}$ es

$$g(n) = \sum_{d\mid n} \varphi(d),$$

y entonces la fórmula de inversión de Möbius que vimos en en Ejercicio 9.6.3 nos dice que para

todo $n \in \mathbb{N}$ es

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d},$$

y esto es lo que afirma el corolario. □

§10.3. El Teorema de Euler

10.3.1. El Teorema de Fermat 10.1.4 nos dice que si p es un número primo y a un entero coprimo con p entonces $a^{p-1} \equiv 1 \mod p$. Esto no es cierto si p no es primo: por ejemplo, 3 es coprimo con 4 pero $3^{4-1} \equiv 3 \not\equiv 1 \mod 4$. El siguiente teorema de Euler generaliza al de Fermat a módulos compuestos:

Proposición. *Sea $m \in \mathbb{N}$. Si a es un entero coprimo con m, entonces $a^{\varphi(m)} \equiv 1 \mod m$.*

Observemos que como $\varphi(p) = p - 1$ para todo primo p, este resultado tiene como caso particular al Teorema de Fermat 10.1.4. De manera similar, si $m = p_1 p_2 \cdots p_r$ es un producto de r primos distintos dos a dos, entonces $\varphi(m) = (p_1 - 1)(p_2 - 1)\cdots(p_r - 1)$, y esta proposición tiene entonces también como casos particulares los resultados de la Proposición 10.1.7 y del Ejercicio 10.1.8

Demostración. Sea a un entero coprimo con m y sean x e y enteros tales que $xa + ym = 1$. Para cada $k \in \mathbb{Z}$ escribamos $q_m(k)$ y $r_m(k)$ al cociente y al resto de la división de k por m y consideremos el conjunto

$$C(m) \coloneqq \{k \in \mathbb{N} : 1 \leq k \leq m, \mathsf{mcd}(k, m) = 1\}.$$

Si $k \in C(m)$, entonces $k = kxa + kym$ y, por lo tanto,

$$\mathsf{mcd}(ka, m) \mid \mathsf{mcd}(kxa, m) = \mathsf{mcd}(k - kym, m) = \mathsf{mcd}(k, m) = 1,$$

de manera que ka es coprimo con m: se sigue de esto que $r_m(ka)$ es un elemento de $C(m)$. Como consecuencia de esto, vemos que hay una función $\pi : C(m) \to C(m)$ tal que para todo $k \in C(m)$ es $\pi(k) = r_m(ka)$. Afirmamos que se trata de una biyección. Como I es finito, para verificar esto suficiente con que mostremos que es sobreyectiva.

Sea entonces $k \in C(m)$. Como $k = kxa + kym$, tenemos que

$$\mathsf{mcd}(kx, m) \mid \mathsf{mcd}(kxa, m) = \mathsf{mcd}(k - kym, m) = \mathsf{mcd}(k, m) = 1,$$

así que el número $l = r_m(kx)$ pertenece a $C(m)$. Es $kx = q_m(kx)m + l$, así que

$$k - kym = kxa = aq_m(kx)m + al.$$

Tomando restos a ambos lados de esta igualdad vemos que

$$k = r_m(k) = r_m(al) = \pi(l).$$

Esto muestra que k está en la imagen de π y, por lo tanto, que esta función π es sobreyectiva, como queríamos.

Sean ahora

$$u_1, \quad u_2, \quad \ldots, \quad u_{\varphi(m)} \tag{3}$$

los $\varphi(m)$ elementos del conjunto $C(n)$ listados sin repeticiones. Como la función π es biyectiva, tenemos entonces que

$$r_m(au_1), \quad r_m(au_2), \quad \ldots, r_m(au_{\varphi(m)})$$

son esos mismos elementos, otra vez sin repeticiones, salvo que listados en otro orden, y cada uno de ellos es congruente módulo m con el correspondiente entero de la lista

$$au_1, \quad au_2, \quad \ldots, \quad au_{\varphi(m)}. \tag{4}$$

Se deduce de esto que el producto de los enteros listados en (3) es congruente módulo m con el producto de los enteros listados en (4), es decir, que

$$u_1u_2\cdots u_{\varphi(m)} \equiv au_1au_2\cdots au_{\varphi(m)} \mod m.$$

Si llamamos w al producto $u_1\cdots u_{\varphi(m)}$, esto nos dice que

$$w \equiv wa^{\varphi(m)} \mod m. \tag{5}$$

El número w es coprimo con m. Existen entonces enteros α y β tales que $\alpha w + \beta m = 1$ y, en particular, $\alpha w \equiv 1 \mod m$. Multiplicando ahora a cada lado de la congruencia (5) por α vemos que

$$1 \equiv \alpha w \equiv \alpha w a^{\varphi(m)} \equiv a^{\varphi(m)} \mod m$$

y esto prueba la proposición. □

Números racionales periódicos

10.3.2. Mostremos una aplicación sencilla del Teorema de Euler 10.3.1. Supongamos que a/b es un número racional entre 0 y 1 cuyas cifras decimales son periódicas, esto es, tal que si escribimos

$$\frac{a}{b} = 0.d_1d_2d_3d_4\cdots d_nd_{n+1}\cdots$$

al desarrollo decimal de a/b, hay un entero positivo N tal que $d_{i+N} = d_i$ para todo $i \in \mathbb{N}$. Esto nos dice que lo que está después de la coma en la escritura decimal de a/b se obtiene repitiendo indefinidamente el bloque de dígitos $d_1d_2\cdots d_N$, al que llamamos un ***periodo*** del número a/b. Por ejemplo, con

$$\frac{9}{37} = 0.\underbrace{234}\,\underbrace{234}\,\underbrace{234}\,\underbrace{234}\ldots$$

podemos tomar $N = 3$, de manera que el periodo es 234, y con

$$\frac{1}{2\,439} = 0.\underbrace{00041}\,\underbrace{00041}\,\underbrace{00041}\,\underbrace{00041}\ldots$$

elegir $N = 5$, con periodo 00041. Notemos que el número N no está completamente determinado — en el primer ejemplo podríamos haber elegido también $N = 6$ — aunque es fácil ver que siempre hay un periodo más corto que todos los otros y que la longitud de este divide a la de todos los otros. Por supuesto, no es cierto que todo número racional sea periódico en este sentido: así, no lo es

$$\frac{1}{2} = 0.5000\ldots$$

Ahora bien, si multiplicamos a a/b por 10^N, obtenemos

$$10^N \cdot \frac{a}{b} = d_1\cdots d_N.\underbrace{d_1\cdots d_N}\,\underbrace{d_1\cdots d_N}\,\underbrace{d_1\cdots d_N}\ldots$$

así que si llamamos c al número $(d_1,\cdots,d_N)_{10}$, tenemos que

$$10^N \cdot \frac{a}{b} - c = \frac{a}{b}$$

o, equivalentemente, que

$$\frac{a}{b} = \frac{c}{10^N - 1}.$$

Como $0 < a/b < 1$, es claro que $0 < c < 10^N - 1$. Tenemos, de hecho, el siguiente resultado:

Proposición. *Un número racional entre* 0 *y* 1 *es periódico si y solamente si es de la forma*

$$\frac{c}{10^N - 1}$$

para algún $N \in \mathbb{N}$ *y algún entero* c *tal que* $0 < c < 10^N - 1$*, y en ese caso tiene un periodo de longitud* N*.*

Demostración. Vimos arriba que un número racional entre 0 y 1 que es periódico es de esa forma, así que la condición es necesaria. Veamos que también es suficiente.

Sea $N \in \mathbb{N}$, sea c un entero tal que $0 < c < 10^N - 1$ y sea $q = c/(10^N - 1)$. Es evidente que q es un número racional y que $0 < q < 1$, así que tenemos que mostrar solamente que es periódico. De la forma en que definimos a q es claro que

$$10^N \cdot q = c + q. \tag{6}$$

Si la expansión decimal de q es

$$0.d_1 d_2 d_3 \ldots, \tag{7}$$

entonces la de $10^N \cdot q$ es

$$d_1 \cdots d_N . d_{N+1} d_{N+2} \ldots$$

Esto es, de acuerdo a (6), igual a $c + q$: como c es un entero y $0 < q < 1$, es claro que debe ser $c = (d_1, \ldots, d_N)_{10}$ y

$$q = 0.d_{N+1} d_{N+2} d_{N+3} \ldots$$

Comparando esto con (7) vemos que $d_{N+i} = d_i$ para todo $i \in \mathbb{N}$, así que q es periódico de periodo $d_1 \cdots d_N$ de longitud N. □

10.3.3. Aunque la Proposición 10.3.2 describe todos los números racionales periódicos entre 0 y 1 no es muy útil para reconocerlos. Por ejemplo, como vimos arriba el número 9/37 es periódico: así como lo escribimos no está escrito como una fracción con denominador de la forma $10^N - 1$, pero de todas formas

$$\frac{9}{37} = \frac{234}{10^3 - 1}.$$

Lo que aquí sucede es que el denominador de la fracción de la derecha es un múltiplo de 37, ya que $10^3 - 1 = 37 \cdot 27$: si multiplicamos el numerador y denominador de 9/37 por 27 obtenemos esa fracción y esto hace evidente que el número 9/37 es periódico.

Así, el problema de decidir si un número racional a/b entre 0 y 1 es periódico se reduce inmediatamente al de decidir si b divide a un número de la forma $10^n - 1$. Es con este último que el Teorema de Euler nos ayuda:

Proposición. *Un número racional a/b entre 0 y 1 escrito en forma reducida es periódico si y solamente si su denominador es coprimo con 10, y en ese caso la longitud de su periodo más corto es menor o igual a $\varphi(b)$.*

Es importante aquí que la fracción a/b sea reducida: el número $2/18 = 0{,}111\,111\ldots$ es periódico pero su denominador 18 no es coprimo con 10 — lo que sucede en este ejemplo es que $2/18$ puede simplificarse a $1/9$ y 9 sí es coprimo con 10.

Demostración. Sea a/b un número racional entre 0 y 1 escrito en forma reducida. Si b es coprimo con 10, entonces $10^{\varphi(b)} \equiv 1 \mod b$ por el Teorema de Euler 10.3.1, así que b divide a $10^{\varphi(b)} - 1$. Si q es el correspondiente cociente, entonces

$$\frac{a}{b} = \frac{qa}{10^{\varphi(b)} - 1}$$

y, de acuerdo a la proposición anterior, tenemos que a/b es periódico y que tiene un periodo de longitud $\varphi(b)$.

Recíprocamente, si el número a/b es periódico con un periodo de periodo de longitud N, entonces hay un entero c tal que $0 < c < 10^N - 1$ y

$$\frac{a}{b} = \frac{c}{10^N - 1},$$

así que $bc = (10^N - 1)a$. Como a y b son coprimos, esto implica que b divide a $10^N - 1$. Si $d = \mathsf{mcd}(b, 10)$, entonces d divide a 10 y a $10^N - 1$, así que divide a 1: por supuesto, esto nos dice que $d = 1$, es decir, que b es coprimo con 10. □

§10.4. Dos aplicaciones al problema de decisión de primalidad

El algoritmo de decisión de primalidad de Fermat

10.4.1. El Teorema de Fermat 10.1.4 nos dice que si p es un número primo y a es un entero tal que $0 < a < p$, entonces se tiene que $a^{p-1} \equiv 1 \mod p$. Esto nos da una condición necesaria para que un número sea primo. Por ejemplo, consideremos el número $n = 2\,534\,968\,907$. Usando el algoritmo que describimos en el Lema 5.4.20 para calcular potencias, podemos ver — haciendo unas $2 \log_2 n \approx 62.47\ldots$ multiplicaciones, que en la computadora del autor toman 0,000 2 segundos — que

$$2^{2\,534\,968\,907-1} \equiv 1\,475\,261\,599 \not\equiv 1 \mod n.$$

Como consecuencia de esto podemos concluir que n no es primo — notemos que, a pesar esto, seguimos sin conocer siquiera un divisor propio de n. Factorizarlo es mucho más difícil: en este caso, resulta que n es el producto de los primos 40283 y 62929, pero esto no se deduce para nada de la cuenta que hicimos[1].

Esta idea es conocida como el ***algoritmo de Fermat*** para el problema de decidir si un número positivo n es primo o no: si encontramos un entero a tal que $0 < a < n$ y $a^{n-1} \not\equiv 1 \mod n$, entonces podemos concluir con toda certeza que la respuesta a la pregunta es *no*. Llamamos a todo número a con esa propiedad un ***certificado*** de que n es compuesto. Así, vimos arriba que 2 es un certificado de que 1 475 261 599 es compuesto

10.4.2. En la Figura 10.1 en la página siguiente damos una implementación sencilla de esa idea en Haskell. Con esas definiciones, podemos evaluar

```
*Main> fermatRandom 3 1475261599
False
```

Esto nos dice que usando el algoritmo de Fermat y haciendo 3 intentos, alguno de los tres certifica que el número 1 475 261 599 que consideramos antes es compuesto. De manera similar, evaluando

```
*Main> fermatRandom 3 10209288027285050745821549405241 17
False
```

vemos que ese número, que tiene 34 dígitos, es compuesto. De hecho, usando Mathematica podemos ver que su factorización como producto de primos es

$$32452843 \cdot 86028121 \cdot 179424673 \cdot 2038074743.$$

[1] De hecho, armamos el ejemplo eligiendo primero estos dos primos y multiplicándolos para construir el número n.

```
import System.Random

potencia :: Integer -> Integer -> Integer -> Integer
potencia n a 0 = 1
potencia n a k
  | even k    = potencia n a (k `div` 2) ^ 2 `mod` n
  | odd k     = a * potencia n a ((k - 1) `div` 2) ^ 2 `mod` n

fermat :: Integer -> Integer -> Bool
fermat n a = gcd n a == 1 && potencia n a (n - 1) == 1

fermatRandom :: Int -> Integer -> IO Bool
fermatRandom k n = fmap (all (test n) . take m . randomRs (2, n-2)) newStdGen
```

Programa 10.1. El algoritmo de Fermat para decidir si un número es primo.

Por otro lado, podemos calcular:

```
*Main> fermatRandom 10000 2038074743
True
```

Esto eligió al azar 10 000 números entre 1 y 2 038 074 743 y ninguno de ellos certificó que este último es compuesto: podemos sospechar entonces que 2 038 074 743 es primo. En este caso, esa sospecha es buena: el número es efectivamente primo.

10.4.3. Si a es un entero positivo mayor que 1, decimos que un entero positivo n es un ***pseudo-primo*** en base a si es compuesto y divide a $a^{n-1} - 1$. Esto significa precisamente que a es una base que no sirve para certificar usando el algoritmo de Fermat que n es compuesto. Por ejemplo, 341 es un pseudo-primo en base 2: es $341 = 11 \cdot 31$ y usando el teorema de Fermat podemos ver que

$$2^{341-1} \equiv 2^{34(11-1)} \equiv 1 \mod 11, \qquad 2^{341-1} \equiv 2^{11(31-1)+10} \equiv 1 \mod 31,$$

ya que $2^{10} \equiv 1 \mod 31$, y usando el teorema chino del resto podemos concluir que $2^{341-1} \equiv 1 \mod 11 \cdot 31$. Por el contrario, 341 no es un pseudo-primo en base 3, así que 3 sirve para certificar que 341 no es primo: es

$$3^{341-1} \equiv 3^{34(11-1)} \equiv 1 \mod 11, \qquad 3^{341-1} \equiv 3^{11(31-1)+10} \equiv 25 \mod 31,$$

porque $3^{10} \equiv 25 \mod 31$, y de esto podemos deducir que $3^{341-1} \equiv 56 \mod 11 \cdot 31$. El primero en observar la existencia de números pseudo-primos fue Pierre Frédéric Sarrus, que encontró el ejemplo del 341 que acabamos de analizar. Con una computadora es fácil ver que los primeros pseudo-primos en base 2 son

$$341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371,$$

4681, 5461, 6601, 7957, 8321, 8481, 8911, . . .

En [OEI2023, A001567] puede encontrarse más información sobre esta sucesión de números, que se llaman también ***números de Sarrus*** o ***de Poulet***, por Paul Poulet.

10.4.4. La existencia de números pseudo-primos implica que para un número compuesto n no necesariamente todo número entre 1 y n es un certificado de que n es compuesto. Más aún, nuestro siguiente lema implica inmediatamente que cualquiera sea el entero a mayor que 1 hay infinitos pseudo-primos en base a, y como consecuencia de esto podemos concluir que no hay ningún número a que tenga la propiedad de que para todo $n \in \mathbb{N}$ valga

$$a^{n-1} \equiv 1 \mod n \implies n \text{ es primo},$$

y, de hecho, que ni siquiera hay un entero a para el que esto sea cierto salvo para finitos elecciones de n. En otras palabras, no hay ningún número que sirva como certificado para casi todos los números compuestos. Es esto lo que nos fuerza, si queremos usar el algoritmo de Fermat para decidir que un número es compuesto, a usar muchos valores distintos de a.

Lema. *Si a es un entero mayor que 1, entonces para cada primo p mayor que $a+1$ el número*

$$\frac{a^p - 1}{a-1} \cdot \frac{a^p + 1}{a+1} \tag{8}$$

es un pseudo-primo en base a.

Por ejemplo, si elegimos $a = 2$ y $p = 5$, el pseudo-primo en base 2 que nos da el lema es 341. Este resultado es debido a Michele Cipolla [Cip1904]. En la sección 2 del capítulo VIII del libro [Rib1996] de Paulo Ribenboim se describen varios otros resultados de este tipo.

Demostración. Sea p un número primo mayor que $a+1$, que necesariamente es impar. Escribamos n_{+1} y n_{-1} a los dos factores del producto (8) y pongamos $n := n_{+1}n_{-1}$.

Sea $\varepsilon \in \{\pm 1\}$. Es

$$\frac{a^p - \varepsilon}{a - \varepsilon} = \varepsilon^{p-1} + \sum_{i=1}^{p-1} a^i \varepsilon^{p-1-i}.$$

La suma que aparece aquí tiene $p-1$ sumandos todos congruentes a a módulo 2, así que es un número par: esto implica que el cociente $(a^p - \varepsilon)/(a - \varepsilon)$ es impar. Por otro lado, como $p > a+1 \geq a - \varepsilon$, el entero $a - \varepsilon$ es coprimo con p y existe un entero u tal que $(a-\varepsilon)u \equiv 1 \mod p$. Usando esto y el teorema de Fermat vemos que

$$\frac{a^p - \varepsilon}{a - \varepsilon} \equiv \frac{a^p - \varepsilon}{a - \varepsilon} \cdot (a-\varepsilon)u \equiv (a^p - \varepsilon)u \equiv (a-\varepsilon)u \equiv 1 \mod p,$$

Vemos así que $n_\varepsilon \equiv 1 \mod 2$ y que $n_\varepsilon \equiv 1 \mod p$, así que $n_\varepsilon \equiv 1 \mod 2p$.

Esto implica, claro, que $n = n_{+1}n_{-1} \equiv 1 \mod 2p$ y, por lo tanto, que hay un entero q tal que $n-1 = 2pq$. Ahora bien, es

$$\frac{a^{2p}-1}{a^2-1} = n,$$

así que $a^{2p} \equiv 1 \mod n$, y esto nos permite concluir que $a^{n-1} = (a^{2p})^q \equiv 1 \mod n$, es decir, que n es un pseudo-primo en base a. □

10.4.5. Hemos visto que si un número n es compuesto no necesariamente todo entero entre 1 y n sirva como certificado de que lo es. De todas formas, podemos ilusionarnos y esperar que para cada número compuesto n exista algún certificado de que lo es. Lamentablemente esto no es así.

Decimos que un entero positivo n es un ***número de Carmichael*** si es compuesto y para todo entero a tal que $1 < a < n$ y coprimo con n se tiene que $a^{n-1} \equiv 1 \mod n$. Estos números fueron estudiados originalmente por Alwin Reinhold Korselt en [Kor1899] y por Robert Daniel Carmichael en [Car1912]. El más chico de estos números fue encontrado por Carmichael: es el 561, que tiene por factorización a $3 \cdot 11 \cdot 17$. Mostremos que este número tiene esa propiedad.

Sea a un entero coprimo con 561. Del teorema de Fermat sabemos que $a^2 \equiv 1 \mod 3$, de manera que $a^{10} \equiv (a^2)^5 \equiv 1 \mod 3$, y $a^{10} \equiv 1 \mod 11$, y entonces $a^{10} \equiv 1 \mod 3 \cdot 11$ y

$$a^{80} = (a^{10})^8 \equiv 1 \mod 3 \cdot 11. \tag{9}$$

Por otro lado, el teorema de Fermat nos dice que $(a^8)^2 = a^{16} \equiv 1 \mod 17$ y es fácil[2] ver que entonces $a^8 \equiv \pm 1 \mod 17$ y, por lo tanto, $a^{80} \equiv 1 \mod 17$. Esta congruencia junto con (9) nos permiten concluir que

$$a^{80} \equiv 1 \mod 3 \cdot 11 \cdot 17.$$

Por otro lado, el resultado del Ejercicio 10.1.8 nos permite concluir que

$$a^{320} = a^{(3-1)(11-1)(17-1)} \equiv 1 \mod 3 \cdot 11 \cdot 17$$

y entonces que

$$a^{561-1} \equiv a^{560}a^{80} \equiv a^{640} \equiv (a^{320})^2 \equiv 1 \mod 3 \cdot 11 \cdot 17.$$

Esto prueba que 561 es un número de Carmichael, como queremos. En particular, el algoritmo de Fermat no nos permite certificar que se trata de un número compuesto.

[2] Si x es un entero tal que $x^2 \equiv 1 \mod 17$, entonces 17 divide a $x^2 - 1 = (x-1)(x+1)$ y, como es primo, divide a $x-1$ o a $x+1$, de manera que $x \equiv 1$ o $x \equiv -1 \mod 17$.

10.4.6. En [AGP1994] William Robert Alford, Andrew Granville y Carl Pomerance probaron que existen infinitos números de Carmichael. Los primeros son

561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911, 10 585, 15 841, 29 341, 41 041, 46 657,

52 633, 62 745, 63 973, 75 361, 101 101, 115 921, 126 217, 162 401, 172 081, 188 461, ...

En [OEI2023, A002997] puede encontrarse más información sobre esta sucesión. El número de Carmichael más grande conocido fue encontrado por William Robert Alford, Jon Grantham, Steven Hayman y Andrew Shallue en [AGHS2014]: tiene 295 486 761 787 dígitos y es el producto de 10 333 229 505 primos distintos dos a dos.

No solamente hay infinitos números de Carmichael sino que, en cierto sentido, hay muchos. En [Har2008] Glyn Harman probó, por ejemplo, que cuando n es grande hay al menos $n^{1/3}$ números de Carmichael menores o iguales que n. Se conocen, además, varios resultados sobre la distribución de los números de Carmichael. Recientemente, Daniel Larsen probó en 2021 [Lar2023] para estos números un resultado similar al llamado *postulado de Bertrand* — Larsen tenía 17 años en ese momento.

10.4.7. La existencia de números de Carmichael implica que el algoritmo de Fermat no puede responder con certeza la pregunta de si un número es primo o no. Ahora bien, si suponemos que n es compuesto y *no es* un número de Carmichael, entonces sabemos que existen certificados de que es compuesto: ¿cuántos hay?

Proposición. *Sea n un entero positivo compuesto que no es un número de Carmichael. Entre los $\varphi(n)$ elementos de $\{1, \dots, n\}$ que son coprimos con n al menos la mitad son certificados de que n es compuesto.*

Demostración. Consideremos los conjuntos

$$A \coloneqq \{a \in \{1, \dots, n\} : \mathsf{mcd}(a, n) = 1, a^{n-1} \not\equiv 1 \mod n\}$$

y

$$B \coloneqq \{a \in \{1, \dots, n\} : \mathsf{mcd}(a, n) = 1, a^{n-1} \equiv 1 \mod n\}.$$

Claramente A y B son disjuntos, y su unión es el conjunto de elementos de $\{1, \dots, n\}$ que son coprimos con n, así que $|A| + |B| = |A \cup B| = \varphi(n)$.

Como n no es un número de Carmichael, el conjunto A no es vacío. Sea x uno de sus elementos. Si y pertenece a B, entonces $(xy)^{n-1} \equiv x^{n-1}y^{n-1} \equiv x^{n-1} \not\equiv 1 \mod n$, así que $xy \in A$. Esto nos dice que hay una función

$$f : y \in B \mapsto xy \in A.$$

Esta función es inyectiva. En efecto, como $\mathsf{mcd}(x, n) = 1$, hay un entero u tal que $ux \equiv 1 \mod n$: si y e y' son dos elementos de B tales que $f(y) = f(y')$, entonces $y \equiv uxy \equiv uxy' \equiv y' \mod n$ y,

como $1 \leq y, y' \leq n$, $y = y'$. Ahora bien, como la función f es inyectiva claramente tenemos que $|B| \leq |A|$ y, por lo tanto, que $2|A| \geq |A| + |B| = \varphi(n)$, de manera que $|A| \geq \varphi(n)/2$. Esto es lo que afirma la proposición. □

Esta proposición nos dice que si n es un entero positivo que es compuesto y no es un número de Carmichael y elegimos al azar un elemento de $\{1, \ldots, n\}$ coprimo con n, entonces la probabilidad de que no sea un certificado de que n es compuesto es como mucho $1/2$. Se sigue de esto que si elegimos k tales elementos la probabilidad de que ninguno de ellos sea un certificado es como mucho $1/2^k$ y esta probabilidad decrece exponencialmente con k. Así, por ejemplo, es suficiente elegir 34 candidatos para que la probabilidad de que ninguno sea un certificado sea menor que 0,000 000 000 1. En 10.4.2 hicimos 10 000 intentos de encontrar un certificado de que 2 038 074 743 es compuesto y no lo encontramos: si suponemos que este número no es un número de Carmichael (y no lo es), entonces la probabilidad de que no sea primo es menor[3] que $1/2^{10\,000} \sim 10^{-3000}$.

De todas formas, hay — como observamos arriba — relativamente muchos números de Carmichael y no es fácil determinar si un numero es o no de estos. Esto hace que, en la práctica, no usemos solamente el algoritmo de Fermat para decidir si un número es *probablemente* primo y que, entonces, lo combinemos con otro posiblemente más costoso computacionalmente pero que no tenga «excepciones».

El algoritmo de decisión de primalidad de Miller–Rabin

10.4.8. En [Mil1976] Gary Miller describió un algoritmo completamente determinístico para decidir si un número es primo o no, pero que es «condicional»: esto significa que su corrección depende de la validez una conjetura — la llamada *hipótesis de Riemann generalizada* — que no está probada. Cuatro años más tarde, Michael Oser Rabin mostró en [Rab1980] cómo modificar el algoritmo para que funcione incondicionalmente pero en forma probabilística.

10.4.9. Para describir este algoritmo necesitamos la siguiente observación bien sencilla:

Lema. *Sea p un número primo. Si x es un entero tal que $x^2 \equiv 1 \mod p$, entonces x es congruente a 1 o a -1 módulo p.*

En otras palabras, 1 tiene como mucho dos raíces cuadradas módulo p — y, de hecho, tiene exactamente dos si p es impar, ya que en ese caso $1 \not\equiv -1 \mod p$.

[3] En realidad, para poder afirmar esto con toda certeza habría que analizar en detalle la forma en que elegimos los candidatos al azar.

Demostración. Si x es un entero tal que $x^2 \equiv 1 \mod p$, entonces $p \mid x^2 - 1 = (x-1)(x+1)$ y, como p es primo, esto nos dice que p divide a $x-1$ o a $x+1$. La afirmación del lema sigue inmediatamente de esto. □

10.4.10. En base a este lema podemos probar el resultado que está en la base del algoritmo de Miller–Rabin

Proposición. *Sea p un número primo impar y sean s y d enteros positivos tales que $p = 2^s d + 1$ y d es impar. Para todo entero positivo a menor que p vale alguna de las siguientes dos afirmaciones:*

(*a*) *Es $a^d \equiv 1 \mod p$.*

(*b*) *Hay exactamente un elemento r de $\{0, \dots, s-1\}$ tal que $a^{2^r d} \equiv -1 \mod p$.*

En la Figura 10.2 ilustramos este resultado cuando $p = 41$.

Demostración. Sea a un entero positivo menor que p. Como p es primo a es coprimo con p y, de acuerdo al teorema de Fermat 10.1.4, tenemos que $a^{2^s d} \equiv a^{p-1} \equiv 1 \mod p$. Esto nos dice que el conjunto

$$S \coloneqq \{i \in \{0, \dots, s\} : a^{2^i d} \equiv 1 \mod p\}$$

no es vacío, ya que contiene a s: podemos entonces considerar su menor elemento. Si $\min S = 0$, es $a^d \equiv 1 \mod p$ y vale la primera de las dos afirmaciones de la proposición. Si, por el contrario, es $\min S > 0$, entonces el número $r \coloneqq \min S - 1$ pertenece a $\{0, \dots, s-1\}$ y no a S, y $r+1 \in S$: esto nos dice que $a^{2^r d} \not\equiv 1 \mod p$ y que $(a^{2^r d})^2 \equiv a^{2^{r+1} d} \equiv 1 \mod p$, y el Lema 10.4.9 nos permite concluir que $a^{2^r d} \equiv -1 \mod p$, de manera que vale la afirmación de existencia de (*b*).

Para verificar la afirmación de unicidad de (*b*) supongamos ahora que hay dos elementos distintos r y r' de $\{0, \dots, s-1\}$ tales que $a^{2^r d} \equiv -1 \mod p$ y $a^{2^{r'} d} \equiv -1 \mod p$, y, sin pérdida de generalidad, que $r < r'$, de manera que $u \coloneqq r' - r$ es un entero positivo. Tenemos entonces que

$$-1 \equiv a^{2^{r'} d} \equiv (a^{2^r d})^{2^u} = (-1)^{2^u} \equiv 1 \mod p,$$

y esto es absurdo, ya que p es un entero impar. □

10.4.11. Esta proposición nos da una condición necesaria para que el número p sea primo, y podemos entonces usarla para probar que un número no lo es. Por ejemplo, si tomamos

$$n = 28\,393\,021 = 2^2 \cdot 7\,098\,255 + 1$$

podemos calcular fácilmente que módulo n es

$$2^{7\,098\,255} \not\equiv 1, \qquad 2^{7\,098\,255} \not\equiv -1, \qquad 2^{2 \cdot 7\,098\,255} \not\equiv -1$$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	$\varnothing$	1	2	0	1	2	2	1	1	$\varnothing$	2	2	2	2	2	$\varnothing$	2	$\varnothing$	2	1

a	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
	1	2	0	2	0	2	2	2	2	2	0	1	1	2	2	1	$\varnothing$	2	1	0

Figura 10.2. Elegimos aquí $p = 41 = 2^3 \cdot 5 + 1$ y para cada entero positivo a menor que p tabulamos el entero $s \in \{0, 1, 2\}$ tal que $a^{2^s d} \equiv -1 \mod p$, si es que hay alguno, o ponemos un símbolo $\varnothing$.

y esto es suficiente para concluir que n no es primo. De manera similar, si

$$n = 9\,629\,970\,333\,103 = 2 \cdot 4\,814\,985\,166\,551 + 1,$$

entonces módulo n es

$$2^{4\,814\,985\,166\,551} \equiv 8\,956\,534\,393\,410,$$

y esto no es congruente ni con 1 ni con -1, así que podemos concluir que n no es primo. Notemos que el cálculo de esta potencia puede hacerse haciendo solamente 44 productos y divisiones entre números menores que n, lo que lleva menos de un milisegundo con una computadora moderna.

10.4.12. El ***algoritmo de Miller–Rabin*** para determinar si un entero positivo impar n es primo consiste en elegir un entero positivo a menor que n y verificar que alguna de las dos afirmaciones de la Proposición 10.4.10 se cumple. Si esto no es así, entonces tenemos certeza de que n no es primo — decimos en ese caso que a es un ***certificado*** de Miller–Rabin para n. Si, por el contrario, alguna de esas afirmaciones se cumple entonces no podemos decir nada, claro.

A diferencia de lo que ocurre con el algoritmo de Fermat — debido a la existencia de números de Carmichael — todo número compuesto impar posee un certificado de Miller–Rabin. No se conoce, de todas formas, una forma de encontrar uno. Miller [Mil1976] y Eric Bach [Bac1990] probaron — asumiendo la verdad de la hipótesis de Riemannn generalizada — que si n es compuesto e impar entonces hay un certificado a que cumple la desigualdad $1 < a < 2(\ln n)^2$, y esto nos dice que es suficiente buscar uno entre los enteros que satisfacen estas desigualdades: esto es conocido como el ***algoritmo de Miller*** y es completamente determinístico. Por ejemplo, si

$$n = 54\,299\,051\,326\,517 = 2^2 \cdot 13\,574\,762\,831\,629 + 1$$

entonces $2(\ln n)^2 = 2\,000{,}348\,02\ldots$ así que estamos seguros de que, si es que es compuesto, podemos encontrar un certificado entre 1 y 2000. En el peor de los casos, entonces, podremos decidir si n es primo o no calculando 2000 potencias de exponente menor que n módulo n.

10.4.13. En la práctica este algoritmo de Miller no suele usarse. En su lugar, simplemente se elige al azar un número k de enteros positivos menores que n y para cada uno de ellos se verifica si se cumplen o no alguna de las afirmaciones de la proposición. Si para alguno esto no ocurre, entonces podemos concluir que n es compuesto. En el caso contrario, claro, no podemos decir nada, pero Rabin probó en [Rab1980] que

> *si n es compuesto e impar, entonces como mucho $1/4$ de los enteros positivos menores que n no son certificados de Miller–Rabin para n.*

Esto implica que si hacemos k intentos con números elegidos al azar entonces la probabilidad de que n sea compuesto pero no lo podamos certificar con ninguno de ellos es menor que $1/4^k$, y esto decrece rápidamente cuando k aumenta. El algoritmo de Miller–Rabin nos permite establecer que n es primo con mucha probabilidad — que es lo que se llama un ***primo probable***.

10.4.14. Exactamente como con el algoritmo de Fermat es posible probar que no hay ningún entero que sirva como certificado de Miller–Rabin para todo entero compuesto, y esto es lo que nos fuerza a tener que buscar para cada n un certificado. De todas formas, si uno solamente está interesado en enteros n en un rango fijo esta situación puede mejorarse.

Por ejemplo, Carl Pomerance, John Lewis Selfridge y Samuel Wagstaff [PSW1980] y Gerhard Jaeschke [Jae1993] probaron que

- todo entero compuesto impar menor que 2 047 tiene a 2 como certificado de Miller–Rabin,
- todo entero compuesto impar menor que 341 550 071 728 321 tiene a alguno de 2, 3, 5, 7, 11, 13, o 17 como certificado.

Todo esto significa que podemos decidir si un número menor que 341 550 071 728 321 de manera completamente determinística y muy rápido. Más recientemente, Jonathan Sorenson y Jonathan Webster probaron en [SW2017] que

> *todo entero compuesto impar menor que* 3 317 044 064 679 887 385 961 981 *tiene uncertificado de Miller–Rabin que pertenece al conjunto* $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41\}$.

Esto nos da una forma extremadamente rápida de decidir la primalidad de cualquier número de a lo sumo 24 dígitos.

10.4.15. En la Figura 10.2 damos una implemenación sencilla del algoritmo de Miller-Rabin. Usando esas definiciones, podemos evaluar

```
ghci> millerRabin 1475261599 2
False
```

```
import System.Random

valuación :: Integer -> Integer -> Integer
valuación b n
  | n `mod` b == 0 = valuación b (n `div` b) + 1
  | otherwise      = 0

potencia :: Integer -> Integer -> Integer -> Integer
potencia n a 0 = 1
potencia n a d
  | even d     = potencia n a (d `div` 2) ^ 2 `mod` n
  | otherwise  = a * (potencia n a ((d - 1) `div` 2)) ^ 2 `mod` n

millerRabin :: Integer -> Integer -> Bool
millerRabin n a = p == 1 || (n - 1) `elem` ps
  where s = valuación 2 (n - 1)
        d = (n - 1) `div` (2 ^ s)
        p = potencia n a d `mod` n
        ps = take (fromIntegral s) (iterate (\x -> x^2 `mod` n) p)

millerRabinRandom :: Int -> Integer -> IO Bool
millerRabinRandom k n
        = fmap (all (millerRabin n) . take k . randomRs (2, n-2)) newStdGen
```

Programa 10.2. El algoritmo de Miller–Rabin para decidir si un número es primo.

y esto nos dice que 2 es un certificado de que el número 1 475 261 599 es compuesto. Por otro lado, evualuando

```
ghci> millerRabin 2038074743 2
True
```

vemos que 2 no es un certificado de que 2 038 074 743 es compuesto. Finalmente, evaluando

```
ghci> millerRabinRandom 1000 2038074743
True
```

generamos 1 000 enteros entre 2 y 2 038 074 743 − 2 al azar y verificamos que ninguno de ellos es un certificado de que 2 038 074 743 es compuesto.

§10.5. Órdenes

10.5.1. Sea $m \in \mathbb{N}$. Si a es un entero coprimo con m, el teorema de Euler 10.3.1 nos dice que $a^{\varphi(m)} \equiv 1 \mod m$, así que, en particular, el conjunto

$$S_a = \{k \in \mathbb{N} : a^k \equiv 1 \mod m\} \tag{10}$$

no es vacío. Podemos entonces considerar su menor elemento, al que llamamos el ***orden*** de a módulo m y escribimos $\mathsf{ord}_m(a)$. Notemos que definimos el orden módulo m de un entero a sólo cuando este último es coprimo con m y por una buena razón: si no es ése el caso, el conjunto S_a que definimos arriba es vacío.

El orden de a nos permite describir el conjunto S_a completamente:

Proposición. *Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m. Tenemos que $a^{\mathsf{ord}_m(a)} \equiv 1 \mod m$ y, más aún, un entero positivo t es tal que $a^t \equiv 1 \mod m$ si y solamente si es divisible por $\mathsf{ord}_m(a)$.*

Demostración. La primera afirmación es inmediata, ya que $\mathsf{ord}_m(a)$ pertenece al conjunto S_a de (10). Veamos la segunda.

Sea t un entero positivo. Supongamos primero que $a^t \equiv 1 \mod m$ y sean q y r el cociente y el resto de la división de t por $\mathsf{ord}_m(a)$, de manera que $t = q\,\mathsf{ord}_m(a) + r$ y $0 \leq r < \mathsf{ord}_m(a)$. Tenemos entonces que

$$1 \equiv a^t \equiv a^{q\,\mathsf{ord}_m(a)+r} \equiv (a^{\mathsf{ord}_m(a)})^q a^r \equiv a^r \mod m,$$

así que o bien $r = 0$ o bien $r \in S_a$. Como la segunda opción no puede ocurrir, ya que $r < \mathsf{ord}_m(a)$

y $\mathsf{ord}_m(a)$ es el menor elemento de S_a, vemos que $r = 0$, esto es, que r es divisible por $\mathsf{ord}_m(a)$. Esto muestra que la condición del enunciado es necesaria.

Su suficiencia, por otro lado, es casi evidente: si t es un múltiplo de $\mathsf{ord}_m(a)$, de manera que existe $s \in \mathbb{N}$ tal que $t = s\,\mathsf{ord}_m(a)$, entonces $a^t = (a^{\mathsf{ord}_m(a)})^s \equiv 1^s \equiv 1 \mod m$. □

10.5.2. Combinando esta proposición con el teorema de Euler obtenemos lo siguiente:

Corolario. *Si $m \in \mathbb{N}$ y a es un entero coprimo con m, entonces $\mathsf{ord}_m(a)$ divide a $\varphi(m)$. En particular, si m es primo, entonces $\mathsf{ord}_p(a)$ divide a $m - 1$.*

Demostración. De acuerdo al teorema de Euler 10.3.1, es $a^{\varphi(m)} \equiv 1 \mod m$, así que la Proposición 10.5.1 nos dice que $\mathsf{ord}_m(a)$ divide a $\varphi(m)$. Esto prueba la primera afirmación del corolario. La segunda es consecuencia inmediata de ella, ya que cuando m es primo se tiene que $\varphi(m) = m - 1$. □

10.5.3. Si conocemos el orden de un entero coprimo módulo un número m, todas sus potencias quedan determinadas módulo m por un número finito de ellas:

Proposición. *Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m. Si n es el orden de a módulo m, entonces los n enteros*

$$1,\ a,\ a^2,\ \ldots,\ a^{n-1} \tag{11}$$

son no congruentes módulo m dos a dos. Más aún, todas las potencias de a son congruentes a uno y a uno sólo de estos números: más precisamente, si $k \in \mathbb{N}_0$ y r es el resto de la división de k por n, entonces $a^k \equiv a^r \mod m$.

Demostración. Sea n el orden de a módulo m y supongamos, para probar la primera afirmación por el absurdo, que i y j son enteros tales que $0 \le i < j < n$ y $a^i \equiv a^j \mod m$. Tenemos entonces que m divide a $a^j - a^i = a^i(a^{j-i} - 1)$ y, como es coprimo con a, que divide a $a^{j-i} - 1$. En otras palabras, tenemos que $a^{j-i} \equiv 1 \mod m$: esto es imposible, ya que la diferencia $j - i$ es positiva y estrictamente menor que n, el orden de a.

Sea ahora $k \in \mathbb{N}_0$ y sean q y r el cociente y el resto de la división de k por n, de manera que $k = qn + r$ y $0 \le r < n$. Es $a^k = (a^n)^q a^r \equiv a^r \mod m$, así que a^k es congruente a uno de los enteros listados en (11). Sólo puede ser congruente a uno de ellos, ya que sabemos que no hay ahí dos que sean congruentes entre sí. □

10.5.4. La siguiente observación es importante: nos dice cómo calcular el orden de una potencia de un entero cuando conocemos el de este.

Proposición. *Sea $m \in \mathbb{N}$, sea a un entero coprimo con m, y sea $k \in \mathbb{N}_0$. El orden de a^k módulo m es*

$$\mathsf{ord}_m(a^k) = \frac{\mathsf{ord}_m(a)}{\mathsf{mcd}(\mathsf{ord}_m(a), k)}.$$

Demostración. Escribamos $n \coloneqq \mathsf{ord}_m(a)$ y $t \coloneqq \mathsf{ord}_m(a^k)$. Como $a^{kt} = (a^k)^t = 1$, tenemos que n divide a kt y que, por lo tanto, existe un entero positivo m tal que $kt = nm$. Sea $d \coloneqq \mathsf{mcd}(n, k)$ y sean n_1 y k_1 enteros tales que $n = n_1 d$ y $k = k_1 d$; sabemos que es entonces $\mathsf{mcd}(n_1, k_1) = 1$. Como

$$k_1 dt = kt = nm = n_1 dm$$

y, por supuesto, $d \neq 0$, tenemos que $k_1 t = n_1 m$. En particular, esto nos dice que n_1 divide a $k_1 t$ y, como es coprimo con k_1, que de hecho divide a t. Esto implica que $n_1 \leq t$.

Por otro lado, tenemos que

$$(a^k)^{n_1} = a^{kn_1} = a^{k_1 d n_1} = a^{k_1 n} = (a^n)^{k_1} \equiv 1 \mod m,$$

así que $t = \mathsf{ord}_m(a^k) \mid n_1$ y, por lo tanto, $t \leq n_1$. Concluimos de esta forma que

$$t = n_1 = \frac{n}{d} = \frac{\mathsf{ord}_m(a)}{\mathsf{mcd}(\mathsf{ord}_m(a), k)},$$

que es lo que afirma la proposición. □

10.5.5. La proposición que acabamos de probar tiene dos casos particulares útiles:

Corolario. *Sea $m \in \mathbb{N}$, sea a un entero coprimo con m, y sea $k \in \mathbb{N}$.*

(*i*) *Si k divide a $\mathsf{ord}_m(a)$, entonces el orden de a^k es $\mathsf{ord}_m(a)/k$.*

(*ii*) *Si k es coprimo con $\mathsf{ord}_m(a)$, entonces $\mathsf{ord}_m(a^k) = \mathsf{ord}_m(a)$.*

Demostración. Ambas afirmaciones son consecuencia inmediata de la proposición: en el primer caso $\mathsf{mcd}(\mathsf{ord}_m(a), k)$ es k y en el segundo es 1. □

10.5.6. Buscamos ahora información sobre el orden de un producto de dos números.

Proposición. *Sea $m \in \mathbb{N}$ y sean a y b dos enteros coprimos con m.*

(*i*) *El orden de ab es un divisor $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$.*

(*ii*) *Si los órdenes $\mathsf{ord}_m(a)$ y $\mathsf{ord}_m(b)$ son coprimos, entonces $\mathsf{ord}_m(ab) = \mathsf{ord}_m(a)\,\mathsf{ord}_m(b)$.*

Por supuesto, si a y b son coprimos con m también lo es ab, y es por esto que podemos hablar del orden de ab módulo m.

Demostración. Escribamos $x \coloneqq \mathsf{ord}_m(a)$, $y \coloneqq \mathsf{ord}_m(b)$ y $z \coloneqq \mathsf{ord}_m(ab)$.

(*i*) Sea $s \coloneqq \mathsf{mcm}(x, y)$, de manera que hay enteros positivos x_1 e y_1 tales que $s = xx_1$ y $s = yy_1$. Usando esto, vemos que

$$(ab)^s = a^s b^s = (a^x)^{x_1}(b^y)^{y_1} \equiv 1 \mod m$$

y, en particular, que $\mathsf{ord}_m(ab)$ divide a s.

(*ii*) Supongamos que $\mathsf{mcd}(x, y) = 1$. Como

$$(ab)^{xy} = (a^x)^y (b^y)^x \equiv 1^y 1^x \equiv 1 \mod m,$$

se tiene que $z \mid xy$. Por otro lado, tenemos que

$$a^z b^z = (ab)^z \equiv 1 \mod m,$$

así que

$$1 \equiv (a^z b^z)^y = a^{yz}(b^y)^z \equiv a^{yz} \mod m$$

y, por lo tanto, $x \mid yz$: como x es coprimo con y, esto implica que x divide a z. Podemos ver, de manera similar, que y divide a z y, como x e y son coprimos, deducir de estas dos cosas que $xy \mid z$. Se tiene entonces que $xy = z$, que es lo que afirma el enunciado. □

10.5.7. En la situación de la Proposición 10.5.6(*i*) no se tiene en general que el orden de ab sea igual a $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$. Por ejemplo los órdenes de 2 y de 5 módulo 13 son 12 y 6, respectivamente, y el orden de $10 = 2 \cdot 5$ es 6, que es distinto de $\mathsf{mcm}(12, 6) = 12$.

El siguiente resultado nos dice, de todas formas, que podemos construir en la situación de la Proposición 10.5.6(*i*) a partir de a y b un número de orden igual a $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$, aunque de una forma apenas un poco más complicada que simplemente multiplicándolos:

Proposición. *Sea $m \in \mathbb{N}$ y sean a y b dos enteros coprimos con m. Existen enteros positivos r y s tales que el orden de $a^r b^s$ es $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$.*

Demostración. Sean $x \coloneqq \mathsf{ord}_m(a)$ e $y \coloneqq \mathsf{ord}_m(b)$. De acuerdo a la Proposición 9.3.9, existen enteros positivos u y v tales que $\mathsf{mcd}(u, v) = 1$, $\mathsf{mcd}(x, y) = uv$, $u \mid x$ y $v \mid y$. Como x/u divide a x, el Corolario 10.5.5(*i*) nos dice que $\mathsf{ord}_m(a^{x/u}) = \mathsf{ord}_m(a)/(x/u) = u$ y, de manera similar y como y/v divide a y, que $\mathsf{ord}_m(b^{y/v}) = v$. Ahora bien, como u y v son coprimos, la Proposición 10.5.6(*ii*) nos dice que el orden de $a^{x/u} b^{y/v}$ es uv, que es igual a $\mathsf{mcm}(x, y)$. Esto prueba la proposición: basta elegir $r = x/u$ y $s = y/v$. □

10.5.8. Como es habitual, podemos extender la afirmación de la Proposición 10.5.7 al caso en que

tenemos un número arbitrario de enteros:

Corolario. *Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y $a_1, \ldots, a_n$ son enteros coprimos con m, entonces existen enteros positivos $r_1, \ldots, r_n$ tales que $a_1^{r_1} \cdots a_n^{r_n}$ tiene orden*

$$\mathsf{mcm}(\mathsf{ord}_m(a_1), \ldots, \mathsf{ord}_m(a_n))$$

modulo m.

Demostración. Procedemos por inducción con respecto a n, notando que si $n = 1$ no hay nada que probar y que si $n = 2$ lo que afirma el corolario es precisamente lo que dice la Proposición 10.5.7. Supongamos entonces que $n \geq 3$ y sean $a_1, \ldots, a_n$ enteros coprimos con n. De acuerdo a la Proposición 10.5.7 existen enteros positivos r y s tales que el orden de $a_1^r a_2^s$ es $\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2))$. Por otro lado, la hipótesis inductiva obvia nos dice que existen enteros positivos $b_1, \ldots, b_{n-1}$ tales que el orden módulo m del entero

$$(a_1^r a_2^s)^{b_1} a_3^{b_2} \cdots a_n^{b_{n-1}} = a_1^{rb_1} a_2^{sb_1} a_3^{b_2} \cdots a_n^{b_{n-1}}$$

es

$$\mathsf{mcm}(\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2)), \mathsf{ord}_m(a_2), \ldots, \mathsf{ord}_m(a_n)),$$

que, de acuerdo al Ejercicio 6.6.4(*e*), es igual a

$$\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2), \mathsf{ord}_m(a_2), \ldots, \mathsf{ord}_m(a_n)).$$

Esto completa la inducción y, por lo tanto, la prueba del corolario. □

§10.6. Raíces primitivas

10.6.1. Podemos probar ahora un resultado fundamental, que tiene una demostración bastante delicada:

Proposición. *Sea p un número primo y sea $n \in \mathbb{N}$. El número de enteros a tales que $1 \leq a < p$ y $a^n \equiv 1 \mod p$ no supera a n.*

La hipótesis de que p sea primo es en general necesaria: por ejemplo, los cuatro números 1, 4, 11 y 14 tienen todos cuadrado congruente con 1 módulo 15.

Demostración. Todas las congruencias que consideraremos en esta demostración serán módulo p y siempre que calculemos un resto será de una división por p, así que no aclararemos esto nunca. Para cada $n \in \mathbb{N}$ consideremos el conjunto

$$R(n) \coloneqq \{a \in \mathbb{Z} : 1 \leq a < p,\ a^n \equiv 1\}$$

y, para llegar a un absurdo, supongamos que el conjunto $S = \{k \in \mathbb{N} : |R(k)| > k\}$ no es vacío. Sea n su menor elemento. Organizaremos lo que sigue, que es bastante largo, en varios pasos.

Primer paso. Sean $a_1, \ldots, a_t$ todos los elementos de $R(n)$, listados sin repeticiones, de manera que $t > n$, y sea $n' = \mathsf{mcm}(\mathsf{ord}_p(a_1), \ldots, \mathsf{ord}_p(a_t))$. Afirmamos que n' es igual a n.

En efecto, si i es un elemento cualquiera de $\{1, \ldots, t\}$, entonces $a_i^n \equiv 1$, así que $\mathsf{ord}_p(a_i)$ divide a n: como n' es el mínimo común múltiplos de los órdenes $\mathsf{ord}_p(a_1), \ldots, \mathsf{ord}_p(a_t)$, esto nos dice que n' divide a n. Por otro lado, si i pertenece a $\{1, \ldots, t\}$ entonces $\mathsf{ord}_p(a_i)$ divide a n', así que $a_i^{n'} \equiv 1$. Vemos así que todos los elementos $a_1, \ldots, a_t$ pertenecen a $R(n')$: si fuese $n' < n$, la forma en que elegimos a n implicaría entonces que $R(n')$ tiene a lo sumo n' elementos y esto es absurdo, ya que $n' < t$. Vemos así que $n' \geq n$. Como además n' divide a n, concluimos que, de hecho, es $n' = n$, como habíamos dicho.

Usando el Corolario 10.5.8, vemos que hay enteros positivos $\alpha_1, \ldots, \alpha_t$ tales que el orden del producto $a_1^{\alpha_1} \cdots a_t^{\alpha_t}$ es n. Si llamamos x al resto de la división de ese producto por p, entonces $1 \leq x < p$ y $\mathsf{ord}_p(x) = n$. En particular, la Proposición 10.5.3 nos dice que los n enteros

$$1,\ x,\ x^2,\ \ldots,\ x^{n-1} \tag{12}$$

son no congruentes dos a dos. Si $i \in \{0, \ldots, n-1\}$, entonces $(x^i)^n = (x^n)^i \equiv 1$ y por lo tanto los restos de los n números de la lista (12) son n elementos distintos de $R(n)$. Más aún, tenemos que

> *si d es un divisor propio de n, entonces $R(d)$ tiene exactamente d elementos, que son los restos de los enteros $1,\ x^{n/d},\ x^{2n/d},\ \ldots,\ x^{(d-1)n/d}$.* (13)

Para verlo, basta observar que si d es un divisor propio de n, entonces los restos de los d enteros $1,\ x^{n/d},\ x^{2n/d},\ \ldots,\ x^{(d-1)n/d}$ son distintos dos a dos y están en $R(d)$: como $d < n$, la forma en que elegimos n implica que $R(d)$ tiene a lo sumo d elementos y, por lo tanto, tienen que ser precisamente esos.

Segundo paso. Afirmamos que

> *todo elemento de $R(n)$ que no es congruente con ninguno de los enteros listados en (12) tiene orden n.*

Para verlo, supongamos que y es un elemento de $R(n)$ que no es congruente con ninguno de los números de (12) y sea m el orden de y. Como $y^n \equiv 1$, m divide a n. Supongamos por un momento que $m < n$, de manera que m es un divisor propio de n. De acuerdo a nuestra observación (13), los

elementos de $R(m)$ son entonces los restos de 1, $x^{n/m}$, $x^{2n/m}$, …, $x^{(m-1)n/m}$: como y pertenece a $R(m)$, vemos que y es congruente con alguno de ellos y esto es absurdo, dada la forma en que elegimos y. Esta contradicción nos dice que debe ser $m \geq n$. Como además m divide a n, tenemos en definitiva que $m = n$: el entero y tienen orden n, como queríamos ver.

Tercer paso. Sea y un elemento de $R(n)$ que no es congruente con ninguno de los enteros de la lista (12); que tal elemento existe es consecuencia de la forma en que elegimos al número n, por supuesto. Queremos probar ahora que

el número n es primo e impar.

Para ver esto, supongamos que por el contrario n es compuesto y sea q uno de sus divisores primos. Como $(y^q)^{n/q} = y^m \equiv 1$, el entero y^q es congruente a un elemento de $R(n/q)$. Como n/q es menor que n, nuestra observación (13) nos dice que los elementos de $R(n/q)$ son los restos de los enteros 1, x^q, x^{2q}, …, $x^{(n/q-1)q}$ y esto implica que y^q es congruente con uno de ellos. En otras palabras, existe $i \in \{0, \ldots, n/q - 1\}$ tal que $y^q \equiv x^{iq}$.

Como x^i es coprimo con p, sabemos que hay un entero z coprimo con p y tal que $zx^i \equiv 1$. Tenemos entonces que

$$(zy)^q \equiv z^p y^q \equiv z^q (x^i)^q \equiv (zx^i)^q \equiv 1,$$

así que el resto de zy pertenece a $R(q)$. Como los elementos de $R(q)$ son los restos de 1, $x^{n/q}$, …, $x^{(q-1)n/q}$ vemos que $zy \equiv x^j$ para algún entero no negativo j. Se sigue de esto que $x^{i+j} \equiv x^i x^j \equiv x^i zy \equiv y$ y esto es absurdo en vista de la forma en que elegimos a y. Esta contradicción muestra que n tiene que ser primo.

Si z en un elemento de $R(2)$, tenemos que $z^2 \equiv 1$ y, por lo tanto, que p divide a $z^2 - 1 = (z+1)(z-1)$. Esto significa que z es congruente o a 1 o a -1 y, como $1 \leq z < p$, que de hecho z es o bien 1 o bien $p - 1$. Vemos así que $R(2)$ tiene a lo sumo dos elementos y entonces la forma en que elegimos n nos dice que $n > 2$. Así, n es necesariamente un primo impar.

Cuarto paso. Para cada entero u consideramos el producto

$$f(u) \coloneqq (1-u)(x-u)(x^2-u)\cdots(x^{n-1}-u). \tag{14}$$

En particular, tenemos que

$$f(xu) = (1-xu)(x-xu)(x^2-xu)\cdots(x^{n-1}-xu) \tag{15}$$

Ahora bien, para cada $j \in \{1, \ldots, n-1\}$ tenemos que

$$x^j - xu \equiv \begin{cases} x(x^{n-1}-u), & \text{si } j = 1; \\ x(x^{j-1}-u), & \text{si } 1 \leq j < n. \end{cases}$$

Usando esto con cada uno de los factores del producto de (15), vemos que

$$f(xu) \equiv x^n(x^{n-1}-u)(1-u)(x-u)\cdots(x^{n-2}-u)$$

y, como $x^n \equiv 1$ y los n factores finales que aparecen en este producto son los mismos que aparecen en (14) salvo que en otro orden, que

$$f(xu) \equiv f(u).$$

Esta igualdad es cierta cualquiera sea el entero u: haciendo tomar a u los valores u, xu, x^2u, …, $x^{n-2}u$, en orden, vemos inmediatamente que para todo entero u se tiene que

$$f(u) \equiv f(xu) \equiv f(x^2u) \equiv \cdots \equiv f(x^{n-1}u). \tag{16}$$

Quinto paso. Volvamos ahora a considerar el producto $f(u)$ de (14): si distribuimos todos los productos que allí aparecen, obteniendo de esa forma 2^n sumandos, y los asociamos luego de acuerdo a la potencia de u que tienen como factor, encontramos que

$$f(u) = c_0 + c_1u + c_2u^2 + \cdots + c_nu^n \tag{17}$$

para ciertos enteros $c_0, \ldots, c_n$, cada uno de los cuales es una suma con signos de productos de las potencias $1, x, \ldots, x^{n-1}$. Nos interesan en particular dos de ellos:

- El entero c_0 es igual a $1 \cdot x \cdot x^2 \cdots x^{n-1} = x^{n(n-1)/2}$. Como n es impar, el cociente $(n-1)/2$ es un entero, y entonces $c_0 = (x^n)^{(n-1)/2} \equiv 1$.
- Por otro lado, es claro que $c_n = (-1)^n = -1$, ya que n es impar.

Gracias las congruencias (16), tenemos que

$$\begin{aligned} nf(u) &= \underbrace{f(u) + f(u) + f(u) + \cdots + f(u) + \cdots + f(u)}_{n \text{ sumandos}} \\ &\equiv f(u) + f(xu) + f(x^2u) + \cdots + f(x^i) + \cdots + f(x^{n-1}u) \end{aligned}$$

Si usamos ahora la expresión (17) para cada sumando y luego cambiamos el orden de sumación, vemos que

$$nf(u) \equiv \sum_{i=0}^{n-1}\sum_{j=0}^{n} c_j x^{ij} u^j = \sum_{j=0}^{n}\left(\sum_{i=0}^{n-1} x^{ij}\right) c_j u^j$$

Cuando $j = 0$, la suma entre paréntesis es $\sum_{i=0}^{n-1} x^0 = n$. Cuando $j = n$, esa suma es $\sum_{i=0}^{n-1}(x^n)^i \equiv n$, ya que $x^n \equiv 1$. Finalmente, si $0 < j < n$, esa suma es igual a

$$\sum_{i=0}^{n-1}(x^j)^i = 0,$$

ya que el orden de x^j es n. Usando esto, vemos que $nf(u) \equiv nc_0 + nc_n u^n$ y, como n es coprimo con p, que de hecho

$$f(u) = c_0 + c_n u^n \equiv 1 - u^n.$$

Esto vale para todo entero u. En particular, como $y \in R(n)$, tenemos que

$$(1-y)(1-y^2)\cdots(x^{n-1}-y) = f(y) \equiv 1 - y^n \equiv 0$$

y, por lo tanto, que p divide al producto $(1-y)(1-y^2)\cdots(x^{n-1}-y)$. Como p es primo, esto implica que existe $i \in \{0, \ldots, n-1\}$ tal que p divide a $x^i - y$, esto es, tal que $y \equiv x^i$. Esto es absurdo, ya que elegimos a y de manera que no sea congruente con ninguno de los enteros listados en (12). Esta contradicción nos dice que nuestra hipótesis de partida es insostenible y, en consecuencia, que la proposición es cierta. □

10.6.2. La Proposición 10.6.1 nos permite probar fácilmente el siguiente resultado bastante sorprendente y notado por primera vez por Gauss —de hecho, la demostración que damos es exactamente la que él da en sus *Disquisitiones*.

Proposición. *Sea p un número primo y sea n un divisor positivo de $p-1$. El número de enteros a tales que $1 \leq a < p$ que tienen orden n es $\varphi(n)$.*

Demostración. Para cada divisor positivo d de $p-1$ consideremos el conjunto

$$\Psi(d) \coloneqq \{a \in \mathbb{Z} : 1 \leq a < p,\ \mathsf{ord}_p(a) = d\}$$

y sea $\psi(d) \coloneqq |\Psi(d)|$ su cardinal. Como cada entero entre 1 y $p-1$ tiene un orden módulo p que es un divisor de $p-1$, tenemos que

$$\{a \in \mathbb{Z} : 1 \leq a < p\} = \bigcup_{d \mid p-1} \Psi(d),$$

con el índice d de la unión recorriendo los divisores positivos de $p-1$, y claramente esta unión es disjunta. Tomando cardinales a ambos lados de esta igualdad, vemos que

$$p - 1 = \sum_{d \mid p-1} \psi(d). \tag{18}$$

Por otro lado, supongamos que d es un divisor positivo de $p-1$ y que $\psi(d) > 0$, de manera que existe un entero y tal que $1 \leq y < p$ y $\mathsf{ord}_p(y) = d$. En ese caso, sabemos que los restos módulo p de los enteros $1,\ y,\ y^2,\ \ldots,\ y^{d-1}$ son distintos dos a dos y, por lo tanto, de acuerdo a la Proposición 10.6.1, todo número cuya potencia d-ésima es congruente con 1 módulo p es

congruente a uno de ellos. En particular, todos los enteros que tienen orden d son congruentes a una de estas d potencias de y. Si $i \in \{0, \ldots, d-1\}$, sabemos que el orden de y^i es $d/\mathsf{mcd}(d, i)$: esto nos dice que y^i tiene orden d si y solamente si i es coprimo con d. Concluimos de esta forma que el número $\psi(d)$ es o bien 0 o bien $\varphi(d)$.

Esto nos dice que para todo divisor positivo d de $p-1$ se tiene que

$$\psi(d) \leq \varphi(d) \tag{19}$$

y, por lo tanto, que

$$\sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d), \tag{20}$$

ya que cada sumando de la primera suma es menor o igual que el correspondiente sumando de la segunda.

Ahora bien, si para algún divisor positivo d_0 de $p-1$ fuera $\psi(d_0) < \varphi(d_0)$, teniendo en cuenta (18), (19), (20) y la Proposición 10.2.5 tendríamos que

$$p-1 = \sum_{d|p-1} \psi(d) < \sum_{d|p-1} \varphi(d) = p-1.$$

Como esto es imposible, vemos que lo que afirma la proposición es cierto. □

10.6.3. La consecuencia más importante de las dos proposiciones que acabamos de probar es:

Corolario. *Sea p un número primo. Existen enteros a tales que $1 \leq a < p$ y que tienen orden $p-1$ módulo p y hay, de hecho, $\varphi(p-1)$ de ellos.*

Demostración. En efecto, esto es precisamente lo que nos dice la Proposición 10.6.2 cuando $n = p-1$. □

10.6.4. Cuando m es un entero positivo y a es un entero coprimo con m tal que $1 \leq a < m$ y $\mathsf{ord}_m(a) = \varphi(m)$ decimos que a es una ***raíz primitiva*** módulo m. Gauss define esta noción en el Párrafo 57 de sus *Disquisitiones*.

El Corolario 10.6.3 que acabamos de probar afirma que si p es un número primo entonces existen $\varphi(p-1)$ raíces primitivas módulo p. Si a es una raíz primitiva módulo p, sabemos de la Proposición 10.5.3 que las $p-1$ potencias

$$1,\ a,\ a^2,\ \ldots,\ a^{p-2}$$

son coprimas con p y no congruentes módulo p dos a dos, así que sus restos módulo p son precisamente los elementos de $\{1, \ldots, p-1\}$, listados en algún orden.

Por ejemplo, 3 es una raíz primitiva módulo 7, ya que sus primeras potencias son

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \mod 7.$$

El Corolario **10.6.3** nos dice que módulo 7 hay $\varphi(7-1) = 2$ raíces primitivas: la otra es 5 y la correspondiente lista de potencias es

$$5^0 \equiv 1, \quad 5^1 \equiv 5, \quad 5^2 \equiv 4, \quad 5^3 \equiv 6, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1 \mod 7.$$

En la Tabla 10.1 en la página siguiente damos las listas de las raíces primitivas para los primeros primos.

10.6.5. Decidir si un entero a es una raíz primitiva módulo un número primo p no es fácil. Si podemos factorizar a $p-1$, entonces la siguiente proposición nos da un criterio razonable:

Proposición. *Sea p un número primo, sean $q_1, \ldots, q_r$ los divisores primos de $p-1$ y sea a un entero tal que $1 \leq a < p-1$. Si $a^{(p-1)/q_i} \not\equiv 1 \mod p$ para cada $i \in \{1, \ldots, r\}$, entonces a es una raíz primitiva módulo p.*

Así, por ejemplo, el número $p = 503$ es primo y $2 \cdot 251$ es la factorización en factores primos de $p-1$: como $2^2 \equiv 4$ y $2^{251} \equiv 2$ módulo 503, vemos que 2 es una raíz primitiva módulo 503.

Demostración. Sea n el orden de a módulo p y supongamos que a no es una raíz primitiva. Sabemos que n divide a $p-1$. Como la hipótesis implica que $n \neq p-1$, existe un primo q que divide a n tal que $v_q(n) < v_q(p-1)$ y, en particular, n divide a $(p-1)/q$. Si k es el cociente de esa división, tenemos entonces que $a^{(p-1)/q} = (a^n)^k \equiv 1 \mod p$. Esto prueba la implicación contrarrecíproca a la del enunciado. □

10.6.6. Un segundo problema que aparece cuando queremos encontrar una raíz primitiva módulo un primo p es el de decidir cómo elegir qué enteros a probar. Para esto no se conoce ninguna estrategia efectiva y normalmente lo que hacemos es elegir candidatos al azar entre 1 y $p-1$. Esto tiene sentido, porque la proporción de números en ese rango que son raíces primitivas es, de acuerdo a la Proposición **10.2.3**,

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_r}\right)$$

con $q_1, \ldots, q_r$ los primos que dividen a $p-1$, y este número no es muy cercano a 0. Los factores que aparecen a la derecha son todos menores que 1 y están más cerca de 1 mientras mayores son los divisores primos de $p-1$: esto nos dice que si p es tal que $p-1$ tiene pocos divisores primos y estos son grandes, entonces la proporción de raíces primitivas entre los elementos de $\{1, \ldots, p-1\}$ es relativamente alta.

p	
2	1
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24
37	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35
41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
61	2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59
67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63
71	7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69
73	5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68
79	3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77
83	2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80
89	3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86
97	5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92

Tabla 10.1. Raíces primitivas para primos menores que 100.

Por ejemplo, el número $p = 900^{16} + 1$ es primo (probaremos esto en 10.6.14, más adelante) y $p - 1 = 2^{32} \cdot 3^{32} \cdot 5^{32}$, así que la proporción de raíces primitivas módulo p es en este caso

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{4}{15} \approx 0{,}266\,666\ldots,$$

así que cada cuatro números elegidos al azar entre 1 y $p - 1$ es razonable esperar que uno sea una raíz primitiva módulo p.

Una primera aplicación: el Teorema de Wilson

10.6.7. Como primera aplicación de la existencia de raíces primitivas módulo un número primo, podemos dar una nueva demostración del Teorema de Wilson:

Proposición. *Un entero $p > 1$ es primo si y solamente si $(p-1)! \equiv -1 \mod p$.*

Demostración. Sea p un entero mayor que 1. Veamos primero que la condición del enunciado es necesaria para que p sea primo. Si $p = 2$, entonces es inmediato que esa condición se cumple, así que bastará que consideremos el caso en que p es un número primo impar.

Sea a una raíz primitiva módulo p. Sabemos que los restos de dividir por p a los enteros

$$1,\ a,\ a^2,\ \ldots,\ a^{p-2} \tag{21}$$

son los números

$$1,\ 2,\ 3,\ \ldots,\ p-1 \tag{22}$$

listados en algún orden. En particular, el producto de los $p - 1$ enteros de (21) es congruente módulo p con el producto de los de (22), esto es,

$$(p-1)! \equiv a^0 \cdot a^1 \cdot a^2 \cdot \ldots \cdot a^{p-2} = a^{(p-1)(p-2)/2} \mod p. \tag{23}$$

Sabemos que en $\{1, \ldots, p-1\}$ hay a lo sumo dos enteros con cuadrado congruente con 1 módulo p. Como $1^1 \equiv (p-1)^2 \equiv 1$, vemos que hay exactamente dos tales enteros y que son 1 y $p - 1$. Por otro lado, el teorema de Fermat 10.1.4 nos dice que

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \mod p,$$

es congruente con 1 módulo p, así que $a^{(p-1)/2}$ es congruente o con 1 o con -1. Como el orden de a es $p - 1$, no puede ser que $a^{(p-1)/2} \equiv 1$, así que debe ser necesariamente $a^{(p-1)/2} \equiv -1$. Finalmente, como p es impar, tenemos que

$$a^{(p-1)(p-2)/2} = (a^{(p-1)/2})^{p-2} \equiv (-1)^{p-2} \equiv -1 \mod p.$$

Esto junto con (23) nos dice que $(p-1)! \equiv -1 \mod p$, como queremos.

Veamos ahora la suficiencia de la condición. Si el entero p no es primo, entonces tiene un divisor d distinto de 1: como $1 < d < p$, es claro que d divide a $(p-1)!$ y, por lo tanto, que no divide a $(p-1)!+1$. Esto implica que esta suma tampoco es divisible por p y, en consecuencia, que $(p-1)! \not\equiv -1 \mod p$. □

Una segunda aplicación: el criterio de Euler

10.6.8. Veamos ahora como usar la existencia de raíces primitivas para obtener un criterio de Euler para decidir si que un número es congruente a un cuadrado módulo un primo.

Proposición. *Sea p un número primo. Un entero a coprimo con p es congruente a un cuadrado módulo p si y solamente si $a^{(p-1)/2} \equiv 1 \mod p$.*

Observemos que el teorema de Fermat 10.1.4 nos dice que $a^{(p-1)/2}$ tiene cuadrado congruente con 1 módulo p, así que es congruente o bien a 1 o bien a -1.

Demostración. Si hay un entero b tal que $a \equiv b^2 \mod p$, entonces el teorema de Fermat 10.1.4 nos dice que

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \mod p.$$

Esto muestra que la condición de la proposición es necesaria. Veamos que es también suficiente.

Sea r una raíz primitiva módulo p, de manera que, en particular, existe un entero no negativo i tal que $a \equiv r^i \mod p$. Si suponemos que la condición del enunciado vale, entonces tenemos que

$$1 \equiv a^{(p-1)/2} \equiv r^{i(p-1)/2} \mod p.$$

Como r tiene orden módulo p igual a $p-1$, esto implica que $p-1$ divide a $i(p-1)/2$, lo que es posible sólo si i es par, digamos $i = 2j$ para algún entero j. Pero entonces es $a \equiv r^i \equiv (r^j)^2 \mod p$ y a es congruente a un cuadrado módulo p. □

10.6.9. Usando el criterio de Euler 10.6.8 podemos describir muy concretamente con respecto a qué primos -1 es congruente a un cuadrado. Este resultado es conocido habitualmente como el *Primer Suplemento a la Ley de Reciprocidad Cuadrática*.

Corolario. *Sea p un número primo impar. Hay un entero x tal que $x^2 \equiv -1 \mod p$ si y solamente si $p \equiv 1 \mod 4$.*

Demostración. De acuerdo al criterio de Euler 10.6.8, el entero -1 es congruente a un cuadrado módulo p si y solamente si $(-1)^{(p-1)/2} \equiv 1 \mod p$. Ahora bien, como p es impar, es o bien de la forma $4k+1$ o bien de la forma $4k+3$, para algún entero no negativo k. En el primer caso se tiene que $(-1)^{(p-1)/2} = (-1)^{2k} = 1$ y en el segundo que $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. Como p no es 2, $-1 \not\equiv 1 \mod p$. Esto prueba el corolario. □

10.6.10. El criterio de Euler 10.6.8 nos permite probar también el llamado *Segundo Suplemento a la Ley de Reciprocidad Cuadrática*:

Corolario. *Sea p un número primo impar. Existe un entero x tal que $x^2 \equiv 2 \mod p$ si y solamente si 16 divide a $p^2 - 1$.*

Como p es impar, es congruente a 1 o a 3 módulo 4, y usando esto es fácil ver que $(p^2-1)/8$ es un entero. La condición del corolario es entonces que este entero sea par.

Demostración. Sea $s = (p-1)/2$. Es

$$s! = \prod_{1\le k\le s} k = \prod_{1\le k\le s} \left((-1)^k k \cdot (-1)^k\right) = \prod_{1\le k\le s} ((-1)^k k) \cdot \prod_{1\le k\le s} (-1)^k. \tag{24}$$

Sabemos que

$$\prod_{1\le k\le s} (-1)^k = (-1)^{1+2+\cdots+s} = (-1)^{s(s+1)/2}. \tag{25}$$

Por otro lado,

$$\prod_{1\le k\le s} ((-1)^k k) = \prod_{\substack{1\le k\le s\\ k \text{ par}}} ((-1)^k k) \cdot \prod_{\substack{1\le k\le s\\ k \text{ impar}}} ((-1)^k k) = \prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{0\le l\le \frac{s-1}{2}} (-(2l+1)).$$

Como $-(2l+1) \equiv 2(s-l) \mod p$ para todo entero l, este último producto es congruente módulo p con

$$\prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{0\le l\le \frac{s-1}{2}} (2(s-l)).$$

Cambiando el índice del segundo producto, podemos reescribir esto en la forma

$$\prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{\frac{s+1}{2}\le l\le s} (2l)$$

y si consideramos ahora con cuidado qué factores aparecen aquí vemos que este producto es igual a $2^s s!$. Usando esto y (25) en la igualdad (24) vemos que

$$s! \equiv (-1)^{s(s+1)/2} 2^s s! \mod p.$$

Como $s!$ es coprimo con p, esto implica inmediatamente que

$$2^s \equiv (-1)^{s(s+1)/2} = (-1)^{(p^2-1)/8} \mod p.$$

De acuerdo al criterio de Euler 10.6.8, vemos que 2 es congruente con un cuadrado módulo p si y solamente si el entero $(p^2-1)/8$ es par, es decir, si y solamente si 16 divide a p^2-1. □

Una tercera aplicación: raíces primitivas para primos seguros

10.6.11. No hay muchos resultados que nos den raíces primitivas. Uno muy conocido es:

Proposición. *Sea p un número primo tal que $2p+1$ es también primo. Si además $p \equiv 1 \mod 4$, entonces 2 es una raíz primitiva módulo $2p+1$.*

Así, 2 es una raíz primitiva módulo $83 = 2 \cdot 41 + 1$.

Demostración. Sea p un número primo tal que $p \equiv 1 \mod 4$ y $q = 2p+1$ es primo. El orden de 2 módulo q, cualquiera que sea, es un divisor de $q-1 = 2p$, así que es o 1, o 2, o p, o $2p$. Como $q > 4$, es claro que ni 2^1 ni 2^2 son congruentes a 1 módulo q: esto nos dice que $\mathsf{ord}_q(2)$ no es ni 1 ni 2. Por otro lado, la Proposición 10.6.8 nos dice que $2^p = 2^{(q-1)/2}$ es congruente módulo q a 1 si y solamente si 2 es congruente a un cuadrado módulo q, y según el Corolario 10.6.10 esto ocurre si y solamente si 16 divide a q^2-1. Como $p \equiv 1 \mod 4$, existe $k \in \mathbb{N}$ tal que $p = 4k+1$: usando esto, vemos que

$$q^2 - 1 = (2p+1)^2 - 1 = 4p^2 + 4p = 4(4k+1)^2 + 4(4k+1) = 64k^2 + 48k + 8.$$

Como este número no es divisible por 16, vemos que $2^p \not\equiv 1 \mod q$ y, por lo tanto, $\mathsf{ord}_q(2) \neq p$. La única posibilidad que queda, entonces, es que el orden de 2 módulo q sea $2p = q-1$ y esto significa que 2 es una raíz primitiva módulo q. □

10.6.12. Un número primo p tal que $2p+1$ también es primo, como en la proposición que acabamos de probar, se llama un ***primo de Sophie Germain***, por, precisamente, Sophie Germain, quien los consideró en medio de su trabajo sobre el Último Teorema de Fermat. Si p es un primo de Sophie Germain, decimos que el primo $2p+1$ es un ***primo seguro***.

Los primeros primos de Sophie Germain son

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953, 1 013, 1 019, 1 031, 1 049, 1 103, 1 223, 1 229, 1 289, 1 409, 1 439, 1 451, 1 481, 1 499, 1 511, 1 559, …

y se conjetura que hay infinitos; puede encontrarse más información sobre esta sucesión de números

en [OEI2023, A005384]. El más grande de ellos que conocemos (en 2016) es

$$2\,618\,163\,402\,417 \cdot 2^{1\,290\,000} - 1,$$

que tiene 388 342 dígitos decimales.

Germain aprendió matemáticas en su infancia, leyendo los libros que su padre tenía en la biblioteca — aprendió por sí misma latín poder leer a Newton y a Euler — aunque sus padres no veían esto con buenos ojos: la matemática no era considerada algo muy apropiado para las mujeres. Cuando en 1794 se fundó, como parte de la Revolución Francesa, la Escuela Politécnica en París, Germain no podía asistir a las clases porque que la entrada estaba prohibida a las mujeres, pero pudo empezar sus estudios de manera no presencial — adoptando el nombre de Monsieur Antoine-August Le Blanc, para ocultar su identidad — con Joseph Louis Lagrange como tutor. Después de un tiempo, Lagrange, que estaba impresionado con las habilidades de su 'alumno', pidió conocerlo. Ella accedió y él no tuvo mayor problema con la situación.

A lo largo de su vida Germain interactuó por carta y siempre con su seudónimo masculino con varios de los más grandes matemáticos de su época — sobre todo con Adrien-Marie Legendre y Carl Friedrichs Gauss. Gauss fue uno de los pocos a quienes reveló su verdadera identidad. Por carta, Gauss le respondió:

> *Pero cómo describirte mi admiración y asombro al ver que mi estimado corresponsal Sr. Le Blanc se metamorfosea en este personaje ilustre que me ofrece un ejemplo tan brillante de lo que sería difícil de creer. La afinidad por las ciencias abstractas en general y sobre todo por los misterios de los números es demasiado rara: lo que no me asombra ya que los encantos de esta ciencia sublime solo se revelan a aquellos que tienen el valor de profundizar en ella. Pero cuando una persona del sexo que, según nuestras costumbres y prejuicios, debe encontrar muchísimas más dificultades que los hombres para familiarizarse con estos espinosos estudios, y sin embargo tiene éxito al sortear los obstáculos y penetrar en las zonas más oscuras de ellos, entonces sin duda esa persona debe tener el valor más noble, el talento más extraordinario y un genio superior. De verdad que nada podría probarme de forma tan meridiana y tan poco equívoca que los atractivos de esta ciencia que ha enriquecido mi vida con tantas alegrías no son quimeras que las predilección con la que tú has hecho honor a ella.*

Un criterio de primalidad

10.6.13. Es interesante que el Corolario 10.6.3 nos dice que para todo primo hay una raíz primitiva tiene un recíproco parcial:

Proposición. *Sea $m \in \mathbb{N}$. Si existe un entero coprimo con m y de orden $m-1$, entonces m es primo.*

Demostración. En efecto, supongamos que a es un entero coprimo con m y cuyo orden módulo m es $m-1$. En ese caso, los enteros $1, a, a^2, \ldots, a^{m-2}$ son no congruentes módulo m dos a dos. En particular, los restos módulo m de esos $m-1$ números son todos números coprimos con m distintos y que pertenecen al conjunto $S = \{1, \ldots, p-1\}$: esto significa que esos restos son *todos* los elementos de S y, por lo tanto, que todos los elementos de S son coprimos con m. Por supuesto, esto implica inmediatamente que m no posee divisores propios, así que es un número primo. □

10.6.14. Consideremos el número $m = 2^{16} + 1 = 65\,537$. Calculando las potencias elevando al cuadrado repetidas veces, vemos inmediatamente que $3^{2^{15}} \equiv 65\,536$ mientras que $3^{2^{16}} \equiv 1$, todo módulo m. Esto nos dice que 3 tiene orden $m-1$ módulo m y, por lo tanto, que m es primo. Notemos que pudimos concluir esto hacer esto calculando solamente 16 cuadrados y 16 restos módulo m.

Sea, por otro lado, $m = 900^{16} + 1$, que es el número

185 302 018 885 184 100 000 000 000 000 000 000 000 000 000 001

de 48 dígitos. En este caso $m - 1 = 2^{32} \cdot 3^{32} \cdot 5^{32}$. Podemos calcular que $11^{m-1} \equiv 1 \mod m$ haciendo 159 multiplicaciones. Otras 471 multiplicaciones nos permiten concluir que módulo m es

$$11^{(m-1)/2} \equiv 185\,302\,018\,885\,184\,100\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000,$$
$$11^{(m-1)/3} \equiv 23\,872\,712\,020\,769\,780\,231\,829\,076\,893\,206\,244\,805\,098\,674\,046,$$
$$11^{(m-1)/6} \equiv 105\,301\,962\,497\,401\,089\,637\,352\,963\,399\,740\,744\,918\,642\,299\,597.$$

Así, 11 tiene orden $m-1$ módulo m y, en consecuencia, m es primo. Pudimos probar esto calculando 630 productos y unos 630 restos. Si hubiéramos intentando verificar que es primo probando con la división por todos los enteros menores que $\sqrt{m}$ y a cada una de esas divisiones la hubiéramos hecho en una milésima de segundo, el proceso completo nos hubiera llevado unos trece millones de millones de años —esto es unas mil veces más que la edad del universo, según los cálculos más recientes [PAA+2016].

Referencias

[AGHS2014] William Robert Alford, Jon Grantham, Steven Hayman, y Andrew Shallue, *Constructing Carmichael numbers through improved subset-product algorithms*, Math. Comp. **83** (2014), no. 286, 899–915. MR3143697

[AGP1994] William Robert Alford, Andrew Granville, y Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR1283874

[AÖ2001] A. Göksel Ağargün y E. Mehmet Özkan, *A historical survey of the fundamental theorem of arithmetic*, Historia Math. **28** (2001), no. 3, 207–214. MR1849798

[AÖ1997] A. Göksel Ağargün y E. Mehmet Özkan, *The fundamental theorem of arithmetic dissected*, Mathematica Gazette **81** (1997), no. 490, 53–57.

[Bac1990] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR1023756

[BS1956] Georges Browkin y André Schinzel, *Sur les nombres de Mersenne qui sont triangulaires*, C. R. Acad. Sci. Paris **242** (1956), 1780–1781. MR77546

[BSST1940] R. L. Brooks, C. A. B. Smith, A. H. Stone, y W. T. Tutte, *The dissection of rectangles into squares*, Duke Math. J. **7** (1940), 312–340. MR3040

[Can1872] Georg Cantor, *Ueber die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen*, Math. Ann. **5** (1872), no. 1, 123–132. MR1509769

[Can1897] Georg Cantor, *Beiträge zur Begründung der transfiniten Mengenlehre*, Math. Ann. **49** (1897), no. 2, 207–246. MR1510964

[Car1912] Robert Daniel Carmichael, *On Composite Numbers P Which Satisfy the Fermat Congruence* $a^{P-1} \equiv 1 \bmod P$, Amer. Math. Monthly **19** (1912), no. 2, 22–27. MR1517641

[Ces1894] Ernesto Cesàro, *Sur une formule empirique de M. Pervouchine*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences **119** (1894), 848–849.

[Cip1904] Michele Cipolla, *Sui numeri composti, p, che verificano la congruenza di fermat* $a^{p-1} = 1 \pmod{p}$, Annali di Matematica **3** (1904), no. 9, 139–160.

[Deh1903] M. Dehn, *Über Zerlegung von Rechtecken in Rechtecke*, Math. Ann. **57** (1903), no. 3, 314–332. MR1511212

[dLVP1896a] Charles-Jean de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers. Deuxième partie. Les fonctions de Dirichlet et les nombres premiers de la forme linéaire $mx + na$*, Ann. Soc. Scient. Bruxelles, deuxième partie **20** (1896), 281–362.

[dLVP1896b] Charles-Jean de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers. Première partie. La fonction $\zeta(z)$ de Riemann et les nombres premiers en général, suivi d'un Appendice sur des réflexions applicables à une formule donnée par Riemann*, Ann. Soc. Scient. Bruxelles, deuxième partie **20** (1896), 183–256.

[dLVP1896c] Charles-Jean de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers. Troisième partie. Les formes quadratiques de déterminant négatif, suivi d'une Note sur une démonstration de M. Hadamard et sur une simplification de la première partie, et d'une Rectification à la première partie*, Ann. Soc. Scient. Bruxelles, deuxième partie **20** (1896), 368–397.

[dLVP1897a] Charles-Jean de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers. Cinquième partie. Nombres premiers représentables simultanuément par une forme linéaire et une forme quadratique*, Ann. Soc. Scient. Bruxelles, deuxième partie **21** (1897), 343–368.

[dLVP1897b] Charles-Jean de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers. Quatrième partie. Les nombres premiers représentables par une forme quadratique de déterminant positif*, Ann. Soc. Scient. Bruxelles, deuxième partie **21** (1897), 251–342.

[Erd1938] Paul Erdős, *Über die Reihe $\sum 1/p$*, Mathematica (Zutphen) **B7** (1938), 1–2.

[Eul1744] Leonhard Euler, *Variae observationes circa series infinitas*, Commentarii academiae scientiarum Petropolitanae **9** (1744), 160–188.

[Fel1776] Anton Felkel, *Tafel aller einfachen factoren der durch 2, 3, 5 nicht theilbaren zahlen von 1 bis 10000000. entworfen von anton felkel, lehrer an der k. k. normalschule*, Ghelen, Wien, 1776, http://resolver.sub.uni-goettingen.de/purl?PPN620758449.

[Grü1992a] Branko Grünbaum, *Venn diagrams. I*, Geombinatorics **1** (1992), no. 4, 5–12. MR1208440

[Grü1992b] Branko Grünbaum, *Venn diagrams. II*, Geombinatorics **2** (1992), no. 2, 25–32. MR1208448

[Had1896] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France **24** (1896), 199–220. MR1504264

[Har2008] Glyn Harman, *Watt's mean value theorem and Carmichael numbers*, Int. J. Number Theory **4** (2008), no. 2, 241–248. MR2404800

[Hen1963] David W. Henderson, *Classroom Notes: Venn Diagrams for More than Four Classes*, Amer. Math. Monthly **70** (1963), no. 4, 424–426. MR1532112

[HW2008] G. H. Hardy y E. M. Wright, *An introduction to the theory of numbers*, Sixth, Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. MR2445243

[IOfS-IEC2017] International Organization for Standarization – International Electrotechnical Commission, *Annex B: Luhn formula for computing modulus-10. Identification cards — Identification of issuers — Part 1: Numbering system*, 2017. ISO/IEC 7812-1:2017.

[Jac1834] Carl Gustav Jacob Jacobi, *De usu legitimo formulae summatoriae Maclauriniana.*, Zenodo, 1834, https://doi.org/10.1017/cbo9781139568005.007.

[Jae1993] Gerhard Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), no. 204, 915–926. MR1192971

[Ken1996] Richard Kenyon, *Tiling a rectangle with the fewest squares*, J. Combin. Theory Ser. A **76** (1996), no. 2, 272–291. MR1416017

[Knu1969] Donald E. Knuth, *The art of computer programming. Vol. 2: Seminumerical algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR286318

[Knu1993] Donald E. Knuth, *Johann Faulhaber and sums of powers*, Math. Comp. **61** (1993), no. 203, 277–294. MR1197512

[KO1962] Anatoly Karatsuba y Yuri Ofman, *Multiplication of many-digital numbers by automatic computers*, Dokl. Akad. Nauk SSSR **145** (1962), no. 2, 293–294.

[Kor1899] Alwin Reinhold Korselt, *Problème chinois*, L'Interm. des Maths. **6** (1899), 142–143.

[Kos2009] Thomas Koshy, *Catalan numbers with applications*, Oxford University Press, Oxford, 2009.

[Lar2023] Daniel Larsen, *Bertrand's postulate for Carmichael numbers*, Int. Math. Res. Not. IMRN **15** (2023), 13072–13098. MR4621859

[Luh1960] Hans Peter Luhn, *Computer for verifying numbers*, 1960. U.S. patent 2950048A.

[Mea1973] D. G. Mead, *The equation of Ramanujan-Nagell and* $[y^2]$, Proc. Amer. Math. Soc. **41** (1973), 333–341. MR327725

[Mil1976] Gary L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), no. 3, 300–317. MR480295

[New1980] Donald Joseph Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), no. 9, 693–696. MR602825

[OEI2023] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, 2023, `https://oeis.org`.

[PAA+2016] Planck Collaboration, Ade, P. A. R., Aghanim, N., Arnaud, M., Ashdown, M., Aumont, J., Baccigalupi, C., Banday, A. J., Barreiro, R. B., Bartlett, J. G., Bartolo, N., Battaner, E., Battye, R., Benabed, K., Benoît, A., Benoit-Lévy, A., Bernard, J.-P., Bersanelli, M., Bielewicz, P., Bock, J. J., Bonaldi, A., Bonavera, L., Bond, J. R., Borrill, J., Bouchet, F. R., Boulanger, F., Bucher, M., Burigana, C., Butler, R. C., Calabrese, E., Cardoso, J.-F., Catalano, A., Challinor, A., Chamballu, A., Chary, R.-R., Chiang, H. C., Chluba, J., Christensen, P. R., Church, S., Clements, D. L., Colombi, S., Colombo, L. P. L., Combet, C., Coulais, A., Crill, B. P., Curto, A., Cuttaia, F., Danese, L., Davies, R. D., Davis, R. J., de Bernardis, P., de Rosa, A., de Zotti, G., Delabrouille, J., Désert, F.-X., Di Valentino, E., Dickinson, C., Diego, J. M., Dolag, K., Dole, H., Donzelli, S., Doré, O., Douspis, M., Ducout, A., Dunkley, J., Dupac, X., Efstathiou, G., Elsner, F., Enßlin, T. A., Eriksen, H. K., Farhang, M., Fergusson, J., Finelli, F., Forni, O., Frailis, M., Fraisse, A. A., Franceschi, E., Frejsel, A., Galeotta, S., Galli, S., Ganga, K., Gauthier, C., Gerbino, M., Ghosh, T., Giard, M., Giraud-Héraud, Y., Giusarma, E., Gjerløw, E., González-Nuevo, J., Górski, K. M., Gratton, S., Gregorio, A., Gruppuso, A., Gudmundsson, J. E., Hamann, J., Hansen, F. K., Hanson, D., Harrison, D. L., Helou, G., Henrot-Versillé, S., Hernández-Monteagudo, C., Herranz, D., Hildebrandt, S. R., Hivon, E., Hobson, M., Holmes, W. A., Hornstrup, A., Hovest, W., Huang, Z., Huffenberger, K. M., Hurier, G., Jaffe, A. H., Jaffe, T. R., Jones, W. C., Juvela, M., Keihänen, E., Keskitalo, R., Kisner, T. S., Kneissl, R., Knoche, J., Knox, L., Kunz, M., Kurki-Suonio, H., Lagache, G., Lähteenmäki, A., Lamarre, J.-M., Lasenby, A., Lattanzi, M., Lawrence, C. R., Leahy, J. P., Leonardi, R., Lesgourgues, J., Levrier, F., Lewis, A., Liguori, M., Lilje, P. B., Linden-Vørnle, M., López-Caniego, M., Lubin, P. M., Macías-Pérez, J. F., Maggio, G., Maino, D., Mandolesi, N., Mangilli, A., Marchini, A., Maris, M., Martin, P. G., Martinelli, M., Martínez-González, E., Masi, S., Matarrese, S., McGehee, P., Meinhold, P. R., Melchiorri, A., Melin, J.-B., Mendes, L., Mennella, A., Migliaccio, M., Millea, M., Mitra, S., Miville-Deschênes, M.-A., Moneti, A., Montier, L., Morgante, G., Mortlock, D., Moss, A., Munshi, D., Murphy, J. A., Naselsky, P., Nati, F., Natoli, P., Netterfield, C. B., Nørgaard-Nielsen, H. U., Noviello,

F., Novikov, D., Novikov, I., Oxborrow, C. A., Paci, F., Pagano, L., Pajot, F., Paladini, R., Paoletti, D., Partridge, B., Pasian, F., Patanchon, G., Pearson, T. J., Perdereau, O., Perotto, L., Perrotta, F., Pettorino, V., Piacentini, F., Piat, M., Pierpaoli, E., Pietrobon, D., Plaszczynski, S., Pointecouteau, E., Polenta, G., Popa, L., Pratt, G. W., Prézeau, G., Prunet, S., Puget, J.-L., Rachen, J. P., Reach, W. T., Rebolo, R., Reinecke, M., Remazeilles, M., Renault, C., Renzi, A., Ristorcelli, I., Rocha, G., Rosset, C., Rossetti, M., Roudier, G., Rouillé d´Orfeuil, B., Rowan-Robinson, M., Rubiño-Martín, J. A., Rusholme, B., Said, N., Salvatelli, V., Salvati, L., Sandri, M., Santos, D., Savelainen, M., Savini, G., Scott, D., Seiffert, M. D., Serra, P., Shellard, E. P. S., Spencer, L. D., Spinelli, M., Stolyarov, V., Stompor, R., Sudiwala, R., Sunyaev, R., Sutton, D., Suur-Uski, A.-S., Sygnet, J.-F., Tauber, J. A., Terenzi, L., Toffolatti, L., Tomasi, M., Tristram, M., Trombetti, T., Tucci, M., Tuovinen, J., Türler, M., Umana, G., Valenziano, L., Valiviita, J., Van Tent, F., Vielva, P., Villa, F., Wade, L. A., Wandelt, B. D., Wehus, I. K., White, M., White, S. D. M., Wilkinson, A., Yvon, D., Zacchei, A., y Zonca, A., *Planck 2015 results - xiii. cosmological parameters*, A&A **594** (2016), A13.

[PR2013] Yaroslav Pavlyukh y A. R. P. Rau, *1-, 2-, and 6-qubits, and the Ramanujan-Nagell theorem*, Int. J. Quantum Inf. **11** (2013), no. 6, 1350056, 8. MR3149432

[PSW1980] Carl Pomerance, J. L. Selfridge, y Samuel S. Wagstaff Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), no. 151, 1003–1026. MR572872

[Rab1980] Michael Oser Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138. MR566880

[Rib1996] Paulo Ribenboim, *The new book of prime number records.*, 3rd ed., New York, NY: Springer-Verlag, 1996 (English).

[Spr1940] R. Sprague, *Zur Abschätzung der Mindestzahl inkongruenter Quadrate, die ein gegebenes Rechteck ausfüllen*, Math. Z. **46** (1940), 460–471. MR2188

[SS1959] H. S. Shapiro y D. L. Slotnick, *On the mathematical theory of error-correcting codes*, IBM J. Res. Develop. **3** (1959), 25–34. MR98636

[SS1971] Arnolrd Schönhage y Volker Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR292344

[Sta2015] Richard P. Stanley, *Catalan numbers*, Cambridge University Press, New York, 2015, https://doi.org/10.1017/CBO9781139871495. MR3467982

[SW2017] Jonathan Sorenson y Jonathan Webster, *Strong pseudoprimes to twelve prime bases*, Math. Comp. **86** (2017), no. 304, 985–1003. MR3584557

[Ven1880] John Venn, *On the diagramatic and mechanical representation of propositions and reasonings*, The London, Edinburgh, and Dublin Philos. Magazine and Journal of Science **9** (1880), no. 5, 1–18.

[WW2008] Stan Wagon y Peter Webb, *Venn symmetry and prime numbers: a seductive proof revisited*, Amer. Math. Monthly **115** (2008), no. 7, 645–648. MR2444940

[Zag1997] Don Zagier, *Newman's short proof of the prime number theorem*, Amer. Math. Monthly **104** (1997), no. 8, 705–708. MR1476753

[Zec1972] Edouard Zeckendorf, *Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas*, Bull. Soc. Roy. Sci. Liège **41** (1972), 179–182. MR308032

Notaciones

Personas

Índice