Aritmética de Números Enteros

Pablo De Nápoli

versión 0.8.3

Resumen

Este es un apunte de las teóricas de Algebra I, turno noche del primer cuatrimestre de 2007, con algunas modificaciones introducidas en 2014.

"Dios creó los números naturales. Todo lo demás es invento del hombre." Leopold Kronecker (1823-1891)

"La matemática es la reina de las ciencias, y la teoría de los números es la reina de la matemática." (Carl F. Gauss, 1777–1855)

1. Divisibilidad

Recordamos algunas notaciones usuales:
Notamos por $\mathbb{N}$ al conjunto de los números naturales (o enteros positivos)

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

y por $\mathbb{N}_0$ al conjunto de los números naturales incluyendo al cero (también llamados enteros no negativos):

$$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$$

Finalmente, notamos por $\mathbb{Z}$ al conjunto de los números enteros (positivos, negativos y cero)

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

En el conjunto $\mathbb{Z}$ de los números enteros, las operaciones de suma $a+b$, resta $a-b$ y producto ab son siempre posibles[1]. En cambio, la división $a:b$ no es siempre posible.

Por ejemplo, la división $6:3$ es posible, ya que existe un entero 2 tal que $6=3\times 2$. Mientras que la división $7:3$ no es posible, ya que no existe ningún entero c tal que $7=3c$.

Esto motiva la siguiente definición:

Definición 1.1 *Sean $a,b\in\mathbb{Z}$ dos enteros, $b\neq 0$, diremos que b divide a a, o que a es divisible por b, o que a es un múltiplo de b, o que b es un factor de a si existe algún entero $c\in\mathbb{Z}$ (necesariamente único) tal que $a=bc$. (De modo que $a:b=c$). Simbolizamos este hecho mediante la notación: $b|a$*

Por ejemplo, 3 divide a 6, pero 3 no divide a 7.

Algunas propiedades elementales de la divisibilidad son las siguientes:

- Para cualquier $a\in\mathbb{Z}$, $a\neq 0$; $a|a$ (ya que $a=a\times 1$). Es decir, la relación de divisibilidad es reflexiva.
- Para cualquier $a\in\mathbb{Z}$, $a\neq 0$; tenemos que $a|0$.
- Para cualquier $a\in\mathbb{Z}$, $1|a$ y $-1|a$ (ya que $a=1\times a=(-1)\times(-a)$). Vemos que 1 y -1 son divisores universales[2].
- Si $a|b$ y $b|c$ (siendo $a,b\neq 0$) entonces $a|c$, vale decir que la divisibilidad es una relación transitiva.

  Prueba: Como $a|b$, existe un entero e tal que

  $$b=ae$$

  y como $b|c$, existe un entero f tal que

  $$c=bf$$

[1] Esto suele expresarse en álgebra diciendo que $\mathbb{Z}$ es un anillo. Más adelante veremos otros ejemplos de anillos, como los polinomios, en los cuales también es posible desarrollar una teoría de la divisibilidad, en estrecho paralelismo con la aritmética de los enteros.

[2] En la terminología usual en álgebra, esto se expresa diciendo que ± 1 son las unidades de $\mathbb{Z}$

Sustituyendo en esta ecuación el valor de b, y usando la propiedad asociativa del producto:

$$c = (ae)f = a(ef)$$

Concluimos que $a|c$. □

- Si $a|b$, entonces $(-a)|b$, $a|(-b)$ y $(-a)|(-b)$. Vale decir que para las cuestiones de divisibildad los números a y $-a$ son completamente equivalentes[3] (podemos olvidarnos del signo cuando estamos estudiando cuestiones de divisibilidad)

- Si $b|a$ siendo $a, b \neq 0$, entonces $|b| \leq |a|$.

  Prueba: Si $b|a$, entonces existe un c tal que $a = bc$. Tomando módulo, tenemos que:

  $$|a| = |b||c|$$

  y como $|c| \geq 1$ (ya que si $c = 0$ entonces sería $a = 0$), concluimos que:

  $$|a| \geq |b|$$

  □

- Si $a|b$ y $b|a$ (siendo $a, b \neq 0$) entonces $a = \pm b$.

  Prueba: Por la propiedad anterior, $|a| \leq |b|$ y $|b| \leq |a|$. En consecuencia, $|a| = |b|$. Y concluimos que $a = \pm b$. □

- En particular, concluimos que si nos restringimos a los enteros positivos, la relación de orden resulta antisimétrica. Siendo reflexiva, antisimétrica y transitiva, concluimos que la divisibilidad es una relación de orden (en sentido amplio) en $\mathbb{N}$. Sin embargo, no es una relación de orden total, ya que existen elementos incomparables (por ej: 3 y 5 son incomparables, ya que no es cierto que 3 divida a 5, ni tampoco que 5 divida a 3).

- Si $a|b$ y $a|c$, se tiene que $a|b + c$ y que $a|b - c$.

  Prueba: Como $a|b$, existirá un entero e tal que:

  $$b = ae$$

[3] En la terminología usual en álgebra, se dice que a y $-a$ son elementos asociados de $\mathbb{Z}$

y como $a|c$, existirá otro entero f tal que:

$$c = af$$

Sumando estas dos ecuaciones, y aplicando la propiedad distributiva, tenemos que:

$$b + c = ae + af = a(e + f)$$

Concluimos que $a|b + c$. Similarmente, tenemos que:

$$b - c = ae - af = a(e - f)$$

y concluimos que $a|b - c$. □

2. Números Primos

Definición 2.1 *Decimos que un número $p \in N$, $p > 1$ es* **primo**, *cuando sus únicos divisores (en $\mathbb{N}$) son 1 y p. Los números naturales mayores que 1, que no son primos, se denominan* **compuestos**. *Un número n es compuesto si es posible expresarlo en la forma $n = n_1 n_2$ donde $1 < n_1, n_2 < n$.*

Los primeros números primos (menores que 100) son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

La importancia de los números primos radica en que en algún sentido son los "átomos" o "bloques" con los que se forman los demás números:

Teorema 2.1 *Todo entero $n > 1$, o bien es primo o se puede descomponer como producto de números primos.*

Prueba: Hacemos inducción global en n. Para $n = 1$ no afirmamos nada (luego el teorema es trivialmente cierto en este caso). Consideremos pues un número $n > 1$, y supongamos que el teorema es cierto para los números menores que n. Si n es primo, tampoco afirmamos nada. Supongamos pues que n es compuesto. En este caso, por definición, es posible escribir a n como producto de dos números naturales $n_1, n_2 \in \mathbb{N}$ menores que n

$$n = n_1 n_2$$

Pero por hipótesis de inducción entonces, n_1 y n_2 se descomponen como producto de primos:

$$n_1 = p_1 p_2 \dots p_k$$

$$n_2 = q_1 q_2 \dots q_s$$

donde $p_1, p_2, \dots p_k$ y $q_1, q_2, \dots q_s$ son primos. Entonces n también se puede descomponer como producto de primos:

$$n = p_1 p_2 \dots p_k q_1 q_2 \dots q_s$$

En virtud del principio de inducción global, concluimos que el teorema es verdadero para cualquier $n \in \mathbb{N}$. □

Corolario 2.1 *Todo número entero $n > 1$ que no sea primo, es divisible por un primo.*

Por ejemplo, supongamos que queremos obtener una descomposición de 60 como producto de primos. Comenzamos escribiendo $30 = 4 \times 15$. Pero $4 = 2 \times 2$ y $15 = 3 \times 5$, luego

$$60 = 2 \times 2 \times 3 \times 5$$

(Observemos que algunos primos pueden repetirse en la factorización)

Constituye un hecho de fundamental importancia (conocido como teorema fundamental de la aritmética) que la descomposición de un entero como producto de primos **es única**, salvo el orden de los factores. Demostraremos esto más adelante (obtendremos este heho, como una consecuencia del algoritmo de Euclides para el cálculo del máximo común divisor).

Otra observación importante es que si bien es relativamente sencillo obtener la factorización en factores primos para números pequeños, no se conoce ningún algoritmo eficiente (esto es: un procedimiento efectivo) para la obtención de la descomposición en factores primos de números grandes[4].

Otro hecho muy importante, ya demostrado por el matemático griego Euclides (que vivió aproximadamente hacia el 300 A.C.) en sus *Elementos*[5], es que el conjunto de los números primos es infinito:

[4]Por un algoritmo eficiente, queremos decir un algoritmo cuya complexijad (número de operaciones requeridas) sera polinomial, como función del número de dígitos del número n. Se ha conjeturado que la factorización en factores primos tiene complejidad exponencial pero esto no ha sido demostrado.

[5]Libro IX, Proposición 20. Disponible (traducido al inglés) en `http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html`

Teorema 2.2 (Euclides) *Existen infinitos números primos.*

Prueba: La prueba de Euclides de este teorema, ha quedado como un ejemplo clásico de demostración por reducción al absurdo. Este método de demostración consiste en suponer que el teorema es falso, y mediante una serie de pasos lógicos llegar a una contradicción. Esta contradicción nos permite concluir que la suposición de que el teorema es falso no puede sostenerse, y en consecuencia, el teorema debe ser verdadero.

Supongamos pues que sólo existiera una cantidad finita de números primos:

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_N$$

El argumento de Euclides, consiste entonces en formar el número

$$q = p_1 p_2 \ldots p_N + 1$$

Conforme al corolario del teorema anterior, o bien q es primo, o bien es divisible por algún primo $q' < q$. Pero q no es divisible por ninguno de los primos p_1, p_2, $\ldots p_N$ (ya que si $p_i | q$ entonces $p_i | q - p_1 p_2 \ldots p_N = 1$ y sería $p_i = 1$, lo cual es absurdo). En cualquiera de los dos casos, hemos encontrado un primo que no no está en nuestra lista inicial, que de acuerdo a la suposición que hemos hecho era una lista completa de todos los números primos.

Esta contradicción prueba que nuestra hipótesis de que sólo existe un número finito de números primos no puede sostenerse, y en consecuencia, podemos concluir que existe un número infinito de números primos. □

Ejercicio: La prueba de Euclides no es la única prueba posible de la infinitud de los primos. Una prueba alternativa[6] debida a G. Pólya utiliza los denominados números de Fermat:

$$F_n = 2^{2^n} + 1$$

Los primeros F_n son

$$F_0 = 3$$

$$F_1 = 5$$

[6] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 4ta. Edición, teorema 16

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

y son todos primos. Fermat conjeturó entonces, que los números F_n eran todos primos. Sin embargo, esta conjetura resultó ser falsa pues:

$$F_5 = 4294967297 = 641 \times 6700417$$

A pesar de que los F_n no son necesariamente primos, sí es posible probar que los diferentes F_n son coprimos (no tienen factores en común). En consecuencia, cada F_n es divisible por un primo diferente y por lo tanto, podemos concluir que existen infinitos primos.

Sugerencia: Usando la identidad algebraica

$$\frac{x^n + 1}{x + 1} = x^{n-1} - x^{n-2} + x^{n-3} - \ldots + x - 1$$

válida para todo entero n par, demostrar que $F_n | F_m - 2$ si $m > n$. Concluir que F_n y F_m son coprimos si $n \neq m$.

Otra prueba diferente de la infinitud de los primos, fue dada por Juan Pablo Pinasco en [6].

3. El algoritmo de división

Toda la aritmética gira en torno del siguiente hecho fundamental, conocido desde la escuela primaria: Si bien la división $a : b$ puede resultar imposible dentro de los enteros, siempre es posible efectuar una división aproximada, obteniendo un resto menor que el divisor. Por ejemplo: la división entera de 7 por 3 da un cociente de 2 con un resto de 1, y se tiene que $7 = 3 \times 2 + 1$.

El siguiente teorema, formaliza este hecho:

Teorema 3.1 *Dados números naturales $a \in \mathbb{N}_0$ y $b \in \mathbb{N}$ existen únicos números naturales tales que $a = bq + r$ y $0 \leq r < b$.*

Definición 3.1 *En la situación del teorema anterior, diremos que q es el cociente y r el resto en la división entera de a por b.*

Prueba: Primero probaremos la existencia: para ello consideramos el siguiente conjunto

$$C = \{a - bk : k \in \mathbb{N}_0, a - bk \geq 0\} \subset \mathbb{N}_0$$

Afirmamos que C es no vacío. En efecto tomando $k = 0$ vemos que $a \in C$. En consecuencia, por el principio del mínimo entero C tiene un elemento mínimo. Llamamos r a este mínimo. Como $r \in C$, se tiene que r se escribe en la forma $r = a - bq$ para algún $q \in \mathbb{N}_0$ (y por lo tanto $a = bq + r$), y que $r \geq 0$.

Sólo falta pues probar que $r < b$. Si por el contrario fuera $r \geq b$, podemos considerar $r' = r - b \geq 0$. Tenemos que:

$$r' = a - bq - b = a - (q + 1)b$$

Concluimos que $r' \in C$. Pero como $r' < r$, esto contradice el hecho de que r era el mínimo de C. En consecuencia, deducimos que necesariamente $r < b$. Esto concluye la prueba de la parte de existencia.

Ahora hemos de demostrar la unicidad: para ello supongamos que tuvieramos dos posibles cocientes q y q', con sus correspondientes restos r y r'. Es decir que,

$$a = bq + r \text{ con } 0 \leq r < b$$

$$a = bq' + r' \text{ con } 0 \leq r < b$$

Entonces igualando estas ecuaciones tendríamos que:

$$bq + r = bq' + r'$$

y por lo tanto:

$$b(q' - q) = r - r' \tag{1}$$

En particular, vemos que

$$b | r - r'$$

Podemos sin pérdida de generalidad, suponer que $r \geq r'$ (intercambiando sino los nombres). Entonces conclumos que si $r \neq r'$, sería $b \leq r - r'$, y por lo tanto $b \leq r$.

Pero sabíamos que $r < b$. Esta contradicción, muestra que necesariamente se tiene que $r = r'$, y entonces por (1),

$$b(q' - q) = 0$$

Como si el producto de dos enteros da cero, alguno de los dos debe ser cero, concluimos así mismo que $q = q'$. □

Observación: En particular, se tiene que $b|a$ si y sólo si el resto en la división entera de a por b es cero.

En general, en matemática, la palabra *algoritmo* hace referencia a un procedimiento mecánico para calcular algo. En este caso, la prueba anterior no parece proporcionar realmente un algoritmo para calcular q y r; pero es fácil darse cuenta que en efecto hay un algoritmo escondido en la prueba anterior: se trata del algoritmo de división por restas sucesivas[7]

ENTRADA: a (dividendo),b (divisor), siendo $b \neq 0$.

SALIDA: q (cociente) y r(resto), en la división entera de a por b

1. $r \leftarrow a$
2. $q \leftarrow 0$
3. Mientras $r \geq b$, repetir las siguientes instrucciones:
   a) $r \leftarrow r - b$
   b) $q \leftarrow q + 1$

En algunas situaciones será útil considerar divisiones enteras con números negativos. En este caso el algoritmo de división se enuncia del siguiente modo:

Teorema 3.2 *Dados números enteros $a, b \in \mathbb{Z}$ con $b \neq 0$ existen únicos números enteros tales que $a = bq + r$ y $0 \leq r < |b|$.*

[7]Escribimos este algoritmo en forma de *pseudocódigo*, fácilmente traducible a cualquier lenguaje de programación. q y r son variables, es decir espacios en la memoria de la computadora en los que podemos guardar datos (en este caso, números). La flecha $\leftarrow$ representa la operación de asignación de un valor a una variable (es decir que dicho valor se guarda temporariamente en dicha variable). Por ejemplo la asignación $q \leftarrow q + 1$ tiene el efecto de incrementar en uno el valor de la variable q.

Prueba: El caso en que $a \geq 0, b > 0$ ya lo demostramos antes. Consideremos por ejemplo el caso[8] en que $a < 0$ y $b > 0$. En ese caso $-a > 0$, y podemos dividir $-a$ por b utilizando el teorema anterior, para obtener un cociente q' y un resto r', de modo que

$$(-a) = q'b + r' \; y \; 0 \leq r' < b$$

Si $r' = 0$, tenemos que:

$$a = (-q)b$$

Luego tomando $r = 0$ y $q = -q'$ tenemos lo que queremos. Si $r' \neq 0$, notamos que:

$$a = (-q')b - r' = (q' - 1)b + b - r'$$

Como $0 \leq b - r' < b$, tomando $q = q' + 1$ y $r = b - r'$ se cumple el enunciado. Esto concluye la prueba de la existencia del cociente y el resto en este caso, la prueba de la unicidad es análoga a la que dimos antes. Queda ver que sucede en el caso $b < 0$. La idea es similar. Lo dejamos como ejercicio. □

Ejercicio: Completar la prueba del teorema anterior, para el caso en que $b < 0$.

4. Bases de numeración

Desde la escuela primaria estamos familiarizados con la representación de enteros en diferentes bases. Por supuesto, lo primero que se aprende es la base decimal (donde tenemos 10 dígitos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$).

$$1035 = 1 \times 10^4 + 0 \times 10^3 + 3 \times 10^1 + 5 \times 10^0$$

Pero también es posible utilizar otras bases. Por ejemplo en la base binaria (base 2) tenemos sólo dos dígitos 0 y 1, y por ejemplo el número once se escribe como 1011 en binario[9], ya que

$$1011_2 = 1 \times 2^3 + 0 \times 2^3 + 1 \times 2^1 + 1 \times 2^0 = 11$$

[8]Este caso nos será útil más adelante, al estudiar congruencias.

[9]Es costumbre indicar la base como subíndice, así pues 102_3 quiere decir el número cuyo desarrollo en base 3 es 102.

La base binaria es muy utilizada en computación, debido a que los circuitos de las computadoras digitales almacenan la información en unidades (bits) que tienen dos estados posibles [10], que podríamos pensar como encendido (típicamente 5 volt) o apagado (0 volt). Si pensamos al estado "apagado" como cero, y "encendido" como uno. Entonces, un número puede representarse en una computadora como un conjunto de bits, utilizando el sistema binario de numeración.

El algoritmo para expresar un número en una determinada base es bien conocido desde la escuela: consiste en efectuar sucesivas divisiones enteras del número por la base, hasta obtener un cociente nulo.

Por ejemplo: para expresar 11 en la base 2 efectuamos las divisiones:

$$11 = 5 \times 2 + 1$$
$$5 = 2 \times 2 + 1$$
$$2 = 1 \times 2 + 0$$
$$1 = 0 \times 2 + 1$$

Entonces el desarrollo de 11 en base 2 está formado por los sucesivos restos 1, 1, 0 y 1.

Notemos que los ceros a la izquierda no aportan nada: por ejemplo

$$00123 = 123$$

Salvo esta ambigüedad, el desarrollo de un número en una base dada, es único. Ahora enunciaremos esto como un teorema formal:

Teorema 4.1 *Dada una base $b \geq 2$ entera, siempre es posible escribir a cada entero $n \in \mathbb{N}$ de una única forma como:*

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

donde $d_i \in \mathbb{N}_0$ y $0 \leq d_i < b$, y $d_k \neq 0$.

Prueba: Para probar la existencia del desarollo, utilizamos un argumento de inducción global en n.

Claramente $n = 1$ admite el desarollo $1 = 1b^0$.

[10] De hecho la palabra **bit** es una abreviatura de binary digit.

Si $n > 1$, y suponemos que el teorema es cierto para los números menores que n, efectuamos la división entera de n por b, escribiendo entonces:

$$n = qb + d_0$$

donde $0 \leq d_0 < b$. Pero como $b \geq 2$, el cociente q es menor que n. Entonces por la hipótesis inductiva, n admitirá un desarrollo de la forma:

$$q = d_k b^{k-1} + d_{k-1} b^{k-2} + \ldots + d_3 b^2 + d_2 b^1 + d_1 b^0$$

(para algún k y ciertos d_i con $0 \leq d_i < b$, y $d_k \neq 0$).

Sustituyendo vemos que:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

En virtud del principio de inducción global, concluimos que cualquier $n \in \mathbb{N}$ admite algún desarrollo en base b.

Para establecer la unicidad del desarrollo, procedemos también por inducción global en n.

Claramente el único desarrollo posible de $n = 1$ es $1 = 1 \times b^0$ (pues si $d_i \neq 0$ para algún $i > 1$, $n \geq b$. Y entonces debe ser $1 = d_0$).

Supongamos pues, que el número n admitiera dos desarrollos en base b:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

$$n = d'_j b^j + d'_{k-1} b^{k-1} + \ldots + d'_2 b^2 + d'_1 b^1 + d'_0 b^0$$

donde $0 \leq d_i < b$ y $0 \leq d'_i < b$ para todo i, $d_k \neq 0$, $d'_j \neq 0$; y supongamos que los números menores que n admiten un único desarrollo.

Nuevamente, tenemos que:

$$n = qb + d_0$$

$$n = q'b + d'_0$$

donde

$$q = d_k b^{k-1} + d_{k-1} b^{k-2} + \ldots + d_3 b^2 + d_2 b^1 + d_1 b^0$$

$$q' = d'_j b^{j-1} + d'_{j-1} b^{j-2} + \ldots + d'_3 b^2 + d'_2 b^1 + d'_1 b^0$$

Pero entonces, por la unicidad del cociente y del resto en la división entera de n por b, tendremos que $q = q'$ y que $d_0 = d'_0$.

Pero entonces como $q < n$, en virtud de la hipótesis de inducción global, los desarrollos de q y q' (que son el mismo número) deben coincidir, es decir que $k = j$ y $d_i = d'_i$ para $1 \leq i \leq k$.

En virtud del principio de inducción global, esto prueba que cualquier $n \in \mathbb{N}$ admite un único desarrollo en base b. □

Otras bases muy utilizadas en computación son la base 8 (octal) y 16 (hexadecimal), porque son útiles como abreviatura de la base binaria, pues como $8 = 2^3$ y $16 = 2^4$ cada dígito octal equivale a tres dígitos binarios y cada dígito hexadecimal equivale a cuatro dígitos binarios.

Por ejemplo: el número $202 = 2^8 + 2^4 + 2^3 + 2^1$ se representa en binario como 11001010. Para escribirlo en octal agrupamos sus dígitos de a tres como 11 001 011, ahora 11 es 3 en binario, 001 es 1 y 010 es 2, concluimos que 202 se escribe como 312 en octal, y en efecto:

$$202 = 3 \times 8^2 + 1 \times 8^1 + 2 \times 8^0$$

Para escribir un número en hexadecimal necesitamos 16 dígitos. Por ello, además de los dígitos usuales 0,1,2,3,4,5,6,7,8,9; se emplean las letras A (=10), B (=11), C (=12), D (=13), E (=14) y F (=15).

Continuando con el ejemplo anterior, para escribir 202 en hexadecimal, agrupamos sus dígitos binarios de a cuatro:

$$1100\ 1010$$

Ahora 1100 es 12 ($= C$) en binario, y 1010 es 10 ($= A$) en binario. Concluimos que 202 se escribr como CA en hexadecimal. Y en efecto,

$$202 = 12 \times 16^1 + 10 \times 16^0$$

Ejercicio: Justificar porqué la base octal y la base hexadecimal se pueden utilizar como abreviatura de la base binaria.

Otro ejercicio: ("base factorial") Probar que cada $n \in \mathbb{N}_0$ puede expresarse de una única forma como

$$n = d_1 + d_2 \times 2! + d_3 \times 3! + \ldots + d_k \times k!$$

donde $0 \leq d_i < k$ para $i = 1, 2, \ldots k$.

5. El algoritmo de Euclides para el cálculo del máximo común divisor

El algoritmo de Euclides[11] es un algoritmo para el cálculo del máximo común divisor entre dos números.

Definición 5.1 *Sean $a, b \in \mathbb{N}$ dos enteros positivos. Definimos el máximo común divisor entre a y b como el máximo de los divisores comunes entre a y b, es decir como el máximo de los enteros positivos d tales que $d|a$ y $d|b$. Notación: $d = (a, b)$ o $d = mcd(a, b)$.*

Por ejemplo, sean $a = 18$ y $b = 12$. Los divisores de 18 son[12]

$$1, 2, 3, 6, 9, 18$$

y los de 12 son

$$1, 2, 3, 4, 6, 12$$

Por lo tanto, los divisores comunes son $1, 2, 3$ y 6, y en consecuencia, el máximo común divisor entre 18 y 12 es 6.

Para calcular el máximo común divisor entre dos enteros $r_0 = a$ y $r_1 = b$ el algoritmo de Euclides realiza una serie de divisiones sucesivas (Supondremos por simplicidad que $a > b$, ya que sino podemos intercambiar los roles).

Primero dividimos a por b, obteniendo un primer cociente q_1 y un resto que llamamos r_2, de modo que:

$$a = bq_1 + r_2 \quad (0 \leq r_2 < r_1) \tag{2}$$

(Llamamos r_2 al primer resto y no r_1 porque llamando r_0 a a y r_1 a b podemos escribir esta ecuación como

$$r_0 = r_1 q_1 + r_2 \quad (0 \leq r_2 < r_1)$$

[11] *Elementos*, libro VII, proposición 2, disponible (traducido al inglés) en `http://aleph0.clarku.edu/~djoyce/java/elements/bookVII/propVII2.html`. Como siempre, Euclides presenta sus razonamientos de una manera geométrica, pensando los números dados por longitudes de segmentos. Notar también que la versión original del algoritmo utiliza restas sucesivas en lugar de divisiones, pero esto es notablemente menos eficiente.

[12] Más adelante veremos como obtener todos los divisores de un número en forma sistemática a partir de su factorización como producto de primos.

y esto facilitará la escritura de las demostraciones subsiguientes)

Si $r_2 \neq 0$, podemos dividir r_1 por r_2, obteniendo un nuevo cociente q_2 y un nuevo resto r_3 de modo que:

$$r_1 = r_2 q_2 + r_3 \quad (0 \leq r_3 < r_2)$$

Si $r_3 \neq 0$, podemos volver a dividir r_2 por r_3, obteniendo ahora un cociente q_3 y un resto r_4 de modo que:

$$r_2 = r_3 q_3 + r_4 \quad (0 \leq r_4 < r_3)$$

Así podemos continuar este proceso, mientras $r_k \neq 0$, dividimos a r_{k-1} por r_k, obteniendo un cociente q_k y un resto r_{k+1}, de modo que:

$$r_{k-1} = r_k q_k + r_{k+1} \quad (0 \leq r_{k+1} < r_k) \tag{3}$$

Observamos que la sucesión de restos que vamos obteniendo es decreciente:

$$r_1 > r_2 > r_3 > \dots$$

Por ello, tarde o temprano este proceso recursivo debe detenerse, y obtendremos que $r_N = 0$ para algún N. Afirmamos entonces que el último resto no nulo proporciona el máximo común divisor:

Teorema 5.1 *Sean $a, b \in \mathbb{N}$ y sea $r_0 = a, r_1 = b, r_2, \dots, r_{N-1}, r_N = 0$ la sucesión de restos construida por el algoritmo de Euclides. Entonces,*

$$r_{N-1} = mcd(a, b)$$

Prueba:

Probaremos este teorema en dos etapas:

Etapa 1: Probaremos que $r_{N-1}|r_k$ para todo k y por lo tanto que $r_{N-1}|a$ y $r_{N-1}|b$, es decir que probaremos que r_{N-1} es un divisor común de a y b.

Notamos que la última ecuación del algoritmo de Euclides es [(3) con $k = N - 1$]:

$$r_{N-2} = r_{N-1}\, q_{N-1}$$

En consecuencia $r_{N-1}|r_{N-2}$. La ecuación anterior es:

$$r_{N-3} = r_{N-2}\, q_{N-2} + r_{N-1}$$

Pero como ya sabemos que $r_{N-1}|r_{N-2}$ podemos deducir que $r_{N-1}|r_{N-3}$.

En general, probaremos por inducción global en j que $r_{N-1}|r_{N-j}$ para $j = 1, 2, 3, \ldots, N$: Para $j = 1$ es obvio, y para $j = 2$ ya lo probamos.

Supongamos que efectivamente $r_{N-1}|r_{N-l}$ para $l = 1, 2, \ldots, j-1$. Entonces por (3) con $k = N - (j-1)$

$$r_{N-j} = r_{N-(j-1)}\, q_{N-(j-1)} + r_{N-(j-2)}$$

Pero por hipótesis inductiva, estamos asumiendo que $r_{N-1}|r_{N-(j-1)}$ y $r_{N-1}|r_{N-(j-2)}$. Concluimos que $r_{N-1}|r_{N-j}$.

El principio de inducción global, implica entonces que $r_{N-1}|r_{N-j}$ para todo j con $1 \leq j \leq N$. En particular $r_{N-1}|r_0 = a$ y $r_{N-1}|r_1 = b$, como afirmamos.

Etapa 2: Probaremos que si d es cualquier divisor común de a y b entonces $d|r_{N-1}$, en consecuencia, si $d > 0$, $d \leq r_{N-1}$. Esto probará que r_{N-1} es el máximo común divisor.

Notamos que si d es un divisor común de a y b, la primera ecuación del algoritmo de Euclides:

$$a = bq_1 + r_2$$

implica que $d|r_2$. La segunda ecuación:

$$r_1 = r_2 q_2 + r_3$$

implica entonces que $d|r_3$ y continuando podemos probar por inducción global en k que $d|r_k$ para $k = 1, 2, \ldots, r_{N-1}$.

En efecto, para $k = 1, 2$ ya lo probamos. Si asumimos que $d|r_l$ para $l = 1, 2, \ldots, k-1$, tenemos que por (3) con $k-1$ en lugar de k):

$$r_{k-2} = r_{k-1}\, q_{k-1} + r_k$$

y entonces como por hipótesis inductiva $d|r_{k-1}$ y $d|r_{k-2}$, concluimos que $d|r_k$.

El principio de inducción global permite afirmar entonces que $d|r_k$ para todo k con $1 \leq k \leq N-1$. □

Ejemplo: Calculemos el máximo común divisor entre 360 y 42 utilizando el algoritmo de Euclides: mediante sucesivas divisiones encontramos que:

$$\begin{aligned} 360 &= 8 \times 42 + 24 \\ 42 &= 1 \times 24 + 18 \\ 24 &= 1 \times 18 + 6 \\ 18 &= 3 \times 6 + 0 \end{aligned}$$

En este caso, el último resto no nulo, que proporciona el máximo común divisor es 6.

Incidentalmente la demostración del teorema anterior, proporciona la siguiente caracterización del máximo común divisor[13]:

Corolario 5.1 *El máximo común divisor $d = mcd(a, b)$ entre dos números naturales $a, b \in \mathbb{N}$, está caracterizado por las siguientes propiedades:*

i) Es un divisor común: $d|a$ y $d|b$.

ii) Cualquier otro divisor común d' lo divide: si $d'|a$ y $d'|d$, entonces $d'|d$.

Una consecuencia muy importante del algoritmo de Euclides es la siguiente:

Teorema 5.2 *Sean $a, b \in \mathbb{N}$ y sea $d = mcd(a, b)$ su máximo común divisor. Entonces, existen enteros $\alpha, \beta \in \mathbb{Z}$ tales que:*

$$\alpha a + \beta b = d$$

es decir, que el máximo común divisor entre dos enteros positivos, siempre se puede escribir como una **combinación lineal** *entre ellos, con coeficientes enteros.*

Obtendremos la demostración de este teorema como caso particular ($k = N - 1$) del siguiente lema:

Lema 5.1 *Para $= 0, 1, \ldots, N - 1$, existen enteros $\alpha_k, \beta_k \in \mathbb{Z}$ tales que:*

$$\alpha_k a + \beta_k b = r_k$$

[13]Esta caracterización afirma que el máximo común divisor entre a y b es el **ínfimo** entre ellos (o sea la mayor cota inferior de ambos), en el orden dado por la divisibilidad.

Prueba: Definiremos la sucesiones $(\alpha_k)_{0\leq k\leq N-1}$ y $(\beta_k)_{0\leq k\leq N-1}$ recursivamente. Para $k=0$, definimos $\alpha_0=1$, $\beta_0=0$ de modo que:

$$a = r_0 = \alpha_0\, a + \beta_0\, b$$

Similarmente, para $k=1$, definimos $\alpha_1=0$, $\beta_1=1$, de modo que:

$$b = r_1 = \alpha_1\, a + \beta_1\, b$$

Tomemos ahora un $k>1$, por (3), con $k-1$ en lugar de k, tenemos que:

$$r_{k-2} = r_{k-1}q_{k-1} + r_k$$

o sea:

$$r_k = r_{k-2} - r_{k-1}q_{k-1}$$

Entonces, utilizando nuevamente inducción global en k, tenemos que:

$$r_k = (\alpha_{k-2}a + \beta_{k-2}b) - (\alpha_{k-1}a + \beta_{k-1}b)q_{k-1}$$

$$= (\alpha_{k-2} - \alpha_{k-1}q_{k-1})a + (\beta_{k-2} - \beta_{k-1}q_{k-1})b$$

En consecuencia,definimos α_k y β_k recursivamente por:

$$\alpha_k = \alpha_{k-2} - \alpha_{k-1}q_{k-1} \text{ para } k = 2, 3, \ldots, N-1$$

$$\beta_k = \beta_{k-2} - \beta_{k-1}q_{k-1} \text{ para } k = 2, 3, \ldots, N-1$$

y el principio de inducción global nos permite concluir que el lema se verifica para todo con $1 \leq k \leq N-1$. □

Continuación del ejemplo anterior: En el ejemplo anterior, en el que calculamos el máximo común divisor entre 360 y 42, el proceso descripto nos proporciona las siguientes escrituras de los sucesivos restos como combinación lineal de 360 y 42 (La última igualdad, corresponde a la escritura del máximo común divisor):

$$\begin{array}{rcrrcrr} 24 & = & 1 & \times 360 & + & (-8) & \times 42 \\ 18 & = & (-1) & \times 360 & + & 9 & \times 42 \\ 6 & = & 2 & \times 360 & + & (-17) & \times 42 \end{array}$$

Más adelante, resultará de utilidad extender la noción de máximo común divisor a números enteros negativos o cero. Dado que dos números enteros que

sólo difieren en el signo son equivalentes respecto a la divisibilidad, resulta natural definir que:

$$\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$$

Por ejemplo, de acuerdo a esta definición, tenemos que:

$$\text{mcd}(-4, 6) = \text{mcd}(4, 6) = 2$$

Y también definimos:

$$\text{mcd}(a, 0) = \text{mcd}(0, a) = a$$

Observenos que al extender la noción de máximo común divisor de esta manera, los teoremas anteriores se siguen verificando.

El teorema anterior, proporciona una serie de consecuencias de gran importancia. Comencemos por una definción:

Definición 5.2 *Decimos que dos números $a, b \in \mathbb{Z}$ son coprimos (o primos entre sí) si los únicos divisores comunes de a y b son ± 1. Esto es claramente equivalente a decir que su máximo común divisor $mcd(a, b)$ es 1.*

Corolario 5.2 *Dos enteros $a, b \in \mathbb{Z}$ son coprimos si y sólo si existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha a + \beta b = 1$.*

Prueba: Por el teorema anterior, si el máximo común divisor es 1, es claro que se escribe como una combinación lineal de a y b. Recíprocamente, si existen α y β tales que $1 = \alpha a + \beta b$ entonces si d es un divisor común de a y b, tenemos que $d|\alpha a$, $d|\beta b$ y en consecuencia: $d|\alpha a + \beta b = 1$, luego $d = \pm 1$. Concluimos que a y b son coprimos. □

Corolario 5.3 *Si $a|bc$ y a es coprimo con b, entonces a divide a c.*

Prueba: Como a es coprimo con b, por lo anterior 1 se escribe como una combinación lineal de a y b, es decir existen $\alpha, \beta \in Z$ tales que:

$$\alpha a + \beta b = 1$$

Entonces, multiplicando por c tenemos que:

$$\alpha ac + \beta bc = c$$

Como $a|\alpha ac$, y $a|\beta bc$, concluimos que $a|c$. □

Un caso particular de este corolario, nos conducirá a la prueba del teorema fundamental de la aritmética (unicidad de la descomposición en factores primos):

Corolario 5.4 *Si p es un número primo y $p|ab$, entonces $p|a$ o $p|b$.*

Prueba: Notamos que si p no divide a a, entonces p es coprimo con a (por ser p primo). En consecuencia, por el corolario anterior como $p|ab$, $p|b$. □

Es conveniente observar que este corolario se generaliza sin dificultad a productos de más de dos factores (haciendo inducción en el número de factores)

Corolario 5.5 *Si p es un número primo y $p|a_1a_2\dots a_k$, entonces $p|a_i$ para algún i.*

Ejercicio: Demostrar por inducción que en cada paso del algoritmo de Euclides se tiene que:

$$\text{mcd}(a,b) = \text{mcd}(r_k, r_{k-1})$$

(Una prueba alternativa, quizás más sencilla, del teorema 5.1 puede basarse en este hecho). Una condición como esta, que se mantiene en cada paso de un algoritmo se denomina un **invariante del algoritmo**.

Otro ejercicio: (el algoritmo de Euclides binario) La siguiente es una variante del algoritmo de Euclides que sólo utiliza divisiones por 2, lo que resulta ventajoso si se opera con números escritos en el sistema binario (como sucede en una computadora), ya las divisiones se pueden efectuar mediante operaciones de *shift* (corrimiento de los dígitos hacia la derecha).

El algoritmo puede describirse recursivamente de la siguiente manera:

$$\text{mcd}(u,v) := \begin{cases} u & \text{si } v = 0 \\ 2\text{mcd}\left(\frac{u}{2}, \frac{v}{2}\right) & \text{si u es par y v par} \\ \text{mcd}\left(\frac{u}{2}, v\right) & \text{si u es par y v impar} \\ \text{mcd}\left(u, \frac{v}{2}\right) & \text{si u es impar y v par} \\ \text{mcd}\left(v, \frac{u-v}{2}\right) & \text{si u es impar y v impar} \end{cases}$$

Por ejemplo: para calcular el máximo común divisor entre 60 y 42, procedemos de la siguiente manera:

$$\text{mcd}(60, 42) = 2\text{mcd}(30, 21) = 2\text{mcd}(21, 15) =$$
$$2\text{mcd}(15, 3) = 2\text{mcd}(6, 3) = 2\text{mcd}(3, 3) = 2\text{mcd}(3, 0) = 6$$

El ejercicicio consiste en demostrar que este algoritmo efectivamente funciona (Esto es: que siempre termina y que proporciona el resultado correcto).

Otra pregunta (para pensar): ¿Cómo podría adaptarse este algoritmo de Euclides binario para que también proporcione los coeficientes que permiten escribir al máximo común divisor como una combinación lineal de los números en cuestión (teorema 5.2) ?

Ejercicio optativo (para los que sepan programar): Escribir una implementación del algoritmo de Euclides en su lenguaje de programación favorito, y (más dificil) escribir un programa que proporcione también la escritura del máximo común divisor como combinación lineal[14].

6. Congruencias

En esta sección, introduciremos la notación de congruencias, que resulta de gran utilidad, a la hora de estudiar muchas cuestiones relacionadas con la divisibilidad.

Definición 6.1 *Sean $a, b \in \mathbb{Z}$ y sea $a \in \mathbb{N}$. Decimos que a y b son congruentes módulo n y lo escribimos*

$$a \equiv b \ (mod\, n)$$

cuando $n|b - a$.

Algunos ejemplos:

$$3 \equiv 8 \quad (\text{mód } 5)$$

$$6 \equiv -1 \quad (\text{mód } 7)$$

$$12 \equiv 0 \quad (\text{mód } 3)$$

Otra definición equivalente de congruencia puede darse en términos del resto de la división entera módulo n:

[14]En mi página web, encontrarán una implementación en el lenguaje C.

Proposición 6.1 *Sean $a, b \in \mathbb{Z}$ y sea $n \in \mathbb{N}$. Entonces, $a \equiv b \pmod{n}$ si y sólo si a y b proporcionan el mismo resto cuando los dividimos por n.*

Prueba: Dividamos a y b por n, es decir escribamos:

$$a = nq + r \text{ donde } 0 \leq r < n$$

$$b = nq' + r' \text{ donde } 0 \leq r' < n$$

Hemos de demostrar que $a \equiv b \pmod{n}$ si y sólo si $r = r'$.

Supongamos primero que $r = r'$. Entonces $b - a = nq' - nq = n(q' - q)$. Luego $n|b - a$ o sea $a \equiv b \pmod{n}$.

Por otra parte, supongamos que $a \equiv b \pmod{n}$. Entonces:

$$b - a = n(q' - q) + r' - r$$

Si suponemos que $r' \geq r$ entonces como $0 \leq r' - r < n$, tenemos que $r' - r$ debe ser el resto (y $q' - q$ el cociente) en la división enterea de $b - a$ por n. Pero entonces en virtud de la unicidad del resto en la división entera, $r' - r = 0$, ya que $n|b - a$.

(Si fuera $r' < -r$, la prueba es análoga pues $b \equiv a \pmod{n}$) □

Las congruencias comparten muchas de las propiedades de la igualdad, por ejemplo:

Proposición 6.2 *La relación de congruencia tiene las siguientes propiedades:*

- **Reflexividad***: $a \equiv a \pmod{n}$.*
- **Simetría***: Si $a \equiv b \pmod{n}$, entonces $b \equiv a (mod\, n)$.*
- **Transitividad***: Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$*

Prueba:

1. Para cualquier $a \in \mathbb{Z}$, tenemos que:

   $$n|a - a = 0$$

   en consecuencia,

   $$a \equiv a \pmod{n}$$

2. Si $a \equiv b \pmod{n}$ entonces, de acuerdo a la definición, $n|b-a$ y por lo tanto $n|-(b-a)$, o sea $n|a-b$. Lo que nuevamente, de acuerdo a la definición, significa que $b \equiv a \pmod{n}$.

3. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $n|b-a$ y $n|c-b$. En consecuencia, $n|(b-a)+(c-b)$ y por lo tanto $n|c-a$, lo que de acuerdo a la definición dice que $a \equiv c \pmod{n}$.

□

Recordamos que una relación que verifica estas tres propiedades se llama una **relación de equivalencia**, y que una relación de equivalencia determina una **partición** del conjunto donde está definida en clases de equivalencia. Para ser explícitos, definimos la clase de $\overline{a}$ de un $a \in \mathbb{Z}$ módulo n por:

$$\overline{a} = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$$

y definimos $\mathbb{Z}_n$ como el conjunto de clases de equivalencia módulo n.

En virtud de la proposición 6.1, existen tantas clases módulo n como posibles restos en la división entera por n. Pero los posibles restos en la división módulo n son $0, 1, \ldots, n-1$. Concluimos que existen exactamente n clases en $\mathbb{Z}_n$, o sea:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Por ejemplo, si $n = 5$, existen exactamente 5 clases de congruencia módulo 5, a saber:

$$\overline{0} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$$

$$\overline{1} = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}$$

$$\overline{2} = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$$

$$\overline{3} = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

$$\overline{4} = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$$

y

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

Notemos que cada clase es infinita, pero el número de clases es finito. El hecho de que estas clases forman una partición de $\mathbb{Z}$ significa que cada número entero pertenece exactamente a una de estas clases.

Una propiedad muy importante de las congruencias es que pueden sumarse, restarse y multiplicarse como si fueran igualdades:

Proposición 6.3 *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces se verifican:*

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

Prueba: Por hipótesis, $n|b-a$ y $n|d-c$, en consecuencia:

$$n|(b-a)+(d-c) \;\Rightarrow\; n|(b+d)-(a+c)$$

es decir que $a + c \equiv b + d \pmod{n}$, como afirmamos. Por otra parte,

$$n|(b-a)-(d-c) \;\Rightarrow\; n|(b-d)-(a-c)$$

es decir que: $a - c \equiv b - d \pmod{n}$, que es nuestra segunda afirmación.

Por otra parte, como $n|b-a$ y $n|d-c$, podremos escribir:

$$b - a = ne$$

$$d - c = nf$$

para ciertos enteros $n, f \in \mathbb{Z}$. Entonces:

$$bd = (a+ne)(c+nf) = ac + nec + naf + n^2ef = ac + n(ec + af + nef)$$

En consecuencia: $ac \equiv bd \pmod{n}$. □

Decimos entonces, que la relación de congruencia **es compatible** con las operaciones de suma, resta y multiplicación.

El hecho de ser compatible la relación de congruencia con las operaciones de suma, resta y producto hace posible definir las correspondientes operaciones entre las clases de restos módulo n (es decir en $\mathbb{Z}_n$)

Definición 6.2 *Sean $A, B \in \mathbb{Z}_n$ dos clases de restos módulo n. Para definir la suma $A + B$ procedemos del siguiente modo, elegimos un elemento cualquiera $a \in A$ y otro elemento $b \in B$. Entonces definimos la clase $A+B$ como la clase en $\mathbb{Z}_n$ que contiene al elemento $a + b$. Del mismo modo para definir la resta $A - B$ o el producto $A \times B$ procedemos del mismo modo, eligiendo un elemento $a \in A$ y otro $b \in B$, y definiendo $A - B$ (respectivamente $A \times B$ como la clase en $\mathbb{Z}_n$ que contiene al elemento $a - b$ (respectivamente ab).*

En virtud de la proposición 6.3, estas operaciones entre las clases módulo n resultan bien definidas ya que el resultado sólo depende de las clases A y B, y no de los elementos que $a \in A, b \in B$ que hayamos elegido.

La aritmética definida en $\mathbb{Z}_n$ de esta manera se denomina también **aritmética modular** (módulo n).

Veamos algunos ejemplos:

Ejemplo 1: Consideremos dos clases módulo 5 por ejemplo,

$$A = \overline{3} = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

$$B = \overline{4} = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$$

Para efectuar la suma $A+B$ podemos elegir cualquier número en la clase A, por ejemplo $a = 13$ y cualquier número en la clase B por ejemplo $b = -6$, efectuamos la suma $a + b = 7$ y nos fijamos en qué clase módulo 5 cae el resultado (mirando cuál es el resto en la división entera de 7 por 5). En este caso $7 \in C$, siendo

$$C = \overline{2} = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$$

por lo que, de acuerdo a la definición tenemos que, $A+B = C$, o también podemos expresarlo del siguiente modo:

$$\overline{13} + \overline{-6} = \overline{7}$$

¿Qué pasaría si hubieramos elegido otros **representantes** de las clases A y B por ejemplo $a = 3$ y $b = 9$?. En este caso, $a + b = 12$, pero notemos que 12 pertenece a la misma clase C que obtuvimos antes, y en consecuencia volvemos a obtner que $A + B = C$. Esto se debe a que justamente como

$$13 \equiv 3 \pmod 5$$

y

$$-6 \equiv 9 \pmod 5$$

podemos concluir que:

$$13 + (-6) \equiv 3 + 9 \pmod 5$$

En general, la definición 6.2 significa que:

$$\overline{a+b} = \overline{a} + \overline{b}$$

$$\overline{a-b} = \overline{a} - \overline{b}$$

$$\overline{a \times b} = \overline{a} \times \overline{b}$$

La siguiente es una tabla de las operaciones de suma y producto en $\mathbb{Z}_5$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ejemplo 2: El ejemplo más sencillo de aritmética modular con el que en realidad estamos familiarizados desde la escuela primaria, es $\mathbb{Z}_2$.

De hecho, existen dos clases módulo 2, la de los números pares

$$P = \overline{0} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

y la de los números impares:

$$I = \overline{1} = \{\ldots - 5, -3, -1, 1, 2, 3, 5, \ldots\}$$

Las operaciones entre estas nos clases son familiares: por ejemplo la suma de dos números pares es par

$$P + P = P \text{ o } \overline{0} + \overline{0} = \overline{0}$$

la de un par y un impar es impar:

$$P + I = I \text{ o } \overline{0} + \overline{1} = \overline{1}$$

y la de dos impares es par:

$$I + I = P \text{ o } \overline{1} + \overline{1} = \overline{0}$$

Análogamente podemos considerar el producto, por ejemplo: el producto de un par y un impar es par

$$P \times I = P \text{ o } \overline{0} \times \overline{1} = \overline{0}$$

Estas operaciones nos dan las siguientes tablas:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Como se ve en estos ejemplos $\mathbb{Z}_n$ resulta un conjunto (finito) donde están definidas las operaciones de suma, resta y multiplicación con propiedades similares a las de dichas operaciones en los enteros. En el lenguaje del álgebra esto se esxpresa diciendo que $\mathbb{Z}_n$ es (al igual que $\mathbb{Z}$) un **anillo**[15].

Ejercicio: Confeccionar las correspondientes tablas de la suma y el producto para los módulos 3, 4, 6 y 7. ¿Qué similitudes y diferencias se observan?

A pesar de las muchas similitudes entre las igualdades y las congruencias, es necesario notar que algunas propiedades de las igualdades no valen para las congruencias. Por ejemplo, en general no es posible cancelar factores no nulos en las congruencias. Por ejemplo:

$$2 \times 1 \equiv 2 \times 4 \pmod 6$$

[15]Más adelante veremos otros ejemplos de anillos, como los polinomios. Para la definición formal de anillo véase por ejemplo el libro Álgebra Moderna, de Birkoff y Mc. Lane. Si bien (formalmente) no estudiaremos las estructuras algebraicas como anillos y cuerpos en este curso; es conveniente ir acostumbrándose a la terminología.

Sin embargo,

$$1 \not\equiv 4 \pmod 6$$

En consecuencia, en general **no se puede dividir** congruencias.

La siguiente proposición afirma que sin embargo, es posible cancelar factores que sean coprimos con el módulo:

Proposición 6.4 *Si* $ac \equiv bc \pmod n$ *y* c *es coprimo con* n*, entonces* $a \equiv b \pmod n$

Prueba: Si $ac \equiv bc \pmod n$, entonces $n|bc - ac = (b-a)c$. Pero como c es coprimo con n, por el corolario 5.3, concluimos que $n|b-a$, es decir que $a \equiv b \pmod n$. □

Un caso particular, especialmente sencillo, es cuando el módulo es primo.

Corolario 6.1 *Si* $ac \equiv bc \pmod p$ *y* p *es primo, entonces si* $c \not\equiv 0 \pmod p$*, tenemos que* $a \equiv b \pmod p$

Observación 6.1 *Si* $a \equiv b \pmod n$ *y* $m|n$ *entonces también tenemos que* $a \equiv b \pmod m$*.*

Prueba: Por hipótesis $n|b-a$. Como $m|n$, por transitividad deducimos que $m|b-a$, o sea $a \equiv b \pmod m$. □

6.1. Criterios de divisibilidad

Las congruencias permiten demostrar en forma sencilla algunos criterios de divisibilidad conocidos desde la escuela:

Criterio de divisibilidad por 3 o por 9: Un número natural (escrito en el sistema decimal) es divisible por 3 (o por 9) si y sólo si la suma de sus cifras es divisible por 3 (respectivamente por 9).

Prueba: Sea

$$n = d_k \times 10^k + d_{k-1} \times 10^{k-1} + \ldots + d_2 \times 10^2 + d_1 \times 10 + d_0$$

la escritura de n en decimal, con $0 \leq d_i < 10$. Entonces como

$$10 \equiv 1 \pmod 3$$

deducimos que:

$$10^k \equiv 1 \pmod 3 \text{ para todo } k \geq 1$$

y consecuentemente

$$n \equiv S = d_k + d_{k-1} + \ldots + d_2 + d_1 + d_0 \pmod 3$$

En particular n es congruente con 0 módulo 3, si y sólo sí la suma S de sus cifras lo es. Para la divisibilidad por 9, la demostración es enteramente similar. □

Otro criterio similar es el siguiente:

Criterio de divisibilidad por 11**:** Un número natural (escrito en el sistema decimal) es divisible por 11 si y sólo la diferencia entre la suma de sus cifras de los lugares pares, y la suma de sus cifras de los lugares impares es disible por 11.

Prueba: Ahora, tenemos que:

$$10 \equiv -1 \pmod{11}$$

y en consecuencia:

$$10^k \equiv (-1)^k \pmod{11} \text{ para todo } k \geq 1$$

Entonces, manteniendo la notación de la prueba anterior, vemos que:

$$n \equiv D = \sum_{j=0}^{k} (-1)^j d_j \pmod{11}$$

pero notemos que:

$$D = \left(\sum_{j \text{ par}} d_j \right) - \left(\sum_{j \text{ impar}} d_j \right)$$

y n congruente a 0 módulo 11 si y sólo si D lo es. □

Ejercicio: Demostrar los criterios de divisibilidad por 4 y por 5, a saber:

1. Un número n es divisible por 5 si y sólo si el dígito de las unidades es 0 o 5.

2. Un número n es divisible por 4 si y sólo si el número formado por el dígito de las decenas y el de las unidades lo es.

7. Ecuaciones Diofánticas Lineales

Como otra aplicación más del algoritmo de Euclides, podemos estudiar el problema de resolver ecuaciones diofánticas lineales. Una ecuación diofántica es una ecuación en la que interesa encontrar las soluciones enteras (reciben este nombre en honor al matemático Diofanto de Alejandría (siglo III), quien estudió estas ecuaciones en su *Aritmética*).

Una ecuación diofántica lineal en dos variables es una ecuación de la forma:

$$ax + by = c \tag{4}$$

siendo a, b y c números enteros.

Geométricamente, este problema significa que buscamos los puntos en el plano de coordenadas enteras que estén situados sobre una recta.

Teorema 7.1 *La ecuación diofántica lineal (4) tiene solución si y sólo si $d = mcd(a, b)$ divide a c.*

Prueba: Como $d|a$ y $d|b$, si hay una solución debemos tener que $d|ax$ y $d|ay$ y por lo tanto que $d|ax + by = c$. Esto prueba que la condición es necesaria.

Para demostrar que es suficiente, supongamos que $d|c$. Entonces $c = dc'$ para algún $c' \in \mathbb{Z}$. Pero en virtud del teorema 5.2, existen $\alpha, \beta \in \mathbb{Z}$ tales que:

$$\alpha a + \beta b = d$$

Multiplicando entonces esta ecuación por c':

$$c'\alpha a + \beta c' b = c$$

y por lo tanto $x_0 = c'\alpha$, $y_0 = c'\beta$ es una solución particular de la ecuación diofántica (4).

□

Ejemplo: consideremos la ecuación diofántica

$$10x + 12y = 3$$

Entonces $\text{mcd}(10, 12) = 2$ y como 2 no divide a 3, de acuerdo al teorema anterior la ecuación no tiene soluciones (Esto es particularmente obvio en este ejemplo, pues el primer miembro es necesariamente par)

Otro ejemplo: Consideremos por otra parte la ecuación diofántica:

$$5x + 3y = 12 \tag{5}$$

Como $\text{mcd}(3, 5) = 1$ podemos asegurar, de acuerdo al teorema anterior que siempre existe una solución. Para encontrarla, utilizamos el algoritmo de Euclides para escribir al 1 como combinación lineal de 3 y 5:

$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$

En consecuencia, usando el procedimiento descripto en el teorema 5.2, encontramos que:

$$2 = 1 \times 5 + (-1) \times 3$$
$$1 = -1 \times 5 + 2 \times 3$$

Multiplicando esta ecuación por 12, tenemos que:

$$12 = (-12) \times 5 + 24 \times 3$$

En consecuencia, $x_0 = -12$, $y_0 = 24$ es una solución particular de la ecuación diofantica (5).

Si bien la demostración del teorema anterior proporciona una solución particular, en caso de que tal solución exista, no proporciona todas las soluciones.

Supongamos pues que hayamos encontrado una solución particular (x_0, y_0) de (4) y que (x, y) es otra solución de dicha ecuación. Entonces, restando y utilizando que dicha ecuación es lineal, vemos que:

$$a(x - x_0) + b(y - y_0) = 0$$

Vale decir que $\tilde{x} = x - x_0$, $\tilde{y} = y - y_0$ es una solución de la **ecuación homogénea** asociada:

$$a\tilde{x} + b\tilde{y} = 0 \tag{6}$$

Por lo que podemos concluir que: toda solución de la ecuación (no homogénea) (4) se puede escribir como la suma de una solución particular (x_0, y_0) más una solución $(\tilde{x}, \tilde{y})$ de la ecuación homogénea (6):

$$(x, y) = (x_0, y_0) + (\tilde{x}, \tilde{y})$$

Para encontrar entonces todas las soluciones de 4, nos falta entonces encontrar las soluciones de la ecuación homogénea (6).

Supongamos primero que a y b fueran coprimos. En este caso, (6) implica que:

$$a| - b\tilde{y}$$
$$b|a\tilde{x}$$

y como a y b son coprimos, por el corolario 5.3, deducimos que $a|y$ y $b|x$. Por lo tanto, existen $s, t \in \mathbb{Z}$ tales que:

$$\tilde{x} = bs, \quad \tilde{y} = at$$

y entonces utilizando (6), vemos que:

$$abs + bat = 0 \ \Rightarrow \ t = -s$$

Concluimos que en el caso en que a y b son coprimos podemos concluir que todas las soluciones de la ecuación homogénea son de la forma:

$$\tilde{x} = bs, \quad \tilde{y} = -as$$

y en consecuencia las de la no homogénea son:

$$x = x_0 + bs, \quad y = y_0 - as$$

Continuación del ejemplo: En el ejemplo anterior (5), todas las soluciones enteras son de la forma:

$$x = -12 + 3s, \quad y = 24 - 5s$$

Nos queda considerar el caso en que a y b no son coprimos. En este caso, observamos que como $d = \text{mcd}(a, b)$ divide a a, b y c por hipótesis, podemos dividir ambos miembros de la ecuación por d, obteniendo una ecuación equivalente:

$$a'x + b'y = c' \tag{7}$$

siendo $a' = a : d, \quad b' = b : d, \quad c' = c : d.$

Notamos que ahora a' y b' son coprimos: en efecto, por el teorema 5.2 existen enteros α y β tales que

$$\alpha a + \beta b = d$$

y dividiendo ambos miembros de la ecuación por d, resulta que:

$$\alpha a' + \beta b' = 1$$

y en consecuencia a', b' son coprimos como afirmamos. Como (7) es equivalente a (4), el problema se reduce al caso ya considerado. En definitiva, uniendo todas estas observaciones, hemos demostrado el siguiente teorema:

Teorema 7.2 *Cuando $d = mcd(a, b)$ divide a c, la ecuación diofántica (4) admite infinitas soluciones enteras dadas por:*

$$\begin{cases} x = x_0 + b' \cdot s \\ x = y_0 - a' \cdot s \end{cases} \qquad k \in \mathbb{Z}$$

donde $a' = a : b$, $b' = b : d$ y (x_0, y_0) es una solución particular de dicha ecuación (que se encuentra como en la demostración del teorema 7.1).

Ejercicio:(para pensar) ¿Qué sucede si consideramos una ecuación diofántica en tres variables?

$$ax + by + cz = d$$

donde $a, b, c, d \in \mathbb{Z}$. ¿Cuál sería el resultado análogo al teorema (7.1) ? Intentar demostrarlo. Sugerencia: el máximo común divisor entre a, b y c puede calcularse de la siguiente manera:

$$\text{mcd}(a, b, c) = \text{mcd}(\text{mcd}(a, b), c)$$

(Es decir: el máximo común divisor es una operación asociativa)

8. Ecuaciones de Congruencia

Un problema íntimamente relacionado con las ecuaciones diofánticas lineales, es la resolución de ecuaciones de congruencia lineales, de la forma:

$$ax \equiv b \pmod{n} \tag{8}$$

o equivalentemente

$$\overline{a}\,\overline{x} = \overline{b} \text{ en } \mathbb{Z}_n$$

Por ejemplo, consideramos la ecuación de congruencia:

$$2x \equiv 3 \pmod{5}$$

Entonces, haciendo una tabla de la función $x \mapsto 2x$ en $\mathbb{Z}_5$:

x	$2x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{3}$

vemos que la única solución es $x \equiv 4 \pmod{5}$. Esta situación, no tiene porqué ocurrir en general: las ecuaciones de congruencia lineales pueden tener varias soluciones o ninguna. Por ejemplo, consideremos la ecuación

$$2x \equiv 4 \pmod{6}$$

entonces efectuando una tabla como antes de la función $x \mapsto 2x$ en $\mathbb{Z}_6$:

x	$2x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$
$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{4}$

vemos que esta ecuación posee dos soluciones no congruentes: a saber, $x \equiv 2 \pmod 6$ y $x \equiv 5 \pmod 6$. Por otro lado, la misma tabla nos muestra que la ecución de congruencia

$$2x \equiv 3 \pmod 6$$

no admite ninguna solución.

Obviamente, la resolución de las ecuaciones de congruencia mediante una tabla de restos como hemos hecho en estos ejemplos, sólo resulta practicable cuando el módulo es pequeño. Por ello, resulta deseable desarrollar métodos generales para resolver este problema.

Para ello, observemos que la ecuación de congruencia (8), significa que:

$$ax - b = ny \text{ para algún } y \in \mathbb{Z}$$

o sea:

$$ax - ny = b$$

y esta última ecuación, es una ecuación diofántica lineal. Por lo tanto, podemos resolverla por los métodos de la sección anterior.

Ejemplo 1: Volvamos a la ecuación de congruencia:

$$2x \equiv 3 \pmod 5$$

Por lo que hemos dicho, esta ecuación significa que:

$$2x - 5y = 3 \text{ para algún } y \in \mathbb{Z} \tag{9}$$

Conforme a la teoría que desarrollamos en la sección anterior, como $\text{mcd}(2, -5) = 1$, esta ecuación admite infinitas soluciones enteras. Para encontrarlas, notamos que 1 se escribe como una combinación lineal de 2 y -5 en la siguiente forma:

$$(-2) \times 2 + (-1) \times (-5) = 1$$

luego

$$(-6) \times 2 + (-3) \times (-5) = 3$$

y por lo tanto: $x_0 = -6$, $y_0 = -3$ es una solución particular de (9). Todas las soluciones enteras, vendrán entonces dadas por:

$$x = -6 + 5s \; y = -3 + 2s$$

En consecuencia, la solución de nuestra ecuación en congruencias será:

$$x \equiv -6 \pmod 5$$

o lo que es equivalente:

$$x \equiv 4 \pmod 5$$

(Notamos que el valor de la variable auxiliar y no interesa al resolver la ecuación de congruencias).

Ejemplo 2: Volvamos a mirar ahora la ecuación de congruencia:

$$2x \equiv 4 (\text{mod } 6)$$

Esta ecuación de congruencia, conduce a la ecuación diofántica lineal:

$$2x - 6y = 4$$

Ahora los coeficientes de la ecuación no son coprimos, por ello dividimos por su máximo común divisor (que es 2), la ecuación:

$$x - 3y = 2$$

Despejando tenemos que,

$$x = 2 + 3y$$

y se obtiene una solución para cada $y \in \mathbb{Z}$.

Por lo tanto, la solucioes se determinan por la condición

$$x \equiv 2 \pmod 3$$

Nos gustaría expresar esta solución en términos del módulo 6, para ello efectuamos la división entera de y por 2, escribiendo

$$y = 2y' + r$$

donde $r = 0$ o 1. Luego, sustituyendo:

$$x = 2 + 6y' + 3r$$

o sea:

$$x \equiv 2 + 3r \pmod 6$$

Si $r = 0$ obtenemos la solución

$$x \equiv 2 \pmod 6$$

y si $r = 1$ obtenemos la solución:

$$x \equiv 5 \pmod 6$$

que son las que obtuvimos antes.

Ejemplo 3: Finalmente consideremos la ecuación de congruencia:

$$2x \equiv 3 \pmod 6$$

El método anterior conduce a la ecuación diofántica:

$$2x - 6y = 3$$

y como $\text{mcd}(2, 6) = 2$ no divide a 3, concluimos conforme al teorema 7.1, que no existe ninguna solución.

Ahora podemos generalizar los hechos que observamos en estos ejemplos, en un teorema general:

Teorema 8.1 *Sean $a, b \in \mathbb{Z}$,$n \in \mathbb{N}$ y $d = mcd(a, n)$. Consideramos la ecuación de congruencia lineal:*

$$ax \equiv b \pmod n$$

Entonces la ecuación de congruencia lineal admite soluciones si y sólo si $d|b$. En ese caso existen exactamente d soluciones no congruentes módulo n.

Prueba: Como observamos antes, la ecuación de congruencias del enunciado es equivalente a la ecuación diofántica:

$$ax - ny = b$$

y conforme al teorema 7.1, esta ecuación tiene solución si y sólo si $d = \text{mcd}(a, n)$ divide a b.

Si esto sucede, llamando $a' = a : d$, $n' = n : d$, $b' = b : d$ y dividiendo por d, obtenemos la ecuación equivalente:

$$a'x - n'y = b'$$

donde ahora a' y b' son coprimos (como en la sección anterior), y todas las soluciones enteras de esta ecuación se pueden expresar en la forma:

$$x = x_0 + n's, \quad y = y_0 - a's \text{ para algún } s \in \mathbb{Z}$$

siendo (x_0, y_0) alguna solución particular. Por lo tanto, x será solución de nuestra ecuación de congruencia, si y sólo si

$$x \equiv x_0 \pmod{n'}$$

Para expresar esto en términos del módulo n, como en el ejemplo anterior, efectuamos la división entera de s por d, escribiendo:

$$s = qd + r \text{ con } 0 \leq r < d$$

Entonces, sustituyendo obtenemos

$$x = x_0 + nq + n'r$$

y las soluciones serán

$$x \equiv x_0 + n'r \pmod{n}$$

con $r = 0, 1, 2, \ldots, d-1$.

Finalmente, observemos que estas soluciones no son congruentes módulo n, pues si

$$x \equiv x_0 + n'r_1 \equiv x \equiv x_0 + n'r_2 \pmod{n}$$

entonces

$$n'r_1 \equiv n'r_2 \pmod{n}$$

o sea:

$$n'r_1 - n'r_2 = nk \text{ para algún } k \in \mathbb{Z}$$

Luego multiplicando por d:

$$nr_1 - nr_2 = dnk$$

o sea:

$$r_1 - r_2 = dk$$

o

$$r_1 \equiv r_2 \pmod{d}$$

Pero como $0 \leq r_1, r_2 < d$, concluimos que $r_1 = r_2$. □

Corolario 8.1 *La ecuación de congruencia lineal:*

$$ax \equiv b \pmod{n}$$

tiene solución única si y sólo si $mcd(a, n) = 1$.

8.1. Inversos módulo n

Veamos otra forma de pensar las ecuaciones de congruencia que a veces resulta útil:

Si tenemos una ecuación lineal con números

$$ax = b$$

(y $a \neq 0$), uno puede obtener la solución multiplicando por el inverso multiplicativo de a, $a^{-1} = \frac{1}{b}$ (lo que equivale a dividir por b), o sea:

$$x = b^{-1}a$$

Esto motiva el siguiente teorema[16]:

Teorema 8.2 *Dados $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ coprimo con n, existe una única clase $\overline{a'}$ en $\mathbb{Z}_n$ tal que:*

$$\overline{a} \cdot \overline{a'} = \overline{1}$$

Vale decir que:

$$aa' \equiv 1 \pmod{n}$$

y dos posibles a' que cumplan esta condición son congruentes módulo n.

a' se denomina un invereso multiplicativo de a módulo n.

Recíprocamente si $\overline{a}$ admite un inverso multiplicativo en $\mathbb{Z}_n$, entonces a es coprimo con n.

Este teorema es realmente el caso particular $b = 1$ del teorema 8.1.

En particular, notamos que si p es primo, en $\mathbb{Z}_p$ todos los elementos no nulos (que no sean la clase del cero), admiten un inverso multiplicativo (es decir: se puede dividir por elementos no nulos[17]).

Ejercicio: Dar una demostración directa[18] usando el teorema 5.2.

Ejemplo: Volvamos a mirar la congruencia lineal:

[16] Este teroema significa que las clases $\overline{a}$ con a coprimo con n, son exactamente los elementos que admiten un inverso multiplicativo en $\mathbb{Z}_n$, es decir las **unidades** del anillo $\mathbb{Z}_n$

[17] Decimos entonces que si p es primo, $\mathbb{Z}_p$ es un **cuerpo**, esto es un anillo en el que es posible la división por elementos no nulos. Otros ejemplos familiares de cuerpos son $\mathbb{Q}$ (los números racionales) y $\mathbb{R}$ (los núeros reales).

[18] ¡fue la que di en clase!

$$2x \equiv 3 \pmod 5$$

Entonces dado que 2 y 5 con coprimos, el 1 se escribe como combinación lineal de ambos:

$$(-2) \times 2 + 1 \times 5 = 1$$

pero entones:

$$(-2) \times 2 \equiv 1 \pmod 5$$

Es decir que $\overline{2}$ y $\overline{-2} = \overline{3}$ son inversos multiplicativos en $\mathbb{Z}_5$. Entonces, para "pasar dividiendo el 2" en nuestra congruencia lineal, multiplicamos ambos miembros de la congruencia por 3:

$$3 \times 2x \equiv 3 \times 3 \pmod 5$$

y obtenemos nuevamente que:

$$x \equiv 9 \equiv 4 \pmod 5$$

8.2. El teorema de Wilson

Como aplicación de las ideas anteriores, podemos probar el siguiente teorema que proporciona un criterio para saber cuando un número es primo:

Teorema 8.3 (Teorema de Wilson) *Sea $p \in \mathbb{N}$, $p > 1$. Entonces p es primo si y sólo si p divide a $(p-1)! + 1$, o lo que es equivalente:*

$$(p-1)! \equiv -1 \pmod p$$

Prueba: Primero probaremos que si p divide a $(p-1)! + 1$, entonces p es primo. Supongamos que por el contrario p no fuera primo, estonces p admitiría un divisor d con $1 < d < p$. Observemos que entonces $d|(p-1)!$ y como d divide a p, por transitividad también tenemos que $d|(p-1)! + 1$. Pero entonces, $d|[(p-1)! + 1] - (p-1)! = 1$, lo cuál es una contradicción, pues los únicos divisores de 1 son ± 1. En consecuencia, p debe ser primo.

Ahora probemos que si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$. Para ello observemos que para cada número $1 \leq a < p$, existe en virtud del teorema 8.2 un único entero a' con $1 \leq a' < p$ tal que:

$$aa' \equiv 1 \pmod{p}$$

es decir, tal que a' y a son inversos módulo p.

Notamos además que debe ser $a \neq a'$, salvo si $a = 1$ o $a = p-1$. En efecto: si $a = a'$, entonces

$$a^2 \equiv 1 \pmod{p}$$

o también

$$a^2 - 1 \equiv 0 \pmod{p}$$

Factorizando, podemos escribir esto como:

$$(a-1)(a+1) \equiv 0 \pmod{p}$$

De lo cual en virtud del corolario 5.4, deducimos que:

$$a \equiv 1 \pmod{p} \quad \text{o} \quad a \equiv -1 \pmod{p}$$

Entonces, para calcular $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$ módulo p, agrupamos cada factor con su inverso multiplicativo (usando las propiedades asociativa y conmutativa del producto; ver ejemplo después del teorema), y resulta:

$$(p-1)! \equiv (p-1) \equiv -1 \pmod{p}$$

□

Ejemplo: Para mostrar como funciona el proceso de agrupar cada número con su inverso multiplicativo módulo p, veamos un ejemplo.

Sea $p = 7$. Entonces, tenemos la siguiente tabla de inversos módulo 7:

a	a'
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{5}$
$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{3}$
$\overline{7}$	$\overline{7}$

Entonces:

$$(p-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 6 \equiv -1 \pmod 7$$

Ejercicio: Probar que si p es un primo impar, entonces

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \begin{cases} -1 & \text{si} \quad p \equiv 1 \pmod 4 \\ 1 & \text{si} \quad p \equiv 3 \pmod 4 \end{cases} \pmod p$$

(Sugerencia: calcular $(p-1)!$ de otra manera agrupando cada número con su inverso aditivo[19] módulo p, vale decir agrupando a a con $p-a$).

9. El teorema fundamental de la aritmética

Ahora probaremos el teorema fundamental que ya hemos anunciado con anterioridad:

Teorema 9.1 *Cada entero $n > 1$, o bien es primo, o se descompone como producto de primos, y la descomposición es única, salvo el orden de los factores.*

Para ilustrar el teorema, obtengamos dos factorizaciones del número 360. Un procedimiento posible, es ir dividiendo a 360 por los primos en orden de magnitud, hasta obtener un 1:

360	2
180	2
90	2
45	3
15	3
5	5
1	

Luego obtenemos la factorización:

$$360 = 2 \times 2 \times 2 \times 3 \times 5 \times 5$$

[19] Dos números a y a' son inversos aditivos módulo p si $a + a' \equiv 0 \pmod p$

¿Qué sucede si hubiéramos empezado dividiendo por otro primo? Por ejemplo por 5:

360	5
72	3
24	3
8	2
4	2
2	2
1	

Esto conduce la factorización:

$$360 = 5 \times 3 \times 3 \times 2 \times 2 \times 2$$

Pero ambas factorizaciones sólo difieren en el orden de los factores, tal como afirma el teorema.

Ahora demostraremos el teorema:

Prueba: La existencia ya la probamos antes (teorema 2.1). Queda pues probar la unicidad. Para ello, hagamos nuevamente inducción global en n. Para $n = 1$ el teorema no afirma nada.

Sea entonces $n > 1$, y supongamos que el teorema es válido para todo $n' < n$.

Supongamos que n admite dos factorizaciones como producto de primos:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

siendo los p_i y los q_i primos (eventualmente alguna de las factorizaciones puede constar de un sólo primo).

Tomemos un primo en la factorización de la izquierda, por ejemplo p_1. En virtud del corolario 5.5, deducimos que $p_1|q_i$ para algún i. Pero entonces como q_i es primo, $p_1 = q_i$ o $p_i = 1$ (lo que es imposible pues 1 no es primo); es decir que hemos probado que p_1 debe necesariamente aparecer en la factorización de la derecha.

Podemos entonces. cancelar p_1 en ambos lados de la igualdad obteniendo dos descomposiciones del número $n' = n : p_1$ como producto de primos:

$$n' = p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_{i-1} q_{i+1} \dots q_s$$

Notemos que $n' < n$, entonces en virtud de la hipótesis inductiva, las dos descomposiciones de n' sólo pueden diferir en el orden de los factores: es decir

que $r = s$ y los números $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots q_s$ deben ser los mismos que p_2, p_3, $\ldots p_r$, sólo que en otro orden.

Deducimos entonces que las dos descomposiciones supuestas de n sólo difieren en el orden de los factores.

En virtud del principio de inducción global, hemos demostrado el teorema para todo $n \in \mathbb{N}$. □

Es importante notar que nuestra prueba del teorema fundamental de la aritmética, se basó escencialmente en el corolario 5.4, el cuál a su vez lo obtuvimos como una consecuencia del algoritmo de Euclides.

Ejercicio: Probar que recíprocamente el teorema 9.1 implica el corolario 5.4, por lo que ambos resultados son en cierto modo equivalentes.

Una prueba alternativa

Una prueba alternativa del teorema fundmental, que no depende del algoritmo de Euclides, se puede hacer del siguiente modo[20]:

Prueba: Nuevamente, supongamos que n tiene dos factorizaciones

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

y que ya hemos demostrado la unicidad de la factorización para cualquier $n' < n$.

Podemos ordenar los primos que aparecen en cada factorización de modo que:

$$p_1 \leq p_2 \leq \ldots \leq p_r$$

$$q_1 \leq q_2 \leq \ldots \leq q_s$$

Claramente podemos suponer que $p_1 \leq q_1$. Además si fuera $p_1 = q_1$, podemos cancelarlo en ambas descomposciones, obteniendo dos factorizaciones para $n' < n$. Y usando la hipótesis inductiva, deducimos las dos n factorizaciones de n coinciden salvo el orden de los factores.

Entonces, podemos suponer que $p_1 < q_1$. Consideramos el entero:

$$n' = n - p_1 q_2 \ldots q_r$$

[20] ver [1], suplemento al capítulo I, sección 1

Este entero n' es menor que n y podemos escribirlo de dos maneras:

$$n' = p_1(p_2 \dots p_s - q_2 \dots q_r) = (q_1 - p_1)q_2 \dots q_s$$

Siendo, $n' < n$ la factorización de n' como producto de primos es única, por hipótesis inductiva. Y como p_1 es primo, deducimos entonces que o bien $p_1 = q_i$ para algún i con $2 \leq i \leq s$, o bien $p_1 | q_1 - p_1$ (por un razonamiento similar al del ejercicio anterior).

En el primer caso, razonamos como antes, y deducimos que las dos factorizaciones de n coinciden.

Por otra parte, si $p_1 | q_1 - p_1$, tenemos que: $q_1 - p_1 = p_1 k$ para algún $k \in \mathbb{Z}$, lo que implica que $q_1 = p_1(k+1)$, y q_1 no sería primo pues $p_1 | q_1$.

Esta contradicción prueba que n no puede tener dos factorizaciones diferentes. En virtud del principio de inducción global, el teorema queda demostrado para todo $n \in \mathbb{N}$. □

10. Consecuencias del Teorema Fundamental de la aritmética

Notemos que en la descomposición dada por el teorema fundamental, los primos pueden repetirse. Agrupando los primos que se repiten podemos expresar a cada número n como productos de primos diferentes, elevados a ciertas potencias, por ejemplo

$$360 = 2^3 \times 3^2 \times 5^1$$

Podemos si queremos incluir otros primos que no aparecen en esta factorización con exponente cero, ej:

$$360 = 2^3 \times 3^2 \times 5^1 \times 7^0 \times 11^0$$

Esto motiva la siguiente definición:

Definición 10.1 *Si p es un número primo, definimos una función $v_p : \mathbb{N} \to \mathbb{N}_0$, llamada la* **valuación p-ádica** *del siguiente modo: $v_p(n)$ es el exponente del primo p en la factorización en primos del número n en factores primos. Ponemos $v_p(1) = 0$ para todo primo p.*

Por ejemplo,

$$v_p(360) = \begin{cases} 3 & \text{si} \quad p = 2 \\ 2 & \text{si} \quad p = 3 \\ 1 & \text{si} \quad p = 5 \\ 0 & \text{si} \quad p \neq 2, 3, 5 \end{cases}$$

Claramente la váluación p-ádica está bien definida, en virtud del teorema fundamental de la aritmética.

Más explicitamente podríamos definir v_p como el máximo exponente k tal que p^k divide a n:

$$v_p(n) = \text{máx}\{k \in \mathbb{N}_0 : p^k | n\}$$

Entonces, la factorización de n podemos escribirla como

$$n = \prod_{p \in \mathbb{P}, p|n} p^{v_p(n)}$$

donde $\mathbb{P}$ es el conjunto de los números primos, y el producto se extiende sobre los primos que dividen a n.

A veces resulta útil escribir esto formalmente como:

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

donde el producto se extiende ahora sobre todos los primos; y donde, si bien el producto es formalmente infinito, sólo un número finito de factores son diferentes de 1, por lo que es realmente un producto finito.

Observemos una propiedad importante de la valuación p-ádica[21]:

Proposición 10.1

$$v_p(ab) = v_p(a) + v_p(b)$$

Prueba: Si las factorizaciones de a y b son:

$$a = \prod_{p \in \mathbb{P}, p|a} p^{v_p(n)}$$

[21]Esta propiedad significa que la valuación p-ádica se comporta algebraicamente de modo muy similar a un logaritmo: transforma productos en sumas.

$$b = \prod_{p\in\mathbb{P},p|b} p^{v_p(n)}$$

la de ab es[22]:

$$ab = \prod_{p\in\mathbb{P},p|a \vee p|b} p^{v_p(a)+v_p(b)}$$

En consecuencia,

$$v_p(ab) = v_p(a) + v_p(b)$$

□

Ejercicio: Probar que si $a, b \in \mathbb{N}$, entonces:

$$v_p(a + b) \geq \text{mín}(v_p(a), v_p(b)$$

El teorema fundamental de la aritmética nos permite dar un criterio para saber cuando un número es divisible por otro en términos de su factorización en factores primos:

Teorema 10.1 *Sean $a, b \in \mathbb{N}$, entonces $a|b$ si y sólo si*

$$v_p(a) \leq v_p(b) \text{ para todo primo } p \in \mathbb{P}$$

Es decir: si y sólo si todos los primos que aparecen en la factorización de a aparecen en la de b, y el expoente con que aparecen es en la factorización de a menor o igual que en la de b.

Prueba: Supongamos primero que $a|b$, entonces existe $c \in \mathbb{N}$ tal que $b = ac$, y por el teorema anterior:

$$v_p(b) = v_p(a) + v_p(c)$$

Pero $v_p(c) \geq 0$, luego $v_p(a) \leq v_p(b)$, como afirmamos.

Por otro lado si, $v_p(a) \leq v_p(b)$ para todo primo p y definimos:

$$c = \prod_{p\in\mathbb{P},p|b} p^{v_p(b)-v_p(a)}$$

tendremos que $c \in \mathbb{N}$ (pues los exponentes son enteros no negativos) y, razonando como en el teorema anterior, que $ac = b$. En consecuencia, $a|b$. □

Este teorema tiene a su vez varias consecuencias importantes, por ejemplo permite dar una caracterización del máximo común divisor en términos de la factorización en primos:

[22]En esta fórmula, $\vee$ simboliza el conectivo lógico "o" (no exclusivo)

Teorema 10.2 *Si $a, b \in \mathbb{N}$, el máximo común divisor entre ellos, admite la siguiente factorización:*

$$mcd(a,b) = \prod_{p\in\mathbb{P}, p|a\wedge p|b} p^{\text{mín}(v_p(a),v_p(b))}$$

Es decir, en la factorización de $mcd(a,b)$ aparecen los primos que aparecen en la de a y en la de b, y elevados al menor de los exponentes con que aparezcan en ellas.

Prueba: Sea

$$d = \prod_{p\in\mathbb{P}} p^{\text{mín}(v_p(a),v_p(b))} \in \mathbb{N}$$

Probaremos que d satiface la caracterización del máximo común divisor (corolario 5.1):

i) Es un divisor común: $d|a$ y $d|b$.

ii) Cualquier otro divisor común d' lo divide: si $d'|a$ y $d'|d$, entonces $d'|d$.

Para probar que $d|a$, basta observar que para todo primo $p \in \mathbb{P}$:

$$v_p(d) = \text{mín}(v_p(a), v_p(b)) \leq v_p(a)$$

luego por el teorema 10.1, tenemos que $d|a$. Similarmente:

$$v_p(d) = \text{mín}(v_p(a), v_p(b)) \leq v_p(b) \ \forall\ p \in \mathbb{P}$$

luego $d|b$. Supongamos ahora que d' es otro divisor común: entonces

$$v_p(d') \leq v_p(a), \quad v_p(d') \leq v_p(b)$$

luego para cualquier primo p,

$$v_p(d') \leq \text{mín}(v_p(a), v_p(b)) = v_p(d)$$

y en consecuencia, por el teorema 10.1 concluimos que $d'|d$. Como d satiface la caracterización del máximo común divisor, concluimos que $d = \text{mcd}(a,b)$. □

Una noción dual de la de máximo común divisor es la de mínimo común múltimo (m.c.m). Se tiene el siguiente análogo del teorema 10.2:

Teorema 10.3 *Si $a, b \in \mathbb{N}$, el mínimo común múltiplo entre ellos, admite la siguiente factorización:*

$$mcm(a,b) = \prod_{p\in\mathbb{P}, p|a\vee p|b} p^{\max(v_p(a),v_p(b))}$$

Es decir, en la factorización de $mcm(a,b)$ aparecen los primos que aparecen en la de a o en la de b (donde el "o" es no exclusivo), y elevados al mayor de los exponentes con que aparezcan en ellas.

Ejercicio: Efectuar la prueba de este teorema, probando que

$$m = \prod_{p\in\mathbb{P}, p|a\vee p|b} p^{\max(v_p(a),v_p(b))}$$

satiface la siguiente caracterización del mínimo común múltiplo[23] (dual del corolario 5.1).

i) Es un múltiplo común: $a|m$ y $b|m$.

ii) Cualquier otro múltiplo m' es divisible por m: si $a|m'$ y $b|m'$, entonces $m|m'$.

Muchas propiedades del máximo común divisor o del mínimo común múltiplo se prueban facilmente a partir de esta caracterización:

Proposición 10.2 *Sean $a, b, c \in \mathbb{N}$ entonces:*

i) $mcd(ac, bc) = c\ mcd(a, b)$

ii) $mcm(ac, bc) = c\ mcm(a, b)$

iii) $mcd(a, b)mcm(a, b) = ab$ *En particular, a y b son coprimos si y sólo si* $mcm(a, b) = ab$.

[23]Esta caracterización significa que $\mathrm{mcm}(a,b)$ es el **supremo** de a y b en el orden dado por la divisibilidad

Ejemplo: Sean $a = 60$ y $b = 63$. Tenemos las factorizaciones:

$$a = 2^2 \times 3 \times 5$$

$$b = 3^2 \times 7^1$$

Entonces:

$$\text{mcd}(a, b) = 3^1 = 3$$

$$\text{mcm}(a, b) = 2^2 \times 3^2 \times 5^1 \times 7^1 = 1260$$

y

$$ab = 2^2 \times 3^3 \times 5^1 \times 7^1 = 3780 = 3 \times 1260$$

En la prueba de la proposición 10.2 necesitaremos utilizar ciertas propiedades del máximo y el mínimo de dos números naturales $m, n \in \mathbb{N}_0$:

1.
$$\text{mín}(m + k, n + k) = \text{mín}(m, n) + k \ \forall \ m, n, k \in \mathbb{N}_0 \tag{10}$$

2.
$$\text{máx}(m + k, n + k) = \text{máx}(m, n) + k \ \forall \ m, n, k \in \mathbb{N}_0 \tag{11}$$

3.
$$\text{mín}(m, n) + \text{máx}(m, n) = n + m \ \forall \ m, n \in \mathbb{N}_0 \tag{12}$$

Estas propiedades se comprueban sin dificultad, considerando separadamente los casos en que $n > m$ y en que $n \leq m$.
Prueba: Para demostrar una igualdad entre dos números naturales, como la afirmación i):

$$\text{mcd}(ac, bc) = c \ \text{mcd}(a, b)$$

basta demostrar que todo primo p aparece en ambos miembros elevado al mismo exponente, o sea que:

$$v_p(\text{mcd}(ac, bc)) = v_p(c \ \text{mcd}(a, b)) \ \forall \ p \in \mathbb{P} \tag{13}$$

Pero por el teorema 10.2, y la propiedad (10):

$$v_p(\text{mcd}(ac, bc)) = \text{mín}(v_p(ac), v_p(bc))$$

$$= \text{mín}(v_p(a) + v_p(c), v_p(b) + v_p(c)) = \text{mín}(v_p(a), v_p(b)) + v_p(c)$$

Por otra parte, utilizando nuevamente el teorema 10.2:

$$v_p(c\,\text{mcd}(a, b)) = v_p(c) + v_p(\text{mcd}(a, b)) = v_p(c) + \text{mín}(v_p(a), v_p(b))$$

Esto demuestra (13), y en consecuencia i). La prueba de la afirmación ii) es completamente similar, y se deja como ejercicio. Finalmente, para probar la igualdad iii), nuevamente bastará probar que:

$$v_p(\text{mcd}(a, b)\text{mcm}(a, b)) = v_p(ab)\ \forall\ p \in \mathbb{P} \tag{14}$$

Pero teniendo en cuenta la propiedad (12):

$$v_p(\text{mcd}(a, b)\text{mcm}(a, b)) = v_p(\text{mcd}(a, b)) + v_p(\text{mcm}(a, b))$$

$$= \text{mín}(v_p(a), v_p(b)) + \text{máx}(v_p(a), v_p(b)) = v_p(a) + v_p(b)$$

y por otra parte,

$$v_p(ab) = v_p(a) + v_p(b)$$

lo que demuestra la afirmación (14), y en consecuencia iii). □

Similarmente podemos demostrar otras propiedades, por ejemplo:

Proposición 10.3 *Si $a, b \in \mathbb{N}$ son tales que $a^n | b^n$, entonces $a|b$.*

Prueba: Para ver que $a|b$ basta ver que:

$$v_p(a) \leq v_p(b)$$

pero como por hipótesis, $a^n | b^n$, tenemos que:

$$v_p(a^n) \leq v_p(b^n)$$

o sea:

$$nv_p(a) \leq nv_p(b)$$

y en consecuencia:

$$v_p(a) \leq v_p(b)$$

□

Ejercicio: El teorema 10.1 también puede emplearse para determinar la cantidad de divisores de un número. Definamos $d(n)$ como la cantidad de divisores positivos de n. Probar que entonces,

$$d(n) = \prod_{p|n} (v_p(n) + 1)$$

Otras consecuencias del teorema fundamental de la aritmética, nos serán más útiles más adelante:

Proposición 10.4 *Sean $a, b, c \in \mathbb{N}$. Si $a|c$, $b|c$, y a y b son coprimos, entonces $ab|c$.*

Prueba: Por el teorema 10.1, notamos que basta probar que:

$$v_p(ab) \leq v_p(c) \; \forall \; p \in \mathbb{P} \tag{15}$$

Pero

$$v_p(ab) = v_p(a) + v_p(b)$$

Observemos que como a y b son coprimos, para cualquier primo p, será $v_p(a) = 0$ o $v_p(b) = 0$.

Si $v_p(a) = 0$, entonces $v_p(ab) = v_p(b) \leq v_p(c)$ pues $b|c$. Si $v_p(b) = 0$, entonces $v_p(ab) = v_p(a) \leq v_p(c)$ pues $a|c$ En cuqlquier caso, hemos probado que se verifica (15), en consecuencia $ab|c$. □

11. El teorema de Fermat

Teorema 11.1 (Fermat) *Sean p un número primo y $a \in \mathbb{Z}$. Entonces:*

i)

$$a^p \equiv a \pmod{p}$$

ii) Si p no divide a a entonces,

$$a^{p-1} \equiv 1 \pmod{p}$$

Observemos ante todo, que las dos afirmaciones del enunciado, son equivalentes:

Para probar que i) implica ii), basta observar i) puede escribirse la forma:

$$a \cdot a^{p-1} \equiv a \cdot 1$$

Entonces, siendo p primo, si p no divide a a, p es coprimo con a, y podemos cancelarlo en ambos miembros de la congruencia (por la proposición 6.4).

Recíprocamente es claro que ii) implica i), ya que basta multiplicar ambos miembros de la congruencia por a.

Daremos dos pruebas diferentes de este teorema. La primera prueba se basa en el binomio de Newton, y en un argumento de inducción. (Más adelante, veremos una generalización de este teorema que nos proporcionará también otra prueba diferente).

Recordamos que el binomio de Newton afirma que:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

El siguiente lema afirma que p divide a todos los coeficientes binomiales salvo los de los extremos:

Lema 11.1 *Si p es primo, y $1 < k < p$ entonces*

$$\binom{p}{k} \equiv 0 \pmod{p}$$

Prueba: Recordamos que:

$$\binom{p}{k} = \frac{p(p-1)(p-2)\dots(p-k+1)}{k!} \in \mathbb{N}$$

En consecuencia:

$$p|k!\binom{p}{k}$$

Pero como $k < p$, los factores primos de $k!$ deben ser exclusivamente primos menores que p, por lo tanto p es coprimo con $k!$, y por el corolario 5.3, concluimos que $p|\binom{p}{k}$. □

Corolario 11.1 *Si $a, b \in \mathbb{Z}$ y p es primo, entonces:*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Ahora resulta sencillo probar el teorema 11.1:
Prueba: Ya observamos que i) y ii) son equivalentes, luego basta probar i). Para hacerlo hagamos inducción en a. Si $a = 0$ el teorema es evidente:

$$0^p = 0 \equiv 0 \pmod{p}$$

Si el teorema vale para un cierto a, veremos que se verifica también para $a+1$: en efecto por el corolario 11.1

$$(a+1)^p \equiv a^p + 1^p \pmod{p}$$

y usando la hipótesis inductiva, deducimos que:

$$(a+1)^p \equiv a + 1 \pmod{p}$$

En virtud del principio de inducción, el teorema queda demostrado para cualquier $a \in \mathbb{N}_0$. Si $a < 0$, notemos que $-a > 0$ luego usando lo que ya demostramos:

$$(-a)^p = (-1)^p a^p \equiv -a \pmod{p}$$

pero $(-1)^p \equiv -1 \pmod{p}$ tanto si p es un primo impar como si $p = 2$ (en este caso $1 \equiv -1$). Por lo tanto

$$a^p \equiv a \pmod{p}$$

□

Una observación sobre la demostración anterior: En realidad el teorema de Fermat puede pensarse como teorema sobre clases en $\mathbb{Z}_p$, que afirma que si $\overline{a} \in \mathbb{Z}_p$ y p es primo,

$$\overline{a}^p = \overline{a} \text{ en } \mathbb{Z}_p$$

Ahora en $\mathbb{Z}_n$ (n primo o no), vale una forma más fuerte del principio de inducción: si P es una propiedad de las clases en $\mathbb{Z}_n$ tal que:

1. $P(\overline{a_0})$ para algún $\overline{a_0} \in \mathbb{Z}_n$

2. Si $P(\overline{a})$ es verdadera, entonces $P(\overline{a}+\overline{1})$ es verdadera:

entonces $P(\overline{a})$ es verdadera para cualquier $\overline{a} \in \mathbb{Z}_n$.

Ejercicio: Justificar porqué en $\mathbb{Z}_n$ se verifica esta forma del principio de inducción.

Teniendo en cuenta esta observación en la demostración anterior, no es realmente necesario considerar el caso $a < 0$.

Nota histórica:

Figura 1: Pierre de Fermat

Pierre de Fermat (1601-1665) fue un jurista (en el parlamento de Toulouse, en el sur de Francia) y destacado matemático.

Además de haber obtenido importantes resultados en teoría de números, es uno de los fundadores de la geometría analítica (contemporaneo de Descartes, concibió independientemente de él, su principio fundamental), el cálculo infinitesimal y el cálculo de probabilidades (a través de su correspondencia con Blaise Pascal).

El teorema 11.1 (conocido como el pequeño teorema de Fermat) aparece en una de sus cartas a su confidente Frénicle de Bessy, fechada el 18 de octubre de 1640.

Fermat es también famoso por otro teorema (en realidad conjetura, ya que no dio una demostración), conocido como el "último teorema de Fermat", que afirma que si $n > 2$ la ecuación diofántica

$$x^n + y^n = z^n$$

no admite soluciones enteras con x, y, z no nulas. Este teorema fue formulado por Fermat en un comentario en el margen que escribió mientras leía la aritmética de Diofanto. Fermat dijo tener una demostración notable de esta afirmación pero que el margen era demasiado pequeño para escribirla.

Pese a tratarse de un enunciado elemental, los intentos de demostrar este teorema por numerosos matemáticos de la talla de Euler, Dedekind, Legendre, Lamé,

Kummer, etc. fueron infructuosos (aunque lograron demostrar casos particulares, y estas investigaciones condujeron al desarrollo de nuevas teorías matemáticas de gran importancia en la matemática actual, como la teoría algebraica de números y las curvas elípticas). Finalmente, en 1995 Andrew Wiles dio una demostración de un teorema que implica el último teorema de Fermat (pero esta demostración no es para nada elemental).

12. El Teorema Chino del Resto

Comencemos con una proposición sobre congruencias respecto a módulos que son primos entre sí.

Proposición 12.1 *Sean $m_1, m_2 \in \mathbb{N}$ dos números coprimos, $a, b \in \mathbb{Z}$ y $m = m_1 m_2$. Entonces $a \equiv b \pmod{m}$ si y sólo si se tiene simultáneamente que:*

$$\begin{cases} a \equiv b & (\text{mód } m_1) \\ a \equiv b & (\text{mód } m_2) \end{cases} \tag{16}$$

Prueba: Primero supongamos que $a \equiv b \pmod{m}$ Entonces, como $m_1|m$ y $m_2|m$, por la obseración 6.1, deducimos que se satisface (16). Recíprocamente supongamos que se satisface (16) entonces, $m_1|b-a$ y $m_2|b-a$. Dado que m_1 y m_2 son coprimos, por la proposición 10.4, deducimos que $m_1 m_2|b-a$, es decir que $a \equiv b \pmod{m}$ □

Ejemplo: Para ilustrar la utilidad de la proposición anterior, veamos un análogo del teorema de Fermat, para congruencias respecto a un módulo compuesto de la forma $n = pq$, donde p y q son primos distintos.

Si ni p ni q dividen a a, tendremos en virtud del teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{q-1} \equiv 1 \pmod{q}$$

En consecuencia, elevando la primer congruencia a la potencia $q-1$, y la segunda a la potencia $p-1$, tendremos que:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p}$$
$$a^{(p-1)(q-1)} \equiv 1 \pmod{q}$$

y en virtud de la proposición 12.1, tendremos que:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

Esta congruencia puede considerarse como análoga al teorema de Fermat, para el módulo compuesto $n = pq$. Volveremos sobre este ejemplo más adelante.

Ahora consideremos un sistema de congruencias respecto a dos módulos que son coprimos, por ejemplo:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases} \tag{17}$$

¿Será posible reducirlo a una única congruencia módulo $3 \times 5 = 15$?. Veremos que la respuesta a esta pregunta es afirmativa. Para ello, notemos que el sistema (17) significa que existen $q_1, q_2 \in \mathbb{Z}$ tales que:

$$\begin{cases} x = 3q_1 + 2 \\ x = 5q_2 + 4 \end{cases}$$

Comenzamos multiplicando la primer ecuación por 5 y a la segunda por 3 (para que aparezca 15 como factor):

$$\begin{cases} 5x = 15q_1 + 10 \\ 3x = 15q_2 + 12 \end{cases}$$

Ahora notemos lo siguiente: como los módulos 3 y 5 son coprimos, por el teorema 5.2 (consecuencia del algoritmo de Euclides) existen enteros $\alpha, \beta \in \mathbb{Z}$ tales que:

$$3\alpha + 5\beta = 1$$

De hecho, utilizando el algoritmo de Euclides, es fácil ver que podemos tomar $\alpha = 2$ y $\beta = -1$. Multiplicando entonces a la primera ecuación por β y a la segunda por α, tenemos que:

$$\begin{cases} \beta 5x = 15\beta q_1 + 10\beta \\ \alpha 3x = 15\alpha q_2 + 12\alpha \end{cases}$$

y sumándolas obtenemos que:

$$(5\beta + 3\alpha)x = 15(\beta q_1 + \alpha q_2) + (10\beta + 12\alpha)$$

o sea, teniendo en cuenta la manera en que hemos elegido α y β,

$$x = 15(\beta q_1 + \alpha q_2) + (10\beta + 12\alpha)$$

Pero entonces:

$$x \equiv 10\beta + 12\alpha = 14 \pmod{15}$$

Recíprocamente, si $x \equiv 14 \pmod{15}$, entonces

$$\begin{cases} x \equiv 14 \equiv 4 \pmod{5} \\ x \equiv 14 \equiv 2 \pmod{3} \end{cases}$$

Por lo que vemos que el sistema (17) es equivalente a la congruencia

$$x \equiv 14 \pmod{15}$$

Ahora generalizaremos este ejemplo, en un teorema general:

Teorema 12.1 (Teorema Chino del resto) *Consideramos el sistema de congruencias:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \tag{18}$$

donde $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ y, m_1 y m_2 son coprimos. Entonces existe un $a \in \mathbb{Z}$ tal que el sistema (18) es equivalente a la congruencia:

$$x \equiv a \pmod{m} \text{ donde } m = m_1 m_2$$

Prueba: Procedemos como en el ejemplo anterior: Notamos que el sistema (18) significa que existen $q_1, q_2 \in \mathbb{Z}$ tales que:

$$\begin{cases} x = q_1 m_1 + a_1 \\ x = q_2 m_2 + a_2 \end{cases}$$

Por otra parte, como m_1 y m_2 son coprimos, por el corolario 5.2 (consecuencia del algoritmo de Euclides), existen $\alpha, \beta \in \mathbb{Z}$ tales que:

$$\alpha m_1 + \beta m_2 = 1 \tag{19}$$

Entonces multiplicando a la primer ecuación por $m_2\beta$ y a la segunda por $m_1\alpha$, deducimos que:

$$\begin{cases} m_2\beta x &= \beta q_1 m_1 m_2 + \beta m_2 a_1 \\ m_1\alpha x &= \alpha q_2 m_1 m_2 + \alpha m_1 a_2 \end{cases}$$

y sumando estas ecuaciones, tenemos que:

$$(m_2\beta + m_1\alpha)x = (\beta q_1 + \alpha q_2)m_1 m_2 + (\beta m_2 a_1 + \alpha m_1 a_2)$$

o teniendo en cuenta la forma en que elegimos α y β:

$$x = (\beta q_1 + \alpha q_2)m_1 m_2 + (\beta m_2 a_1 + \alpha m_1 a_2)$$

Llamando a a

$$a = \beta m_2 a_1 + \alpha m_1 a_2$$

esta ecuación implica que:

$$x \equiv a \pmod{m} \tag{20}$$

donde $m = m_1 m_2$.

Así pues hemos probado que cualquier solución de (18) es una solución de (20).

Recíprocamente, vamos a probar que cualquier solución de (20), es una solución de (18). Para ello notemos primero que a satisface que:

$$\begin{cases} a &\equiv a_1 \pmod{m_1} \\ a &\equiv a_2 \pmod{m_2} \end{cases} \tag{21}$$

Para verlo notemos que por la definición de a:

$$\begin{cases} a &\equiv \beta m_2 a_1 \pmod{m_1} \\ a &\equiv \alpha m_1 a_2 \pmod{m_2} \end{cases}$$

pero por (19) tenemos también que:

$$\begin{cases} \beta m_2 &\equiv 1 \pmod{m_1} \\ \alpha m_1 &\equiv 1 \pmod{m_2} \end{cases}$$

(o sea que m_2 y β son inversos módulo m_1, y del mismo modo m_1 y α son inversos módulo m_2)

Utilizando entonces la propiedad multiplicativa de las congruencias podemos concluir que se verifica (21) (lo que dice que a es una solución de 18).

Cualquier otra solución x de (18), verificará entonces (por transitividad de la relación de congruencia) que:

$$\begin{cases} x & \equiv & a & (\text{mód } m_1) \\ x & \equiv & a & (\text{mód } m_2) \end{cases}$$

y entonces por la proposición 12.1, tendremos que:

$$x \equiv a \quad (\text{mód } m)$$

Esto demuestra que (18) y (20) son equivalentes. □

Hagamos algunas observaciones sobre la demostración anterior: en primer lugar notemos que la demostración es constructiva (o sea: no sólo afirmamos que el a del enunciado existe, sino que damos un método para encontrarlo, ya que α y β pueden encontarse utilizando el algoritmo de Euclides. Por otra parte, notemos que $\overline{a}$ es única como clase de $\mathbb{Z}_m$ (esto es: dos posibles valores de a son congruentes módulo m).

El teorema chino puede genrealizarse facilmente a sistemas de más de dos congruencias:

Ejemplo: Consideremos el sistema

$$\begin{cases} x & \equiv & 2 & (\text{mód } 3) \\ x & \equiv & 4 & (\text{mód } 5) \\ x & \equiv & 1 & (\text{mód } 7) \end{cases} \tag{22}$$

formado por las dos congruencias del ejemplo anterior, más una tercera congruencia. Nuestro objetivo es encontrar una congruencia módulo $105 = 3 \times 5 \times 7$ que sea equivalente al sistema (22).

Notemos que en el ejemplo anterior vimos que las dos primeras congruencias eran equivalentes a la congruencia:

$$x \equiv 14 \quad (\text{mód } 15)$$

Sustituyendo, vemos que (22) es equivalente a

$$\begin{cases} x & \equiv & 14 & (\text{mód } 15) \\ x & \equiv & 1 & (\text{mód } 7) \end{cases}$$

Como nuevamente 15 y 7 son coprimos, podemos volver a aplicarle el teorema chino a este sistema. Nuevamente buscamos α y β, tales que:

$$15\alpha + 7\beta = 1$$

Encontramos que $\alpha = 1$, $\beta = -2$ y procediendo como en la demostración del teorema 12.1, encontramos que $a = -181$, es decir que el sistema (22), es equivalente a la única congruencia:

$$x \equiv -181 \pmod{105}$$

Generalizando este ejemplo, podemos dar un enunciado del teorema chino del resto para sistemas de un número arbitrario de congruencias:

Teorema 12.2 (Teorema Chino del resto, versión general) *Consideramos el sistema de congruencias:*

$$\left\{\begin{array}{rcll} x & \equiv & a_1 & (\text{mód } m_1) \\ x & \equiv & a_2 & (\text{mód } m_2) \\ \dots & & & \\ x & \equiv & a_k & (\text{mód } m_k) \end{array}\right. \tag{23}$$

donde $a_i \in \mathbb{Z}$, $m_i \in \mathbb{N}$ y, m_i y m_j son coprimos si $i \neq j$ ($1 \leq i, j \leq k$). Entonces existe un $a \in \mathbb{Z}$ tal que el sistema (23) es equivalente a la congruencia:

$$x \equiv a \pmod{m} \text{ donde } m = m_1 m_2 \dots m_k$$

Ejercicio: Efectuar la prueba de este teorema, por inducción en el número k de ecuaciones (imitando el procedimiento del ejemplo anterior)

A. La función de Euler y el teorema de Fermat-Euler

Vimos en el teorema 8.2 que las clases $\overline{a}$ donde a es coprimo con n, tienen un importante papel en la aritmética de $\mathbb{Z}_n$, a saber son exactamente las clases que admiten un inverso multiplicativo.

Por ello, conviene que estudiemos en más detalle el conjunto formado por estas clases[24]. Introduzcamos una notación para este conjunto:

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n : a \text{ es coprimo con } n\}$$

Notemos que "ser coprimo con n" es realmente una propiedad de la clase $\overline{a}$ (y no sólo del número a) pues si b pertenece a la misma clase en $\mathbb{Z}_n$ que a, es decir que $b \equiv a \pmod{n}$ entonces a es coprimo con n si y sólo si b lo es.
Prueba: Si suponemos que a es coprimo con n y $b \equiv a \pmod{n}$, entonces existe $q \in \mathbb{Z}$ tal que $b = qn + a$. Luego si $d|b$ y $d|n$, tedremos que $d|a$. Pero como a es coprimo con n, y d es un divisor común de ambos, debe ser $d = \pm 1$. En consecuencia b es coprimo con n. □

Notemos que como cada número es congruente módulo n con alguno de los números $0, 1, 2, \ldots, n-1$ podemos describir $\mathbb{Z}_n^*$ de modo un poco más explícito como:

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n : 0 \leq a \leq n-1,\ a \text{ es coprimo con } n\}$$

Una observación importante es que el conjunto $\mathbb{Z}_n^*$ es cerrado para el producto en $\mathbb{Z}_n$ ya que si a y b son coprimos con n, ab también lo es[25].

Definimos también una función $\varphi : \mathbb{N} \to \mathbb{N}$ (conocida como la indicatriz de Euler), del siguiente modo: $\varphi(n)$ es la cantidad de elementos de $\mathbb{Z}_n^*$, o lo

[24]Los temas de este apéndice son extras al programa de la materia, sin embargo constituyen una aplicación y continuación natural de la teoría que venimos desarrollando, y la función de Euler $\varphi(n)$ que introducimos en en esta sección también es importante en conección con las raices primitivas de la unidad (tema que veremos más adelante).

[25]Observamos que $\mathbb{Z}_n^*$ verifica tres propiedades importantes:

1. Es cerrado para el producto
2. El producto tiene un **elemento neutro** (la clase $\overline{1}$ del 1) tal que:
$$\overline{a} \cdot \overline{1} = \overline{1} \cdot a = \overline{a}$$
3. Cada elemento $\overline{a} \in \mathbb{Z}_n^*$ posee un **inverso multiplicativo** $\overline{a'}$ (teorema 8.2) tal que
$$\overline{a} \cdot \overline{a'} = \overline{a'} \cdot a = \overline{1}$$

Se dice entonces que el conjunto $\mathbb{Z}_n^*$ tiene estructura de **grupo** respecto a la operación de producto módulo n definida en él.

que es equivalente: $\varphi(n)$ cuenta cuántos de los números $0, 1, 2, \ldots, n-1$ son coprimos con n.

Veamos algunos ejemplos:

Ejemplo 1 consideremos por ejemplo $n = 6$. Entonces:

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

y

$$\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$$

En particular, $\varphi(6) = 2$.

Ejemplo 2: Si $n = 15 = 3 \times 5$, para determinar $\varphi(15)$ y los elementos de $\mathbb{Z}_{15}^*$ podemos proceder del siguiente modo: escribimos los números del 0 al 14:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14$$

Suprimos los que son múltiplos de 3:

$$1, 2, 4, 5, 7, 8, 10, 11, 13, 14$$

y suprimamos los que son múltiplos de 5:

$$1, 2, 4, 7, 8, 11, 13, 14$$

Los números que nos han quedado son coprimos con 15, en consecuencia:

$$\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

y $\varphi(15) = 8$. Este ejemplo muestra que el valor de $\varphi(n)$ depende de cómo sea la factorización en primos del número n.

Ejemplo 3: Si p es primo, los únicos números que no son coprimos con p son los que son divisibles por p (que corresponden a la clase del cero $\overline{0}$), en consecuencia:

$$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

y por lo tanto $\varphi(p) = p - 1$.

Ejemplo 4: Si tenemos que $n = pq$, donde p y q son dos primos distintos, podemos proceder como en el caso del 15, del siguiente modo: escribamos los números:

$$0, 1, 2, \ldots, n-1$$

y tachemos los que son múltiplos de p: son exactamente q números. Luego tachemos los múltiplos de q: son exactamente p números. Pero hay exactamente un número (el cero) que hemos tachado dos veces. En consecuencia: en total nos quedan sin tachar:

$$pq - q - p + 1$$

números. Este es el valor de[26]

$$\varphi(n) = pq - p - q + 1 = (p-1)(q-1)$$

.

Notemos que en este caso se cumple que:

$$\varphi(pq) = \varphi(p)\varphi(q)$$

Esto motiva la siguiente propiedad que nos permitirá calcular en general el valor de $\varphi(n)$, en términos de su factorización en primos:

Teorema A.1 *Si m_1 y m_2 son coprimos y $m = m_1 \cdot m_2$, entonces:*

$$\varphi(m) = \varphi(m_1)\varphi(m_2)$$

Para probar este teorema, necesitamos un lema sobre los sistemas de congruencias que hemos considerado en el teorema chino del resto:

Lema A.1 *Sean $m_1, m_2 \in \mathbb{N}$ coprimos, y consideremos el sistema de congruencias:*

$$\begin{cases} x \equiv a_1 & (\text{mód } m_1) \\ x \equiv a_2 & (\text{mód } m_2) \end{cases}$$

como en el teorema chino del resto (teorema 12.1). Entonces si $\overline{a}$ es la única solución de este sistema módulo m (dada por el teorema chino), tenemos que: a es coprimo con m, si y sólo si a_1 es coprimo con m_1 y a_2 es coprimo con m_2.

[26] Un argumento combinatorio similar puede utilizarse para determinar el valor de $\varphi(n)$ en general, por medio de la llamada "fórmula de inclusiones y exclusiones", ver por ejemplo [3], capítulo V, sección 2.

Prueba: Supongamos primero que a es coprimo con m. Entonces, conforme al teorema 8.2, a admite un inverso módulo m. Es decir: existe un $a' \in \mathbb{Z}$ tal que:

$$aa' \equiv 1 \pmod{m}$$

En consecuencia, tendremos que:

$$\begin{array}{rcll} aa' & \equiv & 1 & (\text{mód } m_1) \\ aa' & \equiv & 1 & (\text{mód } m_2) \end{array}$$

y por lo tanto

$$\begin{array}{rcll} a_1a' & \equiv & 1 & (\text{mód } m_1) \\ a_2a' & \equiv & 1 & (\text{mód } m_2) \end{array}$$

pero esto, justamente dice que a_1 admite un inverso módulo m_1, por lo que a_1 debe ser coprimo con m_1; y del mismo modo, a_2 admite un inverso módulo m_2, por lo que a_2 debe ser coprimo con m_2. (de nuevo usando el teroema 8.2).

Para probar el recíproco, supongamos que a_1 es coprimo con m_1 y que a_2 es coprimo con m_2. En consecuencia (nuevamente por el teorema 8.2), a_1 admite un inverso a_1' módulo m_1, y a_2 admite un inverso a_2' módulo m_2, o sea existen $a_1', a_2' \in \mathbb{Z}$ tales que:

$$\begin{array}{rcll} a_1a_1' & \equiv & 1 & (\text{mód } m_1) \\ a_2a_2' & \equiv & 1 & (\text{mód } m_2) \end{array}$$

Consideramos entonces el sistema de congruencias:

$$\left\{ \begin{array}{rcll} x & \equiv & a_1' & (\text{mód } m_1) \\ x & \equiv & a_2' & (\text{mód } m_2) \end{array} \right.$$

Conforme al teorema chino, este sistema admite una única solución $\overline{a'}$ módulo m, o sea existe un a' in $\mathbb{Z}$ tal que:

$$\left\{ \begin{array}{rcll} a' & \equiv & a_1' & (\text{mód } m_1) \\ a' & \equiv & a_2' & (\text{mód } m_2) \end{array} \right.$$

(y dos a' posibles son congruentes módulo m). Entonces tendremos que:

$$\left\{ \begin{array}{rcccll} aa' & \equiv & a_1a_1' & \equiv & 1 & (\text{mód } m_1) \\ aa' & \equiv & a_2a_2' & \equiv & 1 & (\text{mód } m_2) \end{array} \right.$$

y por lo tanto:

$$aa' \equiv 1 \pmod{m}$$

Pero esto dice que a admite un inverso módulo m, y en consecuencia a es coprimo con m (teorema 8.2). □

Ahora estamos en condiciones de probar el teorema A.1:

Prueba: Sea $m = m_1 m_2$. Queremos calcular $\varphi(m)$, es decir la cantidad de elementos de $\mathbb{Z}_m^*$.

Definamos para ello una función $f : \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \to \mathbb{Z}_m^*$ del siguiente modo: dadas dos clases $\overline{a_1} \in \mathbb{Z}_{m_1}^*$, $\overline{a_2} \in \mathbb{Z}_{m_2}^*$, definimos $f(\overline{a_1}, \overline{a_2})$ como la única solución $\overline{a}$ módulo m, del sistema de congruencias:

$$\left\{ \begin{array}{rcll} a & \equiv & a_1 & (\text{mód } m_1) \\ a & \equiv & a_2 & (\text{mód } m_2) \end{array} \right. \tag{24}$$

dada por el teorema chino del resto (teorema 12.1). Conforme al lema anterior (lema A.1), f está bien definida (si $\overline{a_1} \in \mathbb{Z}_{m_1}^*$ y $\overline{a_2} \in \mathbb{Z}_{m_2}^*$, efectivamente tenemos que $\overline{a} \in \mathbb{Z}_m^*$).

Más explcitamente, teniendo en cuenta la demostración del teorema chino, podemos definir f del siguiente modo: sean $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha m_1 + \beta m_2 = 1$, entonces:

$$f(\overline{a_1}, \overline{a_2}) = \overline{\beta m_2 a_1 + \alpha m_1 a_2} \quad (\text{clase en } \mathbb{Z}_m)$$

Por otra parte, la que la clase de un $a \in \mathbb{Z}$ en $\mathbb{Z}_m$, determina a qué clase pertenece en $\mathbb{Z}_{m_1}$ y $\mathbb{Z}_{m_2}$ (proposición 12.1). En consecuencia, f admite una función inversa dada por:

$$f^{-1}(\overline{a} \text{ en } \mathbb{Z}_m) = (\overline{a} \text{ en } \mathbb{Z}_{m_1}, \overline{a} \text{ en } \mathbb{Z}_{m_2})$$

Dado que f admite una función inversa, f es una biyección entre $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$ y $\mathbb{Z}_m^*$. En consecuncia, ambos conjuntos tienen la misma cantidad de elementos, o sea justamente:

$$\varphi(m_1)\varphi(m_2) = \varphi(m)$$

□

Ejemplo: Veamos como funciona la demostración anterior en el caso en que $m_1 = 3$ y $m_2 = 5$. En este caso:

$$\mathbb{Z}_3^* = \{\overline{1}, \overline{2}\}, \quad \mathbb{Z}_5^* = \{\overline{1}, \overline{2}.\overline{3}.\overline{4}\}$$

y podemos tomar $\alpha = 2$, $\beta = -1$, de modo que:

$$f(\overline{a_1} \text{ en } \mathbb{Z}_3, \overline{a_2} \text{ en } \mathbb{Z}_5) = \overline{-5a_1 + 6a_2} \text{ en } \mathbb{Z}_{15}$$

La tabla de los valores de f es:

$f(\overline{1},\overline{1})$	$=$	$\overline{1}$	$f(\overline{2},\overline{1})$	$=$	$\overline{-4} = \overline{11}$
$f(\overline{1},\overline{2})$	$=$	$\overline{7}$	$f(\overline{2},\overline{2})$	$=$	$\overline{-4} = \overline{2}$
$f(\overline{1},\overline{3})$	$=$	$\overline{13}$	$f(\overline{2},\overline{3})$	$=$	$\overline{8}$
$f(\overline{1},\overline{4})$	$=$	$\overline{19} = \overline{4}$	$f(\overline{2},\overline{4})$	$=$	$\overline{14}$

de modo que efectivamente f es una biyección entre $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$ y $\mathbb{Z}_{15}^*$.

Definición A.1 *Una función (aritmética*[27]*)* $f : \mathbb{N} \to \mathbb{Z}$ *(o más generalmente* $f : \mathbb{N} \to \mathbb{C}$*) tal que*

$$f(mn) = f(m)f(n) \text{ si } m, n \text{ son coprimos}$$

se denomina **multiplicativa**. *El teorema anterior afirma que la función de Euler* φ *es multiplicativa.*

Observamos que si f es multiplicativa, es fácil probar por inducción en la cantidad de factores k que:

$$f(m_1 m_2 \dots m_k) = f(m_1)f(m_2)\dots f(m_k)$$

si los factores m_i son coprimos dos a dos (es decir si m_i es coprimo con m_j para $1 \leq i \leq j$, $i \neq j$).

Ejercicio: Sea $P(x) = a_0 + a_1 x + \ldots + a_k x^k$ un polinomio con coeficientes enteros ($a_i \in \mathbb{Z}$). Sea para cada n in $\mathbb{Z}$, $N_P(n)$ el número de soluciones módulo n de la congruencia:

$$P(x) \equiv 0 \pmod{n}$$

probar que N_P es una función multiplicativa.

La importancia del teorema (A.1) radica en que nos permitirá calcular facilmente el valor de $\varphi(n)$ para cualquier n a partir del conocimiento de los valores $\varphi(p^k)$ de φ para las potencias de los primos.

[27]Suele denominarse funciones aritméticas a las que tienen como dominio al conjunto de números naturales $\mathbb{N}$, ya que en muchos ejemplos como la función de Euler, $f(n)$ expresa alguna propiedad aritmética del número n.

Supongamos por ejemplo que queremos calcular $\varphi(360)$. La factorización de 360 como producto de primos es:

$$360 = 2^3 \times 3^2 \times 5^1$$

entonces:

$$\varphi(360) = \varphi(2^3) \times \varphi(3^2) \times \varphi(5^1) = (2^3 - 2^2)(3^2 - 3^1)(5 - 1) = 4 \times 6 \times 4 = 96$$

Podemos enunciar esto como un teorema general:

Teorema A.2 *Para todo $n \in \mathbb{N}$, tenemos que:*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

donde el producto se extiende sobre los divisores primos de n.

Prueba: Consideremos la factorización de n como producto de primos:

$$n = \prod_{p|n} p^{v_p(n)}$$

Notamos que las potencias de primos diferentes son coprimas entre sí. Entonces, dado que φ es multiplicativa:

$$\varphi(n) = \prod_{p|n} \varphi(p^{v_p(n)}) = \prod_{p|n} \left(p^{v_p(n)} - p^{v_p(n)-1}\right)$$

$$= \prod_{p|n} p^{v_p(n)} \left(1 - \frac{1}{p}\right) = \left(\prod_{p|n} p^{v_p(n}\right) \left\{\prod_{p|n} \left(1 - \frac{1}{p}\right)\right\} =$$

$$= n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

□

Notemos que la misma idea de la prueba de este teorema muestra que en general, si una función es multiplicativa, para calcular su valor en cualquier entero, basta saber hacerlo en las potencias de los primos.

Una de las razones por las que la función φ de Euler resulta importante es porque interviene en la siguiente generalización de Euler del teorema de Fermat, para el caso de módulos no primos:

Teorema A.3 (Fermat-Euler) *Si $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ es coprimo con n, entonces*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ejermplo 1: Si $n = p$ es primo, $\varphi(p) = p - 1$, y se obtiene el teorema de Fermat.

Ejemplo 2: Si $n = pq$, siendo p y q primos distintos, entonces $\varphi(n) = (p-1)(q-1)$ y obtenemos el resultado del ejemplo que vimos al comienzo de la sección 12.

Prueba: Para demostrar el teorema de Fermat-Euler, consideramos la función $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ dada por

$$f(\overline{x}) = \overline{a} \cdot \overline{x} = \overline{ax}$$

Afirmamos que f es una biyección. En efecto, como a es coprimo con n, por hipótesis; $\overline{a}$ tiene un inverso $\overline{a'}$ en $\mathbb{Z}_m^*$ (teorema 8.2). En consecuencia f admite una inversa dada por:

$$f^{-1}(\overline{y}) = \overline{a'} \cdot \overline{y} = \overline{a'y}$$

(porque la operación inversa de multiplicar por $\overline{a}$, es multiplicar por su inverso $\overline{a'}$, que funciona como "dividir por $\overline{a}$").

En consecuencia, como f admite una inversa, f es una biyección. Se sigue que si

$$\mathbb{Z}_n^* = \{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}\} \text{ (todos elementos distintos)}$$

siendo $k = \varphi(n)$, deducimos que

$$\{f(\overline{x_1}), f(\overline{x_2}), \ldots, f(\overline{x_k})\}$$

los son mismos elementos de $\mathbb{Z}_n^*$, en otro orden (pues una biyección no hace más que permutar los elementos de un conjunto).

Deducimos que si los multiplicamos todos, tendremos que:

$$\prod_{i=1}^{k} \overline{x_i} = \prod_{i=1}^{k} f(\overline{x_i}) \text{ en } \mathbb{Z}_n$$

o sea:

$$\prod_{i=1}^{k} x_i \equiv \prod_{i=1}^{k} (ax_i) \pmod{n}$$

Agrupando las a que aparecen como factores en el segundo miembro, tenemos que:

$$\prod_{i=1}^{k} x_i \equiv a^k \left(\prod_{i=1}^{k} x_i \right) \pmod{n}$$

o llamando

$$x = \prod_{i=1}^{k} x_i$$

tenemos que:

$$x \equiv a^k \cdot x \pmod{n}$$

Pero como x es coprimo con n, podemos cancelarlo y deducir que:

$$a^k = a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

Otra propiedad notable de la función de Euler es la siguiente:

Teorema A.4 *Para todo $n \in \mathbb{N}$,*

$$\sum_{d|n} \varphi(d) = n \tag{25}$$

La suma en este teorema se extiende sobre todos los divisores positivos de n. Sumas de este tipo aparecen con frecuencia en la teoría de números.

Para demostrar este teorema, probaremos primero dos lemas que son de interés independiente:

Lema A.2 *Sea $m = m_1 m_2$ donde $m_1, m_2 \in \mathbb{N}$ son coprimos. Entonces cada divisor $d \in N$ de m se puede escribir de manera única en la forma $d = d_1 d_2$ donde $d_1 | m_1$, $d_2 | m_2$ y d_1 es coprimo con m_2 y d_2 es coprimo con m_1. Recíprocamente todo divisor de m es de esta forma.*

Prueba: Si $d|m$ consideramos su descomposición en factores primos:

$$d = \prod_{p|d} p^{v_p(d)}$$

y observamos que los primos que dividen a d deben ser algunos de los que dividen a m. Pero cada primo que divide a m, debe dividir a m_1 o a m_2 (y ambas cosas no pueden suceder simultáneamente). Luego podemos clasificar los primos que aparcen en la factorización de d en los que dividen a m_1 y los que divide a m_2, y escribir a d como $d = d_1 d_2$ siendo

$$d_1 = \prod_{p|d \wedge p|m_1} p^{v_p(d)}$$

$$d_2 = \prod_{p|d \wedge p|m_2} p^{v_p(d)}$$

Como para cualquier primo p que divida a m_1 tenemos que:

$$v_p(d_1) = v_p(d) \leq v_p(m) = v_p(m_1)$$

deducimos que $d_1|m_1$, por el teorema 10.1. Similarmente, $d_2|m_2$ Finalmente, es claro que d_1 y d_2 son coprimos, pues no comparten factores primos. Recíprocamente si $d = d_1 d_2$ donde $d_1|m_1$ y $d_2|m_2$, entonces $d_1|m_1 m_2$ y $d_2|m_1 m_2$. Por lo tanto, $d_1 d_2|m_1 m_2 = m$, en virtud de la proposición 10.4. □

Corolario A.1 *La función $d(n)$ que cuenta el número de divisores*[28] *(positivos) de n es multiplicativa.*

Lema A.3 *Sea $f : \mathbb{N} \to \mathbb{Z}$ (o más generalmente, $f : \mathbb{N} \to \mathbb{C}$) una función aritmética. Si f es multiplicativa, y definimos:*

$$g(n) = \sum_{d|n} f(d)$$

entonces g es así mismo multiplicativa.

Prueba: Sen $m_1, m_2 \in \mathbb{N}$ coprimos, y sea $m = m_1 m_2$ entonces por el lema A.2 tenemos que:

$$g(m) = \sum_{d|m} f(m) = \sum_{d_1|m_1 \wedge d_2|m_2} f(d_1 d_2)$$

[28]Introdujimos esta función en un ejercio de la sección 10. Este corolario puede utilizarse para resolver dicho ejercicio de otra manera.

Como f es multiplicativa, vemos que esta suma es igual a

$$\sum_{d_1|m_1 \wedge d_2|m_2} f(d_1)f(d_2) = \left(\sum_{d_1|m_1} f(d_1)\right)\left(\sum_{d_2|m_2} f(d_2)\right) = g(m_1)g(m_2)$$

□

Ahora resulta fácil demostrar el teorema A.4:
Prueba: Consideremos la función

$$g(d) = \sum_{d|n} \varphi(d)$$

Como φ es multiplicativa, por el lema A.3, g es multiplicativa. En consecuencia: para calcular $g(n)$ en cualquier $n \in \mathbb{N}$, basta saber hacerlo cuando $n = p^k$ con p primo.

Pero si $n = p^k$, los divisores (positivos) de n son de la forma p^j con $0 \leq j \leq k$, y resulta:

$$g(p^k) = \sum_{j=0}^{k} \varphi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1})$$

Desarrollándo esta suma:

$$g(p^k) = 1 + (p-1) + (p^2 - p) + \ldots + (p^k - p^{k-1})$$

vemos que cada término se cancela con el siguiente, salvo p^k ("suma telescópica") y resulta que $g(p^k) = p^k$.

En general, dado $n \in \mathbb{N}$, si su factorización en primos es

$$n = \prod_{p|n} p^{v_p(n)}$$

como g es multiplicativa, tendremos que:

$$g(n) = \prod_{p|n} g\left(p^{v_p(n)}\right) = \prod_{p|n} p^{v_p(n)} = n$$

□

Ejercicio: Sean $f, g : \mathbb{N} \to \mathbb{C}$ funciones aritméticas, y definamos una nueva función $h : \mathbb{N} \to \mathbb{C}$ por:

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Probar que si f y g son multiplicativas, entonces h también lo es.

Ejercicio: Una función aritmética muy emparentada con φ es la función μ de Möbius definida del siguiente modo:

$$\mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad \text{si } n \text{ es divisible por el cuadrado de algún primo} \\ (-1)^k & \text{si} \quad n = p_1 p_2 \dots p_k \text{ siendo los } p_i \text{ primos distintos} \end{cases}$$

Por ejemplo, $\mu(12) = 0, \mu(15) = 1, \mu(30) = -1$.
Probar las siguientes propiedades de μ:

1. μ es multiplicativa.

2. $$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases}$$

3. $$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} d\mu\left(\frac{n}{d}\right) \tag{26}$$

   (Sugerencia: desarrollar el producto del teorema A.2, usando la propiedad distributiva).

4. (Fórmula de inversión de Möbius) Si $f : \mathbb{N} \to \mathbb{C}$ es una función aritmética, y $g : \mathbb{N} \to \mathbb{C}$ está dada por:

   $$g(n) = \sum_{d|n} f(d)$$

   entonces, f se puede expresar en términos de g de la siguiente manera:

   $$f(n) = \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right) \mu(d)$$

B. El orden de un entero módulo n

Definición B.1 *Sea $\overline{a} \in \mathbb{Z}_n^*$. Definimos el órden (multiplicativo) de $\overline{a}$ en $\mathbb{Z}_n^*$ (o el orden de $a \in \mathbb{Z}$ módulo n, siendo a coprimo con n), como el menor expoente $d \in \mathbb{N}$ tal que*

$$\overline{a}^d = 1 \text{ en } \mathbb{Z}_n$$

o lo que es lo mismo:

$$a^d \equiv 1 \pmod{n}$$

Observación B.1 *En virtud del teorema de Fermat-Euler (y del principio del mínimo entero), d está bien definido, y se tiene que $d \leq \varphi(n)$.*

Teorema B.1 *Sea $\overline{a} \in \mathbb{Z}_n^*$. Entonces la sucesión de las potencias*

$$\overline{a}^0 = \overline{1}, \overline{a}, \overline{a}^2, \overline{a}^3, \ldots, \overline{a}^k, \ldots,$$

(en $\mathbb{Z}_n^*$) es períodica, con período d, siendo d el orden de a módulo n. Es decir que se verifica que:

$$a^i \equiv a^j \pmod{n}$$

sí y sólo si

$$i \equiv j \pmod{d}$$

En particular, se tiene que

$$a^i \equiv 1 \pmod{d}$$

si y sólo si $d|i$, y en consecuencia d debe ser un divisor de $\varphi(n)$.

Prueba: Podemos suponer claramente que $i \geq j$. Si $i \equiv j \pmod{d}$, entonces: $i - j = kd$ para algún $k \in \mathbb{N}_0$. Luego:

$$a^i = a^{i-j}a^j = (a^d)^k a^j \equiv a^j \pmod{n}$$

Recíprocamente si,

$$a^i \equiv a^j \pmod{n}$$

tendremos que:

$$a^{i-j}a^j \equiv a^j \pmod{n}$$

y como a^j es coprimo con n, por hipótesis, podremos cancelarlo, en esta congruencia: obteniendo que:

$$a^{i-j} \equiv 1 \pmod{n}$$

Efectuemos la división entera de $i - j$ por d, de modo que:

$$i - j = qd + r \text{ con } 0 \leq r < d$$

Si fuera $r \neq 0$, tendremos que:

$$a^{i-j} = (a^q)^d \cdot a^r \equiv a^r \pmod{n}$$

y consecuentemente:

$$a^r \equiv 1 \pmod{d}$$

Pero $1 \leq r < d$, contradiciendo la definición de d. Consecuentemente, debe ser $r = 0$, es decir que $d|i - j$, o sea que:

$$i \equiv j \pmod{d}$$

□

Referencias

[1] R. Courant, H. Robbins, ¿Qué es la matemática?. Editorial Aguilar, 1964. (suplemento al capítulo primero)

[2] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 4ta. Edición,

[3] J.V. Upspensky, M. A. Heaslet. Elementary Number Theory. Mc Gaw Hill, New York, 1939.

[4] I. Vinogradov, Fundamentos de la Teoría de los Números, Editorial Mir. Moscú, 1977.

[5] W. Stein, Elementary Number Theory (disponible en la página web de su autor, `http://sage.math.washington.edu/ent/`).

[6] J.P. Pinasco, *New Proofs of Euclid's and Euler's Theorems* American Mathematical Monthly, 116 (2009) 172–174.

Agradecimiento: Quiero agradecer a todos los colegas y alumnos que aportaron correcciones o comentarios sobre estas notas; especialmente a Jorge Guccione.