# Capítulo 1

# 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 $0, 1, 2, \cdots$. 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 donde 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 axioms de Peano, se enlazacon 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 $\mathbb{C}$).

## 1.1. Principio de inducción y recurrencia

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 $\mathbb{Q}^+$, $\mathbb{R}^+$, los múltiplos positivos de $\frac{1}{2}$, 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:

$0 \in A$

Si $n \in A$ entonces $n + 1 \in A$

Entonces $A = \mathbb{N}$.

Este principio es la base de muchas demostraciones en las que intervienen los números naturales. Veamos un ejemplo.

**Ejemplo 1.1.1.** *Vamos a demostrar que para todo $n \in \mathbb{N}$ se verifica que*

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

*Para esto, consideramos el conjunto $A$ cuyos elementos son los números naturales para los que se verifica la propiedad anterior, es decir,*

$$A = \{n \in \mathbb{N} : 2^0 + \cdots + 2^n = 2^{n+1} - 1\}$$

*Claramente se tiene que $0 \in A$, pues $2^0 = 2^{0+1} - 1$.*

*Supongamos ahora que $n \in A$, y veamos que $n+1 \in A$, es decir, supongamos que $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$ y comprobemos que $2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1$.*

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

*Por el principio de inducción se tiene que $A = \mathbb{N}$, es decir, la propiedad es cierta para todo $n \in \mathbb{N}$.*

Una demostración basada en el principio de inducción es lo que se conoce como una demostración por inducción.

Si queremos demostrar por inducción que $P(n)$ es cierto para todo $n \in \mathbb{N}$ (donde $P(n)$ es una propiedad que hace referencia a $n$), hemos de realizar dos pasos:

- Paso 1: Demostramos que $P(0)$ es cierto.
- Paso 2: Demostramos que si $P(n)$ es cierto, entonces también es cierto $P(n+1)$.

La suposición de que $P(n)$ es cierto es lo que se conoce como *Hipótesis de inducción.*

Si quisiéramos demostrar que $P(n)$ es cierto para todo $n \geq k$, el primer paso deberá ser demostrar que $P(k)$ es cierto, mientras que el segundo no variaría.

**Ejemplo 1.1.2.** *Demuestra que para todo $n \geq 1$ se verifica que*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

*Hacemos esto por inducción:*

- *Paso 1: Para $n = 1$ el resultado es trivialmente cierto.*
- *Paso 2: La hipótesis de inducción es que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. A partir de ella hemos de probar que $1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}$*

$$(1 + 2 + \cdots + n) + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

El principio de inducción nos dice que si $A$ es un subconjunto de $\mathbb{N}$ que satisface las dos siguientes propiedades:

- $0 \in A$
- $n \in A \Longrightarrow n + 1 \in A$

Entonces $A = \mathbb{N}$. Este axioma puede leerse de la forma siguiente:

> Si $A$ es un subconjunto de $\mathbb{N}$ que es distinto de $\mathbb{N}$, entonces, o $0 \notin A$, o existe $n \in \mathbb{N}$ tal que $n \in A$ y $n + 1 \notin A$.

Esta formulación del principio de inducción (equivalente a la vista anteriormente) nos permite demostrar una propiedad importante de los números naturales.

**Teorema 1.1.1.** *[Principio de buena ordenación] Sea $A$ un subconjunto de $\mathbb{N}$ distinto del conjunto vacío. Entonces $A$ tiene mínimo.*

Se dice que $m$ es el mínimo de $A$ si $m \in A$ y $m \leq n$ para todo $n \in A$.

*Demostración:* Sea $B$ el conjunto de las cotas inferiores de $A$, es decir

$$B = \{m \in \mathbb{N} : m \leq n \ \text{ para todo } n \in A\}$$

Claramente $B \neq \mathbb{N}$ (pues si $m \in A$, $m + 1 \notin B$).

También es cierto que $0 \in B$ (¿por qué?).

Por tanto, debe existir $m \in \mathbb{N}$ tal que $m \in B$ y $m + 1 \notin B$

Por pertenecer $m$ a $B$ se tiene que $m \leq n$ para todo $n \in A$. Queda entonces comprobar que $m \in A$.

Ahora bien, supongamos que $m \notin A$, entonces, para cualquier $n \in A$ se tiene que $m \leq n$ (pues $m \in B$) y que $m \neq n$ (pues $m \notin A$), luego $m + 1 \leq n$ para todo $n \in A$. Por tanto, tendríamos que $m + 1 \in B$, lo cual no es posible.

Deducimos por tanto que $m \in A$, como queríamos. ■

Hasta ahora hemos usado el principio de inducción para demostrar propiedades referentes a los números naturales. Veamos ahora como definir funciones con dominio en $\mathbb{N}$.

**Definición 1.** *Sea $X$ un conjunto. Una sucesión en $X$ es una aplicación $x : \mathbb{N} \to X$.*

Si $x : \mathbb{N} \to X$ es una sucesión, denotaremos normalmente al elemento $x(n)$ como $x_n$.

A la hora de definir una sucesión en $X$, podemos optar, bien por definir explícitamente el valor de $x_n$ para todo $n \in \mathbb{N}$, o bien, definir el valor de $x_0$, y a partir de $x_n$ definir lo que vale $x_{n+1}$. El principio de inducción nos asegura que de esta forma se define una función $x : \mathbb{N} \to X$ (aunque formalizar esto es bastante engorroso, la idea consiste en considerar $A$ el subconjunto de los números naturales $n$ para los que $x_n$ está definido. Claramente, $0 \in A$ y si $n \in A$ entonces $n + 1 \in A$, luego $A = \mathbb{N}$).

Esta forma de definir sucesiones se llama recursiva, pues para obtener el valor de $x_n$ necesitamos el valor de $x_{n-1}$, que a su vez necesita el valor de $x_{n-2}$, y así, hasta $x_0$. Es decir, la sucesión recurre a la propia sucesión para obtener un valor determinado.

**Ejemplo 1.1.3.**

1. *Dado $a \in \mathbb{R}^*$, definimos la sucesión $x_n$ como sigue:*

   $$x_0 = 1$$
   $$x_{n+1} = a \cdot x_n$$

   *Es fácil comprobar que $x_n = a^n$.*

2. *Definimos la sucesión $x_n = 2^{n+1} - 1$. En este caso hemos dado explícitamente $x_n$ para cada $n \in \mathbb{N}$. Definimos ahora $y_n$ como sigue:*

   $$y_0 = 1$$
   $$y_{n+1} = y_n + 2^{n+1}$$

   *Que ha sido definida de forma recursiva.*

   *En el ejemplo 1.1.1 se ha comprobado que $x_n = y_n$ para todo $n \in \mathbb{N}$.*

3. *La sucesión $x_n = 1 + 2 + \cdots + n$ puede ser definida recursivamente como:*

   $$x_1 = 1 \qquad x_{n+1} = x_n + n + 1$$

   *También se podría comenzar con $x_0 = 0$.*

   *En el ejemplo 1.1.2 se comprueba que $x_n = \frac{n(n+1)}{2}$.*

4. *Podemos definir $n!$ de forma recursiva:*

   a) $0! = 1$
   b) $(n + 1)! = (n + 1) \cdot n!$

5. *Sea $m \in \mathbb{N}$. Definimos la sucesión:*

   $$x_0 = 0 \qquad x_{n+1} = x_n + m$$

   *Es fácil comprobar que $x_n = m \cdot n$ (hágase). Vemos entonces como definir el producto de números naturales a partir de las suma.*

Consideremos ahora la sucesión dada por

$$f_0 = 1 \quad f_1 = 1 \qquad f_n = f_{n-1} + f_{n-2}$$

Es fácil calcular los primeros términos de esta sucesión:

$f_2 = 1 + 1 = 2$; $f_3 = 1 + 2 = 3$; $f_4 = 2 + 3 = 5$; $f_5 = 3 + 5 = 8$

y así sucesivamente. Parece claro que está bien definido el valor de $f_n$ para cualquier $n \in \mathbb{N}$. Sin embargo, esta definición no se ajusta al método de recurrencia dado anteriormente (pues en este caso, para calcular un término es necesario recurrir a los dos términos anteriores, mientras que en el método dado anteriormente, únicamente necesitamos conocer el término anterior). Para subsanar este problema, veamos un nuevo principio de inducción.

**Teorema 1.1.2.** *[Segundo principio de inducción]*
*Sea $A$ un subconjunto de $\mathbb{N}$. Supongamos que se verifica:*

1. $0 \in A$.

2. *Para cualquier $n$, $\{0, 1 \cdots n-1\} \subseteq A \Longrightarrow n \in A$*

*Entonces $A = \mathbb{N}$.*

Formalmente, la primera condición no es necesaria, pues para $n = 0$ la segunda condición afirma $\emptyset \subseteq A \Longrightarrow 0 \in A$, y puesto que la primera parte es siempre cierta ($\emptyset \subseteq A$), la condición 2 implica que $0 \in A$. Sin embargo, en la práctica suele ser necesario comprobar que $0 \in A$.

Notemos también que si la condición 1 se cambia por una de la forma $0, 1, \cdots, k \in A$, la tesis del teorema sigue siendo cierta.

*Demostración:* Supongamos que $A \neq \mathbb{N}$. Entonces el conjunto $B = \mathbb{N} \setminus A$ es distinto del conjunto vacío. Por tanto, por el principio de buena ordenación tenemos que $B$ tiene un mínimo. Sea este $n_0$. Esto implica que $\{0, 1, \cdots, n_0 - 1\} \subseteq A$ (pues ninguno de sus elementos pertenece a $B$), luego por la condición 2 tenemos que $n_0 \in A$, lo que es imposible, pues $n_0 \in B$. Deducimos entonces que $A = \mathbb{N}$ ■

Este segundo principio puede usarse, tanto para definir sucesiones como para probar propiedades de los números naturales.

**Ejemplo 1.1.4.** *Sea $x_n$ la sucesión definida mediante*

$$x_0 = 1 \qquad x_{n+1} = \sum_{k=0}^{n} x_k$$

*Calculemos una fórmula general para $x_n$. Para esto, hallemos los primeros términos:*
$x_0 = 1$; $x_1 = x_0 = 1$; $x_2 = x_0 + x_1 = 1 + 1 = 2$; $x_3 = 1 + 1 + 2$; $x_4 = 1 + 1 + 2 + 4 = 8$; $x_5 = 1 + 1 + 2 + 4 + 8 = 16$.
*Parece ser que $x_n$ responde a la expresión*

$$x_n = \begin{cases} 1 & si \quad n = 0 \\ 2^{n-1} & si \quad n \geq 1 \end{cases}$$

*Comprobémosla por inducción, utilizando el segundo principio*

*Paso 1: El resultado es cierto para $n = 0$ y $n = 1$.*

*Paso 2: La hipótesis de inducción es*

$x_0 = 1;\ x_1 = 1;\ \cdots\ x_n = 2^{n-1}$
*A partir de esto tenemos que $x_{n+1} = 1+1+2+\cdots+2^{n-1} = 1+(1+2+\cdots+2^{n-1}) = 1+2^n-1 = 2^n$, como queríamos.*
*En esta demostración se ha sustituido $(1 + 2 + \cdots + 2^{n-1})$ por $2^n - 1$, algo que podemos hacer como vimos en el ejemplo 1.1.1*
*Podemos comprobar que realizar esta demostración usando el primer principio de inducción no es posible. Nuestra hipótesis de inducción sería que $x_n = 2^{n-1}$, y a partir de ella, tendríamos que demostrar que $x_{n+1} = 2^n$. Sin embargo, lo único que podemos hacer es*

$$x_{n+1} = x_0 + x_1 + \cdots + x_{n-1} + x_n = x_0 + x_1 + \cdots + x_{n-1} + 2^{n-1}$$

*y puesto que nuestra hipótesis no nos dice nada del valor de $x_{n-1}$, $x_{n-2}$, etc., no podemos demostrar concluir que $x_{n+1} = 2^n$.*

## 1.2. Representación de números naturales. Sistemas de numeración

Comenzamos esta sección con un resultado de todos conocidos.

**Teorema 1.2.1.** *[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:*
$a = bc + r$ *y* $r < b$.

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 $b$.

*Demostración:* Sea $b \neq 0$. Demostremos, en primer lugar, la existencia de $c$ y $r$ para cualquier $a \in \mathbb{N}$. Esta demostración la haremos usando el primer principio de inducción.
Para $a = 0$ el resultado es cierto. Basta tomar $c = r = 0$.
Supongamos que $a = bc' + r'$ con $r' < b$. Entonces $a + 1 = bc' + (r' + 1)$. Dado que $r' < b$ se tiene que $r' + 1 \leq b$. Pueden ocurrir dos cosas:

a) $r + 1 < b$. Entonces tomamos $c = c'$ y $r = r' + 1$, y se tiene que $a + 1 = bc + r$ y $r < b$.

b) $r + 1 = b$. Tomamos $c = c' + 1$ y $r = 0$. Claramente, $a + 1 = bc + r$ y $r < b$.

Para ver la unicidad razonamos como sigue:
Supongamos que $a = bc + r = bc' + r'$ con $r, r' < b$. Entonces:
- Si $r = r'$, $bc = bc'$ y al ser $b \neq 0$ deducimos que $c = c'$.
- Si $r \neq r'$ podemos suponer $r < r'$, de donde se deduce que $0 < r' - r < b$ de donde $0 < r' - r = b(c - c') < b$, y esto último no es posible, ya que $b(c - c') \geq b$, ya que al ser $c - c' \neq 0$ se tiene que $c - c' \geq 1$). ■

**Definición 2.** *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*

$$a = b \cdot (a \ div \ b) + (a \ mód \ b); \qquad a \ mód \ b < b$$

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 1.2.1.** *Se tiene que* $13 \ mód \ 3 = 1$ *y* $13 \ div \ 3 = 4$, *pues* $13 = 3 \cdot 4 + 1$.

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 pueden 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 1.2.2.** *Sean $a, b \in \mathbb{N}$ con $a \neq 0$ y $b \geq 2$. Entonces existen únicos $m \in \mathbb{N}$ y $a_0, a_1 \cdots, a_m \in \mathbb{N}$ tales que:*

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

*Demostración:* Haremos la demostración de existencia por inducción en $a$, usando el segundo principio de inducción. La unicidad se deja como ejercicio.

El paso inicial consiste en este caso en probarlo para $a = 1, 2, \cdots, b-1$. En estos casos basta tomar $m = 0$ y $a_0 = a$.

Sea ahora $a \in \mathbb{N}$, con $a \geq b$. La hipótesis de inducción nos garantiza, para cualquier $c < a$, $c \neq 0$, que se satisface la tesis del teorema.

Por el teorema 1.2.1 existen $c, r$ tales que $a = bc + r$ y $r < b$. Además, por ser $a \geq b$ tenemos que $c \neq 0$, y al ser $b \geq 2$ se tiene que $c < a$. Le aplicamos a este número $c$ la hipótesis de inducción y obtenemos la existencia de un número $k \in \mathbb{N}$ y números $c_0, \cdots, c_k$ tales que $c_k \neq 0$, $c = c_k b^k + \cdots + c_1 b + c_0$ y $c_i < b$.

Tomamos ahora $m = k + 1$, $a_0 = r$ y $a_i = c_{i-1}$ para $1 \leq i \leq m$ y se tiene que:

$$a = bc + r = b(c_k b^k + \cdots c_1 b + c_0) + r = c_k b^{k+1} + \cdots + c_1 b^2 + c_0 b + r = a_m b^m + \cdots + a_1 b + a_0$$

Además, $a_m = c_k \neq 0$, $a_0 = r < b$ y $a_{i+1} = c_i < b$. ■

**Ejemplo 1.2.2.** *Tomemos, por ejemplo, $b = 5$ y hallemos los distintos números que nos aparecen en el teorema para diferentes valores de $a$.*

$a = 3$. *En este caso, al ser $a < b$ tomamos $m = 0$ y $a_0 = a$.*

$a = 17$. *Dividimos 17 entre 5; $17 = 5 \cdot 3 + 2$, luego $a_0 = r = 2$ y el resto de los números los hallamos de los obtenidos para $c = 3$. Aquí $m = 0 + 1$ y $a_1 = 3$. Fácilmente se comprueba que $17 = 3 \cdot 5 + 2$.*

$a = 89$. *Dividimos nuevamente entre 5, y obtenemos $89 = 17 \cdot 5 + 4$. Por tanto $a_0 = 4$ y el resto lo obtenemos a partir de lo hallado para 17. Por tanto, $k = 1 + 1 = 2$, $a_1 = c_0 = 2$ y $a_2 = c_1 = 3$. Se observa como $89 = 3 \cdot 5^2 + 2 \cdot 5 + 4$.*

$a = 441$. *Se tiene que $446 = 5 \cdot 89 + 1$, luego $a_0 = 1$, $m = 2 + 1 = 3$, $a_1 = c_0 = 4$, $a_2 = c_1 = 2$ y $a_3 = c_2 = 3$. Ahora se ve como $446 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$.*

**Definición 3.** *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 esto es posible).
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 decimal, salvo que el contexto deje suficientemente claro la base en que estamos trabajando.

**Ejemplo 1.2.3.**

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*

$$446 = (3241)_5$$

*Si analizamos como se obtuvo esta expresión podemos notar que la cifra de la derecha es el resto de dividir* $446$ *entre* $5$*, mientras que el resto de las cifras resultan de la expresión de* $89 = 446$ *div* $5$ *en base* $5$*, por tanto la segunda cifra por la derecha es el resto de dividir* $89$ *entre* $5$*, y así sucesivamente.*

*Por tanto, para expresar un número en base* $b$*, lo dividimos entre* $b$ *y tomamos el resto. El cociente de la división lo dividimos entre* $b$ *y volvemos a tomar el resto, y así, hasta que el cociente sea menor que* $b$*. En el ejemplo anterior se procedería como sigue:*

$$446 = 5 \cdot 89 + 1$$
$$89 = 5 \cdot 17 + 4$$
$$17 = 5 \cdot 3 + 2$$

*Tomando los restos y el último cociente tenemos las cifras que forman el número* $446$ *en base* $5$*.*

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

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

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

*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.*

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

*Realizamos las divisiones por* $8$ *hasta obtener un cociente menor que* $8$

$$5746772 = 8 \cdot 718346 + 4$$
$$718346 = 8 \cdot 89793 + 2$$
$$89703 = 8 \cdot 11224 + 1$$
$$11224 = 8 \cdot 1403 + 0$$
$$1403 = 8 \cdot 175 + 3$$
$$175 = 8 \cdot 21 + 7$$
$$21 = 8 \cdot 2 + 5$$

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

*Para expresar un número en base* $16$ *necesitamos* $16$ *símbolos. Emplearemos los números* $0, 1, \cdots, 9$ *junto con las letras* $A, B, C, D, E, F$*. Estas últimas representan los números* $10, 11, 12, 13, 14, 15$ *respectivamente.*

*Realizamos a continuación las divisiones por* $16$*.*

$$5746772 = 16 \cdot 359173 + 4$$
$$359173 = 16 \cdot 22448 + 5$$
$$22448 = 16 \cdot 1403 + 0$$
$$1403 = 16 \cdot 87 + 11$$
$$87 = 16 \cdot 5 + 7$$

*luego* $(10101111011000001010100)_2 = (57B054)_{16}$

*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*.*

$$\underbrace{1\,0}_{2}\underbrace{1\,0\,1}_{5}\underbrace{1\,1\,1}_{7}\underbrace{0\,1\,1}_{3}\underbrace{0\,0\,0}_{0}\underbrace{0\,0\,1}_{1}\underbrace{0\,1\,0}_{2}\underbrace{1\,0\,0}_{4} \qquad \underbrace{101}_{5}\underbrace{0111}_{7}\underbrace{1011}_{B}\underbrace{0000}_{0}\underbrace{0101}_{5}\underbrace{0100}_{4}$$

*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* $b=5$*.*

## 1.3. Números enteros. Divisibilidad

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 $| \ | : \mathbb{Z} \to \mathbb{N}$ 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, $-b \leq a \leq b$.

El teorema 1.2.1 tiene ahora una versión para los números enteros.

**Teorema 1.3.1.** *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 1.3.1.**

$a = 86$, $b = 15$. $\quad 86 = 15 \cdot 5 + 11$

$a = 86$, $b = -15$. $\quad 86 = (-15) \cdot (-5) + 11$

$a = -86$, $b = 15$. $\quad -86 = 15 \cdot (-6) + 4$

$a = -86$, $b = -15$. $\quad -86 = (-15) \cdot (-6) + 4$

Al igual que se hizo con los números naturales, podemos ahora, dados $a, b \in \mathbb{Z}$, con $b \neq 0$ definir los números $a$ div $b$ y $a$ mód $b$ como el cociente y el resto de la división de $a$ entre $b$ respectivamente. Nótese que $a$ mód $b = a$ mód $-b$ para cualquier $b \in \mathbb{Z}^*$.

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

**Definición 4.** *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, $b$ mód $a = 0$.

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 5.** *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".

Nótese también 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 $mcd(a, b)$ al único máximo común divisor de $a$ y $b$ que pertenece a $\mathbb{N}$.

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 6.** *Sean $a, b$ dos números enteros. Se dice que $m$ es un máximo común divisor 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. $mcd(a, b) = mcd(a, -b) = mcd(-a, b) = mcd(-a, -b) = mcd(|a|, |b|)$.
2. $mcd(a, 0) = |a|$ y $mcd(a, 1) = 1$

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

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

*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 $d|b$, 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).

**Corolario 1.3.1.** *Sean $a, b \in \mathbb{Z}$, con $a \neq 0$. Entonces $mcd(a,b) = mcd(b, a \text{ mód } b)$.*

**Algoritmo de Euclides para el cálculo del máximo común divisor.**

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

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

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

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

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 $mcd(a,b) = r_k$ (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: $d = mcd(a,b)$
    $(a,b) := (|a|, |b|)$
    Mientras $b \neq 0$
        $(a,b) := (b, a \text{ mód } b)$

Devuelve $a$

**Ejemplo 1.3.2.** *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 1.3.2.** *[Identidad de Bezout] Sean* $a, b \in \mathbb{Z}$ *y* $d = mcd(a,b)$. *Entonces existen* $u, v \in \mathbb{Z}$ *tales que* $d = au + bv$.

*Demostración:* Sabemos que para el cálculo del máximo común divisor de $a$ y $b$ podemos realizar una serie de divisiones

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

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

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

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 como encontrar los coeficientes $u$ y $v$.

**Ejemplo 1.3.3.** *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 funciónde* 1005 *y* 450.

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

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

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

$30 = 15 \cdot 2 + 0$

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

*Estos datos pueden ser ordenados como sigue:*

| $a$ | $b$ | $r$ | $c$ | $u$ | $v$ |
|---|---|---|---|---|---|
| | | | | *1* | *0* |
| | | | | *0* | *1* |
| *1005* | *450* | *105* | *2* | *1* | *-2* |
| *450* | *105* | *30* | *4* | *-4* | *9* |
| *105* | *30* | *15* | *3* | *13* | *-29* |
| *30* | *15* | *0* | | | |

Donde los valores iniciales son las dos primeras filas, así como los dos primeros elementos de la tercera fila. Es claro como se obtiene la tercera y cuarta columnas a partir de las dos primeras. También es claro como un elemento de la primera columna coincide con el elemento de la segunda columna de la fila superior. De la misma forma se obtiene la segunda columna. Por último, para obtener un elemento de la columna quinta, se toma el que está en su misma fila y en la columna cuarta, se multiplica por el que está inmediatamente encima de él y el resultado se le resta al que está dos posiciones encima suya. De forma análoga se completa la sexta columna.

Veamos un algoritmo que 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: $(d, u, v)$: $d = mcd(a, b)$; $d = au + bv$
  Si $b = 0$
    Devuelve $(a, 1, 0)$;
    Fin
  $(x, u) := (1, 0)$
  $(y, v) := (0, 1)$
  $r := a$ mód $b$
  Mientras $r \neq 0$
    $c := a$ div $b$
    $(x, u) := (u, x - u \cdot c)$
    $(y, v) := (v, y - v \cdot c)$
    $(a, b) := (b, r)$
    $r := a$ mód $b$
  Devuelve $(b, u, v)$
  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 $-1$.

Una consecuencia inmediata del teorema 1.3.2 es el siguiente corolario:

**Corolario 1.3.2.** *Sean $a, b \in \mathbb{Z}$. Entonces existen $u, v \in \mathbb{Z}$ tales que $1 = au + bv$ si, y sólo si, $mcd(a, b) = 1$.*

*Demostración:* El teorema de Bezout nos dice que si $mcd(a, b) = 1$ 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:

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

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

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

**Corolario 1.3.3.** *Sean $a, m, n \in \mathbb{Z}$. Entonces $mcd(a, mn) = 1$ si, y sólo si, $mcd(a, m) = 1$ y $mcd(a, n) = 1$.*

*Demostración:* Si $mcd(a, mn) = 1$ 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 $mcd(a, m) = mcd(a, n) = 1$.

Recíprocamente, supongamos que $mcd(a, m) = mcd(a, n) = 1$. 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

$$1 = au_m + mv_m(au_n + nv_n) = a(u_m + mv_m u_n) + mn(v_m v_n)$$

lo que nos dice que $mcd(a, mn) = 1$. ■

**Corolario 1.3.4.** *Sean $a, b, c \in \mathbb{Z}$. Si $a|(bc)$ y $mcd(a, b) = 1$ 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 1.3.2.** *Sean $a, b \in \mathbb{Z}$. Si $mcd(a, b) = 1$ 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 1.3.1.** *Sean $a, b \in \mathbb{N}$ y $d = mcd(a, b)$. Entonces $mcm(a, b) = \frac{ab}{d}$.*

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

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

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

■

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

**Ejemplo 1.3.4.** *Sabemos que $mcd(4, 6) = 2$. Por tanto, $mcm(4, 6) = \frac{24}{2} = 12$.*

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

## 1.4. 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 derecha es múltiplo de 2, y el miembro de la izquierda 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 $d \not| 135$.

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 $d=mcd(a,b)$. 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 1.4.1.** *Sean $a,b,c\in\mathbb{Z}$ y $d=mcd(a,b)$. Entonces la ecuación*

$$ax+by=c$$

*tiene solución entera si, y sólo si, $d|c$*

*Demostración:* La condición necesaria ($ax+by=c$ tiene solución $\Longrightarrow$ $d|c$) es fácil de probar.

Veamos la condición suficiente (nos garantiza la existencia de solución).

Supongamos que $d|c$. Sea $z=\frac{c}{d}$

Por el teorema de Bezout, existen $u$ y $v$ tales que $d=au+bv$. Multiplicamos ambos miembros por $z$, y obtenemos que

$$c=dz=(au+bv)z=a(uz)+b(vz)$$

luego $x=uz$ e $y=vz$ es una solución de la ecuación. ■

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 encontrar una.

**Ejemplo 1.4.1.** *Vamos a encontrar, si es posible, una solución a la ecuación* $105x+465y=195$.

*Calculamos el máximo común divisor de* 105 *y* 465.

| $a$ | $b$ | $r$ | $c$ | $u$ | $v$ |
|---|---|---|---|---|---|
| | | | | *1* | *0* |
| | | | | *0* | *1* |
| *105* | *465* | *105* | *0* | | |
| *465* | *105* | *45* | *4* | | |
| *105* | *45* | *15* | *2* | | |
| *30* | *15* | *0* | | | |

*Vemos que* $mcd(105,465)=15$*, que divide a* 195 *(pues* $195=15\cdot 13$*). Completamos entonces la tabla*

| $a$ | $b$ | $r$ | $c$ | $u$ | $v$ |
|---|---|---|---|---|---|
| | | | | *1* | *0* |
| | | | | *0* | *1* |
| *105* | *465* | *105* | *0* | *1* | *0* |
| *465* | *105* | *45* | *4* | *-4* | *1* |
| *105* | *45* | *15* | *2* | *9* | *-2* |
| *30* | *15* | *0* | | | |

*luego* $15=105\cdot 9-465\cdot 2$*. Multiplicamos por* 13 *y nos queda*

$$195=105\cdot 117-465\cdot 26$$

*Por tanto una solución es* $x=117$*,* $y=-26$.

Sabemos ya, dada una ecuación de la forma $ax+by=c$ decidir si tiene o no solución, y en caso afirmativo, encontrar una. Sin embargo, cuando existe una solución a esta ecuación pueden encontrarse otras más. Así, por ejemplo, tenemos que

$$195=105\cdot 117-465\cdot 26 \qquad 195=105\cdot 86-465\cdot 19 \qquad 195=105\cdot 55-465\cdot 12$$
$$195=105\cdot 24-465\cdot 5 \qquad 195=105\cdot(-7)+465\cdot 2 \qquad 195=105\cdot 148-465\cdot 33$$

**Proposición 1.4.2.** *Sean $a, b, c \in \mathbb{Z}$ y $d = mcd(a, b)$. Supongamos que $x_0$, $y_0$ es una solución de la ecuación $ax + by = c$. Entonces todas las soluciones de esta ecuación son:*

$$\begin{array}{rcl} x & = & x_0 + k\,\frac{b}{d} \\ y & = & y_0 - k\,\frac{a}{d} \end{array} \qquad k \in \mathbb{Z}$$

*Demostración:* Se tiene que $a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = ax_0 + ak\frac{b}{d} + by_0 - bk\frac{a}{d} = ax_0 + by_0 + ak\frac{b}{d} - bk\frac{a}{d} = c$, 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 $mcd(a', b') = 1$ (¿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 1.4.2.** *Una solución de la ecuación $105x + 465y = 195$ es $x_0 = 117$ e $y_0 = -26$. Todas las soluciones de esta ecuación son entonces*

$$\begin{array}{l} x = 117 + 31k \\ y = -26 - 7k \end{array} \qquad k \in \mathbb{Z}$$

*Si la damos distintos valores a $k$ obtenemos distintas soluciones:*

$k = 1$*:* $\quad x = 148, \quad y = -33.$
$k = 2$*:* $\quad x = 179, \quad y = -40.$
$k = -1$*:* $\quad x = 86, \quad y = -19.$
$k = -4$*:* $\quad x = -7, \quad y = 2.$

## 1.5. 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 7.** *Sea $p$ un número entero distinto de 0, 1 y $-1$. Se dice que $p$ es irreducible si sus únicos divisores son $\pm 1$ y $\pm p$.*

**Ejemplo 1.5.1.** *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 1.5.1.** *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 1.5.2.** *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 $p|ab \implies p|a$ 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 $mcd(p, a) = 1$. El corolario 1.3.4 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 $a_1, a_2, \cdots, a_n \in \mathbb{Z}$ tales que $p|(a_1 a_2 \cdots a_n)$ entonces existe $i \in \{1, 2, \cdots, n\}$ tal que $p|a_i$.

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

**Teorema 1.5.1 (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:* Demostremos en primer lugar la existencia de la factorización. Esto lo haremos haciendo uso del segundo principio de inducción.

El primer paso consiste en demostrarlo para $a = 2$. Pero como 2 es primo, el resultado es cierto en ese caso.

La hipótesis de inducción afirma que el resultado es cierto para todo $c < a$. Bajo esa hipótesis hemos de demostrar el resultado para $a$.

Si $a$ es primo, ya tenemos que el resultado es cierto.

Si $a$ no es primo, entonces tendrá un divisor que no será ni $a$ ni 1 (ni $-a$ ni $-1$). Supongamos que es $b$, y además lo tomamos perteneciendo a $\mathbb{N}$. Se tiene entonces que $a = bc$, y ambos números $b$ y $c$ son menores que $a$. Por la hipótesis de inducción $b$ se expresa como producto de primos ($b = p_1 \cdots p_s$) y $c$ también ($c = q_1 \cdots q_s$). Por tanto $a = p_1 \cdots p_s q_1 \cdots q_s$. Es decir, $a$ es producto de números primos.

Demostremos ahora la unicidad. Esta demostración también se hará por inducción.

Para $a = 2$ el resultado es trivialmente cierto.

La hipótesis de inducción dice ahora que todo número $c < a$ se expresa de forma única como producto de números primos.

Supongamos que tenemos dos factorizaciones del número $a$ como producto de números primos positivos:

$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$.

Entonces se tiene que $p_1|(q_1 \cdots q_s)$, y por ser $p_1$ primo, debe existir algún $i$ tal que $p_1|q_i$. Reordenamos los primos $q_1, \cdots, q_s$ para que el primo al que divida $p_1$ sea el primero (es decir, $p_1|q_1$). Como $q_1$ es primo, entonces $p_1 = q_1$. Tenemos entonces que $\frac{a}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$. Por hipótesis de inducción, los primos que aparecen en la primera factorización de $\frac{a}{p_1}$ son los mismos que aparecen en la segunda.

■

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

De esta forma es fácil comprobar que el conjunto

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

es el conjunto de todos los divisores positivos de $a$.

**Ejemplo 1.5.3.** *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,*

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

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

**Proposición 1.5.2.** *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:*

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

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

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

**Ejemplo 1.5.4.** *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*

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

## 1.6. Clases residuales módulo m

En esta sección vamos a construir, para cada $m \geq 2$ los conjuntos $\mathbb{Z}_m$, de los que estudiaremos su aritmética.

**Definición 8.** *Sean $a, b, m \in \mathbb{Z}$. Se dice que $a$ es congruente con $b$ módulo $m$, y se escribe $a \equiv b(mód\ m)$ ó $a \equiv_m b$, si $m|(b-a)$. Es decir:*

$$a \equiv b(mód\ m) \text{ si existe } k \in \mathbb{Z} \text{ tal que } b - a = km$$

Nótese que $a \equiv b(\text{mód } m)$ si, y sólo si, $a \equiv b(\text{mód } -m)$. Por tanto, al hablar de congruencias módulo $m$ podemos suponer que $m \in \mathbb{N}$.

Además, la relación de congruencia módulo 0 es la relación de igualdad ($a \equiv b(\text{mód } 0)$ si, y sólo si, $a = b$) que no nos aporta nada nuevo. En la relación de congruencia módulo 1 todos los elementos están relacionados con todos los elementos, luego también carece de interés. Nos centraremos entonces en módulos $m$ que sean mayores que 1.

**Ejemplo 1.6.1.** *Claramente, $5 \equiv 17(mód\ 4)$ pues $17 - 5$ es múltiplo de 4. De la misma forma $5 \equiv 17(mód\ 6)$. Sin embargo $5 \not\equiv 15(mód\ 8)$ pues $17 - 5$ no es múltiplo de 8.*

**Proposición 1.6.1.** *Dado $m \geq 2$. Entonces la relación $\equiv_m$ es una relación de equivalencia.*

*Demostración:* Hemos de demostrar que la relación es reflexiva, simétrica y transitiva.

- Reflexiva: Dado que $0 = a - a$ es múltiplo de $m$ tenemos que para cualquier $a \in \mathbb{Z}$ se verifica que $a \equiv a(\text{mód } m)$.

- Simétrica: Supongamos que $a \equiv b(\text{mód } m)$. Entonces $m|(b-a)$, luego $m|(a-b)$, es decir, $b \equiv a(\text{mód } m)$.

- Transitiva:

$$\left.\begin{array}{rcl} a \equiv b(\text{mód } m) & \Longrightarrow & m|(b-a) \\ b \equiv c(\text{mód } m) & \Longrightarrow & m|(c-b) \end{array}\right\} \Longrightarrow m|[(b-a)+(c-b)] \Longrightarrow m|(c-a) \Longrightarrow a \equiv c(\text{mód } m)$$

■

Como ejercicio se pide probar que $a \equiv b(\text{mód } m)$ si, y sólo si, $a \text{ mód } m = b \text{ mód } m$.

Puesto que para cada $m$ la relación $\equiv_m$ es de equivalencia, podemos considerar el conjunto cociente. Este conjunto será denotado por $\mathbb{Z}_m$. La clase de un número entero $a$ en $\mathbb{Z}_m$ será denotada por $[a]_m$ o simplemente $[a]$.

Veamos a continuación qué conjunto es $\mathbb{Z}_m$.

**Ejemplo 1.6.2.**

*Comenzemos con el conjunto $\mathbb{Z}_2$. Para ello calculemos las clases de equivalencia.*

$$[0]_2 = \{a \in \mathbb{Z} : 0 \equiv a(\textit{mód } 2)\}$$

*Ahora bien, $0 \equiv a(\textit{mód } 2)$ si, y sólo si, $2|(a-0)$, es decir, $[0]_2$ está constituida por todos los números múltiplos de 2 (números pares)*

*De la misma forma se tiene que*

$$[1]_2 = \{a \in \mathbb{Z} : 1 \equiv a(\textit{mód } 2)\} = \{a \in \mathbb{Z} : a \textit{ mód } 2 = 1 \textit{ mód } 2\}$$

*es decir, los números impares.*

*Se tiene entonces que*

$$[0]_2 = \{\cdots, -4, -2, 0, 2, 4, 6, \cdots\} \qquad [1]_2 = \{\cdots, -5, -3, -1, 1, 3, 5 \cdots\}$$

*Y como todo número entero pertenece a $[0]_2$ o a $[1]_2$ deducimos que $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$.*

*De la misma forma se comprueba que*

$$[0]_3 = \{\cdots, -6, -3, 0, 3, 6, \cdots\} \quad [1]_3 = \{\cdots, -5, -2, 1, 4, 7, \cdots\} \quad [2]_3 = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$$

*y que $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$*

*En general, dado $m \geq 2$ y $r$ tal que $0 \leq r < m$ se verifica que*

$$[r]_m = \{a \in \mathbb{Z} : a \textit{ mód } m = r\}$$

*es decir, en la clase de $r$ están los números enteros que al dividir por $m$ da resto $r$, y puesto que al dividir un número entre $m$ el resto sólo puede tomar los valores $0, 1, \cdots, m-1$ deducimos que*

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \cdots, [m-1]_m\}$$

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

**Lema 1.6.1.** *Sean $a, b, c, d \in \mathbb{Z}$ y $m \geq 2$. Entonces:*

1. $\left.\begin{array}{l} a \equiv c(\textit{mód } m) \\ b \equiv d(\textit{mód } m) \end{array}\right\} \Longrightarrow a + b \equiv c + d(\textit{mód } m)$

2. $\left.\begin{array}{l} a \equiv c(\textit{mód } m) \\ b \equiv d(\textit{mód } m) \end{array}\right\} \Longrightarrow ab \equiv cd(\textit{mód } m)$

*Demostración:*

1. $$\left.\begin{array}{rcl} a \equiv c(\text{mód } m) & \Longrightarrow & m|(c-a) \\ b \equiv d(\text{mód } m) & \Longrightarrow & m|(d-b) \end{array}\right\} \Longrightarrow m|(c-a+d-b) \Longrightarrow m|(c+d-(a+b))$$
$$\Longrightarrow a + b \equiv c + d(\text{mód } m)$$

2.
$$\left.\begin{array}{lllll} a \equiv c(\text{mód } m) & \Longrightarrow & m|(c-a) & \Longrightarrow & m|(c-a)b \\ b \equiv d(\text{mód } m) & \Longrightarrow & m|(d-b) & \Longrightarrow & m|c(d-b) \end{array}\right\} \begin{array}{ll} \Longrightarrow & m|[c(d-b)+(c-a)b] \\ \Longrightarrow & m|(cd-ab) \\ \Longrightarrow & ab \equiv cd(\text{mód } m) \end{array}$$

■

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

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

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

**Ejemplo 1.6.3.** *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 $23$) 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

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

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 1.6.2.** *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 1.6.4.** *Veamos las tablas de suma y producto en $\mathbb{Z}_5$ y $\mathbb{Z}_6$.*

| $+$ | $0$ | $1$ | $2$ | $3$ | $4$ |
|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ | $3$ | $4$ |
| $1$ | $1$ | $2$ | $3$ | $4$ | $0$ |
| $2$ | $2$ | $3$ | $4$ | $0$ | $1$ |
| $3$ | $3$ | $4$ | $0$ | $1$ | $2$ |
| $4$ | $4$ | $0$ | $1$ | $2$ | $3$ |

| $\cdot$ | $0$ | $1$ | $2$ | $3$ | $4$ |
|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $3$ | $4$ |
| $2$ | $0$ | $2$ | $4$ | $1$ | $3$ |
| $3$ | $0$ | $3$ | $1$ | $4$ | $2$ |
| $4$ | $0$ | $4$ | $3$ | $2$ | $1$ |

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

| $\cdot$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ |
|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ |
| $2$ | $0$ | $2$ | $4$ | $0$ | $2$ | $4$ |
| $3$ | $0$ | $3$ | $0$ | $3$ | $0$ | $3$ |
| $4$ | $0$ | $4$ | $2$ | $0$ | $4$ | $2$ |
| $5$ | $0$ | $5$ | $4$ | $3$ | $2$ | $1$ |

**Definición 10.** *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 1.6.5.**

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, $ab = ac \Longrightarrow b = c$). 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 1.6.6.**

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

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

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

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 $mcd(a, n) = mcd(a + kn, n)$, 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 1.3.2 nos dice ahora que $mcd(a, n) = 1$.

En cuanto a la condición suficiente, suponemos que $mcd(a, n) = 1$. 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 necesesaria 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 1.6.7.** *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* $4^{-1} = 3$.

Veamos a continuación un algoritmo, basado en el algoritmo BEZOUT para determinar si un elemento de $\mathbb{Z}_n$ tiene o no inverso, y en caso afirmativo, calcularlo.

Algoritmo INVERSO$(n, a)$
Entrada: $n, a \in \mathbb{Z} : n \geq 2$
Salida: $u$: $u = a^{-1}$ en $\mathbb{Z}_n$ (si existe)
    $(y, v) := (0, 1)$
    $r := n$ mód $a$
    Mientras $r \neq 0$
        $c := n$ div $a$
        $(y, v) := (v, y - v \cdot c)$
        $(n, a) := (a, r)$
        $r := n$ mód $a$
    Si $a \neq 1$
        Devuelve "No existe inverso"
        Fin
    Devuelve $a$
    Fin

**Ejemplo 1.6.8.** *Vamos a estudiar si* 391 *tiene inverso en* $\mathbb{Z}_{1542}$*, y en caso afirmativo vamos a calcularlo.*

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

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

Antes de teminar la sección estudiaremos la función $\varphi$ de Euler.

**Definición 11.** *Sea* $m \geq 2$ *Se define* $\varphi(m)$ *como el número de elementos del conjunto* $\{0, 1, 2, \cdots, m-1\}$ *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 $\varphi : \mathbb{N} \setminus \{0, 1\} \to \mathbb{N}$. Esta aplicación se conoce como la aplicación $\varphi$ de Euler.

**Ejemplo 1.6.9.** *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* $mcd(a, p) = 1$*. 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 $mcd(m,n) = 1$ entonces $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

La primera propiedad es fácil de justificar. Es fácil ver que $mcd(a, p^n) \neq 1$ si, y sólo si, $p|a$. Por tanto, los elementos del conjunto $\{1, 2, \cdots, p^n - 1, p^n\}$ que son primos relativos con $p$ son exactamente los que no son múltiplos de $p$. Puesto que en $\{1, 2, \cdots, p^n - 1, p^n\}$ hay exactamente $p^{n-1}$ múltiplos de $p$ (los del conjunto $\{p \cdot 1, p \cdot 2, \cdots, p \cdot p^{n-1}\}$) deducimos que $\varphi(p^n) = p^n - p^{n-1}$.

La segunda propiedad la demostraremos más adelante.

Esta segunda propiedad se puede generalizar al siguiente caso:

Si $m_1, m_2, \cdots, m_k$ son números naturales tales que $mcd(m_i, m_j) = 1$ 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 1.6.10.**

1. *Puesto que* $12 = 2^2 3$ *se tiene que*
$$\varphi(12) = \varphi(2^2 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2) \cdot (3 - 1) = 4$$
2. $30 = 2 \cdot 3 \cdot 5$, *luego* $\varphi(30) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = (2-1)(3-1)(5-1) = 8$.
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 1.6.1 (Euler-Fermat).** *Sea* $a \in \mathbb{Z}$, $m \in \mathbb{N}^*$ *tales que* $mcd(a, m) = 1$. *Entonces* $a^{\varphi(m)} \equiv 1 (mód\ m)$.

*Demostración:* Nótese que lo que decir que $mcd(a, m) = 1$ 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 $f : \mathcal{U}(\mathbb{Z}_m) \to \mathcal{U}(\mathbb{Z}_m)$ 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 $\mathcal{U}(\mathbb{Z}_m) = \{x_1, x_2, \cdots, x_{\varphi(m)}\}$ entonces se tiene que

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

Por tanto, $x_1 x_2 \cdots x_{\varphi(m)} = (ax_1)(ax_2) \cdots (ax_{\varphi(m)}) = a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)}$, y puesto que todo lo que interviene en el producto son unidades podemos simplificar y nos queda $a^{\varphi(m)} = 1$. ■

**Ejemplo 1.6.11.**

1. *Se tiene que* $\varphi(5) = 4$. *Por tanto* $2^4 \equiv 1 (mód\ 5)$.
2. $\varphi(7) = 6$ *luego* $3^6 \equiv 1 (mód\ 7)$, *o* $4^6 \equiv 1 (mód\ 7)$.
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*
$$4^{1000} = 4^{3 \cdot 333} 4^1 = (4^3)^{333} 4 = 1^{166} 4 = 4$$

## 1.7. 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.

Nos limitaremos a aquellas congruencias en las que la incógnita aparece en expresiones de grado 1. El caso más simple es la congruencia

$$x \equiv a(\text{mód } m)$$

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 ecuación $x \equiv 2(\text{mód } 5)$ 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 congruencias, diremos que son equivalentes si ambas tienen las mismas soluciones.

Puesto que las congruencias con las que vamos a trabajar son de grado 1, sólo veremos congruencias de la forma

$$ax + b \equiv cx + d(\text{mód } m)$$

Fácilmente se ve que esta congruencia es equivalente a $(a - c)x \equiv d - b(\text{mód } m)$, por lo que nos limitaremos a congruencias de la forma $ax \equiv b(\text{mód } m)$

Nuestro primer objetivo es, dada una congruencia de la forma $ax \equiv b(\text{mód } m)$, estudiar si tiene o no solución, y en caso afirmativo, transformarla en una equivalente a ella que sea de la forma $x \equiv c(\text{mód } n)$. 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 $ax \equiv b(\text{mód } m)$

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

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

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

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

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

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

   De la misma forma de demuestra que toda solución de $a'x \equiv b'(\text{mód } m)$ es solución de $ax \equiv b(\text{mód } m)$ ■

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

   $$29x \equiv 67(\text{mód } 7)$$

   es equivalente a la congruencia

   $$x \equiv 4(\text{mód } 7)$$

   pues $29 \equiv 1(\text{mód } 7)$ y $67 \equiv 4(\text{mód } 7)$.

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

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

   La otra parte se demuestra de forma análoga. ■

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

$$6x \equiv 14(\text{mód } 22) \quad \text{y} \quad 3x \equiv 7(\text{mód } 11)$$

son equivalentes.

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

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

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

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

   $$6x \equiv 16(\text{mód } 17)$$

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

   $$18x \equiv 48(\text{mód } 17)$$

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

   $$x \equiv 14(\text{mód } 17)$$

   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

   $$7x \equiv 5(\text{mód } 12)$$

   y multiplicamos por 2, obtenemos

   $$14x \equiv 10(\text{mód } 12)$$

   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 $mcd(c, m) = 1$, entonces las congruencias $ax \equiv b(\text{mód } m)$ y $\frac{a}{c}x \equiv \frac{b}{c}(\text{mód } m)$ son equivalentes.

   *Demostración:* Es semejante a la propiedad anterior. ■

**Proposición 1.7.1.** *Sean $a, b, m \in \mathbb{Z}$, con $m \geq 2$. Entonces la congruencia $ax \equiv b(\text{mód } m)$ tiene solución si, y sólo si, $mcd(a, m)|b$.*

*Demostración:* Supongamos que la congruencia tiene solución. Sea $x_0$ una tal solución. Entonces $ax_0 - b = km$ para algún $k \in \mathbb{Z}$. Entonces la pareja $(x_0, -k)$ es una solución a la ecuación diofántica $ax + my = b$. La proposición 1.4.1 nos dice que $mcd(a, m)|b$.

Recíprocamente, supongamos que $mcd(a, m)|b$. Entonces la ecuación $ax + my = b$ tiene solución. Sea $(x_0, y_0)$ una tal solución. En ese caso $x_0$ es una solución de $ax \equiv b(\text{mód } m)$. ■

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

- Reducimos $a$ y $b$ módulo $m$. Este paso no es necesario, pero puede facilitar los cálculos.

- Se comprueba si $mcd(a,m)|b$. Si la respuesta es negativa, entonces la congruencia no tiene solución. Si la respuesta es afirmativa, podemos dividir toda la congruencia por $mcd(a,m)$ (ver propiedad 2).

  Hemos transformado la congruencia en una de la forma $ax \equiv b(\text{mód } m)$, pero ahora se tiene que $mcd(a,m) = 1$.

- Buscamos el inverso de $a$ en $\mathbb{Z}_m$. Llamémoslo $u$.

- Multiplicamos ambos miembros de la congruencia por $u$. Por la propiedad 3 obtenemos una congruencia equivalente, y ésta adopta la forma $x \equiv c(\text{mód } m)$.

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

**Ejemplo 1.7.1.**

1. *La congruencia* $2x \equiv 3(\text{mód } 4)$ *no tiene solución, pues* $mcd(2,4) = 2$*, 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* $4x \equiv 2(\text{mód } 6)$ *sí tiene solución, pues* $mcd(4,6) = 2$ *y* $2|2$*. Dividimos entonces todo por* 2 *y obtenemos la congruencia* $2x \equiv 1(\text{mód } 3)$*. Puesto que* $2^{-1} = 2$ *(en* $\mathbb{Z}_3$*) la congruencia es equivalente a* $x \equiv 2(\text{mód } 3)$*, cuyas soluciones son* $x = 2 + 3k$*.*

3. *Vamos a resolver la congruencia* $48x \equiv 25(\text{mód } 15)$*. En primer lugar, reducimos módulo* 15*. La congruencia nos queda* $3x \equiv 10(\text{mód } 15)$*. Dado que* $mcd(3,15) = 3$*, y éste no divide a* 10 *la congruencia no tiene solución.*

4. *Resolvamos ahora* $27x \equiv 13(\text{mód } 10)$*.*

   *Reducimos todos los coeficientes módulo* 10*.*

   $$7x \equiv 3(\text{mód } 10)$$

   *Puesto que* $mcd(7,10) = 1$ *la congruencia tiene solución.*

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

   $$x \equiv 9(\text{mód } 10)$$

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

5. *Vamos a resolver la ecuación diofántica* $48x + 21y = 75$*. Para ello planteamos la congruencia*

   $$48x \equiv 75(\text{mód } 21)$$

   *Reducimos módulo* 21 *y nos queda* $6x \equiv 12(\text{mód } 21)$*.*

   *Dividimos todo por* $3 = mcd(6,21)$*:* $\quad 2x \equiv 4(\text{mód } 7)$*.*

   *Dividimos por* 2*:* $\quad x \equiv 2(\text{mód } 7)$*.*

   *Por tanto* $x = 2 + 7k$*. Hallemos el valor de* $y$*.*

   $$48(2+7k)+21y = 75 \Longrightarrow 16(2+7k)+7y = 25 \Longrightarrow 7y = 25-16(2+7k) \Longrightarrow 7y = -7-7\cdot 16k \Longrightarrow y = -1-16k$$

   *Las soluciones son entonces* $x = 2 + 7k; \ \ y = -1 - 16k$*.*

6. *Consideramos la congruencia* $6x \equiv 12(\text{mód } 27)$*. 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* $2x \equiv 4(\text{mód } 27)$*. En este caso tenemos que* 11 *no es solución, pues* $2 \cdot 11 - 4 = 18$ *que no es múltiplo de* 27*.*

7. *Obviamente, si partimos de la congruencia* $2x \equiv 4(\text{mód } 27)$ *y multiplicamos ambos miembros por* 3 *obtenemos una congruencia que no es equivalente.*

El siguiente algoritmo recoje 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: $(c, n)$: $x \equiv c(\text{mód } n)$ y $ax \equiv b(\text{mód } m)$ son equivalentes.
    $a := a$ mód $m$
    $b := b$ mód $m$
    $(d, u, v) := BEZOUT(a, m)$
    Si $b$ mód $d \neq 0$
        Devuelve "No tiene solución"
        Fin
    $(a, b, m) := (a \text{ div } d, m \text{ div } d, m \text{ div } d)$
    $c := a \cdot u$ mód $m$
    Devuelve $(c, m)$
    Fin

Nos planteamos a continuación como resolver sistemas de congruencias con una sola incógnita. Puesto que toda congruencia que tenga solución es equivalente a una de la forma $x \equiv a(\text{mód } m)$ nos planteamos resolver un sistema de la forma

$$\begin{aligned} x &\equiv a_1(\text{mód } m_1) \\ x &\equiv a_2(\text{mód } m_2) \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_p(\text{mód } m_p) \end{aligned}$$

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

**Ejemplo 1.7.2.**

1. *El sistema de congruencias*
$$\begin{aligned} x &\equiv 2(\textit{mód } 6) \\ x &\equiv 5(\textit{mód } 9) \end{aligned}$$
*tiene a* $x = 14$ *como una solución, pues* $14 - 2$ *es múltiplo de* $6$ *y* $14 - 5$ *es múltiplo de* $9$.

2. *El sistema*
$$\begin{aligned} x &\equiv 2(\textit{mód } 6) \\ x &\equiv 6(\textit{mód } 9) \end{aligned}$$
*no tiene solución, pues si* $x \equiv 6(\textit{mód } 9)$ *se tiene que* $x \equiv 0(\textit{mód } 3)$, *mientras que si* $x \equiv 2(\textit{mód } 6)$ *entonces* $x \equiv 2(\textit{mód } 3)$.

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

**Teorema 1.7.1 (Teorema chino del resto).** *Sean* $a_1, a_2, \cdots, a_p \in \mathbb{Z}$, *y* $m_1, m_2, \cdots, m_p \in \mathbb{N}^*$. *Supongamos que* $mcd(m_i, m_j) = 1$ *para* $i \neq j$. *Entonces el sistema de congruencias*

$$\begin{aligned} x &\equiv a_1(\textit{mód } m_1) \\ x &\equiv a_2(\textit{mód } m_2) \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_p(\textit{mód } m_p) \end{aligned}$$

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

$$x \equiv a(\textit{mód } M)$$

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

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

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

Se tiene entonces que $mcd(m_i, M_i) = 1$. Por el teorema 1.3.2, existen $u_i, v_i \in \mathbb{Z}$ tal que $m_i u_i + M_i v_i = 1$. Es claro entonces que

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

luego

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

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

$$b \equiv a(\text{mód } m_1) \quad b \equiv a(\text{mód } m_2) \quad \cdots \quad b \equiv a(\text{mód } m_p)$$

es decir,

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

lo que es equivalente a que $mcm(m_1, m_2, \cdots, m_p) | (b-a)$. Y como $mcm(m_1, m_2, \cdots, m_p) = M$, 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 $x \equiv a(\text{mód } M)$. ■

Nótese que el teorema chino del resto, lo que nos dice es que la aplicación $f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_p}$ dada por

$$f(x) = (x \text{ mód } m_1, x \text{ mód } m_2, \cdots x \text{ mód } m_p)$$

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 1.3.3) que la aplicación $f$ induce una biyección

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

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 $mcd(m_1, m_2) = 1$.

**Ejemplo 1.7.3.** *Consideramos el sistema:*

$$\begin{aligned} x &\equiv 1(\textit{mód } 2) \\ x &\equiv 2(\textit{mód } 5) \\ x &\equiv 3(\textit{mód } 7) \end{aligned}$$

*Es claro que* $mcd(2,5) = mcd(2,7) = mcd(5,7) = 1$. *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* $x \equiv -123(\textit{mód } 70)$, *que a su vez es equivalente a* $x \equiv 17(\textit{mód } 70)$. *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 (*$297 \equiv -123(\textit{mód } 70)$*).*

*En un ejemplo anterior hemos estudiado dos sistemas con dos congruencias en los que* $mcd(m_1, m_2) \neq 1$. *En un caso el sistema tiene solución y en el otro no.*

**Ejemplo 1.7.4.** *Consideramos la aplicación* $f : \mathbb{Z}_{18} \to \mathbb{Z}_2 \times \mathbb{Z}_9$ *dada por* $f(x) = (x \text{ mód } 2, x \text{ mód } 9)$.

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

*que claramente es una biyección, mientras que si definimos* $f : \mathbb{Z}_{18} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ *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.*

El teorema chino del resto nos proporciona una condición suficiente para que un sistema de congruencias tenga solución, y en caso afirmativo nos proporciona una forma de hallarla, como acabamos de ver. Sin embargo, cuando el sistema no se ajusta a las hipótesis del teorema no tenemos ninguna herramienta para determinar si tiene o no solución, y en caso de que la tenga, para resolverlo.

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 cuando lleguemos a una congruencia que no tiene solución.

Veamos algunos ejemplos.

1.

$$\left.\begin{array}{l} x \equiv 1(\text{mód } 2) \\ x \equiv 2(\text{mód } 5) \\ x \equiv 3(\text{mód } 7) \end{array}\right\}$$

| | | |
|---|---|---|
| $x \equiv 1(\text{mód } 2)$ | Calculamos las soluciones | $x = 1 + 2k_1$ |
| $x \equiv 2(\text{mód } 5)$ | Introducimos la solución | $1 + 2k_1 \equiv 2(\text{mód } 5)$ |
| | | $2k_1 \equiv 1(\text{mód } 5)$ |
| | Multiplicamos por $3 = 2^{-1}$ en $\mathbb{Z}_5$ | $k_1 \equiv 3(\text{mód } 5)$ |
| | | $k_1 = 3 + 5k_2$ |
| | Sustituimos | $x = 1 + 2(3 + 5k_2) = 7 + 10k_2$ |
| $x \equiv 5(\text{mód } 7)$ | Introducimos la solución | $7 + 10k_2 \equiv 3(\text{mód } 7)$ |
| | | $10k_2 \equiv -4(\text{mód } 7)$ |
| | Reducimos módulo 7 | $3k_2 \equiv 3(\text{mód } 7)$ |
| | Multiplicamos por $15 = 3^{-1}$ en $\mathbb{Z}_7$ | $k_2 \equiv 1(\text{mód } 7)$ |
| | | $k_2 = 1 + 7k_2$ |
| | Sustituimos | $x = 7 + 10(1 + 7k_2) = 17 + 70k_2$ |

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

2.

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

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

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

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

| | | |
|---|---|---|
| $x \equiv 2(\text{mód } 6)$ | Calculamos las soluciones | $x = 2 + 6k_1$ |
| $x \equiv 6(\text{mód } 9)$ | Introducimos la solución | $2 + 6k_1 \equiv 6(\text{mód } 9)$ |
| | | $6k_1 \equiv 4(\text{mód } 9)$ |

Y el sistema no tiene solución, pues $mcd(6, 9) = 3$, 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 $mcd(27, 100) = 1$ 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. Procedemos entonces como sigue:

- Calculamos $27^{3636}$ en $\mathbb{Z}_4$.
  En ese caso se tiene que $27 = 3$, y como $\varphi(4) = 2$ entonces $3^2 = 1$, luego $3^{3636} = 1$.
- 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:

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

- Resolvemos el sistema

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

$x = 1 + 4k_1$, 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:

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

Deducimos que las dos últimas cifras son 61.

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

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

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

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

$p \in \mathbb{N} : \ p \geq 2$
$a_1, \cdots, a_k, b_1, \cdots, b_k \in \mathbb{Z}$
$m_1, \cdots, m_k \in \mathbb{N}^*$

Salida: $(c, n)$.

El sistema

$a_1x \equiv b_1(\text{mód } m_1)$
$a_2x \equiv b_2(\text{mód } m_2)$
$\cdots\cdots\cdots\cdots$
$a_px \equiv b_p(\text{mód } m_p)$

y la congruencia $x \equiv c(\text{mód } n)$ son equivalentes.

$(c, n) :=$ CONGRUENCIA$(a_1, b_1, m_1)$
Desde $k = 2$ hasta $p$

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

$(u, v) :=$ CONGRUENCIA$(a_k, b_k, m_k)$

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

Devuelve $(c, n)$

Fin