Capítulo 3

Enteros – Primera parte.

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
(Dios hizo los números enteros,
todo lo demás es obra del hombre.)
Leopold Kronecker (1823-1891),
matemático alemán.

3.1. Hechos generales.

El conjunto de los *números enteros* es:

$$\mathbb{Z} \;=\; \{\dots,-3,-2,-1,0,1,2,3,\dots\} \;=\; -\mathbb{N}\cup\{0\}\cup\mathbb{N} \quad (\text{donde} -\mathbb{N} := \{-n; n\in\mathbb{N}\}).$$

Una de las razones de la necesidad de trabajar con estos números es que en $\mathbb{N}$ no se puede restar (en general), es decir la ecuación $x+a=b$ con $a>b\in\mathbb{N}$ no tiene solución en $\mathbb{N}$. Así $\mathbb{Z}$ se obtiene a partir de $\mathbb{N}$ agregándole los números negativos.

Esta construcción se puede formalizar, definiendo a $\mathbb{Z}$ como el conjunto de clases de equivalencia de la relación de equivalencia $\sim$ en $\mathbb{N}\times\mathbb{N}$ dada por:

$$(a,b)\sim(c,d) \iff a+d=b+c,\ \forall\,(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}.$$

Es fácil verificar que ésta es una relación de equivalencia en $\mathbb{N}\times\mathbb{N}$.

La motivación de que las clases de equivalencia de esta relación dan el conjunto que conocemos como el conjunto de números enteros $\mathbb{Z}$ proviene de que $a+d=b+c$ es lo mismo que decir (en $\mathbb{Z}$) que $a-b=c-d$, y por ejemplo se puede pensar en el $-2=4-6$ como el par $(4,6)\in\mathbb{N}\times\mathbb{N}$, pero también como el par $(5,7)$, ya que $-2=5-7$ también, o como cualquier par $(n,n+2)$ con $n\in\mathbb{N}$. Del mismo modo el número entero $0=n-n$ se corresponde con cualquier par

(n,n), $n \in \mathbb{Z}$. Así, se tiene

- $\overline{(1,1)} = \{(n,n),\ n \in \mathbb{N}\} \underset{\text{def}}{=} 0 \in \mathbb{Z}$
- $\overline{(m+1,1)} = \{(m+n+1,n+1),\ n \in \mathbb{N}\} \underset{\text{def}}{=} m \in \mathbb{Z},\ \forall\, m \in \mathbb{N}$
- $\overline{(1,m+1)} = \{(n+1,m+n+1),\ n \in \mathbb{N}\} \underset{\text{def}}{=} -m \in \mathbb{Z},\ \forall\, m \in \mathbb{N}.$

Se puede probar que con esta construcción, en $\mathbb{Z}$ la operación $+$ cumple que para todo $a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$, y satisface además las siguientes propiedades, que le dan una estructura de *Grupo Conmutativo*:

- *Conmutatividad:* Para todo $a, b \in \mathbb{Z}$, $a+b = b+a$.
- *Asociatividad:* Para todo $a, b, c \in \mathbb{Z}$, $(a+b)+c = a+(b+c)$ (y por lo tanto, se puede escribir $a+b+c$ sin aclarar qué se suma primero).
- *Existencia de Elemento Neutro:* Existe un elemento en $\mathbb{Z}$ (que resulta único), el 0, que satisface que para todo $a \in \mathbb{Z}$, $a+0 = a$.
- *Existencia de Opuesto:* Para todo $a \in \mathbb{Z}$, existe un (único) elemento, que se nota $-a$, que satisface que $a+(-a) = 0$.

A los grupos conmutativos, se los suele llamar *Grupos Abelianos*, por el matemático noruego *Niels Henrik Abel*, 1802-1829, y en honor a quién se otorga anuamente desde el año 2003 el Premio Abel, distinción matemática comparable a los Premios Nobel. (¿Sabía que no hay Premio Nobel de Matemática?)

O sea $(\mathbb{Z}, +)$ es un Grupo Abeliano. La razón por la que se le da un nombre a los conjuntos con una operación que sastisface las 4 propiedades mencionadas, es que se observó que hay muchísimos conjuntos que, junto con una operación, satisfacen esas propiedades (por ejemplo, con la suma, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^2$, $\mathbb{R}[X]$, ...) y entonces, a fin de estudiar las consecuencias de esas propiedades, conviene hacerlo de una vez por todos en el caso abstracto general y luego aplicarlo en cada caso en lugar de estudiarlas para cada conjunto en particular.

En $\mathbb{Z}$ también se puede multiplicar: la operación $\cdot$ cumple que para todo $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$. Y además cumple propiedades parecidas a $+$, aunque no todas:

- *Conmutatividad:* Para todo $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.
- *Asociatividad:* Para todo $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c) (= a \cdot b \cdot c = a\,b\,c)$.
- *Existencia de Elemento Neutro:* Existe un elemento en $\mathbb{Z}$ (único) que es el 1, que verifica que para todo $a \in \mathbb{Z}$, $1 \cdot a = a$.

La propiedad siguiente relaciona el producto con la suma:

- *Distributividad del producto sobre la suma:* Para todo $a, b, c \in \mathbb{Z}$, $a \cdot (b+c) = a \cdot b + a \cdot c$.

Estas propiedades de la suma y el producto en $\mathbb{Z}$ hacen que $\mathbb{Z}$ tenga una estructura de *Anillo Conmutativo* (estructura que conviene estudiar en general por las mismas razones que conviene estudiar la de Grupo). O sea $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

El conjunto de los números enteros $\mathbb{Z}$ con el producto también cumple otra importante propiedad, que lo convierte en un *dominio íntegro*:

$$\forall\, a, b \in \mathbb{Z}: \quad a \cdot b = 0 \implies a = 0 \text{ o } b = 0.$$

Esta propiedad es la que permite simplificar un factor común no nulo:

$$a \cdot b = a \cdot c \text{ y } a \neq 0 \implies b = c,$$

ya que $ab = ac \Leftrightarrow a(b-c) = 0$, y si $a \neq 0$ entonces $b - c = 0$, o sea $b = c$.

El conjunto $\mathbb{Z}$ se diferencia del conjunto de los números racionales $\mathbb{Q}$ (que como veremos más adelante tiene una estructura de cuerpo) ya que como veremos enseguida, en general los números enteros no tienen inverso multiplicativo: los únicos elementos inversibles a de $\mathbb{Z}$ para el producto, o sea que satisfacen que existe $a^{-1} \in \mathbb{Z}$ de manera que $a \cdot a^{-1} = 1$, son el 1 y el -1.

Recordemos otras propiedades que ya conocemos de $\mathbb{Z}$ o también de subconjuntos de $\mathbb{Z}$:

- $\mathbb{Z}$ es un conjunto inductivo, que contiene estrictamente a $\mathbb{N}$ y para el cual no vale así nomás el principio de inducción ya que no tiene primer elemento por el cual empezar la inducción.
- Si fijamos $n_0 \in \mathbb{Z}$, en $\mathbb{Z}_{n_0} := \{m \in \mathbb{Z}; m \geq n_0\}$ vale el principio de inducción empezando en n_0. Por ejemplo en $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ vale el principio de inducción.
- Equivalentemente, $\mathbb{Z}_{n_0}$ y $\mathbb{N}_0$ son conjuntos bien ordenados, o sea, cualquier subconjunto no vacío de $\mathbb{Z}_{n_0}$ o $\mathbb{N}_0$ tiene primer elemento o mínimo (un elemento en el subconjunto menor o igual que todos los demás).

3.2. Divisibilidad.

El hecho que los números enteros no son divisibles (con cociente entero) por cualquier otro número entero hace interesante estudiar la noción y consecuencias de la *divisibilidad*. (Este estudio no se justifica por ejemplo de la misma manera en $\mathbb{Q}$ o $\mathbb{R}$ donde todo número racional o real es divisible (con cociente racional o real) por cualquier otro número racional o real no nulo.)

Definición 3.2.1. (Divisibilidad.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$. Se dice que d *divide a* a, y se nota $d \mid a$, si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot d$ (o sea si el cociente $\dfrac{a}{d}$ es un número entero). También se dice en ese caso que a es divisible por d, o que a es múltiplo de d. O sea:

$$d \mid a \iff \exists\, k \in \mathbb{Z} \,:\, a = k \cdot d.$$

En caso contrario, se dice que d no divide a a, y se nota $d \nmid a$. Eso es cuando el cociente $\frac{a}{d} \notin \mathbb{Z}$, o sea no existe ningún entero $k \in \mathbb{Z}$ tal que $a = k \cdot d$.

El conjunto de los divisores positivos y negativos de un entero a se notará por $\mathrm{Div}(a)$ y el de los divisores positivos por $\mathrm{Div}_+(a)$.

Nota: En algunos textos o clases no excluyen el caso $d = 0$ pero se conviene que 0 divide únicamente al 0, pues $a = k \cdot 0$ implica $a = 0$. Igualmente en estas notas excluiremos el caso $d = 0$ para no "dividir por 0".

Ejemplos:

- $7 \mid 56$ pues $56 = 8 \cdot 7$.
- $7 \mid -56$, $-7 \mid 56$, $-7 \mid -56$.
- $7 \nmid 54$.
- $\mathrm{Div}(-12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ y $Div_+(-12) = \{1, 2, 3, 4, 6, 12\}$.
- $\mathrm{Div}(1) = \{-1, 1\}$.

Propiedades 3.2.2. (De la divisibilidad.)

- Todo número entero $d \neq 0$ satisface que $d \mid 0$ pues $0 = 0 \cdot d$ (aquí $k = 0$). Así el 0 tiene infinitos divisores : $\mathrm{Div}(0) = \mathbb{Z} \setminus \{0\}$.
- $d \mid a \Leftrightarrow -d \mid a$ (pues $a = k \cdot d \Leftrightarrow a = (-k) \cdot (-d)$).

  De la misma manera $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -d \mid -a$.

  Se concluye que $d \mid a \Leftrightarrow |d| \mid |a|$ (donde $|x|$ denota el módulo o valor absoluto de x).

  En particular a cada divisor negativo de a le corresponde un divisor positivo.
- Si $a \neq 0$, $d \mid a \Rightarrow |d| \leq |a|$ (pues $|a| = k|d|$ con $|a| \neq 0$ implica k es un entero no nulo y positivo, es decir $k \geq 1$; por lo tanto, $|a| = k|d| \geq |d|$).

  En particular, todo número entero a no nulo tiene sólo un número finito de divisores, todos pertenecientes al conjunto

  $$\{-|a|, \ldots, -1, 1, \ldots, |a|\}.$$

  O sea $\mathrm{Div}_+(a) \subset \{1, \ldots, |a|\}$.

  Además, por la observación del inciso anterior, el número total de divisores de a es el doble del número de divisores positivos.

- Ahora podemos probar facilmente que los únicos números enteros que son inversibles son 1 y -1, ya que $a \in \mathbb{Z}$ inversible significa que existe $b \in \mathbb{Z}$ tal que $ab = 1$. Esto implica que $a \neq 0$ (pues $0 \cdot b = 0,\ \forall\, b \in \mathbb{Z}$), y por lo tanto $a \mid 1$. Pero por lo anterior, esto implica que $|a| \leq 1$, es decir $a = \pm 1$. Y se verifica facilmente que tanto 1 como -1 son inversibles (sus inversas son ellos mismos).

- $d \mid a$ y $a \mid d \Leftrightarrow a = \pm d$ (pues $a = k \cdot d$ y $d = j \cdot a$ implica que $a = (k \cdot j) \cdot a$, por lo tanto k y j son dos números enteros que satisfacen $k \cdot j = 1$, o sea, $k = \pm 1$).

- Para todo $a \in \mathbb{Z}$, se tiene $1 \mid a$ y $-1 \mid a$, y también $a \mid a$ y $-a \mid a$.

  Así, si $a \neq \pm 1$, a tiene por lo menos 4 divisores distintos ($\pm 1, \pm a$), o 2 divisores positivos distintos (1, $|a|$).

  Hay números enteros que tienen únicamente esos 4 divisores, que son los asegurados, otros tienen más. Esto motiva la separación de los números enteros (distintos de 0, 1 y -1) en dos categorías, la de los números *primos* y la de los números *compuestos* :

Definición 3.2.3. (Números primos y compuestos.)

- Se dice que $a \in \mathbb{Z}$ es un número *primo* si $a \neq 0, \pm 1$ y tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \ldots$.

  (En general los números primos se notan con las letras p, q,...)

- Se dice que a es un número *compuesto* si $a \neq 0, \pm 1$ y tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \ldots$.

  Se observa que a es compuesto si y sólo si tiene un divisor positivo d que satisface $2 \leq d \leq |a| - 1$ (pues ya vimos que $\mathrm{Div}_+(a) \subset \{1, \ldots, |a|\}$ y si a tiene más que 2 divisores positivos, tiene que haber uno en "algún lugar en el medio").

<u>*Nota:*</u> Esta definición de número primo es la histórica que aprendemos todos en el colegio y está en todos lados. Pero de hecho en matemática se hace una distinción, cuando se trabaja en dominios íntegros arbitrarios, entre los conceptos de *irreducible* (que es tener únicamente los divisores triviales, o sea lo que acá llamamos primo), y *primo*, que corresponde a una propiedad crucial que veremos más adelante. En el caso de los números enteros, como estos dos conceptos coinciden, adoptamos en estas notas el nombre tradicional.

Más adelante, se trabajará mucho más con los números primos, que cumplen propiedades importantísimas, y constituyen los ladrillos de base para construir todos los números, en el sentido que cualquier número entero (distinto de 0 y ± 1) se escribe en forma única como $\pm$ un producto de primos positivos.

Se verán ahora algunas propiedades importantes de la divisibilidad :

Propiedades 3.2.4. (De la divisibilidad.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$.

- $d \mid a$ y $d \mid b \Rightarrow d \mid a+b$.
  (Pues si $a = k \cdot c$ y $b = j \cdot c$ con $k, j \in \mathbb{Z}$, entonces $a+b = (k+j) \cdot c$, donde $k+j \in \mathbb{Z}$.)
- $d \mid a$ y $d \mid b \Rightarrow d \mid a-b$.
- $d \mid a+b$ no implica que $d \mid a$ y $d \mid b$: Por ejemplo, $6 \mid 4+8$ pero $6 \nmid 4$ y $6 \nmid 8$.
- Sin embargo si $d \mid a+b$ y *se sabe que* $d \mid a$, entonces $d \mid b$.
  (Pues $d \mid (a+b)-a$.)
- $d \mid a \Rightarrow d \mid k \cdot a, \ \forall\, k \in \mathbb{Z}$.
- $d \mid a \Rightarrow d^2 \mid a^2$ y $d^n \mid a^n, \ \ \forall\, n \in \mathbb{N}$.
  (Pues si $a = k \cdot d$, entonces $a^2 = k^2 \cdot d^2$ y $a^n = k^n \cdot d^n$.)
  Veremos más adelante que vale la recíproca también: si $d^2 \mid a^2$ entonces $d \mid a$, etc.)
- $d \mid a \cdot b$ no implica $d \mid a$ o $d \mid b$: Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.
  Veremos más adelante que la propiedad $d \mid a \cdot b \Rightarrow d \mid a$ o $d \mid b$ se cumple cuando d es un número primo (es la propiedad más importante que cumplen los números primos). Si d no es primo, siempre se pueden econtrar a y b tales que $d \mid a \cdot b$ pero $d \nmid a$ y $d \nmid b$. ¿Quiénes?

Ejemplos:

- Hallar todos los $a \in \mathbb{Z}, a \neq 1$, tales que $a-1 \mid a^2+5$.
  Para resolver esto, se trata de poner a la derecha del símbolo $\mid$ un número fijo, de manera de trabajar después con los divisores de ese número. Para ello se puede usar por ejemplo que se sabe que $a-1 \mid a-1$, por lo tanto $a-1 \mid b(a-1)$ (para todo $b \in \mathbb{Z}$) y en particular $a-1 \mid (a+1)(a-1)$. Así se tiene $a-1 \mid a^2+5$ y $a-1 \mid a^2-1$, por lo tanto $a-1$ divide a la diferencia, es decir $a-1 \mid 6$. Es decir $a-1 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Por lo tanto $a \in \{-5, -2, -1, 0, 2, 3, 4, 7\}$, y se concluye verificando que para cada valor de ese conjunto es cierto que $a-1 \mid a^2+5$, o bien verificando y mostrando que en realidad todas las implicaciones usadas son equivalencias.
- Probar que para todo $a \in \mathbb{Z}, a \neq 1$, y para todo $n \in \mathbb{N}$ vale que $a-1 \mid a^n-1$.
  Esto ya se puede hacer a este nivel de distintas formas (despues veremos otra incluso) :
  - Usando la Serie Geométrica :
    $$\sum_{i=0}^{n-1} a^i = \frac{a^n-1}{a-1}$$
    Por lo tanto
    $$a^n - 1 = (a-1) \sum_{i=0}^{n-1} a^i$$
    y dado que la sumatoria da un número entero (pues es una suma de potencias de enteros) resulta que $a-1 \mid a^n-1$.

- Usando el Binomio de Newton :

  $$a^n = ((a-1)+1)^n = \sum_{i=0}^{n} \binom{n}{i}(a-1)^i = 1 + n(a-1) + \binom{n}{2}(a-1)^2 + \cdots + (a-1)^n$$

  Por lo tanto

  $$a^n - 1 = (a-1)\Big(n + \binom{n}{2}(a-1) + \cdots + (a-1)^{n-1}\Big) = k\,(a-1)$$

  donde $k \in \mathbb{Z}$ es la sumatoria que está dentro del gran paréntesis.
- Por inducción en n. La proposición es $p(n)$: "$a-1 \mid a^n - 1$"
  $p(1)$ es Verdadera pues $a-1 \mid a-1$.
  $p(h)$ Verdadera $\Rightarrow p(h+1)$ Verdadera :
  HI : $a-1 \mid a^h - 1$. Se quiere probar que $a-1 \mid a^{h+1} - 1$.
  Pero $a^{h+1} - 1 = a(a^h - 1) + (a-1)$, y por HI, $a-1 \mid a^h - 1$, y por otro lado, $a-1 \mid a-1$, por lo tanto $a-1$ divide a la suma, como se quería probar.

(Las dos primeras tienen la ventaja sobre la última de dar también la expresión del cociente, y la primera es la más sencilla.)

- Sean $m, n \in \mathbb{N}$. Probar que si $m \mid n$, entonces para todo $a \neq \pm 1$, $a^m - 1 \mid a^n - 1$.

  Se tiene $n = k \cdot m$, luego $a^n = (a^m)^k$. Si ponemos $A := a^m$, por el inciso anterior se tiene que $A - 1 \mid A^k - 1$, es decir $a^m - 1 \mid a^n - 1$.

3.2.1. Congruencia.

Introducimos ahora una notación debida a Carl Friedrich Gauss. La notación facilita mucho la forma de escribir y trabajar con los números enteros y la divisibilidad, además de ofrecer una clasificación muy importante de los números, como veremos en este curso.

Definición 3.2.5. (Congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Dados $a, b \in \mathbb{Z}$, se dice que a *es congruente a* b *módulo* d sii $d \mid a - b$.

Se nota $a \equiv b \pmod{d}$ o también $a \equiv b\ (d)$. O sea:

$$a \equiv b \pmod{d} \iff d \mid a - b.$$

En caso contrario se nota $a \not\equiv b \pmod{d}$ o $a \not\equiv b\ (d)$.

Ejemplos:

- $5 \equiv 3 \pmod{2}$, $5 \equiv -1 \pmod{2}$, $5 \equiv 1 \pmod{2}$, $5 \not\equiv 2 \pmod{2}$, $4 \equiv 0 \pmod{2}$, $\forall\, k \in \mathbb{Z}$, $2k \equiv 0 \pmod{2}$ y $2k + 1 \equiv 1 \pmod{2}$.

- $13 \equiv 8 \pmod 5$ y $13 \equiv 3 \pmod 5$.
- Observemos que $a \equiv 0 \pmod d \iff d \mid a$.

Sea $d \in \mathbb{Z}$, $d \neq 0$. Se verá ahora que la relación de congruencia módulo d es una relación de equivalencia en $\mathbb{Z}$.

Proposición 3.2.6. (La congruencia es una relación de equivalencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Sea $\mathcal{R}$ la relación en $\mathbb{Z}$ dada por

$$a \mathcal{R} b \iff a \equiv b \pmod d, \quad \forall\, a, b \in \mathbb{Z}.$$

Entonces $\mathcal{R}$ es una relación de equivalencia.

Demostración.

- *Reflexividad :* Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod d$ pues $d \mid a - a$.
- *Simetría :* Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod d$, entonces $b \equiv a \pmod d$. Pero $a \equiv b \pmod d$ significa que $d \mid a - b$, y por lo tanto $d \mid -(a-b) = b - a$, luego $b \equiv a \pmod d$.
- *Transitividad :* Hay que probar que para todo $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod d$ y $b \equiv c \pmod d$ entonces $a \equiv c \pmod d$. Pero $a \equiv b \pmod d$ significa que $d \mid a - b$, y $b \equiv c \pmod d$ significa que $d \mid b - c$. Por lo tanto $d \mid (a-b) + (b-c) = a - c$, es decir $a \equiv c \pmod d$.

□

La proposición anterior implica que la relación de equivalencia $\equiv \pmod d$ parte a los números enteros en clases de equivalencia, subconjuntos de elementos congruentes entre sí, que se "identifican"de esa manera. Por ejemplo si se toma congruencia módulo 2, quedan por un lado los pares (que son todos congruentes entre sí y también congruentes a 0 módulo 2), y por otro lado los impares (que son congruentes entre sí y congruentes a 1 módulo 2). Cuando se toma congruencia módulo 3, $\mathbb{Z}$ queda subdividido en 3 subconjuntos : los que son de la forma $3k$, $k \in \mathbb{Z}$, por un lado, por otro lado los que son de la forma $3k+1$ y por último los que se escriben como $3k+2$. Enseguida veremos el Algoritmo de División, y se verá que la congruencia módulo d clasifica (e identifica) los números enteros según su resto módulo d.

A continuación, se enuncian propiedades de la congruencia con respecto a la suma y al producto, que son muy útiles para trabajar.

Proposición 3.2.7. (Propiedades de la congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Entonces :

1. $\forall\, a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_1 \equiv b_1 \pmod d$ *y* $a_2 \equiv b_2 \pmod d \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod d$.

2. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\begin{cases} a_1 \equiv b_1 \pmod{d} \\ \quad \vdots \\ a_n \equiv b_n \pmod{d} \end{cases} \implies a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{d}.$$

3. $\forall\, a, b, k \in \mathbb{Z}$, $a \equiv b \pmod{d} \implies k\,a \equiv k\,b \pmod{d}$, $\forall\, a, b, k \in \mathbb{Z}$.

4. $\forall\, a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_1 \equiv b_1 \pmod{d}$ *y* $a_2 \equiv b_2 \pmod{d} \Rightarrow a_1\,a_2 \equiv b_1\,b_2 \pmod{d}$.

5. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\begin{cases} a_1 \equiv b_1 \pmod{d} \\ \quad \vdots \\ a_n \equiv b_n \pmod{d} \end{cases} \implies a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{d}.$$

6. $\forall\, a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $a \equiv b \pmod{d} \Rightarrow a^n \equiv b^n \pmod{d}$.

Demostración. 1. $a_1 \equiv b_1 \pmod{d}$ y $a_2 \equiv b_2 \pmod{d}$ implican por definición $d \mid a_1 - b_1$ y $m \mid a_2 - b_2$. Por lo tanto $d \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$, es decir $a_1 + a_2 \equiv b_1 + b_2 \pmod{d}$.

2. Por inducción en n.

3. Se deja como ejercicio.

4. Para probar esto se puede usar por ejemplo el inciso (1) y la transitividad : como $a_1 \equiv b_1 \pmod{d}$, entonces $a_1\,a_2 \equiv b_1\,a_2 \pmod{d}$ (multiplicando por a_2), y por otro lado, como $a_2 \equiv b_2 \pmod{d}$, se tiene $b_1\,a_2 \equiv b_1\,b_2 \pmod{d}$ (multiplicando por b_2), y finalmente por transitividad, se concluye que $a_1\,a_2 \equiv b_1\,b_2 \pmod{d}$.

5. Por inducción en n.

6. Se tomando en el inciso anterior $a_1, \ldots, a_n$ todos iguales a un mismo número a y $b_1, \ldots, b_n$ todos iguales a un mismo número b.

□

<u>*Ejemplos:*</u>

- Probemos ahora usando congruencia que $\forall\, a \in \mathbb{Z}, a \neq 1$, $\forall\, n \in \mathbb{N}$, $a - 1 \mid a^n - 1$:

$$a - 1 \mid a - 1 \Rightarrow a \equiv 1 \pmod{(a-1)} \Rightarrow a^n \equiv 1^n \pmod{(a-1)} \Rightarrow a - 1 \mid a^n - 1.$$

- Probar que para todo $n \in \mathbb{N}_0$ vale que $64 \mid 49^n + 16n - 1$:

  Se probará por inducción en n.

$$p(n): \quad 64 \mid 49^n + 16n - 1.$$

- $p(0)$ es Verdadera pues $64 \mid 49^0 + 16 \cdot 0 - 1 = 0$.
- $p(h)$ Verdadera $\Longrightarrow p(h+1)$ Verdadera :
  HI : $64 \mid 49^h + 16h - 1$, o sea $49^h \equiv -16h + 1 \pmod{64}$.
  Se quiere probar que $64 \mid 49^{h+1} + 16(h+1) - 1$.
  Por HI, $49^{h+1} = 49 \cdot 49^h \equiv 49\,(-16h+1) \pmod{64}$.
  Por lo tanto, $49^{h+1} + 16(h+1) - 1 \equiv 49\,(-16h+1) + 16(h+1) - 1 \pmod{64}$.
  Distribuyendo y factorizando, resulta : $49^{h+1}+16(h+1)-1 \equiv -48\cdot 16h+64 \pmod{64}$.
  Pero $64 \equiv 0 \pmod{64}$ (pues $64 \mid 64$) y $-48\cdot 16h \equiv 0 \pmod{64}$ (pues $64 \mid -48\cdot 16h$), por lo tanto $-48 \cdot 16h + 64 \equiv 0 + 0 \pmod{64}$, y, de nuevo por transitividad, resulta $49^{h+1} + 16(h+1) - 1 \equiv 0 \pmod{64}$, o sea $64 \mid 49^{h+1} + 16(h+1) - 1$ como se quería probar.
  Se concluye que $64 \mid 49^n + 16n - 1$ para todo $n \in \mathbb{N}$.

3.3. Algoritmo de división.

Vamos a enunciar y demostrar ahora el bien conocido algoritmo de división entera.

Teorema 3.3.1. (Algoritmo de división.)

Dados $a, d \in \mathbb{Z}$ *con* $d \neq 0$, existen $k, r \in \mathbb{Z}$ *que satisfacen*

$$a = k \cdot d + r \quad \text{con} \quad 0 \leq r < |d|.$$

Además, k *y* r *son* únicos *en tales condiciones.*

Se dice que k es el *cociente* y r es el *resto* de la división de a por d (a es el *dividendo* y d el *divisor*). Al resto r lo notaremos $r_d(a)$ para especificar que es el "resto de a al dividir por d".

Antes de pasar a la demostración, hagamos algunos ejemplos:

Ejemplos:

- $a = 1038, d = 14$:

  $$1038 = 74 \cdot 14 + 2 \iff k = 74, r = r_{14}(1038) = 2 \text{ ya que } 0 \leq 2 < 14 = |d|.$$

- $a = 1038, d = -14$:

  $1038 = 74\cdot 14+2 = (-74)\cdot(-14)+2 \iff k = -74, r = r_{-14}(1038) = 2$ ya que $0 \leq 2 < 14 = |d|$.

- $a = -1038, d = 14$:

  $$1038 = 74 \cdot 14 + 2 \implies -1038 = -74 \cdot 14 - 2 \text{ pero } -2 < 0.$$

  Hay que corregirlo, se hace restando y sumando el (módulo del) divisor 14:

  $-1038 = (-74 \cdot 14 - 14) + (14 - 2) = -75 \cdot 14 + 12 \iff k = -75, r = r_{14}(-1038) = 12$

  ya que $0 \leq 12 < 14 = |d|$.

- $a = -1038, d = -14$:

$$1038 = 74 \cdot 14 + 2 \iff -1038 = 74 \cdot (-14) - 2 \text{ pero } -2 < 0.$$

Se corrige nuevamente como arriba restando y sumando el módulo del divisor -14:

$$-1038 = (74 \cdot (-14) - 14) + (14 - 2) = 75 \cdot (-14) + 12 \implies k = 75, r = r_{-14}(-1038) = 12$$

ya que $0 \leq 12 < 14 = |d|$.

La conclusión —como veremos en la demostración del teorema— es que para saber dividir números positivos o negativos por divisores positivos o negativos, alcanza saber hacerlo para números y divisores positivos y luego corregir cociente y/o resto en cada caso.

Demostración. El teorema consta de dos afirmaciones, la parte existencial, que requiere mostrar que existen k y r en las condiciones del teorema, y luego la unicidad: mostrar que no puede haber dos pares distintos de cociente y resto para a y d dados.

Existencia: Vamos a probar primero en detalle el caso $a \geq 0, d > 0$, ya que, como nos sugieren los ejemplos, los otros casos se reducen a ese.

- Caso $a \geq 0, d > 0$:

Aquí, $|d| = d$. La idea intuitiva es considerar los elementos

$$a,\ a - d,\ a - 2d,\ a - 3d, \ldots$$

hasta que caigamos en algún elemento menor que d pero aún mayor o igual que cero. Este será el resto. Formalizamos esta idea de la manera siguiente:

Sea A el subconjunto de $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ formado por los números de la forma $a - j\,d$ para algún $j \in \mathbb{Z}$, es decir:

$$A = \{\, a - j\,d,\ j \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

Claramente A es un subconjunto de $\mathbb{N}_0$ que no es vacío ya que $a = a - 0 \cdot d$ pertenece a A (estamos considerando el caso $a \geq 0$). Luego, el conjunto A tiene un mínimo. Llamemos r a ese mínimo. Se tiene que $r \in A$ por un lado, y por otro lado r es menor o igual que todos los demás elementos de A.

Como $r \in A$, existe un elemento natural o cero, llamémoslo k, que satisface que $r = a - k\,d$, o sea $a = k\,d + r$.

Falta probar que $0 \leq r < d$ (ya que $|d| = d$ en el caso que estamos considerando):

Claramente $r \geq 0$ ya que pertenece a A que es un subconjunto de $\mathbb{N}_0$.

Si r fuese mayor o igual que d, entonces $r - d \geq 0$ aún. Luego se tendría que el elemento $r - d = a - k\,d - d = a - (k + 1)\,d$ está también en el conjunto A pero es menor que r ! Eso contradice que r sea el mínimo. Así, se concluye que no puede ocurrsir que $r \geq d$, luego $r < d$.

- Caso $a \geq 0, d < 0$:

  En este caso, $-d > 0$ (y por lo tanto $|d| = -d$) y se tiene que por el caso anterior, existen k', r' tal que $a = k'(-d) + r'$ con $0 \leq r' < |d|$. Se obtiene directamente $a = (-k')\,d + r'$, luego $k = -k', r = r'$.

- Caso $a < 0$:

  En este caso, tenemos $-a > 0$, y de los casos anteriores existen k', r' tal que $-a = k'\,d + r'$ con $0 \leq r' < |d|$. Luego $a = (-k')\,d - r'$.

  Si $r' = 0$, r' cumple la condición de resto y se obtiene $k = -k', r = r' = 0$.

  Pero si $r' \neq 0$, hay que corregirlo restando y sumando $|d|$ a la expresión:

$$a = (-k')\,d - r' = ((-k')\,d - |d|) + (|d| - r').$$

  Así, si se define $k := -k' \pm 1$ según si $d < 0$ o $d > 0$, y $r := |d| - r'$, se tiene $a = k\,d + r$ con $0 < r < |d|$, ya que

$$0 < r' < |d| \iff -|d| < -r' < 0 \Longrightarrow |d| - |d| < |d| - r' < |d| - 0 \Longrightarrow 0 < r < |d|.$$

Unicidad: Supongamos que tenemos dos pares de cocientes y restos, k y r, y k' y r'. Vamos a probar que entonces $k = k'$ y $r = r'$.

Sin perdida de generalidad, podemos suponer que $r \leq r'$, y luego:

$$a = k\,d + r = k'\,d + r' \text{ con } 0 \leq r \leq r' < |d|.$$

Así, $(k - k')\,d = r' - r \Rightarrow d \,|\, r' - r \Rightarrow |d| \,|\, r' - r$. Como $r' - r \geq 0$ por ser $r' \geq r$, si $r' - r \neq 0$, se tiene, por lo que vimos en divisibilidad, que $|d| \leq r' - r$. Pero es facil verificar que, dado que $r' < |d|$, $r' - r < |d| - r < |d|$ (ya que $r \geq 0$). Luego no puede ser $r' - r \neq 0$, es decir tiene que ser $r' = r$.

Se concluye que $(k - k')\,d = 0$ y como $d \neq 0$, $k - k' = 0$, es decir $k = k'$ también. □

Observación 3.3.2. Si $0 \leq a < |d|$, entonces $a = 0 \cdot d + a$ implica $k = 0$ y $r = r_d(a) = a$ pues a cumple la condición que tiene que cumplir el resto (se aplica la unicidad del cociente y el resto).

Algoritmo de división iterativo para calcular (k, r) donde k es el cociente y r es el resto de la división de a por $d \neq 0$.

- Si $a \geq 0$ y $d > 0$:
  - Tomar $k = 0$, $r = a$.
  - Mientras que $r \geq d$, reemplazar
    - $k \leftarrow k + 1$
    - $r \leftarrow r - d$.
  - Dar como respuesta (k, r).
- Si $a \geq 0$ y $d < 0$:

  - Aplicar el algoritmo a a y $-d$.
  - Dar como respuesta $(-k, r)$.
- Si $a < 0$ y $d > 0$:
  - Aplicar el algoritmo a $-k$ y d.
  - Si $r = 0$, dar como respuesta $(-k, 0)$.
  - Si no, dar como respuesta $(-k - 1, d - r)$.
- Si $a < 0$ y $d < 0$:
  - Aplicar el algoritmo a $-a$ y $-d$.
  - Si $r = 0$, dar como respuesta $(-k, 0)$.
  - Si no, dar como respuesta $(k + 1, -r - d)$.

De hecho el algoritmo para obtener el cociente y el resto tiene una naturaleza intrínsecamente recursiva. Esto es facil de ver para números no negativos ya que si $a \geq d$ y $a - d = k'd + r'$ con $0 \leq r' < d$, entonces $a = (k' + 1)d + r'$. Es decir $a = kd + r$ con $0 \leq r < d$, donde $k = k' + 1$ y $r = r'$.

En Haskell existen funciones preestablecidas que dan el cociente y el resto de la división entera: éstas son las funciones *div* y *mod*: div a d devuelve el cociente k y mod a d devuelve el resto $r_d(a)$ de la división de a por d. En el caso de números no negativos, si uno quisiera describir un algoritmo en Haskell que devuelva el par (div, mod), uno muy ingenuo y muy lento podría ser, módulo posibles errores de sintáxis:

Algoritmo de división recursivo en Haskell para calcular (k, r) donde k es el cociente y r es el resto de la división de a por d para números enteros *no negativos* a y d.

```
division :: Integer → Integer → (Integer,Integer)
division a d | a < d = (0, a)
             | otherwise = (1 + k, r)
               where (k, r) = division(a − d) d
```

La observación siguiente relaciona el algoritmo de división con la divisibilidad. Es inmediata pero esencial:

Observación 3.3.3. (Divisibilidad y resto.)

Sean $a, d \in \mathbb{Z}$, $d \neq 0$. Entonces

$$r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}.$$

Esto observación se extiende inmediatamente:

Proposición 3.3.4. (Congruencia y resto.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

1. $a \equiv r_d(a) \pmod{d}$, $\forall\, a \in \mathbb{Z}$.
2. $a \equiv r \pmod{d}$ *con* $0 \leq r < |d| \;\Rightarrow\; r = r_d(a)$.
3. $r_1 \equiv r_2 \pmod{d}$ *con* $0 \leq r_1, r_2 < |d| \;\Rightarrow\; r_1 = r_2$.
4. $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$.

Demostración. 1. Pues $a = k\,d + r_d(a) \;\Rightarrow\; a - r_d(a) = k\,d \;\Rightarrow\; a \equiv r_d(a) \pmod{d}$.

2. $a \equiv r \pmod{d} \;\Rightarrow\; d \mid a - r \;\Rightarrow\; a - r = k\,d$ para algún $k \in \mathbb{Z} \;\Rightarrow\; a = k\,d + r$.
Pero la condición $0 \leq r < |d|$ implica entonces que $r = r_d(a)$. (Se usa aquí la unicidad del resto.)

3. $r_1 = 0 \cdot d + r_1$ con $0 \leq r_1 < |d| \;\Rightarrow\; r_1 = r_d(r_1)$.
Pero por otro lado, por (2), $r_1 \equiv r_2 \pmod{d}$ con $0 \leq r_2 < |d| \;\Rightarrow r_2 = r_d(r_1)$. Se concluye que $r_1 = r_2$ por la unicidad del resto.

4. ($\Rightarrow$) $a \equiv b \pmod{d}$ por hipotesis, y por (1), $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$. Por transitividad (y simetría), se concluye que $r_d(a) \equiv r_d(b) \pmod{d}$,. Ahora por (3), $r_d(a) = r_d(b)$.
($\Leftarrow$) $r_d(a) = r_d(b) \;\Rightarrow\; r_d(a) \equiv r_d(b) \pmod{d}$, y juntando por transitividad (y simetría) con $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$, resulta $a \equiv b \pmod{d}$.

□

Por lo tanto la relación de equivalencia $\equiv \pmod{d}$ parte a los números enteros en clases de equivalencia

$$\overline{a} = \{b \in \mathbb{Z} :\, b \equiv a \pmod{d}\} = \{b \in \mathbb{Z} :\, r_d(b) = r_d(a)\},$$

formadas por elementos que tienen todos el mismo resto módulo d. En cada clase podemos elegir el representante más sencillo r con $0 \leq r < |d|$, y hay d clases de equivalencia distintas, $\overline{0}, \ldots, \overline{d-1}$. Se obtiene la partición

$$\mathbb{Z} = \overline{0} \cup \cdots \cup \overline{d-1}.$$

Retomaremos este tema más adelante cuando hablaremos del anillo de restos módulo d.

Además la proposición anterior implica que para calcular el resto de un número módulo d, alcanza con lograr poner a la derecha de la congruencia módulo d un número r con $0 \leq r < |d|$. (Justamente ya mencionamos que en Haskell la instrucción que dados $a, d \in \mathbb{Z}$, $d \neq 0$, calcula el resto $r_d(a)$ de a dividido por d es la instrucción mod $a\,d$. Pero no perdamos de vista que a la derecha de la congruencia podemos poner no sólo el resto $r_d(a)$ sino cualquier número b que tiene el mismo resto que a al dividir por d.

Ejemplos:

- Calcular el resto de dividir por 5 a $166^{1328} \cdot 4878 + 199999$:

  Cada número es congruente a su resto, luego

  $$\begin{cases} 166 \equiv 1 \pmod 5 \\ 4878 \equiv 3 \pmod 5 \\ 199999 \equiv 4 \pmod 5 \end{cases} \implies \begin{array}{rcl} 166^{1328} \cdot 4878 + 199999 & \equiv & 1^{1328} \cdot 3 + 4 \pmod 5 \\ & \equiv & 7 \pmod 5 \\ & \equiv & 2 \pmod 5 \end{array}$$

  Dado que 2 cumple la condición de ser resto módulo 5, se concluye que 2 es el resto.

- Calcular el resto de dividir por 35 a $34^{17771} - 6^{1001}$:

  La congruencia es más fuerte que pensar sólo en el resto. A veces en lugar de reemplazar los números por su resto conviene reemplazarlos por -1 (si se puede) u observar algún comportamiento útil. Aquí por ejemplo se puede usar que $6^2 = 36 \equiv 1 \pmod{35}$ y también que $34 \equiv -1 \pmod{35}$. Luego:

  $$\begin{array}{rcl} 34^{17771} - 6^{1001} & = & 34^{17771} - 6^{2 \cdot 500 + 1} \\ & = & 34^{17771} + (6^2)^{500} \cdot 6^1 \\ & \equiv & (-1)^{17771} - 1^{500} \cdot 6 \pmod{35} \\ & \equiv & -1 - 6 \pmod{35} \\ & \equiv & -7 \pmod{35} \\ & \equiv & 28 \pmod{35}. \end{array}$$

  Por lo tanto el resto es 28.

Aplicando la Proposición 3.2.7, también se obtiene como consecuencia de la Proposición 3.2.7 el siguiente comportamiento de los restos con respecto a sumas, productos y potencias.

Corolario 3.3.5. (Tablas de Restos.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

- $r_d(a+b) = r_d\Big(r_d(a) + r_d(b)\Big)$.
- $r_d(a \cdot b) = r_d\Big(r_d(a) \cdot r_d(b)\Big)$.
- $r_d(a^n) = r_d\Big(r_d(a)^n\Big)$, $\forall\, n \in \mathbb{N}$.

Demostración.

$$\begin{cases} a \equiv r_d(a) \pmod d \\ b \equiv r_d(b) \pmod d \end{cases} \implies \begin{cases} a + b \equiv r_d(a) + r_d(b) \pmod d \\ a \cdot b \equiv r_d(a) \cdot r_d(b) \pmod d \\ a^n \equiv r_d(a)^n \pmod d,\ \forall\, n \in \mathbb{N}. \end{cases}$$

Por lo tanto, según la proposición anterior, las expresiones a la izquierda y a la derecha del signo $\equiv$ tienen los mismos restos. □

Ejemplo: Probar que $\forall\ a \in \mathbb{Z}$ tal que $7 \nmid a$, $r_7(a^3) = 1$ o 6. Aplicando las tablas de restos, $r_7(a^3) = r_7\big((r_7(a)^3\big)$ y como $7 \nmid a \Leftrightarrow r_7(a) \neq 0$, alcanza con analizar la tabla

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1
a^3	1	1	6	1	6	6

,

donde la primer fila indica los posibles restos de a módulo 7, la segunda fila los restos correspondientes de a^2 módulo 7 y la tercera fila los restos correspondientes de a^3 módulo 7. O sea por ejemplo si $a \equiv 3 \pmod 7$, entonces $a^3 \equiv 6 \pmod 7$, es decir si $r_7(a) = 3$, entonces $r_7(a^3) = 6$.

3.4. Sistemas de numeración.

El sistema de numeración que utilizamos desde que –según parece– Fibonacci lo introdujo en el mundo occidental, es el sistema decimal indo-arábigo, que es un sistema que funciona por posiciones de los dígitos (observar aquí otra aplicación del hecho que exista el número 0, para significar que hay una posición vacía).

Así, cuando escribimos el número seis mil setescientos ochenta y nueve, 6709, nos referimos al número compuesto por 6 unidades de 1000 más 7 unidades de 100 más 0 unidades de 10 más 9 unidades (de 1), o sea al número

$$6789 = 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 9.$$

El número natural $a = r_n r_{n-1} \dots r_1 r_0$ (donde $0 \leq r_i < 10$ para $0 \leq i \leq n$ y $r_n \neq 0$) simboliza entonces el número $r_n \cdot 10^n + \dots + r_1 \cdot 10 + r_0$.

Las exigencias de un buen sistema de numeración es que cuando vemos un número queremos poder saber en forma bien determinada de qué número estamos hablando, además de requerir que todo número tenga un único desarrollo que le corresponda. Esto se logra con la condición impuesta sobre los dígitos ($0 \leq r_i < 10, 0 \leq i \leq n$): para que un número esté bien determinado, los dígitos tienen que estar entre 0 y 9, ya que el lugar de un dígito en el número determina a qué potencia de 10 corresponde (si uno admitiera por ejemplo el 11 como un dígito, el número 111: ¿correspondería al número $111 = 1 \cdot 10^2 + 1 \cdot 10 + 1$ o al $21 = 1 \cdot 10 + 11 \cdot 1$?, y si uno admitiera el 11 pero con otro símbolo para evitar confusiones como la de arriba, por ejemplo B, el número 11 tendría dos escrituras distintas, una como 11 y la otra como B).

Matemáticamente no hay nada que haga prevalecer el número 10 como elección para la base de numeración: uno puede fijar cualquier número natural $d \geq 2$ como base del sistema de numeración. Para la buena determinación y la unicidad, lo que se tiene que pedir ahora es que los "dígitos", o mejor dicho símbolos, estén entre 0 y $d-1$. Esto se justifica también en la vida real, por ejemplo las computadoras trabajan naturalmente en base 2, o sea con los símbolos, que se llaman *bits*, 0 y 1, ya que esto se corresponde con el paso o no de electricidad.

Teorema 3.4.1. (Desarrollo en base d.)

Sea $d \in \mathbb{N}$ con $d \geq 2$. Todo número $a \in \mathbb{N}_0$ admite *un desarrollo en base d de la forma*

$$a = r_n \cdot d^n + r_{n-1} \cdot d^{n-1} + \cdots + r_1 \cdot d + r_0,$$

con $0 \leq r_i < d$ para $0 \leq i \leq n$ y $r_n \neq 0$ si $a \neq 0$.

Además dicho desarrollo, con las exigencias $0 \leq r_i < d$ impuestas para los símbolos, es único.

Se nota $a = (r_n \dots r_0)_d$.

Observación 3.4.2. En el caso de desarrollo en base 10, $(a)_{10}$ se nota simplemente a, en la forma que estamos acostumbrados.

Ejemplo:

$$6789 = (6789)_{10} = (25536)_7 = (1101010000101)_2 = (204124)_5 = (1A85)_{16}$$

(En base 16 los símbolos $10, 11, 12, 13, 14$ y 15 se reemplazan respectivamente por A, B, C, D, E y F para evitar confusiones.) Se obtiene el desarrollo realizando divisiones sucesivas. Por ejemplo para obtener el desarrollo en base 7 de 6789, se hace

$$\begin{aligned} 6789 &= 969 \cdot 7 + 6 \\ &= (138 \cdot 7 + 3) \cdot 7 + 6 \\ &= \big((19 \cdot 7 + 5) \cdot 7 + 3\big) \cdot 7 + 6 \\ &= \Big(\big((2 \cdot 7 + 5) \cdot 7 + 5\big) \cdot 7 + 3\Big) \cdot 7 + 6 \\ &= 2 \cdot 7^4 + 5 \cdot 7^3 + 5 \cdot 7^2 + 3 \cdot 7 + 6, \end{aligned}$$

y así, $6789 = (25536)_7$.

Demostración. Existencia del desarrollo en base d:

La idea intuitiva es ir dividiendo iteradamente el número a y los sucesivos cocientes por d. Para formalizar la prueba se puede hacer por induccción en $a \in \mathbb{N}_0$:

- Para $a = 0$, se tiene $0 = (0)_d$, es decir estamos en el único caso en que todos los dígitos son cero.
- $a \geq 1$:

  La hipótesis inductiva es que todo número natural o cero menor que a admite un desarrollo en base d. Queremos probar que entonces a admite también un desarrollo en base d.

  Usando el algoritmo de división, dividimos a por d, y obtenemos un cociente k que satisface $0 \leq k < a$ y un resto r_0 que satisface $0 \leq r_0 < d$: Por hipótesis inductiva, al ser $0 \leq k < a$, k admite un desarrollo en base d que notamos por conveniencia en la forma:

  $$k = r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1 \quad \text{con } 0 \leq r_n, \dots, r_1 < d.$$

Entonces

$$\begin{aligned} a &= k \cdot d + r_0 \\ &= (r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1) \cdot d + r_0 \\ &= r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 \end{aligned}$$

donde $0 \leq r_i < d$ para $0 \leq i \leq n$ como se quiere.

Así, todo $a \in \mathbb{N}$ admite un desarrollo en base d.

Unicidad: Es una consecuencia de la unicidad del resto y del cociente en el algoritmo de división: r_0 es el resto de la división de a por d y por lo tanto es único, r_1 es el resto de la división de $(a - r_0)/d$ por d y es único también, etc... Como antes, podemos formalizar esto por inducción en $a \in \mathbb{N}_0$.

- Para $a = 0$, el único desarrollo es claramente 0 para todos los dígitos.
- Para $a \geq 1$, supongamos que

$$a = r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 = s_m \cdot d^m + \cdots + s_1 \cdot d + s_0$$

con $0 \leq r_i, s_j < d$ para $0 \leq i \leq n, 0 \leq j \leq m$ y $r_n \neq 0$, $s_m \neq 0$. Ahora bien, está claro que $r_d(a) = r_0 = s_0$, y además, el cociente de dividir a por d (que es único) es

$$k = r_n \cdot d^{n-1} + \cdots + r_1 = s_m \cdot d^{m-1} + \cdots + s_1.$$

Por hipótesis inductiva, el desarrollo en base d del cociente k es único, luego $n = m$ y $r_i = s_i$, $1 \leq i \leq n$.

Así concluimos que para todo $a \in \mathbb{N}_0$, el desarrollo en base d de a es único. □

Algoritmo iterativo para calcular el desarrollo en base $d > 0$ de un número $a \in \mathbb{N}_0$.

- Si $a = 0$, dar como respuesta $s = (0)_d$.
- Si $a > 0$:
  - Comenzar con $b = a$, $s = (\ )_d$.
  - Mientras que $b \neq 0$:
    - Calcular el cociente k y el resto r de la división de b por d.
    - Agregar r como la cifra de más a la izquierda en s.
    - Reemplazar $b \leftarrow k$.
  - Dar como respuesta s.

Nuevamente este procedimiento tiene un carácter intrínsecamente recursivo, ya que si se tiene $a = k \cdot d + r$ con $0 \leq r < d$ y se obtiene el desarrollo en base d de k: $k = (r_n \dots r_0)_d$, entonces el desarrollo en base d de a es

$$a = (r_n \dots r_0\, r)_d.$$

Un posible algoritmo para calcular el desarrollo en base d de a podría ser entonces (salvo errores de sintáxis):

Algoritmo recursivo en Haskell para calcular el desarrollo en base $d > 0$ de un número $a \in \mathbb{N}_0$.

```
des :: Integer → Integer → [Integer]
des 0 d = [0]
des a d  = des (div a d) d ++ [mod a d]
```

Observación 3.4.3.

- ¿Cómo se escribe el número d^n en base d? La respuesta es

$$d^n = (1\, \underbrace{0 \dots 0}_{n})_d,$$

pues $d^n = 1 \cdot d^n + 0 \cdot d^{n-1} + \dots + 0 \cdot d^1 + 0 \cdot d^0$. Notar que d^n ocupa $n+1$ símbolos en base d, o sea tiene *tamaño* $n+1$ en base d, y es el número más chico que se puede escribir en base d usando $n+1$ símbolos (o sea de tamaño $n+1$).

- ¿Y cuál es el número más grande de tamaño n en base d, y cuál es su desarrollo? Claramente es el número $d^n - 1$ ya que d^n es el número más chico de tamaño $n+1$ en base d. También se puede pensar que tiene que ser el número

$$\sum_{k=0}^{n-1} (d-1) \cdot d^k$$

pues se pone el máximo posible, $d-1$, para cada símbolo (y ese número coincide con $d^n - 1$ por la serie geométrica...), o sea

$$d^n - 1 = (\underbrace{d-1 \dots d-1}_{n})_d.$$

- ¿Cuántos números se pueden escribir usando a lo sumo n símbolos en base d? Son todos los números a con $0 \leq a \leq d^n - 1$, y por lo tanto son d^n. Todos se escriben en la forma

$$a = (\underbrace{r_{n-1} \dots r_0}_{n})_d \quad \text{para } 0 \leq r_i \leq d-1.$$

- ¿Cuál es el tamaño en base d de un número $a \in \mathbb{N}$? (Es decir ¿cuántos símbolos son necesarios para escribir $a = (r_n \dots r_0)_d$ en base d?)

La respuesta es $[\log_d(a)] + 1$, donde $[\ ]$ nota la *parte entera*, o sea para un número real positivo, el número natural (o cero) más grande que es menor o igual que el número, pues por los incisos anteriores, si a requiere exactamente n símbolos, es que

$$d^{n-1} \leq a < d^n,$$

es decir $n - 1 \leq \log_d(a) < n$, lo que implica que $[\log_d(a)] = n - 1$, y por lo tanto $n = [\log_d(a)] + 1$.

Notas:

- En Computación se utiliza, además del sistema binario, el sistema hexadecimal, o en base 16, que permite expresar cualquier número natural a partir de los símbolos siguientes $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$. En esta base, como explicamos más arriba, el símbolo A representa el número 10 en base diez, es decir $10 = (A)_{16}$. Análogamente, $11 = (B)_{16}$, $12 = (C)_{16}$, $13 = (D)_{16}$, $14 = (E)_{16}$ y $15 = (F)_{16}$. Para escribir el 16 en base 16, necesitamos dos símbolos: $16 = (10)_{16}$. Pero por lo visto arriba, usando solamente dos símbolos se pueden escribir $16^2 = 2^8$ números en base 16, lo cual es muy económico en términos computacionales. A raíz de eso, se suele utilizar el *byte*, correspondiente a 8 bits, o sea en almacenamiento a 2 símbolos en base hexadecimal, como unidad de memoria. Por ejemplo $(11111111)_2 = (FF)_{16}$.

- Hay un ejercicio de la práctica que pregunta cuántas operaciones son necesarias para calcular a^k, con $k \in \mathbb{N}$, usando el algoritmo "dividir y conquistar": la respuesta está en calcular el desarrollo binario del exponente $k = (r_{n-1} \dots r_0)_2$.

  Por ejemplo si se quiere calcular a^{16} es más rápido hacer el cálculo

  $$a \to a{\cdot}a = a^2 \to (a^2)^2 = a^{2^2} = a^4 \to (a^{2^2})^2 = a^{2^2 \cdot 2} = a^{2^3} = a^8 \to (a^{2^3})^2 = a^{2^3 \cdot 2} = a^{2^4} = a^{16}$$

  que requiere hacer $4 = \log_2(16)$ productos que hacer ingenuamente

  $$a \to a \cdot a = a^2 \to a \cdot a^2 = a^3 \to a \cdot a^3 = a^4 \to \dots \to a \cdot a^{15} = a^{16}$$

  que requiere 15 productos. Ahora si se quiere calcular a^{22} el algoritmo "ingenuo" requeriría 21 productos mientras que como arriba, haciendo solo 4 productos, se calcula toda la secuencia

  $$a,\ a^2,\ a^{2^2},\ a^{2^3},\ a^{2^4}$$

  y ahora como $22 = (10110)_2$, es decir $22 = 2^4 + 2^2 + 2^1$, se obtiene

  $$a^{22} = a^{2^4+2^2+2^1} = a^{2^4} \cdot a^{2^2} \cdot a^{2^1},$$

  o sea se necesitan realizar 2 productos más para obtener a^{22}.

  Este argumento se puede repetir en general: si $k = r_{n-1}2^{n-1} + \dots + r_0 2^0$ (donde n es la longitud de k en base 2, o sea del orden de $\log_2(k)$), entonces

  $$a^k = a^{r_{n-1}2^{n-1} + r_{n-2}2^{n-2} + \dots + r_1 2^1 + r_0 2^0} = a^{2^{n-1} r_{n-1}} \cdot a^{2^{n-2} r_{n-2}} \cdots a^{2^1 r_1} \cdot a^{2^0 r_0},$$

donde observemos que cada r_i es o bien 1 o bien 0. Luego para obtener a^k se puede calcular recursivamente la secuencia de potencias

$$a \to a^{2^1} \to a^{2^2} \to \cdots \to a^{2^{n-1}}$$

haciendo $n-1$ productos, y luego multiplicar entre sí todas aquellas potencias a^{2^i} que satifacen que $r_i = 1$, que son a lo sumo n (este segundo paso involucra por lo tanto hacer $\leq n-1$ productos). En total hay que hacer $\leq 2(n-1)$ cuentas, o sea del orden de $2\log_2 k$ cuentas, mucho mejor que hacer $k-1$ cuentas si se multiplica recursivamente $a, a^2 = a \cdot a, a^3 = a^2 \cdot a$, etc.

3.4.1. Criterios de divisibilidad.

¡No son magia! Cada criterio de divisibilidad tiene su explicación. Lo ejemplificamos acá con dos de ellos.

Sea $a = \pm\, r_n r_{n-1} \cdots r_1 r_0$ el desarrollo decimal de a.

- Probemos el conocido criterio de divisibilidad por 3:

  $$3 \mid a \iff 3 \mid a_n + a_{n-1} + \cdots + 1 + a_0.$$

  Como $10 \equiv 1 \pmod 3$ entonces $10^i \equiv 1 \pmod 3$, para todo $i \in \mathbb{N}_0$. Luego

  $$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \equiv r_n + r_{n-1} + \cdots + r_1 + r_0 \pmod 3.$$

  En particular

  $$\begin{aligned} 3 \mid a &\iff a \equiv 0 \pmod 3 \\ &\iff r_n + r_{n-1} + \cdots + r_1 + r_0 \equiv 0 \pmod 3 \\ &\iff 3 \mid r_n + r_{n-1} + \cdots + r_1 + r_0. \end{aligned}$$

- Criterio de divisibilidad por 11:

  $$11 \mid a \iff 11 \mid (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0.$$

  Observemos que $r_{11}(10) = 10 \;\Rightarrow\; 10 \equiv 10 \pmod{11}$: esto no ayuda mucho en principio. Como arriba, también vale $10 \equiv -1 \pmod{11}$, y así,

  $$10^i \equiv (-1)^i \pmod{11}$$

  Luego,

  $$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \equiv (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0 \pmod{11}.$$

  En particular

  $$\begin{aligned} 11 \mid a &\iff a \equiv 0 \pmod{11} \\ &\iff (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0 \pmod{11} \\ &\iff 11 \mid (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0. \end{aligned}$$

3.5. Máximo común divisor.

Definición 3.5.1. (Máximo común divisor.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos. El *máximo común divisor* entre a y b, que se nota $(a : b)$, es el mayor de los divisores comunes de a y b. Es decir:

$$(a : b) \mid a,\ (a : b) \mid b \quad \text{y si} \quad d \mid a \text{ y } d \mid b, \text{ entonces } \ d \leq (a : b).$$

Claramente ese número *existe*, ya que la lista de divisores comunes es no vacía (1 es un divisor común) y finita (por ser al menos uno entre a y b no nulo), y es *único* (por ser el mayor de todos). Además es *positivo* por la misma razón.

Notaremos en lo que sigue con $\text{DivCom}(\{a, b\})$ el conjunto de los divisores comunes de a y b y con $\text{DivCom}_+(\{a, b\})$ el conjunto de los divisores comunes positivos, es decir:

$$\text{DivCom}(\{a, b\}) = \{\, d \in \mathbb{Z} : d \mid a \text{ y } d \mid b \,\} \ = \ \text{Div}(a) \cap \text{Div}(b)$$
$$\text{DivCom}_+(\{a, b\}) = \{\, d \in \mathbb{N} : d \mid a \text{ y } d \mid b \,\} \ = \ \text{Div}_+(a) \cap \text{Div}_+(b).$$

Luego, el máximo común divisor es el elemento más grande de cualquiera de esos dos conjuntos.

Ejemplos:

- $(12 : 18) = 6$, pues $\text{Div}_+(12) = \{1, 2, 3, 4, 6, 12\}$, $\text{Div}_+(18) = \{1, 2, 3, 6, 9, 18\}$ $\Rightarrow \text{DivCom}_+(\{12, 18\}) = \{1, 2, 3, 6\}$.
- $(12 : -35) = 1$ ya que $\text{Div}_+(-35) = \{1, 5, 7, 35\} \Rightarrow \text{DivCom}_+(\{12, -35\}) = \{1\}$.
- $(a : b) = (b : a)$, $\forall\, a, b \in \mathbb{Z}$ no ambos nulos.
- $(a : b) = (-a : b) = (a : -b) = (-a : -b) = (|a| : |b|)$, $\forall\, a, b \in \mathbb{Z}$ no ambos nulos.
- $(a : 1) = 1$, $\forall\, a \in \mathbb{Z}$.
- $(a : 0) = |a|$, $\forall\, a \in \mathbb{Z} - \{0\}$.
- Para todo $a, b \in \mathbb{Z}$ con $b \neq 0$, se tiene $b \mid a \Rightarrow (a : b) = |b|$.
- Probar que los únicos valores posibles para $(a^2 + 8 : a + 1)$, $\forall\, a \in \mathbb{Z}$, son 1, 3 o 9, y mostrar con ejemplos que se realizan todos.

  Para ello miramos quiénes son los posibles divisores comunes de $a^2 + 8$ y $a + 1$:

  $$\left\{ \begin{array}{l} d \mid a^2 + 8 \\ d \mid a + 1 \end{array} \right. \implies \left\{ \begin{array}{l} d \mid a^2 + 8 \\ d \mid (a - 1)(a + 1) = a^2 - 1 \end{array} \right. \implies \ d \mid 9,$$

  restando. Por lo tanto en principio los posibles valores para el máximo común divisor son únicamente los divisores positivos de 9: 1, 3 o 9. Efectivamente, para $a = 0$ se consigue $(a^2 + 8 : a + 1) = (8 : 1) = 1$, para $a = 2$ se consigue $(a^2 + 8 : a + 1) = (12 : 3) = 3$ y para $a = -1$ se consigue $(a^2 + 8 : a + 1) = (9 : 0) = 9$.

3.5.1. Algoritmo de Euclides.

Existe un algoritmo para calcular el máximo común divisor entre dos números, que no depende de calcular sus divisores. Este algoritmo fue introducido o recopilado por Euclides ($\sim$325–$\sim$265 AC) en "Los Elementos", y se lo llama directamente *Algoritmo de Euclides*.

Es el algoritmo más eficiente que existe para calcular el máximo común divisor (para números grandes), mucho más eficiente que encontrar los divisores comunes, por ejemplo mediante factorización. Se basa en el resultado sencillo siguiente.

Proposición 3.5.2. *Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{Z}$, entonces:*

$$\mathrm{DivCom}(\{a,b\}) = \mathrm{DivCom}(\{b, a-k\cdot b\}) \quad y \quad \mathrm{DivCom}_+(\{a,b\}) = \mathrm{DivCom}_+(\{b, a-k\cdot b\}).$$

En particular, para todo $k \in \mathbb{Z}$, $\quad (a:b) = (b : a-k\cdot b)$.

Aplicando esto a $r_b(a) = a - k\cdot b$, se obtiene que $(a:b) = (b : r_b(a))$.

Demostración. Alcanza con probar la primer igualdad, la de los conjuntos DivCom:

Sabemos que $d \mid a,\ d \mid b \Rightarrow d \mid a - k\cdot b$, y también $d \mid b,\ d \mid a - k\cdot b \Rightarrow d \mid a$. Por lo tanto

$d \in \mathrm{DivCom}(\{a,b\}) \iff d \mid a$ y $d \mid b \iff d \mid a - k\cdot b$ y $d \mid b \iff d \mid \mathrm{DivCom}(\{b, a-k\cdot b\})$.

□

Vamos a ejemplificar primero el funcionamiento del algoritmo de Euclides en un caso particular.

<u>*Ejemplo:*</u> Cálculo de $(120 : -84)$:

Como $(120 : -84) = (120 : 84)$, calculamos este último para simplificar las divisiones (esto no es esencial para el algoritmo). Se tiene

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} 120 &=& 1\cdot 84 + 36 & (120:84) &=& (84:36) \\ 84 &=& 2\cdot 36 + 12 & (84:36) &=& (36:12) \\ 36 &=& 3\cdot 12 + 0 & (36:12) &=& (12:0). \end{array}$$

Pero $(12:0) = 12$, luego $(120 : -84) = 12$ ya que

$$(120 : -84) = (120 : 84) = (84 : 36) = (36 : 12) = (12 : 0) = 12.$$

Enunciamos y demostramos ahora el *Algoritmo de Euclides* "en palabras"

Teorema 3.5.3. (Algoritmo de Euclides.)

Sean $a, b \in \mathbb{Z}$ no nulos. Existe $\ell \in \mathbb{N}_0$ tal que en una sucesión finita de $\ell + 1$ divisiones

$$\begin{array}{lcll} a &=& k_1\cdot b + r_1 & con \quad 0 \le r_1 < |b| \\ b &=& k_2\cdot r_1 + r_2 & con \quad 0 \le r_2 < r_1 \\ r_1 &=& k_3\cdot r_2 + r_3 & con \quad 0 \le r_3 < r_2 \\ \vdots & & & \\ r_{\ell-2} &=& k_\ell\cdot r_{\ell-1} + r_\ell & con \quad 0 \le r_\ell < r_{\ell-1} \\ r_{\ell-1} &=& k_{\ell+1}\cdot r_\ell + r_{\ell+1} & con \quad 0 \le r_{\ell+1} \le r_\ell, \end{array}$$

se llega por primera vez al resto nulo $r_{\ell+1} = 0$. *Entonces* $(a : b) = r_\ell$, *el último resto no nulo.*

La sucesión de divisiones hasta llegar al último resto no nulo se suele llamar el *Esquema de Euclides extendido.*

Demostración. Siempre se llega en un número finito de pasos (acotado a simple vista por $|b|$) a un resto nulo ya que

$$|b| > r_1 > r_2 > r_3 > \cdots \geq 0,$$

y esta sucesión estrictamente decreciente de restos ≥ 0 no puede ser infinita. Cuando en el procedimiento se llega a un resto nulo, $r_{\ell+1} = 0$, se tiene

$$(a : b) = (b : r_1) = (r_1 : r_2) = \cdots = (r_{\ell-1} : r_\ell) = (r_\ell : 0) = r_\ell.$$

□

Observación 3.5.4. Si $a, b \in \mathbb{Z}$ son tales que $a = 0$ y $b \neq 0$, ya sabemos que $(a : b) = |b|$ (o si $a \neq 0$ y $b = 0$, entonces $(a : b) = |a|$). Por lo tanto el Algoritmo de Euclides permite calcular el máximo común divisor de cualquier par de números enteros no ambos nulos.

Algoritmo de Euclides iterativo para calcular el máximo común divisor entre dos enteros no nulos a y b.

- Comenzar con $r_1 = a$, $r_2 = b$.
- Mientras que $r_2 \neq 0$:
  - Calcular el resto r de la división de r_1 por r_2.
  - Reemplazar
    - $r_1 \leftarrow r_2$
    - $r_2 \leftarrow r$
- Dar como respuesta r_1.

Pero el Algoritmo de Euclides tiene un naturaleza intrínsecamente recursiva, ya que si $a = k \cdot b + r$ entonces $(a : b) = (b : r)$, así que es otro ejemplo perfecto para Haskell!

Algoritmo de Euclides recursivo en Haskell.

```
mcd :: Integer → Integer → Integer
mcd a b | abs b > abs a = mcd b a
mcd a 0 = abs a
mcd a b = mcd b (mod a b)
```

Mencionamos antes que este algoritmo es el más eficiente para calcular el máximo común divisor entre dos números. Para ser más precisos, entre números grandes, o sea con suficientes dígitos

para que calcular su escritura como potencias de primos sea difícil (como detallaremos más adelante): Calcular el máximo común divisor nunca requiere más divisiones que cinco veces la cantidad de dígitos que tienen los números.

Este hecho es una consecuencia de la sucesión de Fibonacci y de la expresión de su término general, como se ve en un ejercicio de la Práctica, y fue probado por el matemático francés *Gabriel Lamé* en 1844, marcando el comienzo de la *Teoría de la complejidad computacional*.

No dejen de hacer ejemplos en el taller para los cuales se note la diferencia entre los tiempos de cálculo aplicando los dos algoritmos: factorización en primos y el algoritmo de Euclides.

Una aplicación no trivial del Algoritmo de Euclides:

Sean $a \in \mathbb{N}$, $a \neq 1$, y $m, n \in \mathbb{N}$. Entonces

$$(a^m - 1 : a^n - 1) = a^{(m:n)} - 1.$$

Demostración. Vamos a probar que en efecto $a^{(m:n)} - 1$ es el último resto no nulo al realizar el algoritmo de Euclides para calcular el máximo común divisor.

Recordemos que vimos en los primeros ejemplos de divisibilidad que: $n \mid m \Rightarrow a^n - 1 \mid a^m - 1$.

En el caso general, si $m = k\,n + r$ con $0 \leq r < n$, entonces

$$a^m - 1 = a^{k\,n+r} - 1 = a^r(a^{k\,n} - 1) + (a^r - 1) = k'(a^n - 1) + (a^r - 1),$$

dado que $n \mid k\,n \Rightarrow a^n - 1 \mid a^{k\,n} - 1$. Además, como $0 \leq a^r - 1 < a^n - 1$ por ser $0 \leq r < n$ y $a \in \mathbb{N}$, $a \neq 0$, se tiene que $a^r - 1$ es el resto de dividir a $a^m - 1$ por $a^n - 1$. Por lo tanto, aplicando la Proposición 3.5.2, se obtiene

$$(a^m - 1 : a^n - 1) = (a^n - 1 : a^{r_n(m)} - 1).$$

Así, se tiene

$$\left\{\begin{array}{ll} m = k_1 \cdot n + r_1 & \text{con} \quad r_1 \neq 0 \\ n = k_2 \cdot r_1 + r_2 & \text{con} \quad r_2 \neq 0 \\ r_1 = k_3 \cdot r_2 + r_3 & \text{con} \quad r_3 \neq 0 \\ \vdots & \\ r_{\ell-2} = k_\ell \cdot r_{\ell-1} + r_\ell & \text{con} \quad r_\ell \neq 0 \\ r_{\ell-1} = k_{\ell+1} \cdot r_\ell + r_{\ell+1} & \text{con} \quad r_{\ell+1} = 0 \end{array}\right. \Longrightarrow \left\{\begin{array}{l} a^m - 1 = k'_1 \cdot (a^n - 1) + (a^{r_1} - 1) \\ a^n - 1 = k'_2 \cdot (a^{r_1} - 1) + (a^{r_2} - 1) \\ a^{r_1} - 1 = k'_3 \cdot (a^{r_2} - 1) + (a^{r_3} - 1) \\ \vdots \\ a^{r_{\ell-2}} - 1 = k'_\ell \cdot (a^{r_{\ell-1}} - 1) + (a^{r_\ell} - 1) \\ a^{r_\ell - 1} - 1 = k'_{\ell+1} \cdot (a^{r_\ell} - 1) + (a^{r_{\ell+1}} - 1) \end{array}\right.$$

donde como $r_i \neq 0$ para $1 \leq i \leq \ell$, entonces $a^{r_i} - 1 \neq 0$ pues $a \in \mathbb{N}$, $a \neq 1$, y $a^{r_{\ell+1}} - 1 = a^0 - 1 = 0$. Así el último resto no nulo es $a^{r_\ell} - 1 = a^{(m:n)} - 1$, ya que $r_\ell = (m : n)$, por el Algoritmo de Euclides. □

Una consecuencia crucial del Algoritmo de Euclides para la teoría de los números enteros es que el máximo común divisor entre dos números siempre se puede escibir como una *combinación*

entera de esos dos números (y de hecho es el número no nulo más chico con esa propiedad). Este hecho que veremos ahora tiene consecuencias importantísimas y sorprendentes que iremos viendo a lo largo de este capítulo.

Teorema 3.5.5. (Mcd y combinación entera.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces existen* $s, t \in \mathbb{Z}$ *tales que*

$$(a : b) = s \cdot a + t \cdot b.$$

Este resultado se demuesta con el *Esquema de Euclides extendido*, mirandolo de atrás para adelante. Miremos cómo se pueden obtener en forma sistemática coeficientes enteros s y t, en el caso particular del ejemplo que calculamos antes:

<u>*Ejemplo:*</u> $(120 : -84) = 12$:

Mirando las dos divisiones que permitieron obtener a 12 como último resto no nulo, pero al revés, se tiene

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} 84 &=& 2 \cdot 36 + 12 & 12 &=& 84 - 2 \cdot 36 \\ 120 &=& 1 \cdot 84 + 36 & 12 &=& 84 - 2 \cdot (120 - 1 \cdot 84) \\ & & & & = & 3 \cdot 84 - 2 \cdot 120. \end{array}$$

Por lo tanto, $12 = -2 \cdot 120 + 3 \cdot 84 = -2 \cdot 120 + (-3) \cdot (-84)$. Aquí, $s = -2$ y $t = -3$ sirven.

Demostración. Se miran de atrás para adelante las sucesivas divisiones hasta la que da al máximo común divisor como último resto no nulo, y, poniendo en factor común los sucesivos divisores y restos y reagrupando, se obtiene una escritura entera de $(a : b)$ como combinación entera de a y b. (Luego, si habíamos —para simplificar las divisiones— cambiado los signos de los a y b originales, se modifican los signos para escribir $(a : b)$ como combinación entera de los a y b originales.) Si $r_\ell = (a : b)$,

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} r_{\ell-2} &=& k_\ell r_{\ell-1} + r_\ell & r_\ell &=& r_{\ell-2} - k_\ell r_{\ell-1} \\ r_{\ell-3} &=& k_{\ell-1} r_{\ell-2} + r_{\ell-1} & r_\ell &=& r_{\ell-2} - k_\ell (r_{\ell-3} - k_{\ell-1} r_{\ell-2}) \\ & & & & = & (1 + k_\ell k_{\ell-2}) r_{\ell-2} - k_\ell r_{\ell-3} \\ \vdots & & & & & \\ r_1 &=& k_3 r_2 + r_3 & r_\ell &=& *\, r_1 + *'\, r_2 \\ b &=& k_2 r_1 + r_2 & r_\ell &=& *\, r_1 + *'\, (b - k_2 r_1) \\ & & & & = & (* - k_2 *') r_1 + *'\, b \\ a &=& k_1 b + r_1 & r_\ell &=& (* - k_2 *')(a - k_1 b) + *'\, b \\ & & & & = & s\, a + t\, b. \end{array}$$

Así, $(a : b) = r_\ell = s\, a + t\, b$ donde claramente $s, t \in \mathbb{Z}$ ya que son obtenidos sumando y multiplicando enteros. □

Observemos para escribir el algoritmo que si definimos $r_{-1} = a$, $r_0 = b$, y si en general $r_{i-2} = k_i\, r_{i-1} + r_i$, y logramos escribir $r_{i-2} = s_{i-2}a + t_{i-2}b$ y $r_{i-1} = s_{i-1}a + t_{i-1}b$ comenzando desde $r_{-1} = 1 \cdot a + 0 \cdot b$, o sea $s_{-1} = 1$, $t_{-1} = b$, y $r_0 = 0 \cdot a + 1 \cdot b$, o sea $s_0 = 0$, $t_0 = b$, entonces tenemos la recurrencia

$$r_i = r_{i-2} - k_i\, r_{i-1} = s_{i-2}a + t_{i-2}b - k_i(s_{i-1}a + t_{i-1}b) = (s_{i-2} - k_i\, s_{i-1})a + (t_{i-2} - k_i\, t_{i-1})b.$$

Es decir $r_i = s_i\, a + t_i\, b$ donde

$$s_i = s_{i-2} - k_i\, s_{i-1} \quad \text{y} \quad t_i = t_{i-2} - k_i\, t_{i-1}.$$

Se recupera la escritura de $(a : b) = r_\ell = s_\ell\, a + t_\ell\, b$ donde r_ℓ es el último resto no nulo.

Esquema extendido de Euclides iterativo para escribir el máximo común divisor $(a : b)$ como combinación entera de a y b.

- Comenzar con $r_1 = a$, $r_2 = b$, $s_1 = 1$, $t_1 = 0$, $s_2 = 0$, $t_2 = 1$.
- Mientras que $r_2 \neq 0$:
  - Calcular el cociente k y el resto r de la división de r_1 por r_2.
  - Calcular $s = s_1 - k * s_2$ y $t = t_1 - k * t_2$
  - Reemplazar
    - $r_1 \leftarrow r_2$
    - $r_2 \leftarrow r$
    - $s_1 \leftarrow s_2$, $t_1 \leftarrow t_2$
    - $s_2 \leftarrow s$, $t_2 \leftarrow t$
- Dar como respuesta r_1, s_1, t_1 (que satisfacen $(a : b) = r_1 = s_1\, a + t_1\, b$).

Este algoritmo también es intrínsecamente recursivo, ya que si $a = k \cdot b + r$ y $(b : r) = s \cdot b + t \cdot r$, entonces,

$$(a : b) = (b : r) = s \cdot b + t \cdot r = s \cdot b + t \cdot (a - k \cdot b) = t \cdot a + (s - t \cdot k) \cdot b.$$

Así:

Esquema extendido de Euclides recursivo en Haskell: Dados a y b no negativos y no ambos nulos, devuelve (d', s', t') tales que $d' = (a : b) = s' \cdot a + t' \cdot b$.

```
mcdExt :: Integer → Integer → (Integer , Integer , Integer)
mcdExt a b | b > a = mcdExt b a
mcdExt a 0 = (a, 1, 0)
mcdExt a b = (d, t, s − t ∗ k)
        where (k, r) = (div a b, mod a b)
              (d, s, t) = mcdExt b r
```

En realidad, se puede caracterizar facilmente todos los números enteros que son combinación entera de a y b:

Observación 3.5.6. (Combinaciones enteras de a y b.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y $c \in \mathbb{Z}$.

$$c = s' \cdot a + t' \cdot b \text{ para } s', t' \in \mathbb{Z} \iff (a : b) \mid c.$$

Demostración.

- ($\Rightarrow$) Dado que $(a : b) \mid a$ y $(a : b) \mid b$, se tiene $(a : b) \mid s'a + t'b$, luego $(a : b) \mid c$.
- ($\Leftarrow$) Si $(a : b) \mid c$, entonces $c = k \cdot (a : b)$. Como sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s \cdot a + t \cdot b$, se tiene

  $$c = k \cdot (a : b) = k(s \cdot a + t \cdot b) = (k \cdot s)a + (k \cdot t)b.$$

  Luego $s' = k \cdot s$ y $t' = k \cdot t$.

□

La observación anterior nos dice que el máximo común divisor $(a : b)$ es el número *natural más chico* que se puede escribir como combinación entera de a y b y que todas las demás combinaciones enteras de a y b son divisibles por él.

El Teorema 3.5.5 tiene otra consecuencia importantísima que no es obvia a primera vista: el máximo común divisor no solo es el más grande de los divisores comunes sino que también es divisible por todos los divisores comunes.

Proposición 3.5.7. (Mcd y divisores comunes.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos y sea $d \in \mathbb{Z}$, con $d \neq 0$. Entonces

$$d \mid a \text{ y } d \mid b \iff d \mid (a : b).$$

Demostración.

- ($\Rightarrow$): Esta es la implicación interesante y no trivial:

  Recordemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s \cdot a + t \cdot b$. Ahora, dado que por hipotesis, $c \mid a$ y $c \mid b$, se tiene que $c \mid s \cdot a + t \cdot b = (a : b)$.

- ($\Leftarrow$): Esta implicación es obvia por la transitividad de la divisibilidad.

□

Otra consecuencia útil del Teorema 3.5.5, de la Observación 3.5.6 y de la Proposición 3.5.7 es la siguiente:

Proposición 3.5.8. (Mcd de múltiplo común de dos números.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos, y sea $k \in \mathbb{Z}$ con $k \neq 0$. Entonces

$$(k\,a : k\,b) = |k| \cdot (a : b).$$

Demostración. Sin pérdida de generalidad, podemos suponer $k > 0$.

Por un lado, aplicando la Proposición 3.5.7, se tiene

$$(a:b) \mid a \text{ y } (a:b) \mid b \implies k\,(a:b) \mid k\,a \text{ y } k\,(a:b) \mid k\,b \implies k\,(a:b) \mid (k\,a:k\,b).$$

Por otro lado, por el Teorema 3.5.5 y la Observación 3.5.6, se tiene

$$(a:b) = s\,a + t\,b \implies k\,(a:b) = s\,(k\,a) + t\,(k\,b) \implies (k\,a:k\,b) \mid k\,(a:b).$$

Como ambos términos son positivos, se concluye que son iguales. □

En realidad, los resultados que se obtuvieron permiten tres caracterizaciones equivalentes del máximo común divisor, que se enuncian a continuación. La primera corresponde a la Definición 3.5.1 del mcd y es la caracterización intuitiva, la segunda corresponde principalmente al Teorema 3.5.5 y la tercera a la Proposición 3.5.7. La segunda y la tercera son las operativas. Se deja la prueba a cargo del lector, mencionando simplemente que alcanza con probar (*1* $\Rightarrow$ *2*), (*2* $\Rightarrow$ *3*) y (*3* $\Rightarrow$ *1*), ya que por ejemplo para probar que (*2* $\Rightarrow$ *1*) se usa (*2* $\Rightarrow$ *3* $\Rightarrow$ *1*).

Teorema 3.5.9. (Equivalencias del mcd.)

Sean $a, b \in \mathbb{Z}$*, no ambos nulos, y sea* $d \in \mathbb{N}$*. Son equivalentes:*

1. $d \mid a$, $d \mid b$ *y si* $c \mid a$ *y* $c \mid b$*, entonces* $c \leq d$.
2. $d \mid a$, $d \mid b$ *y existen* $s, t \in \mathbb{Z}$ *tales que* $d = sa + tb$.
3. $d \mid a$, $d \mid b$ *y si* $c \mid a$ *y* $c \mid b$*, entonces* $c \mid d$.

Un número $d \in \mathbb{N}$ *que cumple cualquiera de esas 3 propiedades es el máximo común divisor* $(a:b)$.

3.5.2. Números coprimos.

Una atención especial merecen los pares de números cuyo máximo común divisor es igual a 1. Juegan un papel central en lo que sigue.

Definición 3.5.10. (Números coprimos.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Se dice que $a, b \in \mathbb{Z}$, no ambos nulos, son *coprimos* si y solo si $(a:b) = 1$, es decir si y solo si los únicos divisores comunes de a y b son ± 1.

En este caso, seguimos la notación introducida por el matemático e informático Donald Knuth (quién de hecho es el creador del TeX (y LATeX), editores con los que escribimos textos matemáticos que lucen tan bonitos, en particular este texto), y escribimos $a \perp b$. O sea:

$$a \perp b \iff (a:b) = 1$$

Ejemplos:

- $103 \perp 98$ pero $12202 \not\perp 43554$.
- $a \perp 0 \Leftrightarrow a = \pm 1$
- Para todo $b \in \mathbb{Z}$, $\pm 1 \perp b$.
- Para $a, b \in \mathbb{Z}$ coprimos, los distintos valores que puede tomar $(2a + b : 3a - 2b)$ son exactamente el 1 y el 7:
  - Investiguemos algunos valores de $(2a + b : 3a - 2b)$ con $a \perp b$:
    $a = 1, b = 0 : (2 : 3) = 1$; $a = 1, b = 1 : (3 : 1) = 1$; $a = 3, b = 1 : (7 : 7) = 7$.
    Luego, efectivamente los dos valores, 1 y 7, se obtienen. Probemos que son los únicos dos posibles.
  - Sea d un divisor común entre $2a + b$ y $3a - 2b$,

$$\left\{ \begin{array}{l} d \mid 2a + b \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 3(2a + b) \\ d \mid 2(3a - 2b) \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 6a + 3b \\ d \mid 6a - 4b \end{array} \right. \implies d \mid 7b.$$

    De la misma manera:

$$\left\{ \begin{array}{l} d \mid 2a + b \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 2(2a + b) \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 4a + 2b \\ d \mid 3a - 2b \end{array} \right. \implies d \mid 7a.$$

    Luego $d \mid 7a$ y $d \mid 7b$. Aplicando las Proposiciones 3.5.7 y 3.5.8 y el hecho que $a \perp b$, se tiene

$$d \mid (7a : 7b) = 7(a : b) = 7 \implies d \mid 7.$$

    Se concluye que el máximo común divisor, que es el mayor de estos d posibles, es o bien 1 o 7 como se quería probar (además efectivamente ya mostramos que había casos en que es 1 y casos en que es 7).

Recordemos que el máximo común divisor se puede escribir como combinación entera. Luego

Observación 3.5.11. (Coprimos y combinación entera.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces

$$a \perp b \iff \exists\, s, t \in \mathbb{Z} \ : \ 1 = s\, a + t\, b.$$

Demostración.
- $(\Rightarrow)$ es el hecho que el mcd 1 es combinación entera de los números.
- $(\Leftarrow)$ es por la Observación 3.5.6: $(a : b) \mid 1 \ \Rightarrow \ (a : b) = 1$.

□

La proposición que sigue trata de propiedades esenciales de divisibilidad cuando hay números coprimos de por medio. No se podrían demostrar estas propiedades si no se tuviera la Observación 3.5.11.

Proposición 3.5.12. (Propiedades esenciales de divisibilidad con coprimalidad.)
Sean $a, b, c, d \in \mathbb{Z}$ *con* $c \neq 0$ *y* $d \neq 0$. *Entonces*

1. $c \mid a,\ d \mid a$ y $c \perp d \implies cd \mid a$.
2. $d \mid ab$ y $d \perp a \implies d \mid b$.

Observemos que estas afirmaciones no son ciertas si no se piden las propiedades de coprimalidad. Por ejemplo $6 \mid 12$ y $4 \mid 12$ pero $24 \nmid 12$, y $6 \mid 2 \cdot 3 \not\Rightarrow 6 \mid 2$ o $6 \mid 3$. Por otro lado, las recíprocas siempre valen: $cd \mid a \Rightarrow c \mid a$ y $d \mid a$, y $d \mid b \Rightarrow d \mid ab$. Luego podemos reformular la Proposición 3.5.12 de la manera siguiente:

1. Sea $c \perp d$. Entonces $c \mid a,\ d \mid a \Leftrightarrow cd \mid a$.
2. Sea $d \perp a$. Entonces $d \mid ab \Leftrightarrow d \mid b$.

Demostración.
1. $c \perp d \Rightarrow 1 = sc + td \Rightarrow a = s(ca) + t(da)$, pero $d \mid a \Rightarrow cd \mid ca$ y $c \mid a \Rightarrow cd \mid da$, luego $cd \mid s(ca) + t(da) = a$.
2. $d \perp a \Rightarrow 1 = sd + ta$, luego $b = (sb)d + t(ab)$, pero $d \mid ab$, y $d \mid d$. Por lo tanto, $d \mid (sb)d + t(ab) = b$.

□

Ejemplo: Cálculo de los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{2}{a} + \frac{a}{b}$ es entero.

$$\frac{2}{a} + \frac{a}{b} = \frac{2b + a^2}{ab} \in \mathbb{Z} \iff ab \mid 2b + a^2.$$

Pero al ser $a \perp b$, $ab \mid 2b + a^2 \Leftrightarrow a \mid 2b + a^2$ y $b \mid 2b + a^2$.

Pero, dado que $a \mid a^2$, $a \mid 2b + a^2 \Leftrightarrow a \mid 2b$, y, dado que $a \perp b$, $a \mid 2b \Leftrightarrow a \mid 2$. Es decir, $a \in \{\pm 1, \pm 2\}$.

De la misma forma, dado que $b \mid 2b$, $b \mid 2b + a^2 \Leftrightarrow b \mid a^2$, y, dado que $b \perp a^2$ (pues $a \perp b$), $b \mid a^2 \cdot 1 \Leftrightarrow b \mid 1$, o sea $b \in \{\pm 1\}$.

Se obtienen luego los 8 pares $a = \pm 1, b = \pm 1$ y $a = \pm 2, b = \pm 1$.

Otra consecuencia muy util de la Proposición 3.5.11, ya que se trata siempre de reducirse a pares coprimos para poder aplicar proposiciones como la anterior, es la siguiente:

Proposición 3.5.13. ("Coprimizando")

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces*

$$\frac{a}{(a:b)} \perp \frac{b}{(a:b)}.$$

Por lo tanto

$$a = (a:b)\,a' \quad y \quad b = (a:b)\,b' \quad \textit{donde } a' = \frac{a}{(a:b)}, b' = \frac{b}{(a:b)} \in \mathbb{Z} \textit{ son coprimos.}$$

Demostración. Se sabe que $(a:b) = s\,a + t\,b$. Luego, dividiendo por $(a:b)$, se obtiene $1 = s\dfrac{a}{(a:b)} + t\dfrac{b}{(a:b)}$, es decir $\dfrac{a}{(a:b)}$ y $\dfrac{b}{(a:b)}$ son coprimos. □

<u>*Ejemplos:*</u>

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a:b) = 6$. ¿Cuáles son los posibles valores de $(6a + 12b : 6\,a - 6\,b)$?

  Coprimizando, se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

  $$(6a+12b : 6a-6b) = (36a'+72b : 36a'-36b') = (36'(a'+2b') : 36(a'-b')) = 36(a'+2b : a'-b').$$

  Para concluir falta averiguar quiénes son los posibles valores de $(a'+2b' : a'-b')$ si $a' \perp b'$.

  Sea entonces d un divisor común:

  $$\left\{\begin{array}{l} d \mid a' + 2b' \\ d \mid a' - b' \end{array}\right. \implies d \mid 3b' \quad \text{y} \quad \left\{\begin{array}{l} d \mid a' + 2b' \\ d \mid a' - b' \end{array}\right. \implies \left\{\begin{array}{l} d \mid a' + 2b' \\ d \mid 2a' - 2b' \end{array}\right. \implies d \mid 3a'.$$

  Obtuvimos $d \mid 3a'$ y $d \mid 3b'$. Luego $d \mid (3a' : 3b') = 3(a' : b') = 3$.

  Por lo tanto, los posibles valores de $(a' + 2b' : a' - b')$ si $a' \perp b'$ son en principio 1 y 3. Efectivamente si por ejemplo $a' = 1$ y $b' = 0$, $(a' + 2b' : a' - b') = 1$ mientras que si $a' = b' = 1$, $(a' + 2b' : a' - b') = (3 : 0) = 3$.

  Por lo tanto hemos probado que si $(a:b) = 6$, los valores que puede tomar

  $$(6a + 12b : 6\,a - 6\,b) = 36(a' + 2b : a' - b')$$

  son $36 \cdot 1 = 36$ o $36 \cdot 3 = 108$.

- Sea $a \in \mathbb{Z}$ tal que $(a:8) = 4$. ¿Cuáles son los posibles valores de $(a^2 + a + 32 : 16)$?

  La condición $(a:8) = 4$ implica que $4 \mid a$, o sea $a = 4\,a'$. Luego

  $$4 = (a:8) = (4a' : 4 \cdot 2) = 4(a' : 2) \implies 1 = (a' : 2),$$

  o sea a' impar. Por lo tanto:

  $$(a^2 + a + 32 : 16) = (16\,a'^2 + 4\,a' + 32 : 16) = \big(4\,(4\,a'^2 + a' + 8) : 4 \cdot 4\big) = 4\,(4a'^2 + a' + 8 : 4),$$

donde a' es impar. Ahora bien, $(4a'^2 + a' + 8 : 4) \in \{1, 2, 4\}$ pues tiene que ser un divisor positivo de 4. Como claramente $2 \nmid 4a'^2 + a' + 8$ pues a' es impar, 2 no es un divisor común (no divide al mcd). Luego $(4a'^2 + 5a' + 8 : 20) = 1$. Por lo tanto $(a^2 + 5a + 32 : 80) = 4$.

De hecho la Proposición 3.5.13 permite presentar otra caracterización del máximo común divisor, como las propuestas en el Teorema 3.5.9:

Observación 3.5.14. Sean $a, b \in \mathbb{Z}$, no ambos nulos. Sea $d \in \mathbb{N}$ un número que satisface que

$$d \mid a,\ d \mid b \quad \text{y} \quad \frac{a}{d} \perp \frac{b}{d}.$$

Entonces $d = (a : b)$.

(Esto vale por ejemplo porque $\frac{a}{d} \perp \frac{b}{d} \Leftrightarrow \exists\, s, t \in \mathbb{Z}$ con $1 = s\frac{a}{d} + t\frac{b}{d}$, lo que implica que $d = sa + tb$, la caracterización (2) del Teorema 3.5.9.)

3.6. Primos y factorización.

Recordemos que un número $p \in \mathbb{Z}$ es *primo* si y solo si es $\neq 0, \pm 1$ y tiene únicamente 4 divisores, o, lo que es lo mismo, si y solo si tiene únicamente 2 divisores positivos. También, que un número $a \in \mathbb{Z}$ es *compuesto* si y solo si es $\neq 0, \pm 1$ y existe $d \in \mathbb{Z}$ con $1 < d < |a|$ tal que $d \mid a$.
Los números primos juegan un papel fundamental en el conjunto de los números enteros, y su estudio es la base de la Teoría de Números o Aritmética.

Una de las propiedades esenciales que distingue a los números primos de los números compuestos es que "todo número es divisible por algún número primo":

Proposición 3.6.1. (Todo número entero $\neq 0, \pm 1$ es divisible por algún primo.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces existe un número primo (positivo) p tal que $p \mid a$.

Demostración. La demostración intuitiva de "si a es primo, ya está pues es divisible por él mismo, y si no, es compuesto, entonces es divisible por algún b más chico, si ese b es primo, ya está, si no es divisible por algún c más chico, etc..."se formaliza por inducción en a.

Claramente alcanza probar la proposición para a positivo, es decir para $a \geq 2$ (pues $a \neq 0, \pm 1$) pues sabemos que $p \mid a \Leftrightarrow p \mid |a|$.

$$p(a): \quad \exists\, p \text{ primo positivo } :\ p \mid a.$$

- Caso base: ¿$p(2)$ V? Sí, pues $p := 2 \mid 2$.
- Paso inductivo: Dado $a > 2$, ¿$p(2), \ldots, p(a-1)$ Verdaderas $\Rightarrow$ $p(a)$ Verdadera?

- HI: $\forall\, d\,,\ 1 < d < a\,$, existe un primo (positivo) $\,p\,$ tal que $\,p \mid d\,$.
- Qpq existe un primo (positivo) $\,p\,$ tal que $\,p \mid a\,$.

Se tiene:

- Si $\,a\,$ es primo, $\,p(a)\,$ es verdadera pues $\,p := a \mid a\,$.
- Si $\,a\,$ no es primo, entonces es compuesto, y por lo tanto existe $\,d \in \mathbb{Z}\,$ con $\,1 < d < a\,$ tal que $\,d \mid a\,$. Por hipotesis inductiva, como $\,1 < d < a\,$, existe un primo positivo $\,p\,$ tal que $\,p \mid d\,$. Se concluye que $\,p \mid a\,$ por transitividad de la divisibilidad.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $\,p(a)\,$ es Verdadero, $\,\forall\, a \geq 2\,$. Así, todo número distinto de $\,0, \pm 1\,$ es divisible por algún primo positivo.

Notemos que éste es un perfecto ejemplo de inducción completa ya que en el caso en que $\,a\,$ es compuesto, no se sabe exactamente quién es divisor $\,d\,$ de $\,a\,$ a quién se le aplica la hipótesis inductiva (es alguno más chico entre $\,1\,$ y $\,a\,$). □

Una consecuencia de este hecho es que hay infinitos primos distintos. (El hecho que haya infinitos números naturales no garantiza de por sí que haya infinitos primos ya que los infinitos números podrían obtenerse multiplicando de distintas formas y a distintas potencias finitos primos.) La demostración que damos a continuación fue hecha por Euclides alrededor el año 300 AC. Hay muchas otras demostraciones de este hecho (por ejemplo otra conocida se basa en qué la serie armónica diverge).

Corolario 3.6.2. (Cantidad de primos.)

Existen infinitos primos (positivos) distintos.

Demostración. Supongamos que no es así y que hay sólo un número finito $\,N\,$ de primos positivos. O sea que el conjunto $\,\mathcal{P}\,$ de primos positivos es $\,\mathcal{P} = \{\, p_1, \ldots, p_N \,\}\,$. Consideremos el siguiente número natural $\,M\,$:

$$M := p_1 \cdot p_2 \cdots p_N + 1.$$

Dado que $\,M \geq 2\,$ pues $\,2 \in \mathcal{P}\,$, existe por la proposición anterior un primo positivo $\,p_i \in \mathcal{P}\,$ que divide a $\,M\,$. Pero

$$p_i \mid M \quad \text{y} \quad p_i \mid p_1 \cdot p_2 \cdots p_N \quad \Longrightarrow \quad p_i \mid 1,$$

contradicción que proviene de suponer que hay sólo finitos primos. □

Otra consecuencia de que todo número $\,\neq 0, \pm 1\,$ es divisible por algún primo es la famosa Criba de Eratóstenes de Cirene ($\sim$276–$\sim$194 AC), que construye recursivamente la lista de todos los primos hasta un número dado. Por ejemplo aquí la lista de primos hasta $\,57\,$:

Criba de Eratóstenes (hasta 57)

- Se escribe la lista de todos los números del 2 al 57:

  $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31,$

  $32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, , 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57.$

- Se tachan los múltiplos estrictos del primero de la lista, el 2, que sabemos que es primo:

  $\boxed{2}, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, 21, \not{22}, 23, \not{24}, 25, \not{26}, 27, \not{28}, 29,$
  $\not{30}, 31, \not{32}, 33, \not{34}, 35, \not{36}, 37, \not{38}, 39, \not{40}, 41, \not{42}, , 43, \not{44}, 45, \not{46}, 47, \not{48}, 49, \not{50}, 51, \not{52}, 53, \not{54}, 55,$
  $\not{56}, 57.$

  El primero que sobrevivió, en este caso el 3, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se tachan los múltiplos estrictos (no tachados en la lista) del 3:

  $\boxed{2}, \boxed{3}, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, 25, \not{26}, \not{27}, \not{28}, 29,$
  $\not{30}, 31, \not{32}, \not{33}, \not{34}, 35, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, 55, \not{56},$
  $\not{57}.$

  El primero que sobrevivió, en este caso el 5, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se repite el procedimiento con el 5:

  $\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29,$
  $\not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56},$
  $\not{57}.$

- Se repite el procedimiento con el 7:

  $\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, \boxed{7}, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29,$
  $\not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, \not{49}, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56},$
  $\not{57}.$

- Se puede probar que alcanza hacer esto hasta que se alcanzó el último primo $p \leq \sqrt{57}$, es decir hasta el primo $p = 7$, pues todo número compuesto n es divisible por algún primo menor o igual que su raíz cuadrada (probarlo). Luego la lista que quedó de números no tachados son todos los primos menores o iguales que 57, es decir:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.$$

Digresión sobre Complejidad (1) Dado un número a, hay un algoritmo muy natural para establecer si a es primo o no: simplemente se divide a a por todos los números d menores que él (o por todos los primos menores que él, produciéndolos por ejemplo con la criba, o en realidad alcanza con dividirlo por todos los primos menores que $\sqrt{a}$, como se comentó arriba). Si nunca da resto 0, es que a es primo. Pero este algoritmo no es muy satisfactorio ya que la cantidad de candidatos a divisores d se asemeja a $\sqrt{a}$ (más precisamente a $\sqrt{a/\ln(a)}$ como


Legendre


Gauss


V. Poussin


Hadamard


Agrawal


Kayal


Saxena

consecuencia del teorema de distribución de primos conjeturado por Adrien-Marie Legendre en 1798, refinado posteriormente por Carl-Fiedrich Gauss, y demostrado independientemente por Jacques Hadamard y Charles-Jean de la Vallée Poussin en 1896).

Es comunmente aceptado que para que un algoritmo sea eficiente, la cantidad de cuentas que realiza tiene que ser lineal en el tamaño de la entrada, o sea la cantidad de espacio de memoria que ocupa el número en una computadora: en este caso $\log_2(a)$, o a lo sumo acotado por una potencia fija de ese tamaño (esto es lo que se llama un algoritmo polinomial, o que pertenece a la clase P).
Hasta muy recientemente, el mejor algoritmo para decidir si un número a es primo realizaba $\log_2(a)^{c \log\log\log(a)}$ para una constante fija c, o sea era "casi" polinomial.

En el año 2002, el informático indio, Manindra Agrawal, y dos de sus alumnos que estaban haciendo su tesis de maestría bajo su dirección, Neeraj Kayal y Nitin Saxena, mostraron que "Primos está en P", es decir que se puede establecer si un número entero a es primo (o no) haciendo una cantidad de cuentas acotada por una potencia fija de $\log_2(a)$.

Este test de primalidad (comunmente denominado test de primalidad AKS) no es en realidad eficiente en la práctica: para ello se siguen usando tests "probabilistas"que dan una evidencia seria de primalidad cuando no pueden probar que un número es compuesto, y son suficientes a efectos prácticos. Sin embargo, el resultado de Agrawal, Kayal y Saxena es fantástico, no sólo por lograr finalmente un objetivo teórico de clasificación buscado por mucha gente durante mucho tiempo, sino por la simplicidad y elegancia de sus métodos. Así fue reconocido por la comunidad matemática: fue publicado en el año 2004 en la revista Annals of Mathematics (considerada la mejor revista matemática del mundo) y le valió a sus autores numerosos premios (y a los dos jóvenes excelentes trabajos).
Para terminar esta disgresión, el número primo más grande conocido hoy (hoy es 7 de Febrero de 2014, puede cambiar mañana!) es el "primo de Mersenne" $2^{57885161} - 1$, que tiene 17425170 dígitos según el sitio web http://primes.utm.edu/largest.html.

Los primos de Mersenne son números primos de la forma $2^p - 1$ con p primo (se puede comprobar que si un número de la forma $2^n - 1$ es primo, entonces el exponente n tiene que ser primo, pero no vale la recíproca: $2^{11} - 1$ no es primo), y se llaman así en honor al monje y matemático francés Marin Mersenne, 1588-1648, que los estudió. Es un problema abierto determinar si hay infinitos primos de Mersenne.

Digresión sobre Complejidad (2) Un problema de otra índole, y cuya resolución haría muy famoso a cualquiera, es el problema de, dado un número a compuesto, encontrarle eficientemente un factor d no trivial (o sea $\neq 1, a$). El mejor algoritmo a la fecha realiza una cantidad de cuentas lineal en $\sqrt[3]{a}\,\log_2(a)^{2/3}$, y el número más grande que se logró factorizar (anunciado en el 2010), usando cientos de computadoras que trabajaron durante más de 2 años, tiene 232 dígitos. Se sabe que este problema está en NP, lo que hablando sin precisión, significa que si un "oráculo" me provee de un candidato a factor d, se puede verificar haciendo una cantidad polinomial (en $\log(a)$) de cuentas, si d es efectivamente un factor o no de a. Se cree que este problema es dificil, o sea que no pertenece a la clase P. De hecho la mayoría de los protocolos criptográficos (para transmisión de datos en forma segura y secreta) que se utilizan hoy en día están basados en la dificultad de factorizar números compuestos grandes (o de problemas relacionados), así que mejor que así sea!

3.6.1. La propiedad fundamental de los números primos.

Si p es un número primo (positivo), y $a \in \mathbb{Z}$ es cualquiera, entonces $\mathrm{Div}_+(p) = \{1, p\}$ y por lo tanto $\mathrm{DivCom}_+(\{p, a\}) \subset \{1, p\}$: es igual a $\{1, p\}$ cuando $p \mid a$ y es igual a $\{1\}$ cuando $p \nmid a$. Por lo tanto el máximo común divisor entre p y a, es igual a p cuando $p \mid a$ y es igual a 1 cuando $p \nmid a$:

$$(p : a) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases}, \qquad \text{y por lo tanto} \qquad p \perp a \;\Leftrightarrow\; p \nmid a.$$

(En particular, observemos que si p y q son primos positivos distintos, entonces $p \perp q$.)

Volvamos a la Proposición 3.5.12,(2) para p y a. En este caso, ella dice:

Teorema 3.6.3. (Propiedad fundamental de los números primos.)

Sea p un primo y sean $a, b \in \mathbb{Z}$. Entonces

$$p \mid a \cdot b \implies p \mid a \quad o \quad p \mid b.$$

Demostración. La Proposición 3.5.12 (2) dice que si $p \mid a \cdot b$ y $p \perp a$ entonces $p \mid b$. Por lo visto arriba, la condición $p \perp a$ es equivalente a $p \nmid a$. Luego la Proposición 3.5.12 (2) dice que si $p \mid a \cdot b$ y $p \nmid a$ entonces $p \mid b$. Esto es claramente lo mismo que decir que si $p \mid a \cdot b$ entonces $p \mid a$ o $p \mid b$, pues si $p \mid a \cdot b$, hay dos posibilidades:

- Si $p \mid a$, ya está,
- Y si $p \nmid a$, entonces $p \mid b$.

□

Esta es la propiedad más importante que cumplen los números primos (comparar con el último inciso de las Propiedades 3.2.4). Más aún, esta propiedad caracteriza los números primos:

p es primo si y solo si cada vez que p divide a un producto divide a alguno de los factores.

Esta es de hecho la definición de elemento primo en un dominio íntegro arbitrario, como verán más adelante los que estudian matemática. En el caso de los números enteros $\mathbb{Z}$, se puede probar que para $p \neq 0, \pm 1$, son equivalentes las propiedades

- p tiene únicamente 2 divisores positivos.
- $\forall\, a, b,\ p \mid a \cdot b \ \Rightarrow\ p \mid a$ o $p \mid b$.

(Pues acabamos de probar que si p tiene únicamente 2 divisores positivos, entonces $p \mid a \cdot b \ \Rightarrow\ p \mid a$ o $p \mid b$. Para probar que la condición $\forall\, a, b,\ p \mid a \cdot b \ \Rightarrow\ p \mid a$ o $p \mid b$ implica que p tiene únicamente 2 divisores positivos, probaremos la contrarecíproca: Si $p \neq 0, \pm 1$ tuviera más que 2 divisores positivos, o sea fuera compuesto, entonces $p = c \cdot d$ con $1 < c, d < p$. Luego se tendría $p \mid c \cdot d$ pero $p \nmid c$ y $p \nmid d$.)

Esta equivalencia justifica la definición histórica de primo que usamos aquí.

El Teorema 3.6.3 se generaliza inmediatamente a

Proposición 3.6.4. *Sea p un número primo y sean $a_1, \ldots, a_n \in \mathbb{Z}$, con $n \geq 2$. Entonces*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ para algún } i,\ 1 \leq i \leq n.$$

En particular, dado $a \in \mathbb{Z}$, si $p \mid a^n$ entonces $p \mid a$.

Demostración. Por inducción en n, empezando en $n = 2$.

$$p(n): \quad \forall\, a_1, \ldots, a_n \in \mathbb{Z},\ \ p \mid a_1 \cdots a_n \implies p \mid a_i \text{ para algún } i,\ 1 \leq i \leq n.$$

- Caso base: ¿$p(2)$ V? Sí, por el Teorema 3.6.3: si $p \mid a_1 \cdot a_2$ entonces $p \mid a_1$ o $p \mid a_2$.
- Paso inductivo: Dado $h \geq 2$, ¿$p(h)$ Verdadera $\Rightarrow$ $p(h+1)$ Verdadera?
  - HI: $\forall\, a_1, \ldots, a_h \in \mathbb{Z},\ \ p \mid a_1 \cdots a_h \ \Rightarrow\ p \mid a_i$ para algún $i,\ 1 \leq i \leq h$.
  - Qpq $\forall\, a_1, \ldots, a_{h+1} \in \mathbb{Z},\ \ p \mid a_1 \cdots a_{h+1} \ \Rightarrow\ p \mid a_i$ para algún $i,\ 1 \leq i \leq h+1$.

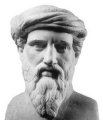
  Llamemos $b = a_1 \cdots a_h$. Entonces $p \mid a_1 \cdots a_{h+1} \ \Leftrightarrow\ p \mid b \cdot a_{h+1}$. Luego por el Teorema 3.6.3 (el caso n=2) aplicado a b y a_{h+1}, $p \mid b \cdot a_{h+1} \ \Rightarrow\ p \mid b$ o $p \mid a_{h+1}$.

  Si $p \mid a_{h+1}$, ya está. Y si $p \mid b = a_1 \cdots a_h$, por HI, $p \mid a_i$ para algún i, $1 \leq i \leq h$. O sea que también está.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \geq 2$. □

3.6.2. El Teorema fundamental de la aritmética.

Estamos ahora en condiciones de demostrar completamente el famoso *Teorema fundamental de la aritmética*, piedra angular de toda la teoría de números, acerca de la factorización única de los números como producto de primos.



Este teorema era ya conocido por los griegos de la época de Pitágoras (S. VI ac), y es el que justifica el interés de los matemáticos por conocer mejor el comportamiento de los primos: cómo se distribuyen, cómo conseguirlos, etc.

Teorema 3.6.5. (Teorema fundamental de la aritmética.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. *Entonces* a se escribe en forma única como producto de primos (positivos), *(o se factoriza en forma única como producto de primos (positivos),) es decir:*

- $\forall\, a \in \mathbb{Z}$, $a \neq 0, \pm 1$, *existe* $r \in \mathbb{N}$ *y* existen *primos positivos* $p_1, \ldots, p_r$ *distintos y* $m_1, \ldots, m_r \in \mathbb{N}$ *tales que*
$$a = \pm\, p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}.$$
- *Esta escritura es* única *salvo permutación de los primos.*

Demostración.

Existencia: Nuevamente, alcanza con probar el teorema para a positivo, y se formaliza por inducción en a, $a \geq 2$:

$$p(a): \quad a \text{ admite una factorización como producto de primos.}$$

- Caso base: $p(2)$ es Verdadera pues $2 = +\,2^1$.
- Paso inductivo:
  - Si a es un primo p, $p(a)$ es verdadera pues $a = p = +\,p^1$.
  - Si a no es primo, entonces por la Proposición 3.6.1, a es divisible por algún primo positivo p más chico que él, y por lo tanto el cociente $k = a/p$ satisface $2 \leq k \leq a-1$. Por hipotesis inductiva, k admite una factorización como producto de primos, en la forma $k = p_1^{m_1} \cdots p_r^{m_r}$. Por lo tanto a admite la factorización
$$a = p \cdot p_1^{m_1} \cdots p_r^{m_r}.$$

Así, todo número distinto de $0, \pm 1$ admite una factorización como producto de primos.

Unicidad: Supongamos que $a = \pm\, p_1^{m_1} \cdots p_r^{m_r} = \pm\, q_1^{n_1} \cdots q_s^{n_s}$ en las condiciones del enunciado. Queremos probar que entonces los signos, los primos y los exponentes coinciden.

Claramente los signos coinciden, así que podemos suponer a positivo.

En la expresión $p_1^{m_1} \cdots p_r^{m_r} = q_1^{n_1} \cdots q_s^{n_s}$, simplifiquemos todos los primos comunes (que aparecen de los dos lados) a la menor potencia a la que aparecen.

Si al hacer eso no sobra nada, o sea obtenemos $1 = 1$, es que todos los primos y las potencias coincidían.

Si no pasa eso y sobra algo de algún lado al menos, obtenemos una expresión del mismo tipo, pero donde $p_i \neq q_j$ (pues son todos los que sobraron). Podemos suponer sin perdida de generalidad que del lado izquierdo sobró un p_i. Entonces tenemos que p_i divide a lo que sobró del lado derecho o al 1 si no sobró nada. O sea $p_i \mid 1$ (lo que es absurdo) o $p_i \mid q_1^{n_1} \cdots q_s^{n_s}$. En este último caso, por la Proposición 3.6.4, existe j tal que $p_i \mid q_j$ pero p_i y q_j son primos distintos. Contradicción, que proviene de suponer que sobró un primo de algún lado. □

Cuando uno conoce la factorización en primos de un número, conoce todo del número, como se verá en lo que sigue.

Ejemplo: Sean $a = 84 = 2^2 \cdot 3 \cdot 7$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$. Entonces

$$a \cdot b = 2^3 \cdot 3 \cdot 5^2 \cdot 7^4 \cdot 11 \quad \text{y} \quad a^9 = 2^{18} \cdot 3^9 \cdot 7^9$$

son las factorizaciones en primos de $a \cdot b$ y a^9 (simplemente se suman (o multiplican) los exponentes). Esto vale siempre. Para formular facilmente este resultado, si $a, b \in \mathbb{Z}$ son dos números no nulos, convenimos en escribirlos como potencias de los mismos primos (positivos) distintos $p_1, \ldots, p_r$, permitiendo poner potencia 0 cuando el primo no aparece. Por ejemplo, para $a = 84 = 2^2 \cdot 3 \cdot 7$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, escribimos

$$a = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 \quad \text{y} \quad b = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^3 \cdot 11^1.$$

Observación 3.6.6. (Primos de productos y potencias.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \ \text{ con } \ m_1, \ldots, m_r \in \mathbb{N}_0, \quad b = \pm p_1^{n_1} \cdots p_r^{n_r} \ \text{ con } \ n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

- $a \cdot b = \left(\pm p_1^{m_1} \cdots p_r^{m_r} \right) \cdot \left(\pm p_1^{n_1} \cdots p_r^{n_r} \right) = \pm p_1^{m_1+n_1} \cdots p_r^{m_r+n_r}$.

  Es decir $a \cdot b$ tiene exactamente los primos de a y de b en su factorización (los exponentes se suman).

- $a^n = \left(\pm p_1^{m_1} \cdots p_r^{m_r} \right)^n = (\pm 1)^n \, p_1^{m_1 n} \cdots p_r^{m_r n}$ es la factorización en primos de a^n, para todo $n \in \mathbb{N}$.

  Es decir a^n tiene exactamente los mismos primos que a en su factorización.

Nota: Otro hecho que se desprende de este (y que de hecho aparece en la demostración de la unicidad de la factorización) es que $p \mid a$ si y solo si p aparece en la factorización en primos de a. Luego cualquiera sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, a es divisible por sólo un número finito de primos distintos.

Ejemplos:

- El Teorema fundamental de la Aritmética permite por ejemplo probar que $\sqrt{2}$ no es un número racional. Pues si fuera $\sqrt{2} = \frac{a}{b}$ con $a, b \in \mathbb{N}$ tendríamos $\sqrt{2} \cdot b = a$, o sea $2b^2 = a$, donde $a = p_1^{m_1} \cdots p_r^{m_r}$ con $m_1, \ldots, m_r \in \mathbb{N}_0$, $b = p_1^{n_1} \cdots p_r^{n_r}$ con $n_1, \ldots, n_3 \in \mathbb{N}_0$. Luego

$$2\, p_1^{2n_1} \cdots p_r^{2n_r} = p_1^{2m_1} \cdots p_r^{2m_r}$$

  lo que es claramente imposible por la unicidad de la factorización en primos, porque a la izquierda el primo 2 aparece un número impar de veces, mientras que a la derecha aparece un número par de veces.

- Sea $d \mid 2^3 \cdot 5^4$. ¿Cómo puede ser d?

  Está claro que si $k \cdot d = 2^3 \cdot 5^4$, entonces en k y en d no pueden aparecer más que los primos 2 y 5 (por la unicidad de la factorización). Además si $d = 2^i \cdot 5^j$ con $0 \leq i, j$ para que $d \in \mathbb{Z}$, y $k = 2^{i'} \cdot 5^{j'}$ con $0 \leq i', j'$ para que $k \in \mathbb{Z}$, tiene que satisfacerse

$$2^3 \cdot 5^4 = k \cdot d = 2^{i'} \cdot 5^{j'} \cdot 2^i \cdot 5^j = 2^{i'+i} \cdot 5^{j'+j}.$$

  Así, $i' + i = 3$ y $j' + j = 4$. Esto implica, dado que $i' \geq 0$ y $j' \geq 0$, que $0 \leq i \leq 3$ y $0 \leq j \leq 4$.

  Así, si $d \mid 2^3 \cdot 5^4$, la factorización en primos de d es

$$d = 2^i \cdot 5^j, \quad \text{con } 0 \leq i \leq 3,\ 0 \leq j \leq 4.$$

  Luego $\mathrm{Div}(2^3 5^4) = \{\pm 2^i 5^j,\ 0 \leq i \leq 3, 0 \leq j \leq 4\}$.

  Por lo tanto, $2^3 5^4$ tiene $(3+1)(4+1) = 20$ divisores positivos distintos, y $2 \cdot 20 = 40$ divisores enteros, positivos y negativos.

Proposición 3.6.7. (Divisores de un número y cantidad.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, y sea $a = \pm p_1^{m_1} \cdots p_r^{m_r}$ la factorización en primos de a. Entonces

1. $d \mid a \iff d = \pm p_1^{n_1} \cdots p_r^{n_r}$ *con* $0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r$.
2. $\#\mathrm{Div}_+(a) = (m_1 + 1) \cdots (m_r + 1)$ *y* $\#\mathrm{Div}(a) = 2(m_1 + 1) \cdots (m_r + 1)$.

Demostración. Es claro que alcanza probar la proposición para $a = p_1^{m_1} \cdots p_r^{m_r}$ positivo.

1. ($\Rightarrow$) $d \mid a \Leftrightarrow \exists\, k \in \mathbb{Z}$ tq $a = k \cdot d$. Luego la factorización en primos de $k \cdot d$ tiene que ser igual a la de a:

$$k \cdot d = p_1^{m_1} \cdots p_r^{m_r}.$$

   Esto implica por la Observación 3.6.6 que la factorización en primos de d debe ser de la forma $d = \pm p_1^{n_1} \cdots p_r^{n_r}$ para $n_1, \ldots, n_r$ que satisfacen $0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r$.

   ($\Leftarrow$) Si $d = \pm p_1^{n_1} \cdots p_r^{n_r}$ con $0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r$, entonces podemos tomar

$$k = \pm p_1^{m_1 - n_1} \cdots p_r^{m_r - n_r}$$

(todos los exponentes son ≥ 0 y por lo tanto $k \in \mathbb{Z}$), y es luego claro que

$$k \cdot d = (p_1^{m_1-n_1} \cdots p_r^{m_r-n_r}) \cdot (p_1^{n_1} \cdots p_r^{n_r}) = p_1^{m_1} \cdots p_r^{m_r} = a.$$

2. Ahora solo se trata de contar:

$$\mathrm{Div}_+(p_1^{m_1} \cdots p_r^{m_r}) = \{p_1^{n_1} \cdots p_r^{n_r} \text{ con } 0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r\},$$

y luego hay (m_1+1) elecciones para n_1 (de 0 a m_1), (m_2+1) elecciones para n_2 (de 0 a m_2), etc.

O sea $\#\mathrm{Div}_+(a) = (m_1+1)\cdots(m_r+1)$, y hay el doble de divisores totales (positivos y negativos).

□

Ejemplos:

- Calcular la suma de los divisores positivos de 10^{10}: Se tiene

$$\mathrm{Div}_+(10^{10}) = \mathrm{Div}_+(2^{10} \cdot 5^{10}) = \{2^i 5^j,\ 0 \leq i \leq 10, 0 \leq j \leq 10\}.$$

Por lo tanto

$$\sum_{d>0, d|10^{10}} d = \sum_{0 \leq i,j \leq 10} 2^i 5^j = \sum_{i=0}^{10}(\sum_{j=0}^{10} 2^i 5^j) = \sum_{i=0}^{10}(2^i \sum_{j=0}^{10} 5^j) = (\sum_{j=0}^{10} 5^j)(\sum_{i=0}^{10} 2^i)$$

$$= \frac{5^{11}-1}{5-1} \cdot \frac{2^{11}-1}{2-1} = (2^{11}-1)\frac{5^{11}-1}{4}.$$

- ¿Cuál es el menor número natural n con 12 divisores positivos?

$a = 1$ tiene únicamente 1 divisor positivo. O sea $a \geq 2$. Sea $a = p_1^{m_1} \cdots p_r^{m_r}$ con $m_1, \ldots, m_r \in \mathbb{N}$ la factorización en primos de a. Sabemos que entonces la cantidad de divisores positivos de a es $(m_1+1)\cdots(m_r+1)$. Observemos que como $m_i \geq 1$, entonces $m_i + 1 \geq 2$, $\forall\, i$. Luego, la condición $12 = (m_1+1)\cdots(m_r+1)$ implica $12 \geq 2^r$, o sea $r \leq 3$: a tiene a lo sumo 3 primos distintos. Por lo tanto a es de una de las siguientes formas:

$$a = p^m \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}.$$

  - Caso $a = p^m$: En ese caso a tiene $m+1$ divisores positivos. Si se quiere que sean 12, entonces $m+1 = 12$ implica $m = 11$: $a = p^{11}$, y el más chico de ellos es claramente $a = 2^{11} = 2048$.
  - Caso $a = p_1^{m_1} \cdot p_2^{m_2}$: En ese caso a tiene $(m_1+1)(m_2+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1) = 12 = 6 \cdot 2 = 4 \cdot 3$ implica $m_1+1 = 6, m_2+1 = 2$ o $m_1+1 = 4, m_2+1 = 3$ (o cambiando el rol de m_1 y m_2). Así se obtiene $m_1 = 5, m_2 = 1$ o $m_1 = 3, m_2 = 4$. Luego $a = p_1^5 \cdot p_2$ o $a = p_1^3 \cdot p_2^2$. Claramente los más chicos de éstos son $a = 2^5 \cdot 3 = 96$ y $a = 2^3 \cdot 3^2 = 72$.

- Caso $a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}$: En ese caso a tiene $(m_1+1)(m_2+1)(m_3+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1)(m_3+1) = 12 = 3 \cdot 2 \cdot 2$ implica $m_1+1 = 3, m_2+1 = 2$ y $m_3+1 = 2$ (o cambiando el rol de m_1, m_2 y m_3). Así se obtiene $m_1 = 2, m_2 = 1, m_3 = 1$. Luego $a = p_1^2 \cdot p_2 \cdot p_3$. Claramente el más chico de éstos es $a = 2^2 \cdot 3 \cdot 5 = 60$.

Por lo tanto en menor número natural con 12 divisores positivos es $a = 60$.

Habíamos visto en la Proposición 3.2.4 que si $d \mid a$ entonces $d^n \mid a^n$ para todo $n \in \mathbb{N}$, y mencionado que vale la recíproca pero aún no teníamos a ese nivel las herramientas para probarlo. Ahora sí...

Proposición 3.6.8. (Divisores y potencias.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$, y sea $n \in \mathbb{N}$. Entonces

$$d \mid a \iff d^n \mid a^n.$$

Ojo que en la Proposición, tiene que ser el mismo exponente n de los dos lados del signo $\mid$. Si no, no es cierto. Por ejemplo $2 \mid 4$ pero $2^{10} \nmid 4^2$, y $8^2 \mid 4^3$ pero $8 \nmid 4$.

Demostración. Solo falta probar $(\Leftarrow)$, que si $d^n \mid a^n$ entonces $d \mid a$.

- Para $a = 0$ no hay nada que probar porque $d \mid 0$, $\forall\, d \neq 0$.
- Para $a = \pm 1$, casi tampoco, ya que si $d^n \mid (\pm 1)^n$, entonces $d^n = \pm 1$, luego $d = \pm 1$, que divide a $a = \pm 1$.
- El caso $a \neq 0, \pm 1$ es el interesante. Si $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, entonces

  $$a^n = (\pm p_1^{m_1} \cdots p_r^{m_r})^n = \pm p_1^{n \cdot m_1} \cdots p_r^{n \cdot m_r}.$$

  Ahora bien, la condición $d^n \mid a^n$ implica que $d \mid a^n$. Por lo tanto $d = \pm p_1^{n_1} \cdots p_r^{n_r}$ no tiene más primos en su factorización que los de a. Pero entonces

  $$d^n = \pm p_1^{n \cdot n_1} \cdots p_r^{n \cdot n_r} \mid a$$

  implica por la Proposición 3.6.7 que $0 \leq n \cdot n_1 \leq n \cdot m_1, \ldots, 0 \leq n \cdot n_r \leq n \cdot m_r$, es decir, simplificando el n, que

  $$0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r.$$

  Esto prueba, nuevamente por la Proposición 3.6.7, que $d \mid a$.

□

Podemos ahora dar la caracterización del *máximo común divisor* y del *mínimo común múltiplo* de dos números no nulos que se suele dar en el colegio, o las fórmulas para calcularlos cuando se conoce la factorización de los números. Por ejemplo, para $a = 588 = 2^2 \cdot 3 \cdot 7^2$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, "sabemos" que el máximo común divisor $(a : b)$ es el producto de los primos comunes a a y b a la menor potencia a la que aparecen, o sea $(a : b) = 2 \cdot 7^2 = 98$.

Proposición 3.6.9. (Máximo común divisor y factorización.)

Sean $a, b \in \mathbb{Z}$ *no nulos de la forma*

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad con \quad m_1, \ldots, m_r \in \mathbb{N}_0, \quad b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad con \quad n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

$$(a : b) = p_1^{\min\{m_1, n_1\}} \cdots p_r^{\min\{m_r, n_r\}}.$$

Demostración. Hay que probar que $p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}}$ es el mayor de los divisores comunes de a y b. Investiguemos luego los divisores comunes (positivos) de a y b:

$$\begin{aligned} d \mid a \implies d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \le k_1 \le m_1, \ldots, 0 \le k_r \le m_r, \\ d \mid b \implies d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \le k_1 \le n_1, \ldots, 0 \le k_r \le n_r. \end{aligned}$$

Por lo tanto

$$d \mid a \quad \text{y} \quad d \mid b \implies d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \le k_1 \le \min\{m_1, n_1\}, \ldots, 0 \le k_r \le \min\{m_r, n_r\}.$$

De esa forma el mayor de los divisores comunes es $(a : b) = p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}}$ como se quería probar. □

Corolario 3.6.10. (Mcd de potencias.)

Sean $a, b \in \mathbb{Z}$ *no nulos.*

1. *Sean* $a, b \neq 0, \pm 1$ *con factorización en primos* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, $m_1, \ldots, m_r \in \mathbb{N}$, *y* $b = \pm q_1^{n_1} \cdots q_s^{n_s}$, $n_1, \ldots, n_s \in \mathbb{N}$. *Entonces*

$$(a : b) = 1 \iff p_i \neq q_j, \ \forall\, i, j.$$

2. $(a : b) = 1$ *y* $(a : c) = 1 \iff (a : bc) = 1$.

3. $(a : b) = 1 \iff (a^m : b^n) = 1, \ \forall\, m, n \in \mathbb{N}$.

4. $(a^n : b^n) = (a : b)^n, \ \forall\, n \in \mathbb{N}$.

   Ojo que para esta 4ta propiedad tiene que ser la misma potencia n*!*

Demostración. 1. Sabemos por la Proposición anterior que $(a : b)$ es igual al producto de los primos comunes a a y b con la mínima potencia a la que aparecen. Esto da $(a : b) = 1$ si y solo si no hay primos en común.

2. ($\Rightarrow$) Si $(a : b) = 1$, a no tiene primos en común con b, y si $(a : c) = 1$, a no tienen primos en común con c. Por lo tanto a no tiene primos en común ni con b ni con c, luego no tiene primos en común con bc, ya que los primos de bc son los de b y los de c. Por lo tanto $(a : bc) = 1$.

   ($\Leftarrow$) Recíprocamente, si a no tiene primos en común con bc, no tiene primos en común ni con b ni con c, luego es coprimo con b y con c.

3. a y b no tienen primos en común si y solo si a^m y b^n no tienen primos en común, ya que sabemos que los primos de a^m son exactamente los mismos que los de a, y los primos de b^n exactamente los mismos primos que los de b.

4. Sea $d := (a : b)$. Coprimizando, se tiene que $a = d\,a'$ y $b = d\,b'$ con $a' \perp b'$. Luego,

$$(a^n : b^n) = \big((d\,a')^n : (d\,b')^n\big) = (d^n a'^n : d^n b'^n) = d^n(a'^n : b'^n) = d^n = (a : b)^n$$

ya que $a'^n \perp b'^n$ al ser $a' \perp b'$.

□

Ejemplos:

- Calcular $(2^n + 3^n : 2^n - 2 \cdot 3^n)$, para todo $n \in \mathbb{N}$.

  Sea d un posible divisor común:

$$\left\{ \begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies d \mid 3^n + 2 \cdot 3^n \implies d \mid 3 \cdot 3^n.$$

  De la misma manera:

$$\left\{ \begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 2 \cdot 2^n + 2 \cdot 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies d \mid 2 \cdot 2^n + 2^n \implies d \mid 3 \cdot 2^n.$$

  Pero

$$d \mid 3 \cdot 3^n \text{ y } d \mid 3 \cdot 2^n \implies d \mid (3 \cdot 3^n : 3 \cdot 2^n) = 3\,(3^n : 2^n) = 3 \cdot 1 = 3.$$

  Por lo tanto, $(2^n + 3^n : 2^n - 2 \cdot 3^n) = 1$ o 3.

  Pero se ve claramente que 3 no puede ser un divisor común ya que $3 \nmid 2^n + 3^n$ (pues si lo dividiera, se tendría que $3 \mid 2^n$, absurdo!). Por lo tanto el 3 queda descartado como posible mcd, y se concluye que $(2^n + 3^n : 2^n - 2 \cdot 3^n) = 1$, $\forall\, n \in \mathbb{N}$.

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a : b) = 6$. Calcular $(a\,b : 6\,a - 6\,b)$.

  "Coprimizando", se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

$$(a\,b : 6\,a - 6\,b) = (36\,a'b' : 36a' - 36b') = (36\,a'b' : 36(a' - b')) = 36(a'b' : a' - b').$$

  Para concluir falta calcular los posibles valores de $(a'b' : a' - b')$ cuando $a' \perp b'$:

  Sea d un divisor común:

$$\left\{ \begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array} \right. \implies \left\{ \begin{array}{l} d \mid a'b' \\ d \mid a'(a' - b') \end{array} \right. \implies \left\{ \begin{array}{l} d \mid a'b' \\ d \mid a'^2 - a'b' \end{array} \right. \implies d \mid a'^2$$

  De la misma manera:

$$\left\{ \begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array} \right. \implies \left\{ \begin{array}{l} d \mid a'b' \\ d \mid b'(a' - b') \end{array} \right. \implies \left\{ \begin{array}{l} d \mid a'b' \\ d \mid a'b' - b'^2 \end{array} \right. \implies d \mid b'^2$$

Obtuvimos $d \mid a'^2$ y $d \mid b'^2$. Luego $d \mid (a'^2 : b'^2)$. Pero, como vimos arriba, $a' \perp b' \Rightarrow a'^2 \perp b'^2$, es decir $(a'^2 : b'^2) = 1$. O sea $d \mid 1$. Así se prueba que los únicos divisores comunes de $a'b'$ y $a' - b'$ son ± 1, luego $a'b' \perp a' - b'$, y se concluye

$$(a\,b : 6\,a - 6\,b) = 36(a'b' : a' - b') = 36.$$

3.6.3. Mínimo común múltiplo.

Definición 3.6.11. (Mínimo común múltiplo.)

Sean $a, b \in \mathbb{Z}$, no nulos. El *mínimo común múltiplo* entre a y b, que se nota $[a : b]$, es el menor número natural que es un múltiplo común de a y b.

Ejemplo: Como todos ya "saben", para $a = 588 = 2^2 \cdot 3 \cdot 7^2$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, el mínimo común múltiplo $[a : b]$ es el producto de todos los primos que aparecen en a y en b a la máxima potencia a la que aparecen, o sea $[a : b] = 2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11$. Probemos este hecho en general.

Proposición 3.6.12. (Mínimo común múltiplo y factorización.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad \textit{con} \quad m_1, \ldots, m_r \in \mathbb{N}_0, \quad b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad \textit{con} \quad n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

$$[a : b] = p_1^{\text{máx}\{m_1, n_1\}} \cdots p_r^{\text{máx}\{m_r, n_r\}}.$$

Demostración. Hay que probar que $p_1^{\text{máx}\{m_1,n_1\}} \cdots p_r^{\text{máx}\{m_r,n_r\}}$ es el menor de los múltiplos comunes de a y b. Investiguemos luego los múltiplos comunes $m > 0$ de a y b:

$$\begin{aligned} a \mid m &\iff m = p_1^{m_1} \cdots p_r^{m_r} \cdot k_1 \qquad \text{para algún } k_1 \in \mathbb{N}, \\ b \mid m &\iff m = p_1^{n_1} \cdots p_r^{n_r} \cdot k_2 \qquad \text{para algún } k_2 \in \mathbb{N}. \end{aligned}$$

Por lo tanto

$$a \mid m \quad \text{y} \quad b \mid m \iff m = p_1^{\text{máx}\{m_1,n_1\}} \cdots p_r^{\text{máx}\{m_r,n_r\}} \cdot k \quad \text{para algún } k \in \mathbb{N}.$$

De esa forma el menor de los múltiples comunes positivos es con $k = 1$ y da $[a : b] = p_1^{\text{máx}\{m_1,n_1\}} \cdots p_r^{\text{máx}\{m_r,n_r\}}$ como se quería probar. □

De la demostración de la proposición anterior se deduce inmediatamente el resultado siguiente:

Corolario 3.6.13. (Mcm y múltiplos comunes.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos y sea $m \in \mathbb{Z}$, con $m \neq 0$. Entonces

$$a \mid m \;\; y \;\; b \mid m \iff [a : b] \mid m.$$

Ejemplo: Observemos que para $a = 2^2 \cdot 3^1 \cdot 7^2$ y $b = 2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$, teníamos $(a : b) = 2^1 \cdot 7^2$ y $[a : b] = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$. Luego

$$\begin{aligned}(a : b) \cdot [a : b] &= (2^1 \cdot 7^2) \cdot (2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \\ &= 2^{1+2} \cdot 3^{0+1} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= 2^{2+1} \cdot 3^{1+0} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= (2^2 \cdot 3^1 \cdot 7^2) \cdot (2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \;=\; a \cdot b.\end{aligned}$$

Es inmediato probar que este resultado vale en general.

Proposición 3.6.14. (Producto mcd y mcm.)

Sean $a, b \in \mathbb{Z}$, no nulos, entonces

$$|a \cdot b| = (a : b) \cdot [a : b].$$

En particular, si $a \perp b$, entonces $[a : b] = |a \cdot b|$.

Esto da una alternativa para calcular el mínimo común múltiplo cuando uno no conoce la factorización de los números. De hecho esta forma de calcular el mínimo común múltiplo es para números grandes más veloz que factorizar los números para luego aplicar la Proposición 3.6.14, ya que calcular el máximo común divisor por el algoritmo de Euclides es para números grandes más veloz que factorizar.

Ejemplo: Determinar todos los pares de números $a, b \in \mathbb{N}$ que satisfacen que

$$(a : b) = 2^2 \cdot 3 \cdot 17 \quad \text{y} \quad [a : b] = 2^5 \cdot 3 \cdot 5^2 \cdot 17^2.$$

Nunca olvidarse que "coprimizar" puede ayudar!

Sabemos que $a = (a : b)\, a'$ y $b = (a : b)\, b'$ con $a' \perp b'$. Luego $(a : b)[a : b] = a\, b = (a : b)^2 a'\, b'$, es decir

$$a'b' = \frac{[a : b]}{(a : b)} = \frac{2^5 \cdot 3 \cdot 5^2 \cdot 17^2}{2^2 \cdot 3 \cdot 17} = 2^3 \cdot 5^2 \cdot 17, \text{ con } a' \perp b'.$$

Al ser $a' \perp b'$ no puede aparecer un mismo primo simultáneamente en a' y b', y por lo tanto las posibilidades son (eligiendo cuáles son los primos que aparecen en a' y luego los restantes estarán en b'):

$$\begin{aligned}&a' = 1,\ b' = 2^3 \cdot 5^2 \cdot 17 \\ &a' = 2^3,\ b' = 5^2 \cdot 17 \\ &a' = 5^2,\ b' = 2^3 \cdot 17 \\ &a' = 17,\ b' = 2^3 \cdot 5^2 \\ &a' = 2^3 \cdot 5^2,\ b' = 17 \\ &a' = 2^3 \cdot 17,\ b' = 5^2 \\ &a' = 5^2 \cdot 17,\ b' = 2^3 \\ &a' = 2^3 \cdot 5^2 \cdot 17,\ b' = 1.\end{aligned}$$

Multiplicando estos números por $(a : b) = 2^2 \cdot 3 \cdot 17$ se obtienen todos los pares (a, b).

Terminemos este capítulo mencionando una famosa y clásica conjetura sobre primos, la *conjetura de los primos gemelos*, y los recientes avances sobre el tema. Se dice que dos números primos son gemelos si difieren en 2, como por ejemplo 41 y 43. La conjetura, aún no resuelta, afirma que existen infinitos pares de primos gemelos.

En Abril 2013, el matemático chino-americano Yitang Zhang anunció el resultado cercano más relacionado en algún sentido con esta conjetura, ya que también se trata de diferencias entre primos: Zhang anunció que existen infinitos pares de primos, no gemelos, pero que difieren en menos de 70 millones.

A partir del resultado de Zhang, se ha promovido una carrera para reducir esa diferencia: el 3 de Octubre del 2013 la brecha llegó a 4680. Es decir hoy en día se sabe que existen infinitos pares de primos que difieren en menos de 4680. Los avances aparecen en la página http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes

Aunque todos concuerdan en que este método no va a permitir reducir tanto la brecha como para llegar a 2, es decir a probar la conjetura de los primos gemelos...