

Capítulo 2

Números naturales y números enteros

Empezamos aquí a estudiar los números naturales. Todos sabemos que al hablar de los números naturales nos estamos refiriendo a los números $0, 1, 2, \dots$. Sin embargo, para un estudio de algunas propiedades de los números naturales esta definición de números naturales es totalmente insuficiente. Necesitamos fijar una base como punto de arranque, a partir de la cual iremos desarrollando la teoría.

La primera cuestión que nos planteamos es dónde situar el punto de partida. Las posibilidades son varias. Por ejemplo, podemos empezar postulando la existencia de un conjunto (los números naturales) que satisface una serie de axiomas (los axiomas de Peano). A partir de estos axiomas podemos definir las operaciones básicas que todos conocemos (suma y producto) y el orden.

También es posible situar el punto de arranque en la teoría de conjuntos, y en el marco de esta teoría construir un conjunto (\mathbb{N}) del cual se demuestra que satisface los axiomas de Peano. En este caso, los axiomas de Peano son una consecuencia de la construcción hecha de \mathbb{N} , mientras que en el caso anterior estos axiomas constituyen el principio de la teoría. Una vez demostrados los axiomas de Peano, se enlaza con el caso anterior.

Estos planteamientos, sin embargo, no nos interesan en este momento. Nosotros supondremos que tenemos un conjunto, representado por \mathbb{N} , cuyos elementos son los números naturales, y que en este conjunto tenemos definidas dos operaciones (suma y producto), de las que conocemos sus propiedades básicas. Tenemos definido también un orden de los números naturales, y sabemos que los números naturales satisfacen el axioma de inducción. En la sección siguiente recordaremos todas estas propiedades y axiomas.

También supondremos la existencia de los números enteros (\mathbb{Z}), los números racionales (\mathbb{Q}), los números reales (\mathbb{R}) y los números complejos (\mathbb{C}) con su estructura algebraica y de orden (salvo en \mathbb{C}).

2.1. Representación de los números naturales. Sistemas de numeración.

2.1.1. El conjunto de los números naturales.

Como hemos dicho, comenzamos suponiendo que tenemos un conjunto \mathbb{N} . Los elementos de este conjunto se llaman *números naturales*.

Dados dos números naturales, m y n , hay definidos dos nuevos números naturales, llamados respectivamente suma y producto de m y n , y representados mediante $m + n$ y $m \cdot n$ (o simplemente mn). Estas operaciones satisfacen las siguientes propiedades:

- i) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m + n) + p = m + (n + p)$ (es decir, la suma es asociativa).
- ii) Para cualesquiera $m, n \in \mathbb{N}$, $m + n = n + m$ (es decir, la suma es conmutativa).
- iii) Existe en \mathbb{N} un elemento, representado por 0 tal que para cada $m \in \mathbb{N}$ se tiene que $m + 0 = m$ (existencia de elemento neutro para la suma).
- iv) Si $m + n = m + p$ entonces $n = p$ (Propiedad cancelativa).

- v) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ (es decir, el producto es asociativo).
- vi) Para cualesquiera $m, n \in \mathbb{N}$, $m \cdot n = n \cdot m$ (es decir, el producto es conmutativo).
- vii) Existe en \mathbb{N} un elemento, representado por 1 tal que para cada $m \in \mathbb{N}$ se tiene que $m \cdot 1 = m$ (existencia de elemento neutro para el producto).
- viii) Si $m \cdot n = m \cdot p$ y $m \neq 0$ entonces $n = p$.
- ix) Para cualesquiera $m, n, p \in \mathbb{N}$, $m \cdot (n + p) = m \cdot n + m \cdot p$ (la suma es distributiva respecto al producto).

También en \mathbb{N} hay definida una relación como sigue:

$$m \leq n \text{ si existe } p \in \mathbb{N} \text{ tal que } m + p = n$$

que satisface las siguientes propiedades:

- x) $m \leq m$ para todo $m \in \mathbb{N}$.
- xi) Si $m \leq n$ y $n \leq m$ entonces $m = n$.
- xii) Si $m \leq n$ y $n \leq p$ entonces $m \leq p$,
- xiii) Para cualesquiera $m, n \in \mathbb{N}$, $m \leq n$ ó $n \leq m$.
- xiv) $m \leq n$ implica que $m + p \leq n + p$ para todo $p \in \mathbb{N}$.
- xv) $m + p \leq n + p$ implica que $m \leq n$.
- xvi) $m \leq n$ implica que $m \cdot p \leq n \cdot p$.
- xvii) Si $m \cdot p \leq n \cdot p$ y $p \neq 0$ entonces $m \leq n$.

Todo lo dicho anteriormente es igualmente válido para otros conjuntos, como \mathbb{Q}^+ , \mathbb{R}^+ , etc. Lo que distingue a \mathbb{N} de estos conjuntos es el *Principio de inducción*.

Principio de inducción:

Si A es un subconjunto de \mathbb{N} tal que:

$$0 \in A$$

$$\text{Si } n \in A \text{ entonces } n + 1 \in A$$

Entonces $A = \mathbb{N}$.

Intuitivamente, nos dice que los números naturales podemos recorrerlos *de uno en uno*, y no nos dejamos ninguno en medio, es decir, cualquier número natural puede ser obtenido a partir del cero sin más que sumar uno las veces que sean necesarias. Si lo pensamos, para los conjuntos \mathbb{Q}^+ o \mathbb{R}^+ no se cumple esta propiedad, pues procediendo así siempre nos dejamos números "en medio".

El principio de inducción está en la base de la recursividad, y por tanto en la de muchas demostraciones en las que intervienen los números naturales. Nosotros, sin embargo, no vamos a profundizar en este principio, ni en las demostraciones por inducción.

Una consecuencia de este principio, junto con las propiedades anteriores es que si $m < n$ entonces $m + 1 \leq n$.

Recordemos también que dados dos números naturales m y n , tenemos definido el número m^n (salvo cuando $m = n = 0$), que representa el producto de m consigo mismo n veces. Es decir, $m^1 = m$, $m^2 = m \cdot m$, $m^3 = m \cdot m \cdot m$, etc. Sabemos que a m^0 se le asigna el valor 1, y que esta operación satisface las siguientes propiedades:

- xviii) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m \neq 0$, $m^{n+p} = m^n \cdot m^p$.

xix) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m \neq 0$, $(m^n)^p = m^{n \cdot p}$.

xx) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m, n \neq 0$, $(m \cdot n)^p = m^p \cdot n^p$.

Una consecuencia del principio de inducción es el siguiente teorema:

Teorema 2.1.1. *[Principio de buena ordenación] Sea B un subconjunto no vacío de \mathbb{N} . Entonces B tiene mínimo.*

Demostración: Tomamos A el conjunto de las cotas inferiores de B . Es claro que $0 \in A$ y que $A \neq \mathbb{N}$ (ya que si $m \in B$ entonces $m + 1 \notin A$). Ahora bien. Si el enunciado $n \in A \implies n + 1 \in A$ fuera cierto, tendríamos que $A = \mathbb{N}$, lo cual no es posible. Por tanto, debe ser falso, lo que nos dice que tiene que existir un elemento m_0 tal que $m_0 \in A$ pero $m_0 + 1 \notin A$.

Entonces, este elemento es el mínimo de B . Para esto, deben ocurrir dos cosas: que sea cota inferior (lo cual es cierto, pues es elemento de A) y que pertenezca a B . Veamos esto último.

Si $m_0 \notin B$ significa que $m_0 < n$ para cualquier $n \in B$, luego $m_0 + 1 \leq n$ para cualquier $n \in B$, lo que implicaría que $m_0 + 1$ es cota inferior de B y por consiguiente pertenecería a A . ■

Como consecuencia de esto, tenemos:

Corolario 2.1.1. *No existen sucesiones en \mathbb{N} infinitas y estrictamente decrecientes.*

Demostración: Si $x_0, x_1, \dots, x_m, \dots$ fuera una tal sucesión, entonces el conjunto $\{x_n : n \in \mathbb{N}\}$ tendría mínimo, que tendría que corresponder con algún término de la sucesión, digamos x_k . Pero en tal caso, $x_{k+1} < x_k$ por ser la sucesión estrictamente decreciente, lo que nos dice que dicho término no puede ser el mínimo. ■

Tras esta introducción, nos adentramos ya en materia. Comenzamos por un resultado de todos conocido.

Teorema 2.1.2. *[Algoritmo de la división] Sean $a, b \in \mathbb{N}$, con $b \neq 0$. Entonces existen únicos elementos $c, r \in \mathbb{N}$ tales que:*

$$\begin{aligned} & \vdash a = bc + r. \\ & \vdash r < b. \end{aligned}$$

Obviamente, lo único que estamos haciendo es la división usual de a entre b .

Los números c y r se llaman respectivamente cociente y resto de la división de a entre b .

La demostración de este teorema se haría usando el principio de inducción. Pero nosotros daremos por cierto este resultado.

Definición 32. *Sean $a, b \in \mathbb{N}$. Se definen los números naturales a mód b y a div b como los únicos números naturales que satisfacen que*

$$a = b \cdot (a \text{ div } b) + (a \text{ mód } b); \quad a \text{ mód } b < b$$

Es decir, a mód b es el resto que resulta de dividir a entre b y a div b es el cociente de dividir a entre b .

Ejemplo 2.1.1. *Se tiene que $13 \text{ mód } 3 = 1$ y $13 \text{ div } 3 = 4$, pues $13 = 3 \cdot 4 + 1$.*

Notemos que si $a \neq 0$ y $b \geq 2$ entonces $a \text{ div } b < a$ (¿por qué?).

2.1.2. Sistemas de numeración.

Sabemos que el conjunto de los números naturales es infinito. Sin embargo, para representar un número natural, empleamos únicamente los símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Con estos símbolos, llamados dígitos, combinados de manera adecuada podemos representar todos los números naturales. Los números 0 y 1 representan los elementos neutros para la suma y el producto. El resto de los números, representados por estos dígitos puede obtenerse fácilmente mediante $2 = 1 + 1$, $3 = 2 + 1$, y así sucesivamente hasta $9 = 8 + 1$. El número siguiente, es decir $9 + 1$ es representado, como todos sabemos como 10.

En una representación de un número natural, el valor de cada uno de estos dígitos depende de la posición que ocupe. Así, en el número 1343 no representa lo mismo el dígito 3 situado a la derecha que el dígito 3 situado entre los dígitos 1 y 4. Analizando algo más el valor de cada uno de los dígitos, vemos que el valor del 1 que se encuentra a la izquierda es 10^3 , el valor del 3 que se encuentra inmediatamente a la derecha es $3 \cdot 10^2$, el valor del 4 es $4 \cdot 10$, mientras que el valor del 3 situado a la derecha es 3. El número representado mediante 1343 es entonces la suma de todos estos resultados, es decir, $1343 = 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 3$.

El origen de la elección de 10 como base de la representación de los números naturales parece ser que se encuentra en el número de dedos que tenemos en las manos. Nos planteamos ahora qué ocurriría si en lugar de elegir como base a 10 eligieramos cualquier otro número b . La respuesta viene en el siguiente teorema.

Teorema 2.1.3. *Sean $a, b \in \mathbb{N}$ con $a \neq 0$ y $b \geq 2$. Entonces existen únicos $m \in \mathbb{N}$ y $a_0, a_1, \dots, a_m \in \mathbb{N}$ tales que:*

- ▮ $a_m \neq 0$.
- ▮ $a = \sum_{k=0}^m a_k b^k = a_m b^m + \dots + a_1 b + a_0$
- ▮ $a_i < b$.

Demostración:

Probemos en primer lugar la existencia de estos números.

En el caso de que $a < b$ entonces podemos tomar $m = 0$, $a_0 = a$.

Supongamos entonces que $a \geq b$. Dividimos a entre b , y obtenemos un cociente que llamaremos c_1 y un resto que llamaremos a_0 . En tal caso, tenemos que $a = b \cdot c_1 + a_0$.

Es claro que $1 \leq c_1 < a$. Si $c_1 < b$ entonces tomamos $m = 1$, $a_1 = c_1$, y ya tendríamos la existencia de m y los coeficientes a_i . Si $c_1 \geq b$, entonces dividimos c_1 entre b , y obtenemos un cociente c_2 y un resto a_1 , es decir, $c_1 = b \cdot c_2 + a_1$, luego

$$a = b \cdot c_1 + a_0 = b \cdot (b \cdot c_2 + a_1) + a_0 = c_2 \cdot b^2 + a_1 \cdot b + a_0$$

Repetimos con c_2 lo mismo que con c_1 , y así tenemos una sucesión decreciente de números naturales $a > c_1 > c_2 > \dots$. Esta sucesión no puede ser infinita (corolario 2.1.1). Si c_k es su último término, entonces $c_k < b$. En tal caso, tomamos $m = k$ y $a_k = c_k$, en cuyo caso:

$$a = b \cdot c_1 + a_0 = c_2 b^2 + a_1 b + a_0 = c_3 b^3 + a_2 b^2 + a_1 b + a_0 = \dots = c_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

como queríamos.

La demostración de la unicidad se deja como ejercicio.

■

Ejemplo 2.1.2. *Tomemos, por ejemplo, $b = 5$ y el número $a = 446$. Vamos a hallar los distintos números que nos dice el teorema.*

Puesto que $446 \geq 5$, realizamos la división $446 = 5 \cdot 89 + 1$. En tal caso, $a_0 = 1$ y $c_1 = 89$.

Al ser $c_1 \geq 5$ repetimos el proceso. $89 = 5 \cdot 17 + 4$. Esto nos da $a_1 = 4$ y $c_2 = 17$. Entonces,

$$446 = 5 \cdot 89 + 1 = 5 \cdot (5 \cdot 17 + 4) + 1 = 5^2 \cdot 17 + 5 \cdot 4 + 1 = 17 \cdot 5^2 + 4 \cdot 5 + 1$$

Continuamos, pues $c_2 \geq 5$. Ahora tenemos $17 = 5 \cdot 3 + 2$. Por tanto, $a_2 = 2$ y $c_3 = 3$. Sustituimos, y nos queda:

$$446 = 17 \cdot 5^2 + 4 \cdot 5 + 1 = (3 \cdot 5 + 2) \cdot 5^2 + 4 \cdot 5 + 1 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$$

Y ya tenemos que el cociente, c_3 , es menor que la base. Por tanto, $m = 3$ y $a_3 = c_3 = 3$.

En resumen, tenemos que $m = 3$ y los coeficientes son $a_0 = 1$, $a_1 = 4$, $a_2 = 2$ y $a_3 = 3$.

La demostración anterior nos proporciona un algoritmo recursivo para calcular estos coeficientes.

Algoritmo BASE(a, b)

Entrada: $a, b \in \mathbb{N}$; $a \geq 1, b \geq 2$.

Salida: m, a_0, a_1, \dots, a_m
 $m \in \mathbb{N}$
 $a_0, a_1, \dots, a_m \in \mathbb{N}$
 $0 \leq a_i < b$
 $a_m \neq 0$
 $a = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + \dots + a_1 \cdot b + a_0$

$m := 0$

Mientras $a \geq b$

$a_m := a \bmod b$

$a := a \operatorname{div} b$

$m := m + 1$

$a_m := a$

Devuelve m, a_0, a_1, \dots, a_m

Ejemplo 2.1.3.

Vamos a repetir el ejemplo anterior, es decir, $a = 446$ y $b = 5$. Los resultados los vamos a ir ordenando en una tabla.

Los valores iniciales son $b = 5$ (que no varía), $a = 446$ y $m = 0$.

b	5
a	446
m	0
a_m	

Puesto que $a \geq b$ entramos en el bucle, lo que nos da $a_m = a_0 = 446 \bmod 5 = 1$, $a = 446 \operatorname{div} 5 = 89$ y $m = 1$.

b	5	
a	446	89
m	0	1
a_m	1	

Ahora también $a = 89$ es mayor que $b = 5$, por lo que volvemos a entrar en el bucle. $a_1 = 89 \bmod 5 = 4$, $a = 89 \operatorname{div} 5 = 17$ y $m = 2$.

b	5		
a	446	89	17
m	0	1	2
a_m	1	4	

Se tiene que $17 \geq 5$. Entonces $a_2 = 17 \bmod 5 = 2$, $a = 17 \operatorname{div} 5 = 3$ y $m = 3$.

b	5			
a	446	89	17	3
m	0	1	2	3
a_m	1	4	2	

Y ahora, como $a < b$, hacemos $a_3 = 3$

b	5			
a	446	89	17	3
m	0	1	2	3
a_m	1	4	2	3

y terminamos: $m = 3$ y $a_0 = 1$, $a_1 = 4$, $a_2 = 2$ y $a_3 = 3$, de donde $446 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$.

Definición 33. Sean $a, b \in \mathbb{N}$ con $b \geq 2$. Elegimos b símbolos que se corresponden con los números desde 0 hasta $b-1$, e identificamos estos números con sus símbolos. Supongamos que $a = a_m b^m + \cdots + a_1 b + a_0$ con $a_i < b$. Diremos entonces que $a_m a_{m-1} \cdots a_1 a_0$ es una representación del número a en base b , y escribiremos

$$a = (a_m a_{m-1} \cdots a_1 a_0)_b$$

Observaciones:

1. Cada uno de los símbolos que aparecen en la representación de un número se denomina cifra.
2. Si $a = (a_m \cdots a_1 a_0)_b$, podemos añadir ceros a la izquierda y obtenemos también una representación de a . Normalmente, elegiremos como representación de a aquella para la que la cifra de la izquierda sea distinta de cero (si el número a es distinto de cero).
3. Si $a = (a_m \cdots a_1 a_0)_b$ y $a_m \neq 0$, diremos que el número a tiene $m+1$ cifras en base b .
4. A la hora de especificar la base lo haremos en base decimal. Si la expresáramos en base b nos quedaría siempre 10.
5. Cuando no se especifique la base en que está expresado un número supondremos que está en base diez, salvo que el contexto deje suficientemente claro la base en que estamos trabajando.
6. Cuando trabajamos en base diez, los símbolos empleados son, como todos sabemos, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Si trabajamos en una base b menor que diez, emplearemos los símbolos anteriores hasta $b-1$. Por ejemplo, en base 2 se emplean 0, 1. Cuando la base sea mayor que 10, como símbolos adicionales se suelen emplear las letras del alfabeto (siempre y cuando la base no sea muy grande). Es muy frecuente trabajar en base dieciseis, en cuyo caso, los símbolos empleados son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Ejemplo 2.1.4.

1. Si queremos expresar el número 446 en base 5, necesitamos una expresión de este número en función de potencias de 5. Sabemos que $446 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$, luego

$$446 = (3241)_5$$

2. Vamos a expresar el número $(23143)_6$ en base 8. Para esto, podemos pasarlo a base decimal y después pasarlo a base 8.

$$(23143)_6 = 2 \cdot 6^4 + 3 \cdot 6^3 + 6^2 + 4 \cdot 6 + 3 = 2 \cdot 1296 + 3 \cdot 216 + 36 + 4 \cdot 6 + 3 = 3303$$

$$3303 = 8 \cdot 412 + 7 \quad 412 = 8 \cdot 51 + 4 \quad 51 = 8 \cdot 6 + 3$$

$$\text{Por tanto tenemos que } (23143)_6 = 3303 = (6347)_8$$

3. Vamos ahora a expresar el número $(10101111011000001010100)_2$ en base 8 y en base 16. En primer lugar lo pasamos a base decimal.

$$(10101111011000001010100)_2 = 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 = 5746772$$

Nos apoyamos ahora en el algoritmo BASE

b	8							
a	5746772	718346	89793	11224	1403	175	21	2
m	0	1	2	3	4	5	6	7
a_m	4	2	1	0	3	7	5	2

y de aquí deducimos que $(10101111011000001010100)_2 = (25730124)_8$

Para expresar el número en base 16, volvemos a hacer uso del algoritmo BASE para los valores $a = 5746772$ y $b = 16$.

b	16					
a	5746772	359173	22448	1403	87	5
m	0	1	2	3	4	5
a_m	4	5	0	11	7	5

luego $(10101111011000001010100)_2 = (57B054)_{16}$ (donde, como dijimos antes, hemos empleado los símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F).

Ahora bien, dado que $8 = 2^3$, podíamos haber procedido como sigue:

$$\begin{aligned}
 (10101111011000001010100)_2 &= 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 \\
 &= 2 \cdot 2^{21} + (2^2 + 1)2^{18} + (2^2 + 2 + 1)2^{15} + (2 + 1)2^{12} + 2^6 + 2 \cdot 2^3 + 2^2 \\
 &= 2 \cdot 8^7 + 5 \cdot 8^6 + 7 \cdot 8^5 + 3 \cdot 8^4 + 8^2 + 2 \cdot 8 + 4
 \end{aligned}$$

y como $16 = 2^4$, podíamos haberlo hecho de forma análoga:

$$\begin{aligned}
 (10101111011000001010100)_2 &= 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 \\
 &= (2^2 + 1)2^{20} + (2^2 + 2 + 1)2^{16} + (2^3 + 2 + 1)2^{12} + (2^2 + 1)2^4 + 2^2 \\
 &= 5 \cdot 16^5 + 7 \cdot 16^4 + 11 \cdot 16^3 + 5 \cdot 16 + 4
 \end{aligned}$$

y de aquí es fácil obtener la representación del número dado en base 8 y en base 16.

Podemos apreciar como para pasar de base 2 a base $8 = 2^3$ podemos agrupar las cifras del número en base 2 de tres en tres (empezando por la derecha). Cada uno de estos tres grupos da lugar a una cifra en base 8. De la misma forma, cada 4 cifras de un número en base 2 da lugar a una cifra del mismo número en base 16.

$$\begin{array}{cccccccccccccccccccc}
 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
 \underbrace{\hspace{1.5cm}}_2 & \underbrace{\hspace{1.5cm}}_5 & \underbrace{\hspace{1.5cm}}_7 & \underbrace{\hspace{1.5cm}}_3 & \underbrace{\hspace{1.5cm}}_0 & \underbrace{\hspace{1.5cm}}_1 & \underbrace{\hspace{1.5cm}}_2 & \underbrace{\hspace{1.5cm}}_4 & & & & & & & & & & & & & & & \\
 \end{array}
 \quad
 \begin{array}{cccccccccccccccc}
 101 & 0111 & 1011 & 0000 & 0101 & 0100 \\
 \underbrace{\hspace{1.5cm}}_5 & \underbrace{\hspace{1.5cm}}_7 & \underbrace{\hspace{1.5cm}}_B & \underbrace{\hspace{1.5cm}}_0 & \underbrace{\hspace{1.5cm}}_5 & \underbrace{\hspace{1.5cm}}_4
 \end{array}$$

En general, para pasar un número de base b a base b^k basta con agrupar las cifras del número escrito en base b en grupos de k cifras, empezando por la derecha. Cada uno de estos grupos determina una cifra en base b^k .

Recíprocamente, para pasar un número de base b^k a base b es suficiente expresar cada cifra del número en base b (completando con ceros a la izquierda para que nos de k cifras).

4. Vamos a encontrar una base b donde se de la igualdad $21 \cdot 23 = 1033$.

Obviamente, b debe ser mayor o igual que 4, pues en otro caso no podríamos tener el dígito 3.

Al estar escritos los números en base b lo que tenemos es la igualdad

$$(2b + 1)(2b + 3) = b^3 + 3b + 3$$

Operando nos queda $b^3 - 4b^2 - 5b = 0$, que podemos comprobar que tiene tres raíces, que son $b = -1$, $b = 0$ y $b = 5$. La solución es por tanto $b = 5$.

Los algoritmos que conocemos para sumar, restar, multiplicar o dividir números escritos en base 10 son válidos ahora para realizar estas operaciones para números escritos en una base b cualquiera.

Así, por ejemplo, para la suma, si $m, n \in \mathbb{N}$; $m = (m_k m_{k-1} \cdots m_1 m_0)_b$ y $n = (n_k n_{k-1} \cdots n_1 n_0)_b$ (hemos supuesto que los dos números tienen igual número de cifras. De no ser así, añadimos "ceros" al que tenga menos), entonces $m + n = (p_{k+1} p_k \cdots p_1 p_0)_b$ donde:

- $p_0 = (m_0 + n_0) \bmod b$

- $p_{i+1} = (m_{i+1} + n_{i+1} + a_i) \bmod b$, donde $a_i = (m_i + n_i + a_{i-1}) \div b$ (hemos tomado $a_{-1} = 0$).

Es fácil comprobar que el número $(p_{k+1}p_k \cdots p_1p_0)_b$ aquí descrito corresponde con la suma de m y n (hágase).

Este algoritmo puede extenderse sin dificultad a la suma de tres o más números. Para el caso que hemos detallado de dos números, a_i únicamente puede tomar los valores 0 y 1.

En el caso $b = 10$, lo que hemos dicho es simplemente el método tradicional que usamos para sumar dos (o más) números.

Ejemplo 2.1.5. Sean $x = (36725)_8$ e $y = (740125)_8$. Vamos a calcular la suma de x e y y la diferencia $y - x$.

$$\begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array}$$

Nótese que $x = 3 \cdot 8^4 + 6 \cdot 8^3 + 7 \cdot 8^2 + 2 \cdot 8 + 5 = 15829$, $y = 7 \cdot 8^5 + 4 \cdot 8^4 + 1 \cdot 8^3 + 2 \cdot 8 + 5 = 245845$, luego

$$x + y = 15829 + 245845 = 261674 = 7 \cdot 8^5 + 7 \cdot 8^4 + 7 \cdot 8^3 + 5 \cdot 8 + 2 = (777052)_8$$

$$\begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array}$$

Para realizar una multiplicación o una división es conveniente tener las tablas de multiplicar. En base 8 éstas serían:

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

Ejemplo 2.1.6. Sean $x = (37142)_8$ e $y = (65)_8$. Vamos a calcular el producto $x \cdot y$, y el cociente y resto que resulta de dividir x entre y .

$$\begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array}$$

$$\begin{array}{r} \\ \\ \hline \end{array} \quad \begin{array}{r} \\ \\ \hline \end{array}$$

Por último, vamos a calcular la división de x entre y .

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ \hline \end{array}$$

Estimamos el valor de 371 entre 65

Como $5 \cdot 6 = 36$ se queda muy próximo a 37, probamos por 4.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ \hline 4 \end{array}$$

$4 \cdot 5 = 24$ hasta 31, 5 y nos llevamos 3.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 5 \quad \quad \hline 4 \end{array}$$

$4 \cdot 6 = 30$ y 3, 33; hasta 37, 4.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 4 \ 5 \quad \quad \hline 4 \end{array}$$

Bajamos el 4.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 4 \ 5 \ 4 \quad \quad \hline 4 \end{array}$$

Como antes, estimamos el valor de 454 entre 65 y ahora nos da 5.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 4 \ 5 \ 4 \quad \quad \hline 4 \ 5 \end{array}$$

$5 \cdot 5 = 31$ hasta 34, 3 y nos llevamos 3.

$5 \cdot 6 + 3 = 36 + 3 = 41$, hasta 45, 4.

Bajamos el 2.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 4 \ 5 \ 4 \quad \quad \hline 4 \ 5 \\ 4 \ 3 \ 2 \end{array}$$

La última cifra del cociente es 5. Calculamos el resto y nos da 21.

$$\begin{array}{r} 3 \ 7 \ 1 \ 4 \ 2 \mid 6 \ 5 \\ 4 \ 5 \ 4 \quad \quad \hline 4 \ 5 \ 5 \\ 4 \ 3 \ 2 \\ 2 \ 1 \end{array}$$

Por tanto, tenemos que $(37142)_8 = (65)_8 \cdot (455)_8 + (21)_8$.

Vamos a expresar estos números en decimal. $(37142)_8 = 15970$, $(65)_8 = 53$, $(455)_8 = 301$ y $(21)_8 = 17$. Calcula el cociente y el resto de la división de 15970 entre 53.

En caso de que estemos en base 2, los cálculos son mucho más sencillos, pues en tal caso, las únicas multiplicaciones que realizamos son por cero o por uno.

Ejemplo 2.1.7.

Vamos a realizar la división de dos números cuya representación en binario es $x = 101101010$ e $y = 1101$.

$$\begin{array}{r} 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \mid 1 \ 1 \ 0 \ 1 \\ \hline \end{array}$$

Como $1011 < 1101$ tomamos una cifra más.

Ponemos un 1 en el cociente y restamos:

$10110 - 1101 = 1001$. El resultado de la resta lo situamos debajo de 10110.

$$\begin{array}{r} 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \mid 1 \ 1 \ 0 \ 1 \\ 1 \ 0 \ 0 \ 1 \quad \quad \hline 1 \end{array}$$

Bajamos el 1 y al ser $10011 > 1101$,

Ponemos un 1 en el cociente y restamos:

$10011 - 1101 = 0110$. El resultado lo situamos debajo de 10011.

$$\begin{array}{cccccccc|cccc}
 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
 & 1 & 0 & 0 & 1 & 1 & & & & 1 & 1 & & \\
 & & 0 & 1 & 1 & 0 & & & & & & &
 \end{array}$$

Bajamos el 0 y como $1100 < 1101$,
0 al cociente y bajamos la cifra siguiente.
Hacemos igual que antes. $11001 - 1101 = 1100$.

$$\begin{array}{cccccccc|cccc}
 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
 & 1 & 0 & 0 & 1 & 1 & & & & 1 & 1 & 0 & 1 \\
 & & 0 & 1 & 1 & 0 & 0 & 1 & & & & & \\
 & & & 1 & 1 & 0 & 0 & & & & & &
 \end{array}$$

Por último, bajamos el 0, llevamos un 1 al cociente,
y colocamos el resultado de la resta $11000 - 1101$,
que es 1011 bajo 11000.

$$\begin{array}{cccccccc|cccc}
 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
 & 1 & 0 & 0 & 1 & 1 & & & & 1 & 1 & 0 & 1 \\
 & & 0 & 1 & 1 & 0 & 0 & 1 & & & & & \\
 & & & 1 & 1 & 0 & 0 & 0 & & & & & \\
 & & & & 1 & 0 & 1 & 1 & & & & &
 \end{array}$$

Y ya hemos terminado la división.

El cociente es $c = 11011$ y el resto $r = 1011$.

Si expresamos x e y en el sistema decimal, nos queda que $x = 362$ e $y = 13$. Al dividir 362 entre 13 nos da de cociente 27, cuya expresión en binario es 11011 y de resto 11, cuya expresión en binario es 1011.

2.2. Números enteros.

Al igual que con los números naturales comenzamos recordando algunos hechos conocidos de los números enteros.

Los números enteros forman un conjunto \mathbb{Z} que contiene a \mathbb{N} . Dados dos números enteros, a y b , hay definidos dos nuevos números enteros, llamados respectivamente suma y producto de a y b , y representados mediante $a + b$ y $a \cdot b$ (o simplemente ab). Estas operaciones satisfacen las siguientes propiedades:

- i) Para cualesquiera $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
- ii) Para cualesquiera $a, b \in \mathbb{Z}$, $a + b = b + a$.
- iii) El elemento neutro para la suma en \mathbb{N} es también un elemento neutro para la suma en \mathbb{Z} .
- iv) Para cada $a \in \mathbb{Z}$ existe un elemento en \mathbb{Z} , representado por $-a$ tal que $a + (-a) = 0$ (Existencia de opuesto para la suma).
- v) Para cualesquiera $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- vi) Para cualesquiera $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.
- vii) El elemento neutro para el producto en \mathbb{N} es también un elemento neutro para el producto en \mathbb{Z} .
- viii) Si $a \cdot b = a \cdot c$ y $a \neq 0$ entonces $b = c$.
- ix) Para cualesquiera $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Nótese que la propiedad iv) implica que la suma es cancelativa. También esta propiedad permite definir la resta o diferencia de dos números enteros. Dados $a, b \in \mathbb{Z}$ se define $a - b$ como el número $a + (-b)$.

También en \mathbb{Z} hay definida una relación como sigue:

$$a \leq b \text{ si } b - a \in \mathbb{N}$$

que satisface las siguientes propiedades:

- x) $a \leq a$ para todo $a \in \mathbb{Z}$.
- xi) Si $a \leq b$ y $b \leq a$ entonces $a = b$.
- xii) Si $a \leq b$ y $b \leq c$ entonces $a \leq c$.
- xiii) Para cualesquiera $a, b \in \mathbb{Z}$, $a \leq b$ o $b \leq a$.

xiv) $a \leq b$ implica que $a + c \leq b + c$ para todo $c \in \mathbb{Z}$.

xv) $a \leq b$ y $c \geq 0$ implica que $a \cdot c \leq b \cdot c$.

xvi) $a \leq b$ y $c \leq 0$ implica $b \cdot c \leq a \cdot c$.

xvii) $a \cdot c \leq b \cdot c$ y $c > 0$ entonces $a \leq b$.

xviii) $a \cdot c \leq b \cdot c$ y $c < 0$ implica que $b \leq a$.

Por último, tenemos definida la aplicación valor absoluto $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$ como sigue:

$$|a| = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

y que satisface las propiedades:

xix) $|a| = 0$ si, y sólo si, $a = 0$.

xx) $|a \cdot b| = |a| \cdot |b|$.

xxi) $|a + b| \leq |a| + |b|$.

xxii) $|a| \leq b$ si, y sólo si, $-b \leq a \leq b$.

2.2.1. Representación en complementos

Hemos estudiado en una sección anterior cómo representar los números naturales. Esto, junto con el signo, nos permite representar todos los números enteros.

Para representar un número entero no nulo a , elegimos una base $b \geq 2$, representamos $|a|$ (que es un número natural) en base b , y le añadimos el signo $-$ al principio si el número a es menor que cero.

Sin embargo, aquí vamos a estudiar otra forma para representar los números enteros, que nos va a permitir reducir las sumas y las restas a un mismo algoritmo: el que tenemos para sumar.

Para esto, al igual que con los números naturales, elegimos un número $b \geq 2$, y vamos a trabajar en base b .

Tenemos dos posibilidades de representar los números: En complemento a $b - 1$ y en complemento a b .

Antes de explicar el caso general, vamos a analizar algunos ejemplos tomando la base que nos resulta más conocida: la base $b = 10$.

Tomemos por ejemplo $x = 75$ e $y = 28$. Su diferencia $x - y$ vale 47.

Para realizar la resta podemos proceder como sigue:

- ▮ Representamos en complemento a 9 el número y . La representación en complemento a 9 consiste en sustituir cada cifra por lo que le falta para llegar a 9. Nos quedaría entonces 71.
- ▮ Sumamos los dos números: $75 + 71 = 146$.
- ▮ Le sumamos 1 y despreciamos el acarreo (el 1 de la derecha), y nos queda 47, que es exactamente la diferencia entre x e y .

A la vista de esto, podríamos utilizar, para representar el número -28 la notación 71, a la que llamaremos *representación en complemento a 9*.

Entonces, para realizar la suma $x + (-y)$ (o lo que es lo mismo, $x - y$), lo que tenemos que hacer es sumarle a x , la representación en complemento a 9 de $-y$. El resultado final hay que interpretarlo (sumarle uno, y eliminar el acarreo)

Si analizamos lo que hemos hecho veremos porqué nos da el resultado esperado:

- Representación en complemento a 9 de $-y$. Tenemos el número $99 - y$.
- Le sumamos este número a x . $x + 99 - y = 99 + (x - y)$.
- Sumamos 1. $100 + (x - y)$
- Despreciamos el 1 de la derecha, es decir, restamos 100. $x - y$.

Supongamos ahora que queremos restar $y = 38$ a $x = 357$. Representamos $-y$ en complemento a 9 (lo que nos da 61), se lo sumamos a 357, y le sumamos 1, y nos queda $357 + 61 + 1 = 419$. La diferencia entre x e y vale 319. Para obtener este resultado a partir del cálculo que hemos hecho en complemento a 9 tendríamos que restar 1 en la cifra más significativa.

Pero esto ya parece un poco rebuscado. Además, esa regla no valdría si quisiéramos hacer $6372 - 57$ (compruébese).

Para solventar este problema, se puede tomar la opción de escribir los dos números con igual cantidad de cifras significativas. En tal caso, tendríamos $x = 357$, $y = 038$. La representación en complemento a 9 de $-y$ es 961. Ahora realizamos la suma: $357 + 961 + 1 = 1319$. El resultado de la resta $x - y$ es 319, como puede deducirse del resultado obtenido.

Tal y como hemos hecho hasta ahora, hay una ambigüedad. Supongamos que tenemos el número representado como 239. ¿Se corresponde con la representación del número *doscientos treinta y nueve*, o se corresponde con la representación del número *menos setecientos sesenta*?

Para solucionar esto, lo que hacemos es añadir una cifra a la izquierda, que será *cero* para el caso de los números positivos, y *nueve* para los negativos.

Entonces, la representación en complemento a nueve del número $x = 528$ será 0528, mientras que la de $y = -528$ será 9471.

Sabemos que si tenemos un número (positivo) y le añadimos ceros a la izquierda, el número que representamos es el mismo ($356 = 0356 = 000356$). De la misma forma, si tenemos un número negativo representado en complemento a nueve, y le añadimos *nueves* a la izquierda, el número representado es el mismo. Así, el número -356 podemos representarlo en complemento a nueve como 9643, como 99643, o como 99999643.

Y ahora, supongamos que tenemos los números $x = 37846$ e $y = 967$, y queremos calcular $x - y$.

- ▮ Representamos x en complemento a 9: 037846.
- ▮ Representamos $-y$ en complemento a 9 con el mismo número de cifras que x : 999032.
- ▮ Realizamos la suma $037846 + 999032 + 1$. El resultado es 1036879.
- ▮ Eliminamos el *uno* de la izquierda: 036879.

Luego $x - y = 36879$.

¿Que ocurre si queremos restar dos números de forma que el primero sea menor que el segundo? En tal caso, la diferencia es negativa, luego el resultado que nos dé deberemos interpretarlo como tal.

Por ejemplo, vamos a tomar $x = 45$ e $y = 123$, y vamos a calcular $x - y$.

- ▮ Representamos $-y$ en complemento a 9: 9876.
- ▮ Representamos x en complemento a 9: 0045.
- ▮ Sumamos ambos números $0045 + 9876 = 9921$.
- ▮ Puesto que el resultado empieza por *nueve* se trata de un número negativo. Su representación en complemento a 9 es 9921. Por tanto, el resultado es -78 (ya que la representación en complemento a 9 de -78 es 9921).

Al igual que antes, lo que hemos hecho ha sido sumar a x el número $9999 - y$. El resultado es $9999 + (x - y) = 9999 - (y - x)$, que es la representación en complemento a nueve de $-(y - x) = x - y$.

Vamos a ver cómo sumar y restar números que están representados en complementos. Lo primero que hemos de hacer es decidir si un número queremos sumarlo o restarlo.

Si sumamos 75 y 71, ¿queremos sumar esos dos números o lo que estamos haciendo es restar 28 a 75? Puesto que restar un número es lo mismo que sumar su opuesto, lo que necesitamos es una forma de representar los números negativos.

Para representar un número positivo en complemento a nueve, utilizamos su representación decimal y añadimos al menos un cero a la izquierda. Para los negativos, su representación en complemento a nueve consiste en sustituir en la representación de su número opuesto cada cifra por lo que le falta a ésta para llegar a 9.

Así, el 25 será representado como 025, o como 0025, etc., mientras que el -25 será representado como 974, 9974, etc.

En tal caso, si x es un número entero, y su representación en complemento a 9 es $b_n b_{n-1} \cdots b_1 b_0$, las cifras de la representación en complemento a 9 de $-x$ son $9 - b_n, 9 - b_{n-1}, \dots, 9 - b_1, 9 - b_0$.

Ejemplo 2.2.1. *Vamos a hacer algunas sumas y restas con números representados en complemento a 9.*

1. $x = 45, y = 26$.

- Para sumarlos, utilizamos la representación en complemento a 9 de ambos, que es 045 y 026, y la sumamos:

$$\begin{array}{r} 0 \ 4 \ 5 \\ + \ 0 \ 2 \ 6 \\ \hline 0 \ 7 \ 1 \end{array}$$

que es la representación en complemento a 9 de la suma.

- Para efectuar $x - y$ utilizamos la representación en complemento a 9 de x y $-y$, que son respectivamente 045 y 973, y volvemos a sumar (y sumamos también 1)

$$\begin{array}{r} 0 \ 4 \ 5 \\ + \ 9 \ 7 \ 3 \\ \hline 1 \ 0 \ 1 \ 9 \end{array}$$

y eliminando el 1 del acarreo, el resultado es la representación en complemento a 9 de la diferencia.

- Para efectuar $y - x$ utilizamos la representación en complemento a 9 de y y $-x$, que son respectivamente 026 y 954, y sumamos:

$$\begin{array}{r} 0 \ 2 \ 6 \\ + \ 9 \ 5 \ 4 \\ \hline 9 \ 8 \ 0 \end{array}$$

que es la representación en complemento a 9 de -19 , es decir, $y - x$.

- Para efectuar $-x - y$ utilizamos las representaciones en complemento a 9 de $-x$ y $-y$, que son respectivamente 954 y 973. Las sumamos y le añadimos 1.

$$\begin{array}{r} 9 \ 5 \ 4 \\ + \ 9 \ 7 \ 3 \\ \hline 1 \ 9 \ 2 \ 8 \end{array}$$

y eliminando el 1 de la derecha obtenemos la representación en complemento a 9 de $-71 = -x - y$.

2. Tomamos ahora $x = 58$ e $y = 62$. La representación en complemento a 9 de x es 058, la de $-x$ es 941, la de y es 062 y la de $-y$ es 937. Realizamos los cálculos de $x + y$, $x - y$, $-x + y = y - x$ y $-x - y$. Para ello, tomamos la representación en complemento a 9 de los cuatro números.

$x + y$	$x - y$	$-x + y$	$-x - y$
$\begin{array}{r} 0 \ 5 \ 8 \\ + \ 0 \ 6 \ 2 \\ \hline 1 \ 2 \ 0 \end{array}$	$\begin{array}{r} 0 \ 5 \ 8 \\ + \ 9 \ 3 \ 7 \\ \hline 9 \ 9 \ 5 \end{array}$	$\begin{array}{r} 0 \ 6 \ 2 \\ + \ 9 \ 4 \ 1 \\ \hline 1 \ 0 \ 0 \ 4 \end{array}$	$\begin{array}{r} 9 \ 4 \ 1 \\ + \ 9 \ 3 \ 7 \\ \hline 1 \ 8 \ 7 \ 9 \end{array}$

El primer resultado no es la representación en complemento a nueve de ningún número, pues no empieza por 0 ni por 9. Si eliminamos el uno de la izquierda, podríamos pensar que el resultado de la suma es 20. En realidad, el resultado de la suma es 120.

El segundo resultado es la representación en complemento a nueve de -4 , que es el resultado de la operación $x - y$.

El tercer resultado, después de eliminar el uno de la izquierda es 4, que es lo que resulta de la operación $-x + y$.

Por último, el cuarto resultado no es la representación en complemento a nueve de ningún número, ni aún eliminando el uno de la izquierda.

Una opción para eliminar estos problemas es escribir los números con una cifra más, añadiendo un cero a la izquierda en el caso de los números positivos, y un 9 en el caso de los negativos.

$x + y$	$x - y$	$-x + y$	$-x - y$
$\begin{array}{r} 0 \ 0 \ 5 \ 8 \\ + \ 0 \ 0 \ 6 \ 2 \\ \hline 0 \ 1 \ 2 \ 0 \end{array}$	$\begin{array}{r} 0 \ 0 \ 5 \ 8 \\ + \ 9 \ 9 \ 3 \ 7 \\ \hline 9 \ 9 \ 9 \ 5 \end{array}$	$\begin{array}{r} 0 \ 0 \ 6 \ 2 \\ + \ 9 \ 9 \ 4 \ 1 \\ \hline 1 \ 0 \ 0 \ 0 \ 4 \end{array}$	$\begin{array}{r} 9 \ 9 \ 4 \ 1 \\ + \ 9 \ 9 \ 3 \ 7 \\ \hline 1 \ 9 \ 8 \ 7 \ 9 \end{array}$

Y ahora vemos que:

- 1 Como resultado de la primera operación tenemos 0120. Este es un número positivo, pues empieza por cero. Se trata, como sabemos del número $120 = x + y$.
- 1 Como resultado de la segunda operación tenemos 9995. Al empezar por nueve se trata de un número negativo. En concreto, el número -4 , que es el resultado de $x - y$.
- 1 Al resultado de la tercera operación le quitamos el uno de la izquierda, y nos queda 0004. Al empezar por cero, se trata de un número positivo. Concretamente el 4.
- 1 También al resultado de la cuarta operación le quitamos el uno de la izquierda. Nos queda entonces 9879. Al empezar por nueve se trata de un número negativo, concretamente de -120 .

Pasamos ya a dar la definición de la representación de un número en complemento a $b - 1$.

Definición 34. Sea $b \geq 2$, x un número entero y $(a_n a_{n-1} \cdots a_1 a_0)_b$ la representación de un número en base b . Diremos que $c_n \cdots c_1 c_0$ es una representación de x en complemento a $b - 1$ si:

- 1 $c_n = 0$ y $x = (c_n c_{n-1} \cdots c_1 c_0)_b$ cuando $x \geq 0$.
- 1 $c_n = b - 1$ y $x = (c_n c_{n-1} \cdots c_1 c_0)_b - (b^n - 1)$ cuando $x < 0$.

Observaciones:

1. En la representación en complemento a $b - 1$ de un número x , la cifra de la izquierda nos indica el signo del número x .
2. Si $c_n c_{n-1} \cdots c_1 c_0$ es una representación en complemento a $b - 1$ de x , entonces también $c_n c_n c_{n-1} \cdots c_1 c_0$ lo es. Es decir, podemos añadir a la izquierda tantas veces como queramos la última cifra de la representación.

Esto es claro en el caso de que x sea un número positivo, pues lo único que hacemos es añadir un cero a la izquierda.

Supongamos que $x < 0$, y que $c_n c_{n-1} \cdots c_1 c_0$ es una representación en complemento a $b - 1$ del número x . En tal caso, $c_n = b - 1$ y

$$x = (c_n c_{n-1} \cdots c_1 c_0)_b - (b^n - 1) = c_n b^{n-1} + c_{n-1} b^{n-2} + \cdots + c_1 b + c_0 - b^n + 1$$

Sea y el número cuya representación en complemento a $b - 1$ es $c_n c_n c_{n-1} \cdots c_1 c_0$. Entonces y es negativo, pues la última cifra es $c_n = b - 1$. Por tanto,

$$\begin{aligned}
y &= (c_n c_{n-1} \cdots c_1 c_0) - (b^{n+1} - 1) = \\
&= c_n b^n + c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\
&= (b-1)b^n + c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\
&= b^{n+1} - b^n + c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\
&= -b^n + c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 + 1 = x
\end{aligned}$$

3. La representación de 0, de acuerdo con la definición es $00 \cdots 0$. Sin embargo, también podría usarse como representación de cero $aa \cdots a$, donde $a = b - 1$.
4. Con $n + 1$ dígitos podemos representar todos los números comprendidos entre $-(b^n - 1)$ y $b^n - 1$.

Sea x un número cuya representación en complemento a $b - 1$ es $c_n c_{n-1} \cdots c_1 c_0$. Tenemos dos posibilidades:

- ▮ $c_n = 0$. Entonces $x \geq 0$ y $x = (c_{n-1} \cdots c_1 c_0)_b = c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 < b^n$. Es decir, $0 \leq x \leq b^n - 1$.
- ▮ $c_n = b - 1$. Entonces $x \leq 0$ y $x = c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 - b^n + 1$, de donde $x + b^n - 1 = c_{n-1} b^{n-1} + \cdots + c_1 b + c_0$, luego $0 \leq x + b^n - 1 \leq b^n - 1$. Por tanto, $-(b^n - 1) = -b^n + 1 \leq x \leq 0$.

Juntando los dos casos, tenemos que $-(b^n - 1) \leq x \leq b^n - 1$.

5. Si $c_n c_{n-1} \cdots c_1 c_0$ es la representación en complemento a $b - 1$ de x , entonces la representación en complemento a $b - 1$ de $-x$ es $d_n d_{n-1} \cdots d_1 d_0$, donde $d_i = (b - 1) - c_i$. Esto vale, tanto si x es positivo como si x es negativo.

Sea x un número cuya representación en complemento a $b - 1$ es $c_n c_{n-1} \cdots c_1 c_0$. Sea y el número cuya representación en complemento a $b - 1$ es $d_n d_{n-1} \cdots d_1 d_0$, donde $d_i = (b - 1) - c_i$. Entonces:

- ▮ Si $x \geq 0$ se tiene que $c_n = 0$, luego $d_n = b - 1$, lo que nos dice que y es negativo. Ahora:

$$\begin{aligned}
y &= d_{n-1} b^{n-1} + d_{n-2} b^{n-2} + \cdots + d_1 b + d_0 - b^n + 1 = \\
&= ((b-1) - c_{n-1}) b^{n-1} + ((b-1) - c_{n-2}) b^{n-2} + \cdots + ((b-1) - c_1) b + ((b-1) - c_0) - b^n + 1 = \\
&= (b-1)(b^{n-1} + b^{n-2} + \cdots + b + 1) - (c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0) - b^n + 1 = \\
&= b^n + b^{n-1} + \cdots + b - (b^{n-1} + b^{n-2} + \cdots + b + 1) - x - b^n + 1 = \\
&= b^n - 1 - x - b^n + 1 = -x
\end{aligned}$$

- ▮ Si $x \leq 0$ se procede de forma análoga. Ahora $c_n = b - 1$, luego $d_n = 0$, lo que nos dice que $y \geq 0$.

$$\begin{aligned}
x &= c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 - b^n + 1 = \\
&= ((b-1) - d_{n-1}) b^{n-1} + ((b-1) - d_{n-2}) b^{n-2} + \cdots + ((b-1) - d_1) b + ((b-1) - d_0) - b^n + 1 = \\
&= (b-1)(b^{n-1} + b^{n-2} + \cdots + b + 1) - (d_{n-1} b^{n-1} + d_{n-2} b^{n-2} + \cdots + d_1 b + d_0) - b^n + 1 = \\
&= b^n + b^{n-1} + \cdots + b - (b^{n-1} + b^{n-2} + \cdots + b + 1) - y - b^n + 1 = \\
&= b^n - 1 - y - b^n + 1 = -y
\end{aligned}$$

Luego en cualquiera de los casos, $y = -x$.

Ejemplo 2.2.2.

1. Vamos a ver algunos ejemplos de representaciones en complemento a nueve.

Sea x el número cuya representación en complemento a nueve es 0583. Entonces x es positivo, pues la cifra de la izquierda es 0. Y se tiene que $x = 5 \cdot 10^2 + 8 \cdot 10 + 3 = 583$.

Ahora sustituimos cada cifra por lo que le falta para llegar a 9 (es decir, sustituimos cada cifra c_i por $9 - c_i$). En este caso, tenemos el número 9416. Esta es la representación en complemento a nueve de un número negativo, pues empieza por 9. Este número, de acuerdo con la definición 34 es $4 \cdot 10^2 + 1 \cdot 10 + 6 - 10^3 + 1 = -583$.

Sea z el número cuya representación en complemento a nueve es 999416. Entonces, según la definición 34 se tiene que

$$z = 9 \cdot 10^4 + 9 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10 + 6 - 10^5 + 1 = 99416 - 99999 = -583.$$

También podríamos haber procedido de la siguiente forma: el número z es negativo, pues empieza por 9. Representamos $-z$, que se consigue cambiando cada cifra por lo que le falta para llegar a 9. Entonces, la representación de $-z$ es 000583. Luego $-z = 583$, de donde $z = -583$.

4734 no es la representación en complemento a nueve de ningún número, pues su primera cifra no es ni cero ni nueve.

2. Un caso especialmente interesante y sencillo es cuando trabajamos en complemento a uno. En tal caso, una sucesión de ceros y unos es siempre la representación en complemento a uno de algún número, que será positivo si la primera cifra es cero, y negativo si la primera cifra es uno. Una sucesión de n dígitos se corresponde con un número entre $-(2^{n-1} - 1)$ y $2^{n-1} - 1$.

Vamos a representar en complemento a uno, todos los números entre $-7 = -(2^3 - 1)$ y $7 = 2^3 - 1$ con cuatro dígitos. Pondremos juntas la representación de un número y su opuesto.

$1 \mapsto 0001$	$2 \mapsto 0010$	$3 \mapsto 0011$	$4 \mapsto 0100$
$-1 \mapsto 1110$	$-2 \mapsto 1101$	$-3 \mapsto 1100$	$-4 \mapsto 1011$
$5 \mapsto 0101$	$6 \mapsto 0110$	$7 \mapsto 0111$	$0 \mapsto 0000$
$-5 \mapsto 1010$	$-6 \mapsto 1001$	$-7 \mapsto 1000$	

Nos queda la secuencia 1111, que como ya hemos dicho antes, se correspondería con el número 0 (o con el -0).

Vemos como para obtener la representación en complemento a uno de $-x$ a partir de la de x basta intercambiar los ceros por unos y viceversa.

Para sumar dos números x e y , positivos o negativos, podemos tomar la representación en complemento a $b - 1$ de ambos números y sumarlos, teniendo en cuenta:

1. Ambos números deben tener el mismo número de cifras. Caso de no ser así, podemos repetir la cifra de la izquierda tantas veces como nos convenga.
2. Las dos últimas cifras deben ser iguales. Esto no siempre es necesario, pero de esta forma nos evitamos algunos errores.
3. Si sumamos dos números negativos, o si sumamos un positivo con un negativo de menor valor absoluto, al resultado final hay que sumarle uno, y eliminar el uno que nos aparece a la izquierda (del acarreo).

Con estas consideraciones, el resultado de la suma es la representación en complemento a $b - 1$ de $x + y$.

Ejemplo 2.2.3.

Vamos a realizar algunas sumas trabajando con la representación en complemento a 1 de los números.

1. Vamos a sumar $x = 45$ e $y = 89$. Para buscar su representación en complemento a 1, los pasamos a binario, y luego completamos las cifras. Omitiremos los subíndices, para no complicar la notación.

Decimal	Binario	Complemento a 1	Completando cifras
45	101101	0101101	000101101
89	1011001	01011001	001011001

Y ahora sumamos:

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & 1 & 1 & 1 & 1 & & 1 & \\
 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1
 \end{array} \\
 + \begin{array}{cccccccc}
 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1
 \end{array} \\
 \hline
 \begin{array}{cccccccc}
 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0
 \end{array}
 \end{array}$$

Y la representación en complemento a uno de $x+y$ es 010000110, que se corresponde con el número 134.

2. $x = 54$, $y = -87$.

Procedemos igual que antes, pero para obtener la representación en complemento a uno de y , pasamos por la representación binaria de $|y|$.

Decimal (N)	Binario ($ N $)	Complemento a 1 ($ N $)	Complemento a 1 (N)	Completando cifras
54	110110	0110110	0110110	000110110
-87	1010111	01010111	10101000	110101000

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & & 1 & & & & & \\
 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0
 \end{array} \\
 + \begin{array}{cccccccc}
 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0
 \end{array} \\
 \hline
 \begin{array}{cccccccc}
 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0
 \end{array}
 \end{array}$$

Y esta es la representación en complemento a uno de $x+y$. Para obtener su representación decimal, podemos:

- Calculamos su opuesto, cuya representación en complemento a uno es 000100001 que es el número $2^5 + 1 = 33$. Por tanto, $x + y = -33$.
- Obtenerlo directamente de la representación. $x + y = 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1 - 2^8 + 1 = -33$.

3. $x = 61$, $y = -34$.

Decimal (N)	Binario ($ N $)	Complemento a 1 ($ N $)	Complemento a 1 (N)	Completando cifras
61	111101	0111101	0111101	00111101
-34	100010	0100010	1011101	11011101

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & 1 & 1 & 1 & 1 & 1 & & 1 & \\
 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1
 \end{array} \\
 + \begin{array}{cccccccc}
 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
 \end{array} \\
 \hline
 \begin{array}{cccccccc}
 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0
 \end{array}
 \end{array}$$

Y como nos ha salido una cifra más, la quitamos y sumamos uno. El resultado es entonces 00011011, que es la representación en complemento a uno de 27.

4. $x = -39$, $y = -52$.

Decimal (N)	Binario ($ N $)	Complemento a 1 ($ N $)	Complemento a 1 (N)	Completando cifras
-39	100111	0100111	1011000	11011000
-52	110100	0110100	1001011	11001011

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & 1 & & 1 & 1 & & & \\
 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0
 \end{array} \\
 + \begin{array}{cccccccc}
 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1
 \end{array} \\
 \hline
 \begin{array}{cccccccc}
 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
 \end{array}
 \end{array}$$

Y al igual que antes, como nos ha salido una cifra más, la quitamos y sumamos uno. El resultado de la suma $x + y$ es entonces 10100100, que es la representación en complemento a uno del número $2^5 + 2^2 - 2^7 + 1 = -91$.

Para evitar los problemas que pueden surgir de la necesidad de sumar o no 1 según los casos, se suele emplear más que la representación en complemento a $b - 1$ la representación en complemento a b . En este caso, lo que se hace es "incluir" el uno en la representación del número.

Para obtener la representación en complemento a b de un número x :

- si el número es positivo, la representación en complemento a b de un número es la misma que la representación en complemento a $b - 1$.
- si x es negativo, se toma la representación en complemento a $b - 1$ de x y se le suma 1.

Dicho de otra forma, si $c_n c_{n-1} \cdots c_1 c_0$ es la representación en complemento a b de x , entonces $c_n = 0$ ó $c_n = b - 1$, y:

- ▮ si $c_n = 0$, $x = (c_n c_{n-1} \cdots c_1 c_0)_b$.
- ▮ si $c_n = b - 1$, $x = (c_n c_{n-1} \cdots c_1 c_0)_b - b^n$.

Definición 35. Sea $b \geq 2$, x un número entero y $(a_n a_{n-1} \cdots a_1 a_0)_b$ la representación de un número en base b . Diremos que $c_n \cdots c_1 c_0$ es una representación de x en complemento a b si:

- ▮ $c_n = 0$ y $x = (c_n c_{n-1} \cdots c_1 c_0)_b$ cuando $x \geq 0$.
- ▮ $c_n = b - 1$ y $x = (c_n c_{n-1} \cdots c_1 c_0)_b - b^n$ cuando $x < 0$.

Observaciones:

1. El decir representación en complemento a *un número* podría ser ambiguo. Por ejemplo, si hablamos de representación en complemento a 2, podríamos estar utilizando la base $b = 3$ y usar la representación en complemento a $b - 1$, o utilizar la base $b = 2$ y usar la representación en complemento a b . Puesto que nosotros usaremos la base $b = 2$ ó $b = 10$, no tendremos este problema.
2. En la representación en complemento a b de un número x , la cifra de la izquierda nos indica el signo del número x .
3. Si $c_n c_{n-1} \cdots c_1 c_0$ es una representación en complemento a b de x , entonces también $c_n c_n c_{n-1} \cdots c_1 c_0$ lo es. Es decir, podemos añadir a la izquierda tantas veces como queramos la última cifra de la representación.
4. Con $n + 1$ dígitos podemos representar todos los números comprendidos entre $-b^n$ y $b^n - 1$.
5. Si $c_n c_{n-1} \cdots c_1 c_0$ es la representación en complemento a b de x , para obtener la representación en complemento a b de $-x$ sustituimos cada cifra c_i por $d_i = (b - 1) - c_i$ y sumamos 1 al resultado, como si estuviéramos trabajando con un número en base b . Esto vale para todos los números comprendidos entre $-b^n$ y $b^n - 1$ salvo para $x = 0$ (la representación de 0 y -0 es, obviamente la misma) y para $x = -b^n$ (pues $-x = b^n$, que no puede representarse con $n + 1$ cifras).

Ejemplo 2.2.4.

1. Vamos a obtener la representación en complemento a 10 de varios números enteros.
 - ▮ $x = 37$. Una representación en complemento a 10 es 037. También podemos tomar 0037, 00037, etc.
 - ▮ Sea $x = -83$. El número $-x$, representado en complemento a 10 es 083, luego la representación de x es $916 + 1 = 917$.
 - ▮ Sea $x = 1000$ (es decir, b^3). Entonces su representación en complemento a 10 es 01000. Necesitamos 5 cifras para representar b^3 .
 - ▮ Sea ahora $x = -1000$. Los pasos para representarlo serían:
 Representamos $-x = 1000$. Esto nos da 01000.
 Sustituimos cada cifra por su complemento a 9. Nos da 98999.
 Sumamos 1. Y nos da 99000

Entonces, una representación de -1000 sería 99000. Pero también lo es 9000 (pues 9000 y 99000 representan el mismo número, ya que se ha añadido un 9 a la izquierda en la representación de un número negativo). Por tanto, vemos como -10^3 podemos representarlo con 4 cifras.

2. Sea ahora x un número entero cuya representación en complemento a 10 es 9673. Entonces, para representar $-x$ sustituimos cada cifra por su complemento a 9 (0326) y sumamos uno (0327). De aquí sacamos que $x = -327$.

También podemos verlo, según la definición 35, calculando $x = 673 - 10^3 = 673 - 1000 = -327$.

3. La representación de -3200 sería 96800 (de $96799 + 1$).
4. En el caso de complemento a 2, se procede de forma análoga.

El objetivo de la introducción de las representaciones en complementos viene dada por el siguiente teorema.

Teorema 2.2.1. Sea $b \geq 2$ y sean x e y dos números enteros, tales que sus representaciones en complemento a b son $c_n c_{n-1} \cdots c_1 c_0$ y $d_n d_{n-1} \cdots d_1 d_0$ y además $c_n = c_{n-1}$ y $d_n = d_{n-1}$.

Sea $s_{n+1} s_n s_{n-1} \cdots s_1 s_0$ el resultado de realizar la suma en base b de los números $c_n c_{n-1} \cdots c_1 c_0$ y $d_n d_{n-1} \cdots d_1 d_0$.

Entonces, $s_n s_{n-1} \cdots s_1 s_0$ es una representación en complemento a b del número $x + y$.

Ejemplo 2.2.5.

Vamos a realizar sumas de números representados en complemento a dos.

En primer lugar, $x = 38$ e $y = -21$. La representación en complemento a 2 de 38 es 0100110 y la de 21 es 010101, por lo que la de -21 es $101010 + 1 = 101011$. Sumamos ambos números

$$\begin{array}{r}
 \begin{array}{ccccccc}
 & 1 & 1 & & 1 & 1 & 1 \\
 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
 + & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
 \hline
 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1
 \end{array}
 \end{array}$$

Como nos ha salido una cifra más, la eliminamos, y el resultado es 00010001, que es una representación del número 17.

Sean ahora $x = -25$ e $y = -43$. La representación en complemento a dos de 25 es 011001, y la de 43 es 0101011, luego la representación de x es $100110 + 1 = 100111$ y la de y es $1010100 + 1 = 1010101$. Sumamos:

$$\begin{array}{r}
 \begin{array}{ccccccc}
 & 1 & & & 1 & 1 & 1 \\
 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
 + & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
 \hline
 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0
 \end{array}
 \end{array}$$

Y al igual que antes, suprimimos la cifra que nos ha salido, y tenemos el resultado, que es 10111100, que es la representación en complemento a 2 de -68 (bastaría cambiar los unos por ceros, los ceros por unos, y sumar uno).

Si aquí no hubiéramos añadido una cifra a la izquierda, habríamos sumado los números 1100111 y 1010101, cuyo resultado es 10111100. Después de eliminar el uno del acarreo, habríamos obtenido 0111100, que es la representación en complemento a dos de 60.

Para sumar los números cuya representación en complemento a dos es 011011 y 1011, lo que hemos de hacer es completar con cifras a la izquierda hasta que los dos tengan el mismo número de cifras, y las dos últimas sean iguales. Entonces tendríamos los números 0011011 y 1111011, que al sumarlos nos da 10010110. Como nos ha salido una cifra de más (hemos pasado de 7 a 8 cifras), eliminamos la de la izquierda, y lo que nos quede es el resultado de la suma en complemento a 2. En este caso es $0010110 = 010110$ que es el número 22.

Representa los dos números iniciales en decimal y efectúa la operación.

2.3. Divisibilidad

Veámos en la sección anterior que dados dos números naturales a, b con $b \neq 0$ podíamos dividir a entre b obteniendo un cociente y un resto (teorema 2.1.2). Ahora vamos a extender ese teorema al caso de los números enteros.

Teorema 2.3.1. *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos números enteros c, r tales que $a = bc + r$ y $0 \leq r < |b|$.*

A los números c y r que nos da el teorema se les llama respectivamente cociente y resto de la división de a entre b .

Para demostrar el teorema, lo que hay que hacer es distinguir casos según sean a y b mayores o menores que 0 y referirse al caso conocido ($a, b \in \mathbb{N}$). El siguiente ejemplo puede ayudar a analizar los diferentes casos.

Ejemplo 2.3.1.

$$\begin{aligned} a = 86, b = 15. & \quad 86 = 15 \cdot 5 + 11 \\ a = 86, b = -15. & \quad 86 = (-15) \cdot (-5) + 11 \\ a = -86, b = 15. & \quad -86 = 15 \cdot (-6) + 4 \\ a = -86, b = -15. & \quad -86 = (-15) \cdot (-6) + 4 \end{aligned}$$

Ahora podemos tomar la definición 32 y extenderla a los números enteros.

Definición 36. *Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Definimos los números $a \operatorname{div} b$ y $a \operatorname{mód} b$ como el cociente y el resto de la división de a entre b respectivamente.*

Dicho de otra forma, $a \operatorname{div} b$ y $a \operatorname{mód} b$ son los únicos números que cumplen las dos condiciones siguientes:

- $a = b \cdot (a \operatorname{div} b) + (a \operatorname{mód} b)$.
- $0 \leq a \operatorname{mód} b < |b|$.

Tal y como lo hemos definido aquí, el resto de una división es siempre un número positivo (o cero) y menor que el divisor (en valor absoluto). En algunas ocasiones, es conveniente tomar el resto de la división entra a y b como el número de menor valor absoluto r tal que $a - r$ es múltiplo de b . Esto daría lugar a restos negativos. Por ejemplo, al dividir 14 entre 5, nosotros tomamos como resto 4, que viene de la igualdad $14 = 5 \cdot 2 + 4$. Pero también podríamos apoyarnos en $14 = 5 \cdot 3 + (-1)$, en cuyo caso el resto sería -1 . En este caso, los posibles restos al dividir por 5 serían $-2, -1, 0, 1$ y 2 .

Pasamos ya a definir la relación de divisibilidad en \mathbb{Z} .

Definición 37. *Dados $a, b \in \mathbb{Z}$, se dice que a divide a b , o que b es un múltiplo de a , y escribiremos $a|b$, si existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$.*

Hagamos un repaso de las propiedades más importantes, y cuya demostración es casi inmediata.

Propiedades:

1. Para cualquier $a \in \mathbb{Z}$ se verifica que $1|a$ y $a|0$.
2. Para cualquier $a \in \mathbb{Z}$, $a|a$.
3. Si $a|b$ y $b|a$ entonces $a = \pm b$.
4. Si $a|b$ y $b|c$ entonces $a|c$.
5. Si $a|b$ y $a|c$ entonces $a|(b + c)$.
6. Si $a|b$ entonces $a|bc$ para cualquier $c \in \mathbb{Z}$.
7. $a|b$ si, y sólo si, $b \operatorname{mód} a = 0$ (esto vale siempre que $a \neq 0$, pues en caso contrario no tiene sentido hablar de $b \operatorname{mód} a$).

Según la definición que acabamos de dar, si $a|b$ existe un elemento c tal que $b = a \cdot c$. Este elemento, salvo cuando $a = 0$ está totalmente determinado por a y b . Lo denotaremos entonces como $\frac{b}{a}$.

Aunque estamos usando una notación de fracción, en este contexto $\frac{b}{a}$ sólo tiene sentido cuando $a|b$, en cuyo caso es un elemento de \mathbb{Z} .

Definición 38. Sean a, b dos números enteros. Se dice que d es un máximo común divisor de a y b si se satisfacen las dos siguientes condiciones:

- ▮ $d|a$ y $d|b$.
- ▮ Si $c|a$ y $c|b$ entonces $c|d$.

Nótese que la primera condición nos dice que d debe ser un divisor común de a y b . La segunda condición nos dice que de todos los divisores comunes es el "más grande", donde por ser el más grande queremos significar que es múltiplo de todos.

Dicho de otra forma, un máximo común divisor de dos números a y b es un divisor común de a y b que es múltiplo de todos los divisores comunes de a y b .

En tal caso se tiene que si d es un máximo común divisor de a y b , también lo es $-d$, de ahí que hayamos hablado de **un** máximo común divisor y no de **el** máximo común divisor. Además, si d es un máximo común divisor, no hay otro máximo común divisor aparte de $-d$. Dados $a, b \in \mathbb{Z}$, denotaremos por $\text{mcd}(a, b)$ al único máximo común divisor de a y b que pertenece a \mathbb{N} .

Ejemplo 2.3.2. Sean $a = 16$ y $b = 30$. Los divisores de a son $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$, y los divisores de 30 son $\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$.

La intersección de ambos conjuntos, es decir, el conjunto de los divisores comunes, es el conjunto $\{1, 2, -1, -2\}$

De esos cuatro, tanto el 2 como el -2 son múltiplos del resto, por tanto, tanto 2 como -2 encajarían en la definición que hemos dado de máximo común divisor.

No obstante, diremos que el máximo común divisor de 16 y 30 es 2 (es decir, elegiremos el positivo, aunque podríamos haber hecho lo mismo con el negativo).

De la misma forma que se ha definido el máximo común divisor de dos números podría hacerse para tres o más.

La definición del mínimo común múltiplo es semejante a la que acabamos de dar.

Definición 39. Sean a, b dos números enteros. Se dice que m es un mínimo común múltiplo de a y b si se satisfacen las dos siguientes condiciones:

- ▮ $a|m$ y $b|m$.
- ▮ Si $a|n$ y $b|n$ entonces $m|n$.

Las mismas observaciones que se han hecho para el máximo común divisor valen ahora para el mínimo común múltiplo.

Algunas propiedades referentes al máximo común divisor son:

Propiedades:

1. $\text{mcd}(a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, b) = \text{mcd}(-a, -b) = \text{mcd}(|a|, |b|)$.
2. $\text{mcd}(a, 0) = |a|$ y $\text{mcd}(a, 1) = 1$
3. Si $a|b$ entonces $\text{mcd}(a, b) = |a|$.
4. $\text{mcd}(a, \text{mcd}(b, c)) = \text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, b, c)$.
5. $\text{mcd}(ac, bc) = \text{mcd}(a, b) \cdot |c|$
6. Si $d|a$ y $d|b$ entonces $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{mcd}(a, b)}{|d|}$.

Se deja como ejercicio enunciar las propiedades correspondientes al mínimo común múltiplo.

Hasta ahora hemos hablado del máximo común divisor, y hemos dado algunas propiedades. Estas propiedades podrían, en un principio, no tener sentido, pues el máximo común divisor de dos números podría no existir. Veremos a continuación que el máximo común divisor de dos números enteros existe, y daremos un método para calcularlo. Comenzamos con el siguiente lema.

Lema 2.3.1. Sean $a, b \in \mathbb{Z}$. Entonces, para cualquier $q \in \mathbb{Z}$ se tiene que $\text{mcd}(a, b) = \text{mcd}(b, a - bq)$.

Demostración: Sea $d \in \mathbb{Z}$, y supongamos que $d|a$ y $d|b$. Entonces $d|bq$, luego $d|b$ y $d|(a - bq)$.

Por otra parte si suponemos que $d|b$ y $d|(a - bq)$ deducimos que $d|bq$, luego $d|(a - bq + bq)$ y $d|a$, es decir, $d|a$ y $d|b$. ■

Nótese que lo que hemos demostrado es que para cualquier $q \in \mathbb{Z}$, los divisores comunes de a y b , y los divisores comunes de b y $a - bq$ son los mismos, luego el máximo común divisor de ambas parejas de números será el mismo (si existe).

Ejemplo 2.3.3. Sean $a = 78$ y $b = 30$. El conjunto de los divisores positivos de a es el conjunto $\{1, 2, 3, 6, 13, 26, 39, 78\}$, mientras que $\{1, 2, 3, 5, 6, 10, 15, 30\}$ es el conjunto de los divisores positivos de b .

Por tanto, el conjunto de los divisores comunes de a y b es $\{1, -1, 2, -2, 3, -3, 6, -6\}$ y de ahí deducimos que $\text{mcd}(a, b) = 6$.

Vamos a tomar diferentes valores de q , y a calcular los divisores de b y $a - bq$.

▮ $q = 1$. En tal caso, $a - bq = 48$. Los divisores positivos de 48 son 1, 2, 3, 4, 6, 8, 12, 16, 24, 48. Los divisores comunes de b y $a - bq$ son los elementos del conjunto $\{1, -1, 2, -2, 3, -3, 6, -6\}$, exactamente igual que para a y b . Por tanto, $\text{mcd}(a, b) = \text{mcd}(b, a - b)$.

▮ $q = 2$. Ahora $a - bq = 18$, que tiene como divisores positivos a 1, 2, 3, 6, 9, 18. El conjunto de los divisores comunes entre b y $a - bq$ vuelve a ser $\{1, -1, 2, -2, 3, -3, 6, -6\}$.

▮ $q = 3$. Ahora $a - bq = -12$, y el conjunto de los divisores positivos de -12 es $\{1, 2, 3, 4, 6, 12\}$. Al igual que antes, los divisores comunes de b y $a - bq$ son 1, -1 , 2, -2 , 3, -3 , 6, -6 .

▮ $q = -2$. Entonces $a - bq = 138$. El conjunto de sus divisores positivos es $\{1, 2, 3, 6, 23, 46, 69, 138\}$ y los comunes vuelven a ser los mismos.

▮ El caso $q = 0$ es un caso trivial.

Vemos como, independientemente del número q que tomemos, los divisores comunes de a y b son los mismos que los divisores comunes de b y $a - bq$.

El papel de a y b es simétrico, luego los divisores comunes de a y b son los divisores comunes de a y $b - aq$.

Consecuencia inmediata del lema anterior es el siguiente corolario.

Corolario 2.3.1. Sean $a, b \in \mathbb{Z}$, con $a \neq 0$. Entonces $\text{mcd}(a, b) = \text{mcd}(b, a \bmod b)$.

Basta tomar como valor de q el cociente de a entre b .

Este resultado es en el que nos vamos a apoyar para dar el siguiente algoritmo.

Algoritmo de Euclides para el cálculo del máximo común divisor.

Sean $a, b \in \mathbb{Z}$. Puesto que $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$, podemos suponer que $a, b \in \mathbb{N}$. Comenzamos a efectuar divisiones:

$$\begin{aligned} a &= b \cdot c_1 + r_1 \\ b &= r_1 \cdot c_2 + r_2 \\ r_1 &= r_2 \cdot c_3 + r_3 \\ &\dots\dots\dots \\ r_{i-2} &= r_{i-1} \cdot c_i + r_i \\ &\dots\dots\dots \end{aligned}$$

Obtenemos una sucesión de números naturales r_1, r_2, \dots , que es decreciente. Deberá por tanto existir $k \in \mathbb{N}$ tal que $r_k \neq 0$ y $r_{k+1} = 0$. Tenemos entonces:

$$\begin{aligned} a &= b \cdot c_1 + r_1 \\ b &= r_1 \cdot c_2 + r_2 \\ r_1 &= r_2 \cdot c_3 + r_3 \\ &\dots\dots\dots \\ r_{i-2} &= r_{i-1} \cdot c_i + r_i \\ &\dots\dots\dots \\ r_{k-2} &= r_{k-1} \cdot c_k + r_k \\ r_{k-1} &= r_k \cdot c_{k+1} + 0 \end{aligned}$$

Por el corolario anterior tenemos que los divisores comunes de a y b coinciden con los divisores comunes de r_i y r_{i+1} , para cualquier $i \leq k$. Como el máximo común divisor de r_k y 0 existe, y vale r_k , deducimos que $\text{mcd}(a, b) = r_k$ (el último resto no nulo).

Con esto es posible diseñar un algoritmo que calcule el máximo común divisor de dos números enteros a y b .

Algoritmo EUCLIDES(a, b)

Entrada: $a, b \in \mathbb{Z}$

Salida: $d = \text{mcd}(a, b)$

$(a, b) := (|a|, |b|)$

Mientras $b \neq 0$

$(a, b) := (b, a \bmod b)$

Devuelve a

Ejemplo 2.3.4. *Vamos a calcular el máximo común divisor de 48 y 30. Al ser a y b positivos, no es necesario ejecutar la primera sentencia.*

$(a, b) = (48, 30)$	Al ser $b = 30 \neq 0$ hacemos
$(a, b) = (30, 18)$	Como $b = 18 \neq 0$ hacemos
$(a, b) = (18, 12)$	Dado que $b = 12 \neq 0$ hacemos
$(a, b) = (12, 6)$	Puesto que $b = 6 \neq 0$ hacemos
$(a, b) = (6, 0)$	Y ahora $b = 0$

Por tanto, el máximo común divisor de 48 y 30 es $a = 6$.

Teorema 2.3.2. [Identidad de Bezout] Sean $a, b \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$. Entonces existen $u, v \in \mathbb{Z}$ tales que $d = au + bv$.

Demostración: Llamemos momentáneamente r_{-1} y r_0 a los números a y b (por este orden). Sabemos que el cálculo del máximo común divisor de $a = r_{-1}$ y $b = r_0$ lo podemos realizar mediante una serie de divisiones

$$\begin{aligned} r_{-1} &= r_0 \cdot c_1 + r_1 \\ r_0 &= r_1 \cdot c_2 + r_2 \\ r_1 &= r_2 \cdot c_3 + r_3 \\ &\dots\dots\dots \\ r_{i-2} &= r_{i-1} \cdot c_i + r_i \\ &\dots\dots\dots \\ r_{k-2} &= r_{k-1} \cdot c_k + r_k \\ r_{k-1} &= r_k \cdot c_{k+1} + 0 \end{aligned}$$

Vamos a demostrar que para cada i tal que $-1 \leq i \leq k$ existen $u_i, v_i \in \mathbb{Z}$ tales que $r_i = a \cdot u_i + b \cdot v_i$.

Claramente, para $i = -1$ e $i = 0$ el resultado es cierto, pues

$r_{-1} = a \cdot 1 + b \cdot 0$ y $r_0 = a \cdot 0 + b \cdot 1$ (es decir, $(u_{-1}, v_{-1}) = (1, 0)$ y $(u_0, v_0) = (0, 1)$).

Supongamos que para todo $j < i$ existen u_j y v_j tales que $r_j = a \cdot u_j + b \cdot v_j$. Entonces:

$$\begin{aligned}
r_i &= r_{i-2} - r_{i-1} \cdot c_i \\
&= (a \cdot u_{i-2} + b \cdot v_{i-2}) - (a \cdot u_{i-1} + b \cdot v_{i-1}) \cdot c_i \\
&= a \cdot (u_{i-2} - u_{i-1} \cdot c_i) + b \cdot (v_{i-2} - v_{i-1} \cdot c_i)
\end{aligned}$$

Basta entonces tomar $u_i = u_{i-2} - u_{i-1} \cdot c_i$ y $v_i = v_{i-2} - v_{i-1} \cdot c_i$ ■

Esta demostración además nos dice cómo encontrar los coeficientes u y v .

Ejemplo 2.3.5. Vamos a hallar el máximo común divisor de 1005 y 450, y a expresarlo en función de estos dos números.

Realizamos las divisiones, y a la vez vamos expresando los restos en función de 1005 y 450.

$$1005 = 450 \cdot 2 + 105 \quad 105 = 1005 \cdot 1 + 450 \cdot (-2)$$

$$\begin{aligned}
450 &= 105 \cdot 4 + 30 & 30 &= 450 - 105 \cdot 4 = 450 - (1005 \cdot 1 + 450 \cdot (-2)) \cdot 4 \\
& & &= 1005 \cdot (-4) + 450 \cdot (1 - (-2) \cdot 4) \\
& & &= 1005 \cdot (-4) + 450 \cdot 9
\end{aligned}$$

$$\begin{aligned}
105 &= 30 \cdot 3 + 15 & 15 &= 105 - 30 \cdot 3 = (1005 \cdot 1 + 450 \cdot (-2)) - (1005 \cdot (-4) + 450 \cdot 9) \cdot 3 \\
& & &= 1005 \cdot (1 - (-4) \cdot 3) + 450 \cdot (-2 - 9 \cdot 3) \\
& & &= 1005 \cdot (13) + 450 \cdot (-29)
\end{aligned}$$

$$30 = 15 \cdot 2 + 0$$

De donde deducimos que $\text{mcd}(1005, 450) = 15$, y $15 = 1005 \cdot 13 + 450 \cdot (-29)$.

Estos datos pueden ser ordenados como sigue:

r	c	u	v
1005		1	0
450		0	1
105	2	1	-2
30	4	-4	9
15	3	13	-29
0			

$$1005 = 1 \cdot 1005 + 0 \cdot 450$$

$$450 = 0 \cdot 1005 + 1 \cdot 450$$

$$105 = 1 \cdot 1005 - 2 \cdot 450$$

$$30 = -4 \cdot 1005 + 9 \cdot 450$$

$$15 = 13 \cdot 1005 - 29 \cdot 450$$

A la derecha de la tabla hemos puesto las comprobaciones de que el primer elemento de cada fila es igual a a por el tercero más b por el cuarto, es decir, $r_i = a \cdot u_i + b \cdot v_i$.

El siguiente algoritmo recoge todos estos cálculos. Este algoritmo calcula, dados $a, b \in \mathbb{Z}$ su máximo común divisor d y los coeficientes u y v tales que $d = au + bv$.

Puesto que en el cálculo de u_i es necesario tener presente los valores de u_{i-1} y u_{i-2} necesitaremos de una variable x donde almacenar u_{i-2} . De la misma forma necesitaremos una variable y para almacenar v_{i-2} .

Algoritmo BEZOUT(a, b)

Entrada: $a, b \in \mathbb{Z}$

Salida: (d, u, v) : $d = \text{mcd}(a, b)$; $d = au + bv$

Si $b = 0$

Devuelve $(a, 1, 0)$;

Fin

$r_{-1} := a, r_0 := b$.

$u_{-1} := 1, u_0 := 0$.

$v_{-1} := 0, v_0 := 1$.

$i := 1$.

$r_1 := r_{-1} \bmod r_0$

Mientras $r_i \neq 0$

$c_i := r_{i-2} \div r_{i-1}$.

$u_i := u_{i-2} - u_{i-1} \cdot c_i$.

$v_i := v_{i-2} - v_{i-1} \cdot c_i$.

$i := i + 1.$
 $r_i := r_{i-2} \bmod r_{i-1}.$
 Devuelve $(r_{i-1}, u_{i-1}, v_{i-1}).$
 Fin

En el caso de que a ó b valieran cero, en el resultado final podría devolver un valor para d negativo. Bastaría entonces multiplicar d , u y v por -1 .

Ejemplo 2.3.6.

Vamos a tomar $a = 69$ y $b = 15$, y vamos a calcular su máximo común divisor, d , así como los coeficientes u y v que verifican que $d = 69 \cdot u + 15 \cdot v$.

Puesto que $b \neq 0$, inicializamos las variables: $r_{-1} = 69$, $r_0 = 15$, $u_{-1} = 1$, $u_0 = 0$, $v_{-1} = 0$ y $v_0 = 1$. Una vez hecho esto, $r_1 = 69 \bmod 15 = 9$.

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9			

Puesto que $r_i = r_1 = 9 \neq 0$, volvemos a entrar en el bucle. Esto nos da $c_1 = 69 \text{ div } 15 = 4$, $u_1 = 1 - 4 \cdot 0 = 1$, $v_1 = 0 - 4 \cdot 1 = -4$, $i = 2$, $r_2 = 15 \bmod 9 = 6$.

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6			

También ahora $r_i \neq 0$. Entonces $c_2 = 15 \text{ div } 9 = 1$, $u_2 = 0 - 1 \cdot 1 = -1$, $v_2 = 1 - 1 \cdot (-4) = 5$, i_3 , $r_3 = 9 \bmod 6 = 3$.

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6	1	-1	5
3	3			

$r_3 \neq 0$. Por tanto, actualizamos: $c_3 = 9 \text{ div } 6 = 1$, $u_3 = 1 - 1 \cdot (-1) = 2$, $v_3 = -4 - 1 \cdot 5 = -9$, $i = 4$, $r_4 = 0$.

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6	1	-1	5
3	3	1	2	-9
4	0			

Y ahora, como $r_i = 0$ terminamos. El resultado es que $d = 3$, $u = 2$ y $v = -9$.

Notemos como $3 = 69 \cdot 2 + 15 \cdot (-9)$.

Una consecuencia inmediata del teorema 2.3.2 es el siguiente corolario:

Corolario 2.3.2. Sean $a, b \in \mathbb{Z}$. Entonces existen números enteros u y v tales que $1 = a \cdot u + b \cdot v$ si, y sólo si, $\text{mcd}(a, b) = 1$.

Demostración: El teorema de Bezout nos dice que si $\text{mcd}(a, b) = 1$ entonces existen $u, v \in \mathbb{Z}$ satisfaciendo la igualdad deseada.

Recíprocamente, supongamos que tenemos $u, v \in \mathbb{Z}$ tales que $1 = au + bv$. Sea ahora d un divisor común de a y b . Entonces:

$$\left. \begin{array}{l} d|a \implies d|au \\ d|b \implies d|bv \end{array} \right\} \implies d|(au + bv) \implies d|1$$

De donde se deduce que $\text{mcd}(a, b) = 1$. ■

Dos números cuyo máximo común divisor vale 1 se dice que son primos relativos.

Corolario 2.3.3. Sean $a, m, n \in \mathbb{Z}$. Entonces $\text{mcd}(a, mn) = 1$ si, y sólo si, $\text{mcd}(a, m) = \text{mcd}(a, n) = 1$.

Demostración: Si $\text{mcd}(a, mn) = 1$ existen $u, v \in \mathbb{Z}$ tales que $1 = au + mnv$. Agrupando de manera apropiada tenemos que $1 = au + m(nv)$ y $1 = au + n(mv)$, luego $\text{mcd}(a, m) = \text{mcd}(a, n) = 1$.

Recíprocamente, supongamos que $\text{mcd}(a, m) = \text{mcd}(a, n) = 1$. Existen entonces $u_m, v_m, u_n, v_n \in \mathbb{Z}$ tales que $1 = au_m + mv_m$ y $1 = au_n + nv_n$, luego

$$1 = au_m + mv_m(au_n + nv_n) = a(u_m + mv_mu_n) + mn(v_mv_n)$$

lo que nos dice que $\text{mcd}(a, mn) = 1$. ■

Corolario 2.3.4. Sean $a, b, c \in \mathbb{Z}$. Si $a|(bc)$ y $\text{mcd}(a, b) = 1$ entonces $a|c$.

Demostración: Sabemos, por el corolario anterior que existen $u, v \in \mathbb{Z}$ tal que $au + bv = 1$, y existe x tal que $bc = ax$. Entonces:

$$c = c(au + bv) = cau + cbv = cau + axv = a(cu + xv)$$

de donde se deduce que c es múltiplo de a . ■

Utilizaremos este corolario para demostrar que dos números cualesquiera tienen también mínimo común múltiplo.

Lema 2.3.2. Sean $a, b \in \mathbb{Z}$. Si $\text{mcd}(a, b) = 1$ entonces ab es un mínimo común múltiplo de a y b .

Demostración: Claramente ab es múltiplo común de a y b .

Supongamos ahora que $a|n$ y $b|n$. Entonces $n = bc$, luego $a|bc$, y por el corolario anterior $a|c$, lo que implica que $c = ax$. Por tanto, $n = abx$, de donde se deduce que $ab|n$. ■

Proposición 2.3.1. Sean $a, b \in \mathbb{N}$ y $d = \text{mcd}(a, b)$. Entonces $\text{mcm}(a, b) = \frac{ab}{d}$.

Demostración: Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$. Entonces $\text{mcd}(a', b') = 1$, luego $\text{mcm}(a', b') = a'b'$.

Se tiene entonces que $\text{mcm}(a'd, b'd) = a'b'd$, o lo que es lo mismo

$$\text{mcm}(a, b) = \frac{ab}{d}$$

■

Nótese que $\text{mcd}(a, b) \cdot \text{mcm}(a, b) = ab$.

Ejemplo 2.3.7. Sabemos que $\text{mcd}(4, 6) = 2$. Por tanto, $\text{mcm}(4, 6) = \frac{24}{2} = 12$.

Sabemos que $\text{mcd}(1005, 450) = 15$. Entonces $\text{mcm}(1005, 450) = 1005 \cdot 30 = 30150$.

2.4. Números primos. Teorema fundamental de la aritmética

En esta sección vamos a demostrar el conocido teorema fundamental de la aritmética, que afirma que todo número natural mayor o igual que 2 se expresa de forma única como producto de números primos.

Comenzamos definiendo los números irreducibles.

Definición 40. Sea p un número entero distinto de 0, 1 y -1 . Se dice que p es irreducible si sus únicos divisores son ± 1 y $\pm p$.

Ejemplo 2.4.1. Son irreducibles 2, 3, 5.

No es irreducible 4, pues 2 es un divisor suyo.

Claramente, si p es irreducible también lo es $-p$.

Veamos a continuación una caracterización de los números irreducibles.

Proposición 2.4.1. Sea p un número entero distinto de 0, 1 y -1 . Entonces:

$$p \text{ es irreducible} \iff (p|ab \implies p|a \text{ ó } p|b)$$

Antes de hacer la demostración veamos algún ejemplo.

Ejemplo 2.4.2. Sabemos que si el producto de dos números es par, al menos uno de ellos debe ser par. Puesto que ser par es equivalente a ser múltiplo de 2, lo que estamos diciendo es que

$$2|ab \text{ implica } 2|a \text{ ó } 2|b$$

lo que de acuerdo con la proposición es decir que 2 es irreducible (algo que ya sabíamos).

De la misma forma, si el producto de dos números es múltiplo de 3, uno de los factores debe serlo.

Por otra parte, si tomamos $a = 8$ y $b = 15$, entonces $ab = 120$, que es múltiplo de 6, mientras que ni a ni b lo son, luego la implicación

$$6|ab \text{ implica } 6|a \text{ ó } 6|b$$

es falsa, pues hemos encontrado a y b para los que se da la primera parte de la implicación, pero no la segunda. De acuerdo con la proposición esto nos diría que 6 no es irreducible.

Vamos ya a la demostración.

Demostración: Hagamos en primer lugar la implicación hacia la izquierda. Es decir, suponemos que la implicación $p|ab \implies p|a \text{ ó } p|b$ es cierta y queremos probar que p es irreducible.

Sea d un divisor de p . Esto implica que $p = dx$, de donde $p|dx$. Pueden ocurrir dos cosas: que p divida a d o que p divida a x .

Si $p|d$, como $d|p$ entonces $d = \pm p$.

Si $p|x$ entonces $x = py$ para algún $y \in \mathbb{Z}$. Se tiene que $p = dx = dyp$, luego $dy = 1$ y por tanto $d = \pm 1$.

Por tanto, si d es un divisor de p entonces $d = \pm p$ o $d = \pm 1$, lo que dice que p es irreducible.

Veamos ahora la implicación hacia la derecha.

Supongamos que p es irreducible y que tenemos dos números enteros a y b tales que $p|ab$ (es decir, $ab = px$).

Puede ocurrir que p divida a a (en cuyo caso no hay nada que probar), o que p no divida a a . Veamos entonces que $p|b$.

Es claro que $\text{mcd}(p, a) = 1$. El corolario 2.3.4 nos dice que $p|b$, como queríamos.

■

Como es bien conocido, a los números irreducibles los llamaremos también números primos.

Como ejercicio, demuestra que si p es un número primo y tenemos $a_1, a_2, \dots, a_n \in \mathbb{Z}$ tales que $p|(a_1 a_2 \dots a_n)$ entonces existe $i \in \{1, 2, \dots, n\}$ tal que $p|a_i$.

Estamos ya en condiciones de dar el teorema fundamental de la aritmética.

Teorema 2.4.1 (Teorema fundamental de la aritmética). Sea $a \in \mathbb{N}$, $a \geq 2$. Entonces, a es primo, o a se expresa de forma única (salvo el orden y el signo) como producto de números primos.

Observación:

Sea $a = 6$. Sabemos que a lo podemos poner como producto de primos de la forma $6 = 2 \cdot 3$. Pero también podemos ponerlo como $6 = (-2) \cdot (-3)$. Aunque estrictamente hablando estas dos factorizaciones son distintas, ambas podrían considerarse iguales. De ahí que digamos que la factorización es única salvo el signo. De la misma forma, las factorizaciones $6 = 2 \cdot 3 = 3 \cdot 2$ son iguales salvo el orden.

Demostración: Para demostrar esto, veremos en primer lugar que todo número mayor que 1 tiene un divisor primo.

Sea a un número natural mayor o igual que 2. Escribamos $b_0 = a$. Si b_0 es primo, entonces b_0 es un divisor primo de a . En caso de que no sea primo, tendrá un divisor positivo que no es ni 1 ni b_0 . Sea este b_1 . Es claro que $b_1 < b_0$.

Si b_1 es primo, ya tenemos un divisor primo de a . De no serlo, tendrá un divisor, b_2 que será menor que b_1 (y mayor que 1).

Obtenemos de esta forma una sucesión estrictamente decreciente b_0, b_1, \dots . Como la sucesión no puede ser infinita, tendrá un término b_k que será un número primo. Este número es un divisor primo de a .

Sea ahora a un número mayor que 1. Si a es primo, ya tenemos a como producto de números primos (habría sólo un factor). Si no es primo, tendrá un divisor primo. Sea este p_1 . Entonces $a = p_1 \cdot c_1$. Claramente $c_1 < a$.

Si c_1 es primo, ya tenemos a como producto de primos. Si no lo es, tomamos un divisor primo de c_1 (llamémoslo p_2 , y tendremos que $c_1 = p_2 \cdot c_2$, luego $a = p_1 \cdot p_2 \cdot c_2$).

Tenemos de esta forma una sucesión c_1, c_2, \dots estrictamente decreciente. Por tanto, algún término c_k será el último, lo que significará que c_k es primo. En tal caso, tendremos escrito a como producto de números primos.

Veamos ahora la unicidad.

Sea a un número natural, y supongamos que tenemos dos factorizaciones de a como producto de primos: $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$.

Entonces se tiene que $p_1 | (q_1 \dots q_s)$, y por ser p_1 primo, debe existir algún i tal que $p_1 | q_i$. Reordenamos los primos q_1, \dots, q_s para que el primo al que divide p_1 sea el primero (es decir, $p_1 | q_1$). Como q_1 es primo, entonces $p_1 = q_1$. Tenemos entonces que $\frac{a}{p_1} = p_2 \dots p_r = q_2 \dots q_s$.

Repetimos ahora el mismo razonamiento, y llegamos (después de reordenar los primos) a que $p_2 = q_2$.

Continuando con este proceso, tendremos que $p_3 = q_3$, etc. Y así, los primos que aparecen en la primera factorización de a son los mismo que aparecen en la segunda. ■

Ejemplo 2.4.3. Sea $a = 6120$. Claramente no es primo. Un divisor primo suyo es 2. Dividimos por 2, y tenemos que $a = 2 \cdot 3060$.

Como 3060 no es primo, buscamos un divisor primo suyo, que podría volver a ser 2. Tenemos $3060 = 2 \cdot 1530$.

Este número vuelve a no ser primo y a tener a 2 como divisor primo suyo. $1530 = 2 \cdot 765$.

Este número no es primo, pero ahora 2 no es divisor suyo. Sí lo es 3. Entonces $765 = 3 \cdot 255$.

El 3 vuelve a ser un divisor primo. Dividimos por 3: $255 = 3 \cdot 85$.

El 5 es un divisor primo de 85. El cociente sale 17. Y este número ya es primo.

Si vemos la sucesión c_i que hemos ido obteniendo ha sido $c_1 = 3060$, $c_2 = 1530$, $c_3 = 765$, $c_4 = 255$, $c_5 = 85$, $c_6 = 17$. Es una sucesión estrictamente decreciente y que acaba en un número primo.

La factorización de 6120 como producto de primos es $6120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 17 = 2^3 \cdot 3^2 \cdot 5 \cdot 17$.

La factorización de un número como producto de primos permite de forma fácil determinar los divisores de un número. Así, si $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ y $b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$ entonces $b|a$ si, y sólo si, $f_i \leq e_i$.

De esta forma es fácil comprobar que el conjunto

$$D(a) = \{p_1^{f_1} p_2^{f_2} \dots p_r^{f_r} : 0 \leq f_i \leq e_i\}$$

es el conjunto de todos los divisores positivos de a .

El cardinal de dicho conjunto es $(e_1 + 1) \cdot (e_2 + 1) \dots (e_r + 1) = \prod_{k=1}^r (e_k + 1)$.

Ejemplo 2.4.4. Sea $a = 180$. Entonces $a = 2^2 3^2 5$. Los divisores de a son entonces:

$$\begin{array}{llllll} 2^0 3^0 5^0 = 1 & 2^0 3^0 5^1 = 5 & 2^0 3^1 5^0 = 3 & 2^0 3^1 5^1 = 15 & 2^0 3^2 5^0 = 9 & 2^0 3^2 5^1 = 45 \\ 2^1 3^0 5^0 = 2 & 2^1 3^0 5^1 = 10 & 2^1 3^1 5^0 = 6 & 2^1 3^1 5^1 = 30 & 2^1 3^2 5^0 = 18 & 2^1 3^2 5^1 = 90 \\ 2^2 3^0 5^0 = 4 & 2^2 3^0 5^1 = 20 & 2^2 3^1 5^0 = 12 & 2^2 3^1 5^1 = 60 & 2^2 3^2 5^0 = 36 & 2^2 3^2 5^1 = 180 \end{array}$$

Es decir,

$$D(180) = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180\}$$

que vemos que tiene 18 elementos (notemos que $18 = (2 + 1) \cdot (2 + 1) \cdot (1 + 1)$).

También podemos calcular el máximo común divisor y el mínimo común múltiplo de dos números.

Proposición 2.4.2. Sean $a, b \in \mathbb{N}^*$. Supongamos que $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y $b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ son las factorizaciones de a y b como producto de irreducibles. Entonces:

$$\text{mcd}(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_r^{\min\{e_r, f_r\}}$$

$$\text{mcm}(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}$$

Esta proposición puede generalizarse fácilmente para el cálculo del máximo común divisor y/o el mínimo común múltiplo de 3 ó más números.

Ejemplo 2.4.5. En el ejemplo 2.3.5 calculamos el máximo común divisor de 1005 y 450, mientras que en el ejemplo 2.3.7 calculamos su mínimo común múltiplo. Vamos a hacerlo ahora siguiendo la proposición que acabamos de ver.

Para eso, factorizamos ambos números:

$1005 = 3 \cdot 5 \cdot 67$; $450 = 2 \cdot 3^2 \cdot 5^2$. Por tanto, de acuerdo con esta proposición tenemos que:

$\text{mcd}(1005, 450) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 67^0 = 15$, y $\text{mcm}(1005, 450) = 2^1 \cdot 3^2 \cdot 5^2 \cdot 67^1 = 30150$

Que coinciden con los valores obtenidos previamente.

Sean $a = 350$ y $b = 1155$. Entonces se tiene que $a = 2 \cdot 5^2 \cdot 7$ y $b = 3 \cdot 5 \cdot 7 \cdot 11$. Por tanto

$$\text{mcd}(350, 1155) = 2^0 3^0 5^1 7^1 11^0 = 5 \cdot 7 = 35 \quad \text{mcm}(350, 1155) = 2^1 3^1 5^2 7^1 11^1 = 11550$$

2.5. Clases residuales módulo m

En el capítulo anterior construimos, para cada número natural $m \geq 1$ el conjunto \mathbb{Z}_m . Este conjunto fue definido como el conjunto cociente de \mathbb{Z} por la relación de equivalencia

$$a \equiv b \pmod{m} \text{ si } m \mid (b - a)$$

Vimos que el conjunto \mathbb{Z}_m tiene exactamente m elementos. De hecho, podemos escribir $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$ donde $[i]_m \in \mathbb{Z}_m$ representa a la clase de equivalencia del elemento i , que está formada por todos los números enteros que al dividir por m dan resto i .

Con la función *módulo* (ver definición 36) tenemos que $a \equiv b \pmod{m}$ si, y sólo si, $a \bmod m = b \bmod m$.

Vamos a continuación a estudiar la estructura algebraica de estos conjuntos. Para ello necesitamos el siguiente lema:

Lema 2.5.1. Sean $a, b, c, d \in \mathbb{Z}$ y $m \geq 2$. Entonces:

$$1. \quad \left. \begin{array}{l} a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array} \right\} \implies a + b \equiv c + d \pmod{m}$$

$$2. \quad \left. \begin{array}{l} a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array} \right\} \implies ab \equiv cd \pmod{m}$$

Demostración:

$$1. \quad \left. \begin{array}{l} a \equiv c \pmod{m} \implies m \mid (c - a) \\ b \equiv d \pmod{m} \implies m \mid (d - b) \end{array} \right\} \implies m \mid (c - a + d - b) \implies m \mid (c + d - (a + b))$$

$$\implies a + b \equiv c + d \pmod{m}$$

$$2. \quad \left. \begin{array}{l} a \equiv c \pmod{m} \implies m \mid (c - a) \implies m \mid (c - a)b \\ b \equiv d \pmod{m} \implies m \mid (d - b) \implies m \mid c(d - b) \end{array} \right\} \implies m \mid [c(d - b) + (c - a)b]$$

$$\implies m \mid (cd - cb + cb - ab)$$

$$\implies m \mid (cd - ab)$$

$$\implies ab \equiv cd \pmod{m}$$

■

Nótese que a partir de este lema se tiene que si $[a]_m = [c]_m$, y $[b]_m = [d]_m$ entonces $[a + b]_m = [c + d]_m$ y $[ab]_m = [cd]_m$. Esto da pie a la siguiente definición.

Definición 41. Sean $a, b \in \mathbb{Z}$ y $m \geq 2$. Se definen en \mathbb{Z}_m las operaciones:

$$[a]_m + [b]_m = [a + b]_m \quad [a]_m [b]_m = [ab]_m$$

El lema anterior nos asegura que estas definiciones no dependen de los representantes que se elijan para $[a]_m$ y $[b]_m$.

Ejemplo 2.5.1. Sea $m = 9$. En \mathbb{Z}_m se tiene que $[5] + [7] = [12] = [3]$. Si en lugar de $[5]$ tomamos $[23]$, y en lugar de $[7]$ tomamos $[34]$ se tiene que $[23] + [34] = [57] = [3]$ (pues $57 - 3 = 9 \cdot 6$). Vemos como la elección del representante del primer sumando (5 ó 23) así como la elección del representante del segundo sumando (7 ó 34) no influye en el resultado final de la suma.

De la misma forma, $[5] \cdot [7] = [35] = [8]$, mientras que $[23] \cdot [34] = [782] = [8]$.

Supongamos que tenemos dos números enteros a, b tales que $b|a$, $m \geq 2$ y quisiéramos definir $\frac{[a]_m}{[b]_m}$ como sigue:

$$\frac{[a]_m}{[b]_m} = \left[\frac{a}{b} \right]_m$$

Tomamos $m = 8$, $a = 6$ y $b = 2$. Entonces tendríamos que $\frac{[6]}{[2]} = [3]$. Ahora bien, $[6]_8 = [14]_8$, mientras que $\frac{[14]}{[2]} = [7]$, y claramente $[3] \neq [7]$ en \mathbb{Z}_8 . Es decir, el resultado final depende de los representantes elegidos. Esta operación, por tanto, no está bien definida.

Nota: A partir de ahora, dado $a \in \mathbb{Z}$, denotaremos por a al elemento $[a]_m \in \mathbb{Z}_m$. En cada momento deberá quedar claro si a representa un número entero o un elemento de \mathbb{Z}_m . Así, se tiene que

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$$

e igualdades como $4 + 6 = 3$, $5 = 1$ ó $9 = 0$ tendrán sentido en un contexto apropiado (la primera igualdad es válida en \mathbb{Z}_7 , la segunda en \mathbb{Z}_4 o \mathbb{Z}_2 y la tercera en \mathbb{Z}_9 o \mathbb{Z}_3).

Proposición 2.5.1. Sea $m \geq 2$. Las operaciones suma y producto verifican las siguientes propiedades:

- i) $a + (b + c) = (a + b) + c$
- ii) $a + b = b + a$
- iii) $a + 0 = a$
- iv) Para cada $a \in \mathbb{Z}_m$ existe $b \in \mathbb{Z}_m$ tal que $a + b = 0$.
- v) $a(bc) = (ab)c$
- vi) $ab = ba$
- vii) $a1 = a$
- viii) $a(b + c) = ab + ac$

Estas propiedades nos dicen que \mathbb{Z}_m es un anillo conmutativo.

Nótese que en general, el producto no tiene la propiedad cancelativa. Así, por ejemplo, en \mathbb{Z}_8 se verifica que $6 \cdot 1 = 6 \cdot 5$, y sin embargo $1 \neq 5$.

Ejemplo 2.5.2. Veamos las tablas de suma y producto en \mathbb{Z}_5 y \mathbb{Z}_6 .

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

\cdot	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definición 42. Sea $a \in \mathbb{Z}_m$. Se dice que a es una unidad si existe $b \in \mathbb{Z}_m$ tal que $a \cdot b = 1$.

Ejemplo 2.5.3.

1. Para cualquier $m \geq 2$, 1 es una unidad en \mathbb{Z}_m .
2. El elemento $3 \in \mathbb{Z}_5$ es una unidad (pues $3 \cdot 2 = 1$), mientras que $3 \in \mathbb{Z}_6$ no es unidad. Puede verse como en \mathbb{Z}_5 todo elemento distinto de cero es una unidad.

Si $a \in \mathbb{Z}_m$ es una unidad, entonces se puede simplificar por a (es decir, $ab = ac \implies b = c$). Razona el por qué.

Como consecuencia de lo anterior, si a es una unidad en \mathbb{Z}_m , hay un único elemento en \mathbb{Z}_m que al multiplicarlo por él da 1. Este elemento se llama *inverso de a* y se representa por a^{-1} .

Denotaremos por $\mathcal{U}(\mathbb{Z}_m)$ al conjunto de todas las unidades de \mathbb{Z}_m .

Si $a, b \in \mathcal{U}(\mathbb{Z}_m)$, entonces $ab \in \mathcal{U}(\mathbb{Z}_m)$, y $(ab)^{-1} = a^{-1}b^{-1}$.

Todo lo dicho sobre unidades se puede hacer extensivo a cualquier anillo conmutativo.

Ejemplo 2.5.4.

$$\mathcal{U}(\mathbb{Z}_2) = \{1\} \quad \mathcal{U}(\mathbb{Z}_3) = \{1, 2\} \quad \mathcal{U}(\mathbb{Z}_5) = \{1, 2, 3, 4\} \quad \mathcal{U}(\mathbb{Z}_6) = \{1, 5\} \quad \mathcal{U}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$$

$$\mathcal{U}(\mathbb{Z}) = \{1, -1\} \quad \mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$$

Los inversos de las unidades en \mathbb{Z}_9 son $1^{-1} = 1$, $2^{-1} = 5$, $4^{-1} = 7$, $5^{-1} = 2$, $7^{-1} = 4$ y $8^{-1} = 8$. Observa como, por ejemplo, $4 \cdot 5 = 20 = 2$ es unidad, y $4^{-1} \cdot 5^{-1} = 7 \cdot 2 = 14 = 5 = 2^{-1}$.

Hemos calculado las unidades en algunos anillos \mathbb{Z}_m . Hasta ahora, la única forma de ver si un elemento en \mathbb{Z}_m es unidad es multiplicarlo por los elementos de \mathbb{Z}_m y comprobar si el algún caso de 1 ó no.

A la luz de los ejemplos anteriores vamos a comprobar la siguiente proposición.

Proposición 2.5.2. Sea $a \in \mathbb{Z}_n$. Entonces a es unidad si, y sólo si, $\text{mcd}(a, n) = 1$.

En el enunciado de esta proposición, las dos primeras veces que hablamos del elemento a hacemos referencia a un elemento de \mathbb{Z}_n , mientras que la tercera consideramos a como un número entero. En la demostración que vamos a hacer de esta proposición, también llamaremos de la misma forma a los elementos de \mathbb{Z}_n y a los elementos de \mathbb{Z} . El contexto nos dirá cual de los dos casos se está considerando.

Nótese que decir $a = b$ (en \mathbb{Z}_n) es lo mismo que decir $b = a + kn$ (en \mathbb{Z}) para algún $k \in \mathbb{Z}$.

Puesto que $\text{mcd}(a, n) = \text{mcd}(a + kn, n)$, no influye para nada el representante que tomemos para comprobar, de acuerdo con la proposición precedente, si $a \in \mathbb{Z}_n$ es una unidad o no en \mathbb{Z}_n .

Demostración: Comprobemos la condición necesaria. Supongamos entonces que a es unidad en \mathbb{Z}_n . Sea $u = a^{-1}$, lo que nos dice que $au = 1$ (en \mathbb{Z}_n), o que $1 = au + kn$ (en \mathbb{Z}). El corolario 2.3.2 nos dice ahora que $\text{mcd}(a, n) = 1$.

En cuanto a la condición suficiente, suponemos que $\text{mcd}(a, n) = 1$. Existen entonces $u, v \in \mathbb{Z}$ tales que $au + nv = 1$. Vista esta igualdad en \mathbb{Z}_n se tiene que $au = 1$ (pues $n = 0$), lo que nos dice que a es una unidad con inverso u . ■

La proposición anterior, junto con su demostración, aparte de darnos una condición necesaria y suficiente para que un elemento de \mathbb{Z}_n tenga inverso, nos da una forma de calcularlo. Basta hacer uso de la identidad de Bezout.

Ejemplo 2.5.5. De la igualdad $1 = 11 \cdot 11 + 15 \cdot (-8)$ deducimos que 11 es una unidad en \mathbb{Z}_{15} y que su inverso es 11.

También deducimos que 15 es una unidad en \mathbb{Z}_{11} , y que su inverso es -8 . Puesto que $15 = 4$ y $-8 = 3$ tenemos que 4 es unidad y $4^{-1} = 3$.

Basándonos en el algoritmo BEZOUT, vamos a dar un algoritmo que nos dirá si un elemento $a \in \mathbb{Z}_n$ tiene o no inverso, y en caso afirmativo, lo calculará.

Algoritmo INVERSO(a, n)

Entrada: $a, n \in \mathbb{Z}, n \geq 2, a \neq 0$.

Salida: $u : a \cdot u = 1$ en \mathbb{Z}_n (si tal elemento existe).

$r_{-1} := a, r_0 := b$.

$v_{-1} := 0, v_0 := 1$.

$i := 1$.

$r_1 := r_{-1} \bmod r_0$

Mientras $r_i \neq 0$

$c_i := r_{i-2} \div r_{i-1}$.

$v_i := v_{i-2} - v_{i-1} \cdot c_i$.

$i := i + 1$.

$r_i := r_{i-2} \bmod r_{i-1}$.

Si $r_{i-1} \neq 1$

Devuelve "No existe el inverso"

Fin

Devuelve v_{i-1} .

Fin

Ejemplo 2.5.6. Vamos a estudiar si 391 tiene inverso en \mathbb{Z}_{1542} , y en caso afirmativo vamos a calcularlo.

r	c	v
1542		0
391		1
369	3	-3
22	1	4
17	16	-67
5	1	71
2	3	-280
1	2	631

Luego 391 tiene inverso en \mathbb{Z}_{1542} y éste vale 631.

La existencia y el cálculo de inversos permite resolver ecuaciones de grado 1 en \mathbb{Z}_n .

Ejemplo 2.5.7.

1. Vamos a intentar resolver en \mathbb{Z}_{93} la ecuación $47x + 25 = 13x + 58$.

Procedemos de forma análoga a como resolvemos ecuaciones con coeficientes racionales o reales:

$$47x + 25 = 13x + 58; \quad 47x - 13x = 58 - 25; \quad 34x = 33.$$

Y ahora comprobamos si 34 tiene o no inverso módulo 93. Nos valemos del algoritmo de Euclides:

r	c
93	
34	
25	2
9	1
7	2
2	1
1	3

Y puesto que $\text{mcd}(93, 34)$

existe $34^{-1} \bmod 93$.

Lo calculamos a continuación.

r	c	v
93		0
34		1
25	2	-2
9	1	3
7	2	-8
2	1	11
1	3	-41

El inverso vale entonces $-41 = 52$. Multiplicamos ambos miembros por $34^{-1} = 52$.

$$34x = 33; \quad quad 52 \cdot 34x = 52 \cdot 33; \quad 1768x = 1716; \quad x = 42.$$

Luego $x = 42$ es solución de la ecuación $47x + 25 = 13x + 58$.

Notemos que esto último que hemos hecho es lo mismo que si resolviéramos la misma ecuación $34x = 33$ en \mathbb{Q} . La solución sería en tal caso $\frac{33}{34}$ que es el resultado de multiplicar 33 por $34^{-1} = \frac{1}{34}$.

2. Si la ecuación que tuviéramos fuera $33x = 34$, puesto que 33 no tiene inverso módulo 93 ($\text{mcd}(33, 93) = 3$) no podemos proceder como en el ejemplo anterior. En este caso, la ecuación no tiene solución.
3. Sin embargo, la ecuación $33x = 36$ sí tiene solución. De hecho, tiene 3 soluciones, que son $x = 18$, $x = 49$ y $x = 80$.

4. La aplicación $f : \mathbb{Z}_{93} \rightarrow \mathbb{Z}_{93}$ dada por $f(x) = 34x$ es biyectiva. Su inversa es la aplicación $g : \mathbb{Z}_{93} \rightarrow \mathbb{Z}_{93}$ dada por $g(x) = 34^{-1}x = 52x$.

Al ser biyectiva, hay un único elemento $x \in \mathbb{Z}_{93}$ tal que $f(x) = 33$ (ese elemento es $x = 42$, como hemos calculado antes).

5. La aplicación $h : \mathbb{Z}_{93} \rightarrow \mathbb{Z}_{93}$ dada por $h(x) = 33x$ no es ni inyectiva ni sobreyectiva.

No es sobreyectiva pues no existe $x \in \mathbb{Z}_{93}$ tal que $h(x) = 1$ (de existir, sería el inverso de 33) y no es inyectiva pues $h(0) = h(31) = 0$.

En los ejemplos que acabamos de hacer tenemos que $34 \notin \text{Im}(h)$, mientras que 33 sí pertenece a la imagen de h . Y hay tres elementos distintos en \mathbb{Z}_{93} tales que $h(x) = 33$.

Antes de teminar la sección vamos a contar cuantas unidades tiene \mathbb{Z}_n . Para eso, introducimos la función φ de Euler.

Definición 43. Sea $m \geq 2$ Se define $\varphi(m)$ como el número de elementos del conjunto $\{0, 1, 2, \dots, m-1\}$ que son primos relativos con m .

Nótese que $\varphi(m)$ es el cardinal del conjunto $\mathcal{U}(\mathbb{Z}_m)$

Tenemos entonces definida una aplicación $\varphi : \mathbb{N} \setminus \{0, 1\} \rightarrow \mathbb{N}$. Esta aplicación se conoce como la aplicación φ de Euler.

Ejemplo 2.5.8. Vamos a dar los valores de $\varphi(m)$ para algunos números naturales.

$\varphi(2) = 1$ pues $\mathcal{U}(\mathbb{Z}_2) = \{1\}$. De la misma forma podemos ver que $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(12) = 4$.

Si p es un número primo, y $1 \leq a \leq p-1$ se tiene que $\text{mcd}(a, p) = 1$. Por tanto, $\varphi(p) = p-1$.

Las dos siguientes propiedades son útiles a la hora de calcular el valor de $\varphi(m)$.

1. Si p es un número primo, entonces $\varphi(p^n) = p^n - p^{n-1}$.
2. Si $\text{mcd}(m, n) = 1$ entonces $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

La primera propiedad es fácil de justificar pues como el único factor primo de p^n es el número p , para que $\text{mcd}(a, p^n) \neq 1$ el número p debe ser un divisor de a . Por tanto, los elementos del conjunto $A = \{0, 1, 2, \dots, p^n - 1, p^n\}$ que no son primos relativos con p^n son exactamente los que son múltiplos de p , y estos son los del conjunto $B = \{0, p, 2 \cdot p, \dots, (p^{n-1} - 1) \cdot p\}$. Este conjunto tiene p^{n-1} elementos.

Entonces los elementos del conjunto A que son primos relativos con p son los que no pertenecen a B , es decir, los de $A \setminus B$. El cardinal de este conjunto es $p^n - p^{n-1}$. Por tanto, $\varphi(p^n) = p^n - p^{n-1}$.

La segunda propiedad la demostraremos más adelante.

Esta segunda propiedad se puede generalizar al siguiente caso:

Si m_1, m_2, \dots, m_k son números naturales tales que $\text{mcd}(m_i, m_j) = 1$ para $i \neq j$ entonces

$$\varphi(m_1 m_2 \cdots m_k) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_k)$$

Ejemplo 2.5.9.

1. Puesto que $12 = 2^2 \cdot 3$ se tiene que

$$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2) \cdot (3 - 1) = 4$$

En la siguiente tabla, vamos a indicar el máximo común divisor con 12 de cada uno de los números comprendidos entre 0 y 11.

a	0	1	2	3	4	5	6	7	8	9	10	11
$\text{mcd}(a, 12)$	12	1	2	3	4	1	6	1	4	3	2	1

y vemos que efectivamente hay cuatro números menores que 12 que son primos relativos con 12.

2. $30 = 2 \cdot 3 \cdot 5$, luego $\varphi(30) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = (2 - 1)(3 - 1)(5 - 1) = 8$.

El conjunto de las unidades de \mathbb{Z}_{30} es $\mathcal{U}(\mathbb{Z}_{30}) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, que vemos que tiene 8 elementos.

3. Si $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ donde todos los primos que intervienen son distintos, y todos los exponentes son mayores que 0 entonces:

$$\varphi(m) = \varphi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

o si queremos expresarlo de otra forma,

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Teorema 2.5.1 (Euler-Fermat). Sea $a \in \mathbb{Z}$, $m \in \mathbb{N}^*$ tales que $\text{mcd}(a, m) = 1$. Entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demostración: Nótese que decir $\text{mcd}(a, m) = 1$ es equivalente a decir que $a \in \mathcal{U}(\mathbb{Z}_m)$, luego hemos de probar que si $a \in \mathcal{U}(\mathbb{Z}_m)$ entonces $a^{\varphi(m)} = 1$ (en \mathbb{Z}_m).

Consideramos la aplicación $f : \mathcal{U}(\mathbb{Z}_m) \rightarrow \mathcal{U}(\mathbb{Z}_m)$ dada por $f(x) = a \cdot x$. Claramente f es inyectiva, pues al ser a una unidad se puede simplificar por a . Por tanto, f es sobreyectiva (pues va de un conjunto finito en sí mismo).

Si $\mathcal{U}(\mathbb{Z}_m) = \{x_1, x_2, \dots, x_{\varphi(m)}\}$ entonces se tiene que

$$\mathcal{U}(\mathbb{Z}_m) = \text{Im}(f) = \{a \cdot x_1, a \cdot x_2, \dots, a \cdot x_{\varphi(m)}\}$$

Por tanto, $x_1 x_2 \cdots x_{\varphi(m)} = (a x_1)(a x_2) \cdots (a x_{\varphi(m)}) = a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)}$, y puesto que todo lo que interviene en el producto son unidades podemos simplificar y nos queda $a^{\varphi(m)} = 1$. ■

Ejemplo 2.5.10.

1. Se tiene que $\varphi(5) = 4$. Por tanto $2^4 \equiv 1 \pmod{5}$.

El conjunto de las unidades de \mathbb{Z}_5 es $\{1, 2, 3, 4\}$. La aplicación $f : \mathcal{U}(\mathbb{Z}_5) \rightarrow \mathcal{U}(\mathbb{Z}_5)$ es la aplicación:

$$1 \mapsto 2 \quad 2 \mapsto 4 \quad 3 \mapsto 1 \quad 4 \mapsto 3$$

y vemos como es biyectiva.

2. $\varphi(7) = 6$ luego $3^6 \equiv 1 \pmod{7}$, o $4^6 \equiv 1 \pmod{7}$.

3. Vamos a calcular el resto de dividir 3^{1000} y 4^{1000} entre 7. Es decir, vamos a calcular el valor de 3^{1000} y 4^{1000} en \mathbb{Z}_7 .

Sabemos que $3^6 = 1$, y como $1000 = 166 \cdot 6 + 4$ tenemos que

$$3^{1000} = 3^{6 \cdot 166} 3^4 = (3^6)^{166} 3^4 = 1^{166} 3^4 = 3^4 = 81 = 4$$

$$4^{1000} = 4^{6 \cdot 166} 4^4 = (4^6)^{166} 4^4 = 1^{166} 4^4 = (4^2)^2 = 2^2 = 4$$

Nótese que en este caso se tiene que $4^3 = 1$, luego se podría haber hecho

$$4^{1000} = 4^{3 \cdot 333} 4^1 = (4^3)^{333} 4 = 1^{333} 4 = 4$$

Si calculamos 3^{1000} nos sale que vale

```
132207081948080663689045525975214436596542203275214816766492036822682859734670489954077831385060806196390977769
68725825595095458210061891186534272525795367402762022519832080387801477422896484127439040011758861804112894781
562309443806156617305408667449050617812548034440554705439703889581746536825491613622083026856377858229022841639
830788789691855640408489893760937324217184635993869551676501894058810906042608967143886410281435038564874716583
2010614366132173102768902855220001
```

El cociente al dividir por 7 sale

```
188867259925829519555779322821734909423631718964592595380702909746689799620957842791539759121515437423415682528
124654622278707797442945558837906103608279096289660032171188686268287824889852120182055771445369802577304135402
231870634008795167579155239212929454017925763486506722056719842259637909750702305174404324080539797470032630914
043983985274079486297842705372767606024549479991242216680716991512587008632298524491266300402050055092678166547
430087766590310443252700407888571
```

mientras que el resto sale 4.

2.6. Sistemas de congruencias

En esta sección vamos a plantearnos resolver algunas ecuaciones, o sistemas de ecuaciones, con una incógnita, en donde esta incógnita aparece en una o varias congruencias. Las soluciones, de existir, serán números enteros.

Una ecuación lineal en congruencias es una expresión de la forma

$$ax + b \equiv cx + d \pmod{m}$$

donde a, b, c, d, m son números enteros y $m \neq 0$.

Por ejemplo, $3x + 4 \equiv -2x + 5 \pmod{12}$ es una ecuación lineal en congruencias. En este caso, $a = 3$, $b = 4$, $c = -2$, $d = 5$ y $m = 12$.

A una ecuación lineal en congruencias de la forma anterior la llamaremos simplemente una *congruencia*.

Dada una congruencia de la forma $ax + b \equiv cx + d \pmod{m}$, una solución de esta congruencia es un número entero, de forma que al sustituir x por ese número entero nos queda una afirmación cierta. Si s es una solución, normalmente escribiremos que $x = s$ es una solución de la congruencia.

Por ejemplo, en la congruencia $3x + 4 \equiv -2x + 5 \pmod{12}$, $x = 5$ es una solución, ya que al sustituir x por 5 nos queda $3 \cdot 5 + 4 \equiv -2 \cdot 5 + 5 \pmod{12}$, o lo que es lo mismo, $19 \equiv -5 \pmod{12}$, lo cual es cierto, pues 12 es un divisor de $-5 - 19$. También es solución $x = -7$. Sin embargo, no es solución $x = 7$, ya que si sustituimos x por 7, nos queda $21 \equiv -11 \pmod{12}$, y esa afirmación es falsa, ya que -32 (que es igual a $-11 - 21$) no es múltiplo de 12.

Nosotros no vamos a estudiar ecuaciones en congruencias que no sean lineales. El caso más simple es la congruencia

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

con $a, m \in \mathbb{Z}$, $m \geq 1$. Esta ecuación claramente tiene solución. De hecho, tiene infinitas soluciones y éstas son $x = a + km : k \in \mathbb{Z}$.

Por ejemplo, la congruencia $x \equiv 2 \pmod{5}$ tiene a $x = 2$ como solución, pero también $x = 7$, $x = 12$, $x = -3$. Todas las soluciones son de la forma $x = 2 + 5k$, con k un número entero. Para $k = 0, 1, 2, -1$ obtenemos las cuatro soluciones que hemos dado.

Dadas dos ecuaciones en congruencias, diremos que son equivalentes si ambas tienen las mismas soluciones.

Dados $a, b, c, d, m \in \mathbb{Z}$, $m \neq 0$, es fácil ver que la congruencia $ax + b \equiv cx + d \pmod{m}$ es equivalente a la congruencia $(a - c)x \equiv d - b \pmod{m}$, por lo que nos limitaremos a congruencias que sean de la forma $ax \equiv b \pmod{m}$

Por ejemplo, la congruencia $3x + 4 \equiv -2x + 5 \pmod{12}$ es equivalente a $(3 - (-2))x \equiv 5 - 4 \pmod{12}$, o lo que es lo mismo $5x \equiv 1 \pmod{12}$. Podemos ver como $x = 5$, ó $x = -7$ son soluciones de ambas, mientras que $x = 7$ no es solución de ninguna.

Nuestro primer objetivo es, dada una congruencia de la forma $ax \equiv b \pmod{m}$, estudiar si tiene o no solución, y en caso afirmativo, transformarla en una equivalente a ella que sea de la forma $x \equiv c \pmod{n}$. Una vez hecho esto, ya tenemos las soluciones de la congruencia de partida.

Veamos a continuación distintas transformaciones que podemos realizar en una congruencia, y que dan lugar a una congruencia equivalente. Supondremos que partimos de una congruencia de la forma $ax \equiv b \pmod{m}$

1. Si $a \equiv a' \pmod{m}$ y $b \equiv b' \pmod{m}$ entonces la congruencia $ax \equiv b \pmod{m}$ es equivalente a $a'x \equiv b' \pmod{m}$.

Demostración: Se tiene que $a' = a + k_a m$, y $b' = b + k_b m$.

Si x_0 es una solución de $ax \equiv b \pmod{m}$ entonces $ax_0 - b = km$, con $k \in \mathbb{Z}$. Entonces:

$$\begin{aligned} a'x_0 - b' &= (a + k_a m)x_0 - (b + k_b m) = ax_0 + k_a mx_0 - b - k_b m = ax_0 - b + (k_a x_0 - k_b)m \\ &= km + (k_a x_0 - k_b)m = (k + k_a x_0 - k_b)m \end{aligned}$$

es decir, $a'x_0 - b'$ es múltiplo de m , o lo que es lo mismo, x_0 es solución de $a'x \equiv b' \pmod{m}$

Por tanto, hemos demostrado que toda solución de $ax \equiv b \pmod{m}$ es solución de $a'x \equiv b' \pmod{m}$

De la misma forma se demuestra que toda solución de $a'x \equiv b' \pmod{m}$ es solución de $ax \equiv b \pmod{m}$ ■

Esta propiedad nos permite, dada una congruencia, reducir los coeficientes módulo m , obteniendo una congruencia equivalente con coeficientes menores. Por ejemplo, la congruencia

$$29x \equiv 67 \pmod{7}$$

es equivalente a la congruencia

$$x \equiv 4 \pmod{7}$$

pues $29 \equiv 1 \pmod{7}$ y $67 \equiv 4 \pmod{7}$.

2. Si d es un divisor común de a , b y m , entonces la congruencia $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ es equivalente a $ax \equiv b \pmod{m}$.

Demostración: Sea x_0 una solución de $ax \equiv b \pmod{m}$. Entonces $ax_0 - b = km$, luego $\frac{a}{d}x_0 - \frac{b}{d} = k\frac{m}{d}$, luego x_0 es solución de $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

La otra parte se demuestra de forma análoga. ■

Esta propiedad también permite reducir los coeficientes de las congruencias. Así, por ejemplo, las congruencias

$$6x \equiv 14 \pmod{22} \quad \text{y} \quad 3x \equiv 7 \pmod{11}$$

son equivalentes.

3. Si $\text{mcd}(c, m) = 1$, entonces las congruencias $ax \equiv b \pmod{m}$ y $cax \equiv cb \pmod{m}$ son equivalentes.

Demostración: Es fácil comprobar que toda solución de $ax \equiv b \pmod{m}$ es también solución de $cax \equiv cb \pmod{m}$ (si $ax_0 - b$ es múltiplo de m también lo es $cax_0 - cb$). Esto es cierto, aún sin que $\text{mcd}(c, m) = 1$.

Sea ahora d tal que $dc \equiv 1 \pmod{m}$. Este tal d existe. Basta tomar el inverso de c en \mathbb{Z}_m , que existe pues $\text{mcd}(c, m) = 1$. Se tiene ahora que toda solución de $cax \equiv cb \pmod{m}$ es solución de $dcax \equiv dcb \pmod{m}$, que tiene las mismas soluciones que $ax \equiv b \pmod{m}$ (ver propiedad 1). ■

Esta propiedad se suele aplicar junto con la propiedad 1, para simplificar congruencias. Por ejemplo, si tenemos la congruencia

$$6x \equiv 16 \pmod{17}$$

podemos multiplicar por 3 los coeficientes a y b , ya que $\text{mcd}(3, 17) = 1$. Obtenemos entonces la congruencia

$$18x \equiv 48 \pmod{17}$$

que es equivalente a la de partida. Por la propiedad primera, tenemos que esta congruencia es equivalente a

$$x \equiv 14 \pmod{17}$$

y de esta congruencia conocemos las soluciones.

El número 3 por el que se ha multiplicado no ha sido elegido al azar, sino que se ha tomado por ser el inverso de 6 en \mathbb{Z}_{17} .

Parece claro entonces que el camino a seguir es multiplicar los coeficientes a y b de la congruencia por el inverso de a en \mathbb{Z}_m . El problema es que no siempre es posible.

Es importante que el número por el que multiplicamos sea primo relativo con m , pues en caso contrario obtenemos una congruencia que no es equivalente. Por ejemplo, si consideramos la congruencia

$$7x \equiv 5 \pmod{12}$$

y multiplicamos por 2, obtenemos

$$14x \equiv 10 \pmod{12}$$

Vemos como $x = 5$ es solución de la segunda congruencia ($14 \cdot 5 - 10$ es múltiplo de 12), pero no es solución de la primera ($7 \cdot 5 - 5$ no es múltiplo de 12).

4. Si c es un divisor común de a y b , y $\text{mcd}(c, m) = 1$, entonces las congruencias $ax \equiv b \pmod{m}$ y $\frac{a}{c}x \equiv \frac{b}{c} \pmod{m}$ son equivalentes.

Demostración: Es semejante a la propiedad anterior. ■

Proposición 2.6.1. Sean $a, b, m \in \mathbb{Z}$, con $m \geq 2$. Entonces la congruencia $ax \equiv b \pmod{m}$ tiene solución si, y sólo si, $\text{mcd}(a, m) | b$.

Demostración: Sea $d = \text{mcd}(a, m)$.

Supongamos que la congruencia tiene solución. Sea x_0 una tal solución. Entonces $ax_0 - b = km$ para algún $k \in \mathbb{Z}$, luego $ax_0 - km = b$.

Puesto que a es múltiplo de d , también lo es ax_0 . De la misma forma, km es múltiplo de d . Por tanto, $ax_0 - km$ es múltiplo de d . Es decir, $d | b$.

Recíprocamente, supongamos que $d | b$, es decir, $b = c \cdot d$ para algún $c \in \mathbb{Z}$. Por el teorema 2.3.2, existen $u, v \in \mathbb{Z}$ tales que $d = a \cdot u + m \cdot v$. Multiplicamos por c , y nos queda $b = a \cdot (uc) + m \cdot (vc)$, de donde deducimos que $a \cdot (uc) - b$ es múltiplo de m . Por tanto, uc es una solución a la congruencia $ax \equiv b \pmod{m}$. ■

A la hora de resolver una congruencia de la forma $ax \equiv b \pmod{m}$ podemos proceder como sigue:

- 1 Reducimos a y b módulo m . Este paso no es necesario, pero puede facilitar los cálculos.
- 2 Se comprueba si $\text{mcd}(a, m) | b$. Si la respuesta es negativa, entonces la congruencia no tiene solución. Si la respuesta es afirmativa, podemos dividir toda la congruencia por $\text{mcd}(a, m)$ (ver propiedad 2). Hemos transformado la congruencia en una de la forma $ax \equiv b \pmod{m}$, pero ahora se tiene que $\text{mcd}(a, m) = 1$.
- 3 Buscamos el inverso de a en \mathbb{Z}_m . Llamémoslo u .
- 4 Multiplicamos ambos miembros de la congruencia por u . Por la propiedad 3 obtenemos una congruencia equivalente, y ésta adopta la forma $x \equiv c \pmod{m}$.

Con esto ya hemos resuelto la congruencia. Las soluciones son $x = c + km : k \in \mathbb{Z}$.

Ejemplo 2.6.1.

1. La congruencia $2x \equiv 3 \pmod{4}$ no tiene solución, pues $\text{mcd}(2, 4) = 2$, que no divide a 3. Claramente, para cualquier valor de x , $2x$ es par, luego $2x - 3$ es impar, y un número impar no puede ser múltiplo de 4.
2. En cambio, la congruencia $4x \equiv 2 \pmod{6}$ sí tiene solución, pues $\text{mcd}(4, 6) = 2$ y $2 | 2$. Dividimos entonces todo por 2 y obtenemos la congruencia $2x \equiv 1 \pmod{3}$. Puesto que $2^{-1} = 2$ (en \mathbb{Z}_3) la congruencia es equivalente a $x \equiv 2 \pmod{3}$, cuyas soluciones son $x = 2 + 3k$.
3. Vamos a resolver la congruencia $48x \equiv 25 \pmod{15}$. En primer lugar, reducimos módulo 15. La congruencia nos queda $3x \equiv 10 \pmod{15}$. Dado que $\text{mcd}(3, 15) = 3$, y éste no divide a 10 la congruencia no tiene solución.

4. Resolvamos ahora $27x \equiv 13 \pmod{10}$.

Reducimos todos los coeficientes módulo 10.

$$7x \equiv 3 \pmod{10}$$

Puesto que $\text{mcd}(7, 10) = 1$ la congruencia tiene solución.

$7^{-1} = 3$. Multiplicamos entonces por 3.

$$x \equiv 9 \pmod{10}$$

Las soluciones son $x = 9 + 10k$.

5. Consideramos la congruencia $6x \equiv 12 \pmod{27}$. Se tiene que $x = 11$ es solución de esta ecuación, pues $6 \cdot 11 - 12 = 54$ que es múltiplo de 27.

Si dividimos ambos miembros por 3 obtenemos $2x \equiv 4 \pmod{27}$. En este caso tenemos que 11 no es solución, pues $2 \cdot 11 - 4 = 18$ que no es múltiplo de 27.

6. Obviamente, si partimos de la congruencia $2x \equiv 4 \pmod{27}$ y multiplicamos ambos miembros por 3 obtenemos una congruencia que no es equivalente.

El siguiente algoritmo recoge esta forma de resolver una congruencia.

Algoritmo CONGRUENCIA(a, b, m)

Entrada: $a, b \in \mathbb{Z}, m \in \mathbb{N} : m \geq 1$

Salida: (c, n) : $x \equiv c \pmod{n}$ y $ax \equiv b \pmod{m}$ son equivalentes.

$a := a \pmod{m}$

$b := b \pmod{m}$

$(d, u, v) := \text{BEZOUT}(a, m)$

Si $b \pmod{d} \neq 0$

Devuelve "No tiene solución"

Fin

$(a, b, m) := (a \text{ div } d, m \text{ div } d, m \text{ div } d)$

$c := a \cdot u \pmod{m}$

Devuelve (c, m)

Fin

Nos planteamos a continuación cómo resolver sistemas de congruencias con una sola incógnita. Puesto que toda congruencia que tenga solución es equivalente a una de la forma $x \equiv a \pmod{m}$ nos centramos inicialmente en resolver un sistema de la forma

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots\dots\dots \\ x &\equiv a_p \pmod{m_p} \end{aligned}$$

Una solución del sistema es un número entero que es simultáneamente solución de todas las congruencias.

Ejemplo 2.6.2.

1. El sistema de congruencias

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

$$x \equiv 5 \pmod{9}$$

tiene a $x = 14$ como una solución, pues $14 - 2$ es múltiplo de 6 y $14 - 5$ es múltiplo de 9.

2. El sistema

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

$$x \equiv 6 \pmod{9}$$

no tiene solución, pues si $x \equiv 6 \pmod{9}$ se tiene que $x \equiv 0 \pmod{3}$, mientras que si $x \equiv 2 \pmod{6}$ entonces $x \equiv 2 \pmod{3}$.

El siguiente teorema nos da una condición suficiente para que un sistema de congruencias tenga solución.

Teorema 2.6.1 (Teorema chino del resto). Sean $a_1, a_2, \dots, a_p \in \mathbb{Z}$, y $m_1, m_2, \dots, m_p \in \mathbb{N}^*$. Supongamos que $\text{mcd}(m_i, m_j) = 1$ para $i \neq j$. Entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots\dots\dots \\ x &\equiv a_p \pmod{m_p} \end{aligned}$$

tiene solución. Además, si a es una solución, dicho sistema es equivalente a la congruencia

$$x \equiv a \pmod{M}$$

donde $M = \prod_{i=1}^p m_i$.

Antes de hacer la demostración del teorema, comprueba que si $a, m_1, m_2, \dots, m_p \in \mathbb{Z}$ y $\text{mcd}(a, m_1) = \text{mcd}(a, m_2) = \dots = \text{mcd}(a, m_p) = 1$ entonces $\text{mcd}(a, m_1 m_2 \dots m_p) = 1$.

Demostración: Sea $M_i = \frac{M}{m_i} = \prod_{j \neq i} m_j$.

Se tiene entonces que $\text{mcd}(m_i, M_i) = 1$. Por el teorema 2.3.2, existen $u_i, v_i \in \mathbb{Z}$ tal que $m_i u_i + M_i v_i = 1$. Es claro entonces que

$$M_i v_i \pmod{m_i} = 1 \quad M_i v_i \pmod{m_j} = 0 \quad \text{para } j \neq i$$

luego

$$a_i M_i v_i \pmod{m_i} = a_i \pmod{m_i} \quad a_i M_i v_i \pmod{m_j} = 0 \quad \text{para } j \neq i$$

Sea entonces $a = \sum_{i=1}^p a_i M_i v_i$. Es fácil comprobar que a es solución del sistema.

Supongamos que b es otra solución. Entonces se tiene que

$$b \equiv a \pmod{m_1} \quad b \equiv a \pmod{m_2} \quad \dots \quad b \equiv a \pmod{m_p}$$

es decir,

$$m_1 | (b - a) \quad m_2 | (b - a) \quad \dots \quad m_p | (b - a)$$

lo que es equivalente a que $\text{mcm}(m_1, m_2, \dots, m_p) | (b - a)$. Y como $\text{mcm}(m_1, m_2, \dots, m_p) = M$, lo que tenemos es que $M | (b - a)$, es decir, $b = a + Km$. Por tanto, todas las soluciones del sistema de congruencias son de la forma $a + Km$, las mismas soluciones que tiene la congruencia $x \equiv a \pmod{M}$. ■

Nótese que el teorema chino del resto, lo que nos dice es que la aplicación

$$f : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_p}$$

dada por

$$f(x) = (x \pmod{m_1}, x \pmod{m_2}, \dots, x \pmod{m_p})$$

es biyectiva (realmente, lo que dice es que es sobreyectiva, pero al tener los dos conjuntos el mismo cardinal eso es suficiente para ser biyectiva).

Nos centramos en el caso $p = 2$. Es fácil ver (corolario 2.3.3) que la aplicación f induce una biyección

$$f : \mathcal{U}(\mathbb{Z}_{m_1 m_2}) \rightarrow \mathcal{U}(\mathbb{Z}_{m_1}) \times \mathcal{U}(\mathbb{Z}_{m_2})$$

Por tanto, los dos conjuntos, dominio y codominio, tienen el mismo cardinal. Deducimos entonces que

$$\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2)$$

si $\text{mcd}(m_1, m_2) = 1$.

Ejemplo 2.6.3.

1. Consideramos el sistema:

$$\begin{aligned}x &\equiv 1 \pmod{2} \\x &\equiv 2 \pmod{5} \\x &\equiv 3 \pmod{7}\end{aligned}$$

Es claro que $\text{mcd}(2, 5) = \text{mcd}(2, 7) = \text{mcd}(5, 7) = 1$. Entonces tomamos $M_1 = 5 \cdot 7 = 35$, $M_2 = 2 \cdot 7 = 14$ y $M_3 = 2 \cdot 5 = 10$.

$$1 = 2 \cdot 18 + 35 \cdot (-1) \implies v_1 = -1$$

$$1 = 5 \cdot 3 + 14 \cdot (-1) \implies v_2 = -1$$

$$1 = 7 \cdot 3 + 10 \cdot (-2) \implies v_3 = -2.$$

Por tanto, podemos tomar $a = 1 \cdot 35 \cdot (-1) + 2 \cdot 14 \cdot (-1) + 3 \cdot 10 \cdot (-2) = -123$.

El sistema de partida es equivalente a la congruencia $x \equiv -123 \pmod{70}$, que a su vez es equivalente a $x \equiv 17 \pmod{70}$. Las soluciones son entonces

$$x = 17 + 70k$$

Nótese que podríamos haber tomado $v_1 = 1$, $v_2 = 4$ y $v_3 = 5$, en cuyo caso nos habría salido $a = 297$, que también es solución ($297 \equiv -123 \pmod{70}$).

2. Consideramos la aplicación $f : \mathbb{Z}_{18} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_9$ dada por $f(x) = (x \pmod{2}, x \pmod{9})$.

$$\begin{array}{llllll}f(0) = (0, 0) & f(1) = (1, 1) & f(2) = (0, 2) & f(3) = (1, 3) & f(4) = (0, 4) & f(5) = (1, 5) \\f(6) = (0, 6) & f(7) = (1, 7) & f(8) = (0, 8) & f(9) = (1, 0) & f(10) = (0, 1) & f(11) = (1, 2) \\f(12) = (0, 3) & f(13) = (1, 4) & f(14) = (0, 5) & f(15) = (1, 6) & f(16) = (0, 7) & f(17) = (1, 8)\end{array}$$

que claramente es una biyección, mientras que si definimos $f : \mathbb{Z}_{18} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_6$ de la misma forma obtenemos

$$\begin{array}{llllll}f(0) = (0, 0) & f(1) = (1, 1) & f(2) = (2, 2) & f(3) = (0, 3) & f(4) = (1, 4) & f(5) = (2, 5) \\f(6) = (0, 0) & f(7) = (1, 1) & f(8) = (2, 2) & f(9) = (0, 3) & f(10) = (1, 4) & f(11) = (2, 5) \\f(12) = (0, 0) & f(13) = (1, 1) & f(14) = (2, 2) & f(15) = (0, 3) & f(16) = (1, 4) & f(17) = (2, 5)\end{array}$$

que claramente no es ni inyectiva ni sobreyectiva.

En un ejemplo anterior hemos estudiado dos sistemas con dos congruencias en los que los módulos no eran primos relativos ($\text{mcd}(m_1, m_2) \neq 1$). En un caso el sistema tiene solución y en el otro no. Lo que pretendemos a continuación es estudiar sistemas de congruencias que no se ajusten a las hipótesis del teorema chino del resto (que los módulos sean primos relativos).

Vamos a desarrollar un método para resolver sistemas de congruencias, independientemente de que satisfagan o no las hipótesis del teorema chino. En caso de que el sistema no tenga solución, lo detectaremos en el desarrollo del proceso.

El método consiste en resolver en primer lugar la primera congruencia (trivial).

Se introduce la solución en la segunda, y se halla la solución del sistema formado por las dos primeras congruencias.

Se introduce en la tercera congruencia y se vuelve a resolver.

El proceso continúa, bien hasta que terminemos con todas las congruencias, bien hasta que lleguemos a una congruencia que no tiene solución.

Veamos algunos ejemplos.

Ejemplo 2.6.4. 1.

$$\left. \begin{aligned}x &\equiv 1 \pmod{2} \\x &\equiv 2 \pmod{5} \\x &\equiv 3 \pmod{7}\end{aligned} \right\}$$

$x \equiv 1(\text{mód } 2)$	<i>Calculamos las soluciones</i>	$x = 1 + 2k_1$
$x \equiv 2(\text{mód } 5)$	<i>Introducimos la solución</i>	$1 + 2k_1 \equiv 2(\text{mód } 5)$
	<i>Multiplicamos por $3 = 2^{-1}$ en \mathbb{Z}_5</i>	$2k_1 \equiv 1(\text{mód } 5)$
		$k_1 \equiv 3(\text{mód } 5)$
	<i>Sustituimos</i>	$k_1 = 3 + 5k_2$
$x \equiv 3(\text{mód } 7)$	<i>Introducimos la solución</i>	$x = 1 + 2(3 + 5k_2) = 7 + 10k_2$
		$7 + 10k_2 \equiv 3(\text{mód } 7)$
		$10k_2 \equiv -4(\text{mód } 7)$
	<i>Reducimos módulo 7</i>	$3k_2 \equiv 3(\text{mód } 7)$
	<i>Multiplicamos por $5 = 3^{-1}$ en \mathbb{Z}_7</i>	$k_2 \equiv 1(\text{mód } 7)$
		$k_2 = 1 + 7k_2$
	<i>Sustituimos</i>	$x = 7 + 10(1 + 7k_2) = 17 + 70k_2$

Por tanto, la solución es $x = 17 + 70k_2$.

$$2. \quad \left. \begin{array}{l} x \equiv 2(\text{mód } 6) \\ x \equiv 5(\text{mód } 9) \end{array} \right\}$$

$x \equiv 2(\text{mód } 6)$	<i>Calculamos las soluciones</i>	$x = 2 + 6k_1$
$x \equiv 5(\text{mód } 9)$	<i>Introducimos la solución</i>	$2 + 6k_1 \equiv 5(\text{mód } 9)$
		$6k_1 \equiv 3(\text{mód } 9)$
	<i>Dividimos todo por $3 = \text{mcd}(6, 3, 9)$</i>	$2k_1 \equiv 1(\text{mód } 3)$
	<i>Multiplicamos por $2 = 2^{-1}$ en \mathbb{Z}_3</i>	$k_1 \equiv 2(\text{mód } 3)$
		$k_1 = 2 + 3k_2$
	<i>Sustituimos</i>	$x = 2 + 6(2 + 3k_2) = 14 + 18k_2$

Las soluciones son entonces $x = 14 + 18k_2$.

$$3. \quad \left. \begin{array}{l} x \equiv 2(\text{mód } 6) \\ x \equiv 6(\text{mód } 9) \end{array} \right\}$$

$x \equiv 2(\text{mód } 6)$	<i>Calculamos las soluciones</i>	$x = 2 + 6k_1$
$x \equiv 6(\text{mód } 9)$	<i>Introducimos la solución</i>	$2 + 6k_1 \equiv 6(\text{mód } 9)$
		$6k_1 \equiv 4(\text{mód } 9)$

Y el sistema no tiene solución, pues $\text{mcd}(6, 9) = 3$, que no divide a 4.

4. Vamos a calcular las dos últimas cifras de 27^{3636} .

Es claro que tenemos que calcular el resto de dividir por 100 de dicho número, o lo que es equivalente, realizar la operación en \mathbb{Z}_{100} . Dado que $\text{mcd}(27, 100) = 1$ se tiene que $27^{\varphi(100)} = 1$, y como $\varphi(100) = \varphi(4 \cdot 25) = 2 \cdot 20 = 40$ tenemos que $27^{40} \equiv 1(\text{mód } 100)$.

Puesto que $3636 = 90 \cdot 40 + 36$ nos queda que $27^{3636} = (27^{40})^{90} 27^{36} = 27^{36}$. Vemos que realizar esta operación no es fácil. Vamos a ver tres formas de resolverlo:

- a) \vdash Calculamos 27^{3636} en \mathbb{Z}_4 .
 En ese caso se tiene que $27 \equiv 3$, y como $\varphi(4) = 2$ entonces $3^2 \equiv 1$, luego $3^{3636} \equiv 1$.
 \vdash Calculamos 27^{3636} en \mathbb{Z}_{25} .
 En este caso hay que calcular 2^{3636} . Dado que $\varphi(25) = 20$ y $3636 \equiv 16(\text{mód } 20)$ lo que hemos de calcular es 2^{16} , que puede ser calculado como sigue:

$$2^2 = 4; \quad 2^4 = (2^2)^2 = 4^2 = 16; \quad 2^8 = (2^4)^2 = 16^2 = 256 \equiv 6; \quad 2^{16} = (2^8)^2 = 6^2 = 36 \equiv 11$$

- \vdash Resolvemos el sistema

$$\begin{array}{l} x \equiv 1(\text{mód } 4) \\ x \equiv 11(\text{mód } 25) \end{array}$$

$x = 1 + 4k_1$, de donde $1 + 4k_1 \equiv 11(\text{mód } 25)$, es decir, $4k_1 \equiv 10(\text{mód } 25)$. Multiplicamos por 19 y nos queda $k_1 \equiv 15(\text{mód } 25)$ de donde $k_1 = 15 + 25k$. Finalmente sustituimos:

$$x = 1 + 4k_1 = 1 + 4(15 + 25k) = 61 + 100k$$

b) Puesto que $27^{40} = 1$ en \mathbb{Z}_{100} tenemos que $27^{36} \cdot 27^4 = 1$, luego $27^{36} = (27^4)^{-1}$.

Tenemos entonces que $27^4 = 729^2 = 29^2 = 841 = 41$. Y ahora lo que hay es que calcular el inverso de 41 en \mathbb{Z}_{100} .

r	c	v
100		0
41		1
18	2	-2
5	2	5
3	3	-17
2	1	22
1	1	-39

Luego $27^{36} = 41^{-1} = -39 = 61$.

c) Vamos calculando las potencias.

- $27^2 = 29$.
- $27^4 = 29^2 = 41$.
- $27^8 = 41^2 = 1681 = 81$.
- $27^{16} = 81^2 = 6561 = 61$.
- $27^{32} = 61^2 = 3721 = 21$.
- $27^{36} = 27^{32} \cdot 27^4 = 21 \cdot 41 = 861 = 61$.

De cualquiera de las formas que lo hagamos vemos que las dos últimas cifras son 61.

Nótese que empleando este método es indiferente que las congruencias estén expresadas de la forma $x \equiv b \pmod{m}$ o de la forma $ax \equiv b \pmod{m}$.

El siguiente algoritmo utiliza esta idea para resolver sistemas de congruencias.

Algoritmo SISTEMA($p, (a_1, b_1, m_1), \dots, (a_p, b_p, m_p)$)

Entrada: $a, b \in \mathbb{Z}, m \in \mathbb{N} : m \geq 1$

$p \in \mathbb{N} : p \geq 2$

$a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$

$m_1, \dots, m_k \in \mathbb{N}^*$

Salida: (c, n) .

El sistema

$$a_1 x \equiv b_1 \pmod{m_1}$$

$$a_2 x \equiv b_2 \pmod{m_2}$$

.....

$$a_p x \equiv b_p \pmod{m_p}$$

y la congruencia $x \equiv c \pmod{n}$ son equivalentes.

$(c, n) := \text{CONGRUENCIA}(a_1, b_1, m_1)$

Desde $k = 2$ hasta p

$$(a_k, b_k) := (a_k n, b_k - a_k c)$$

$$(u, v) := \text{CONGRUENCIA}(a_k, b_k, m_k)$$

$$(c, n) := (c + nu, nv)$$

Devuelve (c, n)

Fin

Ejemplo 2.6.5. Para terminar, vamos a calcular las dos últimas cifras del número 125^{131} expresado en hexadecimal (base 16).

Llamemos x a dicho número. Para calcular esas cifras, deberíamos calcular el cociente y el resto de dividir x entre 16 (llamemos a estos números c_1 y r_1 respectivamente. Y a continuación, calcular el resto de dividir c_1 entre 16. Si este número es r_2 , las dos últimas cifras serán r_2 y r_1 (o sus correspondientes símbolos).

El cálculo de r_1 es fácil, pero no así el de c_1 , lo que nos impediría calcular r_2 .

Supongamos que hemos logrado realizar esos cálculos. En ese caso, tendríamos:

$$x = 16 \cdot c_1 + r_1 = 16 \cdot (16 \cdot c_2 + r_2) + r_1 = 16^2 \cdot c_2 + (16 \cdot r_2 + r_1) = 256 \cdot c_2 + (16 \cdot r_2 + r_1)$$

Y vemos cómo $16 \cdot r_2 + r_1$ es el resto de dividir x entre 256.

Podemos entonces probar el siguiente camino:

1. Calculamos el resto de dividir x entre $256 = 16^2$. Llamemos r a dicho resto, y será un número comprendido entre 0 y 255.

2. Dividimos r entre 16. El cociente y el resto serán las dos últimas cifras del número x en base 16.

Procedemos a realizar los cálculos.

1. Hallamos el resto de dividir x entre 256. O lo que es lo mismo, reducimos x módulo 256.

Puesto que $\text{mcd}(125, 256) = 1$, sabemos que $125^{\varphi(256)} = 1$ módulo 256. Y como $256 = 2^8$, entonces $\varphi(256) = 2^8 - 2^7 = 128$.

Por tanto, $125^{128} = 1$, luego $x = 125^{131} = 125^3 = 1953125 = 101$ (en los cálculos se ha tenido en cuenta que trabajamos en \mathbb{Z}_{256}).

2. Dividimos 101 entre 16. El resultado es $101 = 6 \cdot 16 + 5$.

Las dos últimas cifras de x en base 16 son entonces 65.

Vamos a calcular el número x .

$x = 49569176510071273892070792106065303648898805658224523078243365649208529255650380350242332598745786840423136544096697184503946705907102084038685671048362886297631181635462794275051930091176636852362359905874623262722320258081010801239248142469051572334137745201587677001953125$

Y su expresión en base 16 es:

16E84AD1CAC3DD6CEC6791668C39126FADD071D74AB8AA78DBC8F2C1F546253935407CB1DA9C62E4E0CBBD48B6012ABCA409A571BEC47C5B8B18520495413745358E395EFE27A14C70DBB1EEB2DCC4ECE5AD3C7A37EDB78AEFFCBBC039C52521A26AAC5B6E21D71B22EE763322935769E0A702F65)

Que como vemos termina en 65.

A partir de este ejemplo, podemos ver que un número x , al escribirlo en hexadecimal, acaba en 65 si, y sólo si, $x \equiv 101 \pmod{16^2}$.

2.7. Ecuaciones diofánticas

Nos planteamos en esta sección resolver en \mathbb{Z} ecuaciones de la forma

$$ax + by = c$$

donde $a, b, c \in \mathbb{Z}$. Fácilmente uno observa que estas ecuaciones no tienen siempre solución. Por ejemplo, la ecuación

$$8x + 20y = 135$$

no puede tener solución, pues para cualesquiera x e y números enteros, el miembro de la izquierda es un número par, luego no puede valer 135. Dicho de otra forma, el miembro de la izquierda es múltiplo de 2, y el miembro de la derecha no lo es.

Para tratar de generalizar este hecho, podemos verlo como que hemos encontrado un número d ($d = 2$) que verifica que $d|8$, $d|20$, pero $d \nmid 135$.

Si pensamos ahora, por ejemplo en la ecuación $18x + 48y = 100$, ese razonamiento para $d = 2$ no nos sirve, pues todos los coeficientes que intervienen son múltiplos de 2. Vemos, no obstante que para $d = 3$ podemos razonar como en el ejemplo anterior (el miembro de la izquierda es múltiplo de 3 y no así el miembro de la derecha).

Repetir este razonamiento a una ecuación general de la forma $ax + by = c$ nos lleva a probar con todos los divisores comunes de a y b , pero dado que en el máximo común divisor de a y b están recogidos todos los divisores comunes de a y b , nos quedamos únicamente con éste.

Dada la ecuación $ax + by = c$, sea $d = \text{mcd}(a, b)$. Hemos razonado que una condición necesaria para que tenga solución es que d divida a c .

La siguiente proposición nos asegura que esta condición es también suficiente.

Proposición 2.7.1. Sean $a, b, c \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$. Entonces la ecuación

$$ax + by = c$$

tiene solución entera si, y sólo si, $d|c$

Demostración: La condición necesaria ($ax + by = c$ tiene solución $\implies d|c$) es fácil de probar.

Veamos la condición suficiente (nos garantiza la existencia de solución).

Supongamos que $d|c$.

Planteamos la congruencia $ax \equiv c \pmod{b}$. Como $\text{mcd}(a, b)|c$ la congruencia tiene solución.

Sea $x = u$ una solución. Eso significa que $au - c$ es múltiplo de b , luego $au - c = bv$ para algún $v \in \mathbb{Z}$. Entonces $au - bv = c$, luego $x = u$, $y = -v$ es una solución de $ax + by = c$.

Además, si u' , v' es otra solución de $ax + by = c$, entonces $au' - c$ es múltiplo de b , luego u' es solución de la congruencia $ax \equiv c \pmod{b}$. ■

La demostración anterior no sólo nos dice cuando una ecuación de la forma $ax + by = c$ tiene solución sino que nos proporciona una forma de encontrarlas.

Para ello, lo que tenemos es que resolver la congruencia $ax \equiv c \pmod{b}$ (o si preferimos, la congruencia $by \equiv c \pmod{a}$).

Ejemplo 2.7.1. Vamos a encontrar, si es posible, una solución a la ecuación $105x + 465y = 195$. Para ello, planteamos la congruencia

$$105x \equiv 195 \pmod{465}$$

Necesitamos calcular el máximo común divisor de 195 y 465. Para ello, hacemos uso del algoritmo de Euclides.

r	c
105	
465	
105	0
45	4
15	2
0	

Vemos que $\text{mcd}(105, 465) = 15$, que divide a 195 (pues $195 = 15 \cdot 13$). La congruencia nos queda entonces $7x \equiv 13 \pmod{31}$.

Calculamos el inverso de 7 módulo 31.

r	c	v
31		0
7		1
3	4	-4
1	2	9

Notemos que para calcular v podríamos haber aprovechado los cálculos que hicimos para el cálculo de $\text{mcd}(465, 105)$, pues la columna de los cocientes es la misma en ambos casos.

Vemos entonces que $7^{-1} = 9$. Multiplicando por 9 nos queda la congruencia $x \equiv 13 \cdot 9 \pmod{31}$. Y como $13 \cdot 9 = 117$, que módulo 31 vale 24.

Luego $x = 24 + 31k$.

Sustituimos en la ecuación inicial:

$$105(24 + 31k) + 465y = 195$$

Y despejamos y :

$$y = \frac{195 - 105 \cdot 24 - 105 \cdot 31k}{465} = \frac{-2325 - 3255k}{465} = -5 - 7k$$

La solución de la ecuación $105x + 465y = 195$ es entonces:

$$\begin{aligned} x &= 24 + 31k \\ y &= -5 - 7k \end{aligned} \quad k \in \mathbb{Z}$$

Para cada valor de k obtenemos una solución distinta de la ecuación. Por ejemplo:

- Para $k = 0$ tenemos $x = 24$, $y = -5$.
- Para $k = 1$ tenemos $x = 55$, $y = -12$.
- Para $k = -1$ tenemos $x = -7$, $y = 2$.

Y todas esas parejas son soluciones de nuestra ecuación diofántica.

Proposición 2.7.2. Sean $a, b, c \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$. Supongamos que x_0, y_0 es una solución de la ecuación $ax + by = c$. Entonces todas las soluciones de esta ecuación son:

$$\begin{aligned} x &= x_0 + k \frac{b}{d} \\ y &= y_0 - k \frac{a}{d} \end{aligned} \quad k \in \mathbb{Z}$$

Demostración: Se tiene que $a(x_0 + k \frac{b}{d}) + b(y_0 - k \frac{a}{d}) = ax_0 + ak \frac{b}{d} + by_0 - bk \frac{a}{d} = ax_0 + by_0 + ak \frac{b}{d} - bk \frac{a}{d} = c$, luego todas las parejas (x, y) de la forma dada en el enunciado son soluciones.

Veamos que toda solución adopta esa forma. Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$.

Si x, y es una solución de la ecuación, entonces $ax_0 + by_0 = ax + by$, de donde $a(x - x_0) + b(y - y_0) = 0$, es decir, $a(x - x_0) = b(y_0 - y)$, lo que implica que $a'(x - x_0) = b'(y_0 - y)$.

Se tiene entonces que $b' | a'(x - x_0)$, y como $\text{mcd}(a', b') = 1$ (¿por qué?) deducimos que $b' | (x - x_0)$, o sea, existe $k \in \mathbb{Z}$ tal que $x - x_0 = kb'$, de donde

$$x = x_0 + kb' = x_0 + k \frac{b}{d}$$

$b'(y_0 - y) = a'(x - x_0) = a'kb'$, luego $y_0 - y = ka'$, o, lo que es lo mismo, $y = y_0 - ka'$ ■

Ejemplo 2.7.2. Notemos que en el ejemplo anterior tenemos que $x_0 = 24$, $y_0 = -5$ es una solución particular de la ecuación.

Como $\text{mcd}(a, b) = 15$, la solución general adopta la forma

$$\begin{aligned} x &= 24 + \frac{465}{15}k \\ y &= -5 - \frac{105}{15}k \end{aligned} \quad k \in \mathbb{Z}$$

que es justamente la solución que nos ha salido.

La proposición 2.7.1 puede extenderse fácilmente al caso de ecuaciones diofánticas de 3 o más incógnitas. Por ejemplo, la ecuación $ax + by + cz = d$ tiene solución si, y sólo si, $\text{mcd}(a, b, c) | d$. Dar una expresión general de la solución, como hemos hecho en la proposición 2.7.2 no es tan sencillo.

Vamos a ver un ejemplo de cómo resolver una ecuación diofántica con tres incógnitas. El método puede ser fácilmente generalizado a 4 ó más.

Ejemplo 2.7.3. Consideramos la ecuación $6x + 10y + 15z = 23$. Puesto que $\text{mcd}(6, 10, 15) = 1$, y 23 es múltiplo de 1, la ecuación tiene solución. Veamos cómo resolverla:

- ‡ Elegimos una incógnita (por ejemplo, z), y pasamos el término correspondiente al miembro de la derecha.

$$6x + 10y = 23 - 15z$$

- ‡ Consideramos entonces nuestra ecuación diofántica como una ecuación con dos incógnitas, y tratamos de resolverla.
- ‡ Puesto que $\text{mcd}(6, 10) = 2$, la ecuación tendrá solución si el término de la derecha es múltiplo de 2.
- ‡ Esta condición se traduce en una restricción sobre z . En nuestro caso es $23 - 15z \equiv 0 \pmod{2}$.
- ‡ Resolvemos esta congruencia. La solución de esta congruencia es $z = 1 + 2k$.
- ‡ Sustituimos en la ecuación: $6x + 10y = 23 - 15(1 + 2k)$, lo que nos da $6x + 10y = 8 - 30k$.
- ‡ Transformamos esta ecuación en una congruencia: $6x \equiv 8 - 30k \pmod{10}$.
- ‡ Estudiamos si tiene solución. Como $\text{mcd}(6, 10) = 2$, y $8 - 30k$ es múltiplo de 2, independientemente del valor de k , esta congruencia tiene solución para cualquier valor de k (de hecho, hemos elegido z para que esto ocurra).
- ‡ Resolvemos esta congruencia. Para ello, reducimos módulo 10 y dividimos todo por 2: $3x \equiv 4 \pmod{5}$.
- ‡ Multiplicamos por 2, que es el inverso de 3 módulo 5: $x \equiv 8 \pmod{5}$, o mejor, $x \equiv 3 \pmod{5}$.
- ‡ Calculamos el valor de x : $x = 3 + 5k'$.
- ‡ Sustituimos: $6(3 + 5k') + 10y = 8 - 30k$.
- ‡ Despejamos y :

$$y = \frac{8 - 30k - 6(3 + 5k')}{10} = \frac{8 - 30k - 18 - 30k'}{10} = \frac{-10 - 30k - 30k'}{10} = -1 - 3k - 3k'$$

Y ya tenemos resuelta la ecuación:

$$\begin{array}{rclcl} x & = & 3 & + & 5k' \\ y & = & -1 & - & 3k & - & 3k' \\ z & = & 1 & + & 2k \end{array} \quad k, k' \in \mathbb{Z}$$