Capítulo 2

Los Naturales y los Enteros.

Objetivos del capítulo

- Introducir los Números Naturales y los Números Enteros estudiando sus propiedades respecto de la suma, del producto y del orden. Especialmente el principio de inducción e inducción generalizado.
- Estudio y aplicación del algoritmo de la división. Existencia y unicidad del m. c. d y M. C. M. Teorema de Bezout y factorización única en $\mathbb{Z}$.
- Estudio de los anillos de congruencias módulo n.

---

1. Los Números Naturales y los Números enteros

1.1. Los Números Naturales

Definición 1 Los Números Naturales aparecen por la necesidad que tiene el hombre (primitivo) tanto de contar como de ordenar una cierta cantidad de objetos.

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

En los números naturales podemos sumar y multiplicar, pero no podemos, en la mayoría de los casos, ni restar ni dividir. Históricamente el cero no es considerado un número natural. Matemáticamente los naturales se definen a partir de 5 axiomas, los **Axiomas de Peano**:

1). El 1 es un número natural.

2). Para cada número natural n existe otro número natural n'.

3). Si $n \in \mathbb{N}$, $n' \neq 1$.

4). Si $n, m \in \mathbb{N}$ y $n' = m'$, entonces $n = m$.

5). **Principio de inducción matemática**: Si S es un subconjunto de $\mathbb{N}$ tal que:

   a) $1 \in S$ y

b) si $n \in S$, entonces $n' \in S$. Se tiene que $S = \mathbb{N}$

Nota: Observar que, en la representación usual de los Naturales, para cada $n \in \mathbb{N}$, n' no es más que $n + 1$.

Ejemplos A Demuestra que para todo número natural n se verifica que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

✓**Demo:** Consideremos el conjunto S de los números naturales para los que la igualdad es cierta. Es claro que $1 \in S$, ya que $1 = 1^2$. Supongamos que la igualdad es cierta para n, es decir que $n \in S$ y veamos que es cierta para $n + 1$. Tenemos, por hipótesis, que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Observar que el siguiente impar de $2n - 1$ es $2n + 1$, por tanto, si sumamos en ambos lados de la igualdad $2n + 1$ obtenemos

$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$$

es decir, que $n+1 \in S$. Por tanto aplicando el principio de inducción matemática, $S = \mathbb{N}$, lo que demuestra que la igualdad es cierta para todo número natural. ■

Definición 2 (Principio de inducción generalizado:) Sea S un subconjunto de $\mathbb{N}$ tal que:

- $1 \in S$ y
- si $1, 2, \ldots, n \in S$, entonces $n + 1 \in S$.

Entonces $S = \mathbb{N}$

En este punto nos separamos de la teoría axiomática de los Números Naturales (tanto la suma, el producto como el buen orden de $\mathbb{N}$ se pueden definir usando una pequeña cantidad de axiomas; a partir de ellos se pueden demostrar todas las propiedades que vamos a ver a continuación). Si quieres ver la teoría completa, la puedes encontrar en [1].

Definición 3 (Propiedades de los Números Naturales)

1. Propiedades respecto de la suma:
   a) Propiedad asociativa: $(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{N}$.
   b) Existencia de elemento neutro: $x + 0 = 0 + x = x \quad \forall\, x \in \mathbb{N}$. (si $0 \in \mathbb{N}$)
   c) Propiedad conmutativa: $x + y = y + x \quad \forall\, x, y \in \mathbb{N}$.
2. Propiedades respecto del producto:
   a) Propiedad asociativa: $(x\,y)\,z = x\,(y\,z) \quad \forall\, x, y, z \in \mathbb{N}$.
   b) Existencia de elemento neutro: $x\,1 = 1\,x = x \quad \forall\, x \in \mathbb{N}$.

c) Propiedad conmutativa: $x\,y = y\,x \quad \forall\, x, y \in \mathbb{N}$.

d) Ley de simplificación: $\forall\, x, y, z \in \mathbb{N}$, con $x \neq 0$, si $x\,y = x\,z$, entonces $y = z$.

3. Propiedades respecto del orden: **Los Naturales poseen un buen orden**, es decir, cualquier subconjunto no vacío de $\mathbb{N}$ posee elemento mínimo.

4. Propiedades conjuntas: para todo $x, y, z \in \mathbb{N}$

a) Propiedad distributiva: $(x + y)\,z = x\,z + y\,z$.

b) Si $x \leq y$, entonces $x + z \leq y + z$.

c) Si $x \leq y$, entonces $xz \leq yz$.

Nota: Dado $(X, \leq)$ cualquier conjunto ordenado y dados $x, y \in X$ denotamos por:

- $x < y$, que se leerá x menor estricto que y, si $x \leq y$ con $x \neq y$.
- $x \geq y$, que se leerá x mayor o igual que y, si $y \leq x$.
- $x > y$, que se leerá x mayor estricto que y, si $y \leq x$ con $y \neq x$.

En particular, para $(\mathbb{N}, \leq)$ tenemos que, $1 \leq x$ para todo $x \in \mathbb{N}$, con lo que $1 < x$ siempre que $1 \neq x$.

1.2. Los Números Enteros

Definición 4 Los Números Enteros: aparecen simetrizando el conjunto de números naturales, y añadiéndoles el cero. Los denotaremos por $\mathbb{Z}$. Con este nuevo conjunto de números obtenemos la mejoría de que, ahora sí, la resta de dos números enteros es un número entero.

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

Definición 5 (Propiedades de los Números Enteros)

1. Propiedades respecto de la suma:

a) Propiedad asociativa: $(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{Z}$.

b) Existencia de elemento neutro: $x + 0 = 0 + x = x \quad \forall\, x \in \mathbb{Z}$.

c) Existencia de elemento opuesto: para todo $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ tal que

$$x + (-x) = (-x) + x = 0.$$

d) Propiedad conmutativa: $x + y = y + x \quad \forall\, x, y \in \mathbb{Z}$.

2. Propiedades respecto del producto:

a) Propiedad asociativa: $(x\,y)\,z = x\,(y\,z) \quad \forall\, x, y, z \in \mathbb{Z}$.

b) Existencia de elemento neutro: $x\,1 = 1\,x = x \quad \forall\, x \in \mathbb{Z}$.

c) Propiedad conmutativa: $x\,y = y\,x \quad \forall\, x, y \in \mathbb{Z}$.

d) Ley de simplificación: $\forall\, x, y, z \in \mathbb{Z}$, con $x \neq 0$, si $x\,y = x\,z$, entonces $y = z$.

3. Propiedades conjuntas:

   a) Propiedad distributiva: $(x+y)\,z = x\,z + y\,z \quad \forall\, x, y, z \in \mathbb{Z}$.

4. Propiedades respecto del orden: para todo $x, y, z \in \mathbb{Z}$

   a) Si $x \leq y$, entonces $x + z \leq y + z$.

   b) Si $x \leq y$ y $0 \leq z$, entonces $x\,z \leq y\,z$.

   c) Si $x \leq y$, y $z \leq 0$, entonces $y\,z \leq x\,z$.

Nota: Observar que normalmente los elementos de $\mathbb{Z}$ no poseen inverso.

Definición 6 Se define el **valor absoluto** de un número entero $x \in \mathbb{Z}$ y se representa por $|x|$ como:

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

★ Los ejercicios del 1 al 6 te pueden servir para saber si has asimilado los conceptos de esta sección.

2. Factorización y Divisibilidad en $\mathbb{Z}$

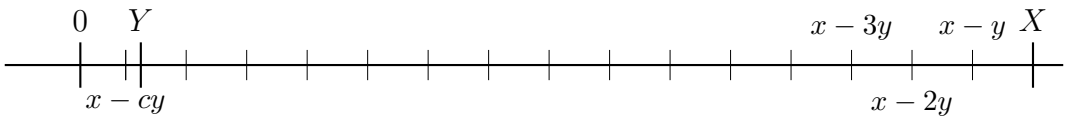
2.1. Algoritmo de la División y Divisibilidad en $\mathbb{Z}$

Proposición 1 (Algoritmo de la división.) Dados dos números enteros $x, y \in \mathbb{Z}$ con $y > 0$ existen $c, r \in \mathbb{Z}$ (únicos), tales que $x = cy + r$ con $0 \leq r < y$.

Demo: Consideremos el conjunto

$$X := \{x - ny \mid x - ny \geq 0,\ n \in \mathbb{Z}\} \subset \mathbb{N}$$

Gráficamente tenemos:



Es claro que $X \neq \emptyset$, ya que:

– Si $x \geq 0$, $\quad x = x - 0y \in X$ y,

– Si $x \leq 0$, $\quad 0 \leq x(1-y) = x - (xy) \in X$.

Por tanto, aplicando que $(\mathbb{N}, \leq)$ es un buen orden, sea $r = \text{Min}(X)$. Así, existe $c \in \mathbb{Z}$ tal que $r = x - cy$, es decir, $x = cy + r$. Veamos ahora que $r < y$. Por reducción al absurdo, si $y \leq r$, tenemos que $0 \leq r - y = x - (c+1)y \in X$, una contradicción, ya que $r - y < r$ y r era el mínimo en X. Por tanto, hemos encontrado $c, r \in \mathbb{Z}$ tales que $x = cy + r$ con $0 \leq r < y$.

Veamos, por último, que c y r son únicos: Supongamos r, r', c, c' tales que

$$\begin{aligned} x &= cy + r \qquad 0 \leq r < y \\ x &= c'y' + r' \qquad 0 \leq r' < y \end{aligned}$$

Podemos suponer $0 \leq r \leq r' < y$. Entonces $cy + r = c'y + r'$ por lo que

$$0 \leq r' - r = (c - c')y. \tag{1}$$

Por tanto, $r' - r$ es múltiplo de y y $r' - r \leq r' < y$, con lo que la única posibilidad es $r' - r = 0$, ver el ejercicio 5 (Pag. 46). Ahora, por la ley de simplificación $c - c' = 0$. ■

Proposición 2 (Algoritmo de la división (ejercicio).) Dados dos números enteros $x, y \in \mathbb{Z}$ con $y \neq 0$ existen $c, r \in \mathbb{Z}$ (únicos), tales que $x = cy + r$ con $0 \leq r < |y|$.

Definición 3 Con la notación del teorema anterior se dice que x es el **dividendo**, y el **divisor**, c el **cociente** y r el **resto**.

Definición 4 Sean x, y dos números enteros. Se dice que y **divide** a x y se representa ${}^{y}|_{x}$ si existe $c \in \mathbb{Z}$ tal que $x = cy$.

2.2. Máximo Común divisor

Definición 5 Sean x e y dos número enteros alguno de ellos no nulo. Se define el **máximo común divisor** de x e y, y se representa por $\text{m. c. d}(x, y)$ como un número $d \in \mathbb{Z}$ con las siguientes propiedades:

1. $d > 0$.
2. ${}^{d}|_{x}$ y ${}^{d}|_{y}$.
3. Si ${}^{r}|_{x}$ y ${}^{r}|_{y}$, entonces ${}^{r}|_{d}$.

Proposición 6 Sean x, y dos enteros alguno no nulos. Entonces existen $\text{m. c. d}(x, y)$ y es único. Es más, existen $r, s \in \mathbb{Z}$ tales que $rx + sy = m.c.d(x, y)$.

✔ **Demo:** Sea el conjunto

$$X = \{ax + by \mid a, b \in \mathbb{Z}, \text{ con } ax + by > 0\} \subset \mathbb{N}.$$

Es claro que $X \neq \emptyset$, ya que $x^2 + y^2 \in X$. Por tanto, aplicando que $(\mathbb{N}, \leq)$ posee un buen orden, existe

$$d = rx + sy = \text{Min}(X) \in \mathbb{N}. \tag{1}$$

Veamos que $d = \text{m. c. d}(x, y)$: por definición, $d > 0$. demostremos que d divide a x. Aplicando el algoritmo de la división a x, d, existen $c, r \in \mathbb{Z}$ tal que $x = cd + r$ con $0 \leq r < d$. Por tanto, $x = c(rx + sy) + r$, luego $r = (1 - cr)x + (-cs)y$. Así, si $r \neq 0$, $r \in X$ con $r < d$, que es imposible. Luego $r = 0$, o lo que es lo mismo, d divide a x. Cambiando los papeles de x e y demostramos que d divide a y. Por último, Si a divide a x y divide a y, entonces $x = ax'$, $y = ay'$ y por tanto $d = rx+sy = rax'+say' = (rx'+sy')a$ lo que demuestra que a divide a d.

Veamos la unicidad: si d y d' verifican las propiedades de $\text{m. c. d}(x, y)$, entonces ${}^{d}|_{d'}$ y ${}^{d'}|_{d}$ por lo que $d = \pm d'$ pero como ambos son números naturales, tenemos que $d = d'$. ■

Nota: Observar que hemos conseguido, a partir de una demostración indirecta, demostrar que existen dos enteros r, s tales que $rx + sy = \text{m. c. d}(x, y)$. Es más, el máximo común divisor de x e y es el menor natural que puede ser escrito en esta forma. No obstante, en un caso concreto, no sabemos encontrar dichos números. El siguiente teorema, debido a Euclides, nos da un algoritmo para calcularlos.
Nota: Aunque pueda parecer una demostración extraña, cuando estudiemos la noción de ideal y los ideales de $\mathbb{Z}$ veremos que el resultado (y su demostración) son muy obvios.
Nota: En ningún momento se ha dicho que r y s sean únicos. Así: $\text{m. c. d}(2, 3) = 1$ y,

$$\begin{aligned} 1 \quad &\cdot 3 + (-1) \cdot 2 = 1 \\ (-3) \cdot 3 + \quad &5 \quad \cdot 2 = 1. \end{aligned}$$

Lema 7 (Ejercicio 7 (Pag. 46)) *Sean $x, y, a, b \in \mathbb{Z}$, Entonces:*

(i) Si ${}^{x}|_{y}$, entonces $\text{m. c. d}(x, y) = x$.

(ii) Si ${}^{x}|_{a}$ y ${}^{x}|_{b}$, entonces ${}^{x}|_{\alpha a+\beta b}$ para todo $\alpha, \beta \in \mathbb{Z}$.

Teorema 8 (Algoritmo de Euclides) Sean x, y dos enteros no nulos. Supongamos que $x = cy + r$ con $r \neq 0$. Entonces

(i) $\text{m. c. d}(x, y) = \text{m. c. d}(y, r)$.

(ii) Aplicando el algoritmo de la división a x e y: $x = cy + r_1$. Si $r_1 \neq 0$ volvemos a aplicar el algoritmo de la división a y y r_1: $y = c_2 r_1 + r_2$, y reiterando el proceso:

$$\begin{aligned} x &= c_1 y + r_1 \quad \text{si} \quad r_1 \neq 0 \\ y &= c_2 r_1 + r_2 \quad \text{si} \quad r_2 \neq 0 \\ r_1 &= c_3 r_2 + r_3 \quad \text{si} \quad r_3 \neq 0 \\ &\vdots \\ r_k &= c_{k+2} r_{k+1} + r_{k+2} \quad \dots \end{aligned}$$

$\exists\, n \in \mathbb{N}$ tal que $r_n = 0$, entonces $r_{n-2} = c_n r_{n-1}$ y $\text{m. c. d}(x, y) = r_{n-1}$.

✓ **Demo:** (1). Sea $d = \text{m. c. d}(x, y)$ y $d' = \text{m. c. d}(y, r)$.

$$x = cy + r \tag{1}$$

Como ${}^{d}|_{x}$, ${}^{d}|_{y}$ y $r = x - cy$, ${}^{d}|_{r}$. Ahora, aplicando que $d' = \text{m. c. d}(y, r)$, ${}^{d}|_{d'}$. Análogamente, como d' divide a y y a r, por (1), d' divide a x y por tanto ${}^{d'}|d$. Así, $d = \pm d'$ y por tanto $d = d'$.

(2). La cadena decreciente de números naturales $r_1 > r_2 > r_3 \cdots > r_k > \cdots$ debe de llega a cero (principio del buen orden). Supongamos que $r_n = 0$, entonces $r_{n-2} = c_{n-1} r_{n-1}$. Ahora, aplicando reiteradamente el apartado anterior

$$\text{m. c. d}(x, y) = \text{m. c. d}(r_{n-2}, r_{n-1}) = r_{n-1}$$

■

Ejemplos A Calcula $\text{m. c. d}(1567, 4763)$.

$$\begin{aligned}
4763 &= 3 \cdot 1567 + 62 && (2.1)\\
1567 &= 25 \cdot 62 + 17 && (2.2)\\
62 &= 3 \cdot 17 + 11 && (2.3)\\
17 &= 1 \cdot 11 + 6 && (2.4)\\
11 &= 1 \cdot 6 + 5 && (2.5)\\
6 &= 1 \cdot 5 + \boxed{1} && (2.6)\\
5 &= 5 \cdot 1 + 0 && (2.7)
\end{aligned}$$

Luego $\text{m. c. d}(1567, 4763) = 1$. En cualquier caso, observar que rápidamente nos encontramos con números pequeños a los que les podemos calcular de forma fácil su máximo común divisor, $\text{m. c. d}(62, 17) = 1$.

⋆ Veamos ahora como calcular $r, s \in \mathbb{Z}$ tales que $r \cdot 1567 + s \cdot 4763 = 1$. Despejamos el 5 de (2.5) y lo sustituimos en (2.6): $6 = 1 \cdot (11 - 6) + 1$,

$$1 = (-1) \cdot 11 + 2 \cdot 6 \tag{♣}$$

Despejamos de (2.4) el 6, y lo sustituimos en (♣), $6 = 17 - 11$:

$$1 = (-1) \cdot 11 + 2 \cdot (17 - 11) = (-3) \cdot 11 + 2 \cdot 17 \tag{♦}$$

Despejamos el 11 de (2.3) y lo sustituimos en (♦):

$$1 = (-3) \cdot (62 - 3 \cdot 17) + 2 \cdot 17 = (-3) \cdot 62 + 11 \cdot 17 \tag{♠}$$

Despejamos el 17 de (2.2) y lo sustituimos en (♠):

$$1 = (-3) \cdot 62 + 11 \cdot (1567 - 25 \cdot 62) = 11 \cdot 1567 - 278 \cdot 62 \tag{▲}$$

Por último, despejamos 62 de (2.1) y lo sustituimos en (▲):

$$1 = 11 \cdot 1567 - 278 \cdot (4763 - 3 \cdot 1567) = -278 \cdot 4763 + 845 \cdot 1567 \tag{★}$$

Definición 9 Se dice que un número entero p es **primo** si $|p| \neq 1$ y sólo es divisible por $\{1, -1, p, -p\}$.

Nota: Como ejemplos de números primos: 2,3,5,7,11,13,17,19,23 o incluso el número 29.996.224.275.833 que es el primo número 10^{12}.

Definición 10 Sean x e y dos número enteros no nulos. Se dice que x e y son **primos relativos** si $\text{m. c. d}(x, y) = 1$.

Corolario 11 (Teorema de Bezout) Sean x, y dos enteros no nulos. Las siguientes condiciones son equivalentes:

(i) x, y son primos relativos.

(ii) existen $r, s \in \mathbb{Z}$ tales que $rx + sy = 1$.

Demo:
$(i) \implies (ii)$. Si x, y son primos relativos, por definición, $\text{m. c. d}(x, y) = 1$ luego por el teorema 6 (Pag. 31) existen $r, s \in \mathbb{Z}$ tal que $rx + sy = 1$.
$(ii) \implies (i)$. Supongamos que existen $r, s \in \mathbb{Z}$ tales que $rx+sy = 1$ y $d = \text{m. c. d}(x, y)$. Como d divide a x y d divide a y, $x = dx'$, $y = dy'$ y por tanto

$$1 = rx + sy = rdx' + sdy' = d(rx' + sy')$$

Por tanto d divide a 1 lo que implica que $d = 1$, ver el ejercicio 6 (Pag. 46). Es decir, x e y son primos relativos. ■

Teorema 12 (Teorema Generalizado de Bezout) Sean $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tales que si $k \in \mathbb{N}$ divide a todo n_i, $k = 1$. Entonces existen $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}$ tales que $\alpha_1 n_1 + \alpha_2 n_2 + \cdots + \alpha_r n_r = 1$.

Demo: Vamos a dar una demostración por inducción a r, el número de elementos que tenemos:
(i). Si $r = 2$ tenemos que este resultado es el teorema de Bezout, por lo que no tenemos nada que demostrar.
(ii). Supongamos que el resultado es cierto para $r - 1$ y consideremos r naturales no nulos $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tales que si $k \in \mathbb{N}$ divide a todo n_i, $k = 1$. Sean los naturales $n_1, n_2, \ldots, n_{r-1}$ y sea el conjunto

$$\Delta := \{\lambda \in \mathbb{N} \mid \lambda \text{ divide a todos los } n_i \; i = 1, \ldots, r-1\}$$

Es claro que $1 \in \Delta$ y que todo elemento de Δ es menor que cualquiera de los n_i, por lo que es un conjunto finito. Sea β el mayor elemento de Δ. Tenemos entonces que $n_i = \beta n_i'$ con $n_i' \in \mathbb{Z}$ y que el conjunto $\{n_1', n_2', \ldots, n_{r-1}'\}$ verifica la hipótesis de inducción (si hubiera un γ que dividiera a todos los n_i', $\gamma\beta > \beta$ dividiría a todos los n_i, $i = 1, \ldots, r-1$, una contradicción ya que β era el mayor. Por tanto, aplicando la hipótesis de inducción existen $\alpha_i' \in \mathbb{Z}$ tal que

$$\alpha_1' n_1' + \alpha_2' n_2' + \cdots + \alpha_{r-1}' n_{r-1}' = 1. \qquad (*)$$

Por otro lado $\mathrm{m.c.d}(\beta, n_r) = 1$ ya que si algún natural dividiera a β y a n_r dividiría a todos los n_i (que no puede ser por hipótesis). Luego aplicando el teorema de Bezout existen $a, b \in \mathbb{Z}$ tal que

$$a\beta + bn_r = 1. \qquad (**)$$

Luego por $(**)$, y sustituyendo $(*)$, tenemos:

$$\begin{aligned} 1 &= a\beta + bn_r = a\beta(1) + bn_r = a\beta(\alpha'_1 n'_1 + \alpha'_2 n'_2 + \cdots + \alpha'_{r-1} n'_{r-1}) + bn_r \\ &= a\alpha'_1 \beta n'_1 + a\alpha'_2 \beta n'_2 + \cdots + a\alpha'_{r-1} \beta n'_{r-1} + bn_r \\ &= a\alpha'_1 n_1 + a\alpha'_2 n_2 + \cdots + a\alpha'_{r-1} n_{r-1} + bn_r \end{aligned}$$

que nos demuestra el resultado. ■

Proposición 13 Sean $n_1, n_2, \ldots, n_k$ números enteros no nulos y $p \in \mathbb{Z}$ un número primo. Supongamos que ${}^{p}|_{n_1 n_2 \ldots n_k}$ entonces existe $i \in \{1, 2, \ldots, k\}$ tal que ${}^{p}|_{n_i}$.

✔ **Demo:** Vamos a dar una demostración por inducción a k. Demostremos el caso $k = 2$. Supongamos que p no divide a n_1. Entonces $m.c.d(p, n_1) = 1$ por lo que por el Teorema de Bezout existen $\alpha, \beta \in \mathbb{Z}$ tal que

$$\alpha n_1 + \beta p = 1 \qquad (1)$$

Ahora, como por hipótesis $n_1 n_2 = cp$, multiplicando en (1) por n_2,

$$n_2 = n_2(\alpha n_1 + \beta p) = \alpha(n_1 n_2) + \beta p n_2 = \alpha(cp) + \beta p n_2 = (\alpha c + \beta n_2)p \qquad (2)$$

Por tanto, n_2 es divisible por p.

Supongamos que el resultado es cierto para $k-1$, entonces, si ${}^{p}|_{n_1 n_2 \ldots n_k}$, aplicando el caso anterior a los números $(n_1 \ldots n_{k-1})$ y n_k tenemos que, ${}^{p}|_{n_1 \ldots n_{k-1}}$ o ${}^{p}|n_k$ y por el proceso de inducción, si ${}^{p}|_{n_1 \ldots n_{k-1}}$, existe un i tal que ${}^{p}|_{n_i}$. Lo que demuestra la proposición. ■

2.3. Factorización en $\mathbb{Z}$

Definición 14 (Teorema de Factorización) Dado un número entero n con $|n| > 1$ existen unos únicos $p_1 < \cdots < p_k$ primos y $n_1, \ldots, n_k \in \mathbb{N}$ tales que $n = \pm p_1^{n_1} \ldots p_k^{n_k}$.

✔ **Demo:** Es claro que podemos suponer $n \in \mathbb{N}$. Vamos a usar el principio de inducción generalizado: si $n = 2$, ya está factorizado. Supongamos que todo número natural menor que n esta factorizado como producto de primos. Si n es primo, no hay nada que demostrar, caso contrario existen $a, b \in \mathbb{N}$ mayores que 1 tales que $n = ab$. Entonces $a, b < n$ y por hipótesis de inducción, a y b factoriza como producto de primos.

Veamos la unicidad: El caso $n = 2$ es trivial. Por tanto, y aplicando el principio de inducción generalizado puedo suponer que tenemos factorización única para todo natural $< n$. Supongamos $n = p_1^{n_1} \ldots p_k^{n_k} = p_1^{m_1} \ldots p_k^{m_k}$ con $n_i, m_i \in \mathbb{N}$ (puedo suponer que los primos que aparecen en la factorización son los mismos al haber permitido el exponente cero). Reordenando puedo suponer $n_1 \neq 0$ y por tanto n es divisible por p_1. Aplicando el resultado anterior, ${}^{p_1}|_{p_1^{m_1} \ldots p_k^{m_k}}$ y como p_1 no puede dividir a ningún primo que no sea el mismo, $m_1 \geq 1$, Tenemos entonces que $p_1^{n_1 - 1} \ldots p_k^{n_k} = p_1^{m_1 - 1} \ldots p_k^{m_k} < n$, aplicando ahora el proceso de inducción $n_i = m_i$ para todo i. ■

Corolario 15 Sean x, y dos enteros no nulos. Entonces el máximo común divisor de x e y es el producto de los primos comunes elevado al menor exponentes (en sus respectivas factorizaciones).

Corolario 16 (Teorema de Euclides) Existen infinitos primos.

Demo: Vamos a dar una demostración por reducción al absurdo. Supongamos que el número de primos es finito, $p_1, p_2, \ldots, p_k$. Sea $n = p_1 p_2 \cdots p_k + 1 \in \mathbb{Z}$. Tenemos que n se factoriza como producto de primos, sea p uno de estos primos. Entonces n es divisible por p, pero $p_1 p_2 \cdots p_k$ es divisible por p, por tanto 1 es divisible por p, una contradicción (si $1 = p\alpha$, $p = \pm 1$ y no puede ser primo). ■

Definición 17 Sean x, y dos número enteros alguno no nulos. Se define el mínimo común múltiplo de x e y y se representa por $\mathrm{M.C.M}(x, y)$ como un número $m \in \mathbb{Z}$ con las siguientes propiedades:

1. $m > 0$.
2. ${}^{x}|_{m}$ e ${}^{y}|_{m}$.
3. Si ${}^{x}|_{r}$ e ${}^{y}|_{r}$, entonces ${}^{m}|_{r}$.

Demo: Hay que demostrar que tal número existe y es único. Una posible demostración consiste en considerar el conjunto

$$\Delta := \{0 < a \in \mathbb{N} \mid {}^{x}|_{a},\ {}^{y}|_{a}\}$$

Demostrar que es no vacío y que es mínimo de este conjunto, digamos m, es el $\mathrm{M.C.M}(x, y)$. Por hipótesis, m verifica 1. y 2. por último, si ${}^{x}|_{r}$ e ${}^{y}|_{r}$, por el algoritmo de la división $r = mc + r'$ (demostrar que $r' = 0$). ■

Proposición 18 Sean x, y dos enteros no nulos. Entonces el mínimo común múltiplo de x e y es el producto de los primos comunes y no comunes elevado al mayor de los exponentes (en sus respectivas factorizaciones).

Corolario 19 (Ejercicio 8 (Pag. 46)) La relación de divisibilidad en $\mathbb{Z}$ es reflexiva, transitiva y verifica que para todo $a, b \in \mathbb{Z}$, si

$${}^{a}|_{b} \text{ y } {}^{b}|_{a} \quad \text{entonces } a = \pm b.$$

Por tanto, es una relación de orden en $\mathbb{N}$. Es más, el ínfimo de dos elementos $a, b \in \mathbb{N}$ coincide con $\mathrm{m.c.d}(a, b)$, y el supremo de dos elementos $a, b \in \mathbb{N}$ coincide con $\mathrm{M.C.M}(a, b)$, por lo que $\mathbb{N}$ con la relación de divisibilidad es un retículo.

Corolario 20 Sean x, y dos enteros no nulos. Entonces

$$|xy| = m.c.d(x, y).\, \mathrm{M.C.M}(x, y).$$

★ Los ejercicios del 7 al 21 de este tema pueden servirte para comprobar si has asimilado las nociones de estas dos secciones.

3. Congruencias.

3.1. Anillos de congruencias

En esta sección vamos a trabajar con nuevos conjuntos de números: $\mathbb{Z}_n$, los **anillos de congruencias modulo** n.

Definición 1 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Dados $a, b \in \mathbb{Z}$, diremos que a es congruente con b módulo n, y lo representaremos por $a \equiv b \pmod{n}$ si ${}^{n}|_{a-b}$.

Proposición 2 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Entonces:

(i) Para todo $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ si y sólo si el resto de dividir a por n coincide con el resto de dividir b por n.

(ii) La relación de congruencia es una relación de equivalencia,

(iii) Las clases de equivalencia de la relación de congruencia módulo n son

$$\mathbb{Z}_n := \mathbb{Z}/_{(\mathrm{mod}\, n)} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}.$$

Demo: (i). Aplicando el algoritmo de la división $a = cn + r$, $b = c'n + r'$. Podemos suponer que $r' \leq r$ (en caso contrario les cambiamos los nombres). Ahora, $a - b = (c - c')n + r - r'$ con $0 \leq r - r' \leq r < n$, por tanto $a - b$ es múltiplo de n si y sólo si $r - r' = 0$.

(ii). Trivial a partir de (i).

(iii). Dado $a \in \mathbb{Z}$, aplicando el algoritmo de la división, $a = cn + r$ con $0 \leq r < n$. Por tanto $a - r = cn$ y $a \equiv r \pmod{n}$ o lo que es lo mismo $\overline{a} = \overline{r}$ (hemos demostrado que a lo sumo hay n clases de equivalencia, $\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$). Veamos ahora que todas son distintas: sean $0 \neq i \leq j < n$ y supongamos que $\overline{i} = \overline{j}$. Entonces $j \equiv i \pmod{n}$ por lo que $j - i = cn$. Por otro lado, $0 \leq j - i \leq j < n$, con lo que la única posibilidad es $j - i = 0n = 0$, es decir $i = j$ y hay n clases de equivalencia. ■

Nota: En el anillo de congruencias módulo n, con $n \in \mathbb{N}$, tenemos que la clase de equivalencia de un elemento $r \in \mathbb{Z}$ es:

$$\overline{r} = \{r + \alpha n \mid \alpha \in \mathbb{Z}\}$$

Es decir, cualquier elemento de este conjunto es un representante para la clase $\overline{r} \in \mathbb{Z}_n$.

Teorema 3 Sea $\mathbb{Z}$ el conjunto de los enteros y $n \in \mathbb{N}$. Entonces podemos definir una suma y un producto en el conjunto cociente, $\mathbb{Z}_n$:

(i) $\overline{a} + \overline{b} := \overline{a + b}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

(ii) $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

(iii) Las operaciones anteriores verifican las propiedades 1.(a),(b),(c),(d), 2.(a),(b),(c), 3.(a). de la definición 5 (Pag. 29).

Nota: No hay ninguna relación de orden asociada a este conjunto cociente. A $\mathbb{Z}_n$ con las operaciones anteriores se le denomina el **anillo de congruencias** módulo n. Observar que $\overline{0} = \{kn \mid k \in \mathbb{Z}\}$, es decir, los múltiplos de n son el elemento neutro de la suma.

Demo: En (i) y en (ii) se ha definido la suma y el producto respecto de representantes de cada clase, por lo que hay que demostrar que la suma y el producto están bien definidos (no dependen de representantes). Sean

$$\begin{array}{l} \overline{a} = \overline{a}' \\ \overline{b} = \overline{b}' \end{array} \implies \begin{array}{l} a - a' = cn \\ b - b' = c'n \end{array} \tag{1}$$

(i). Veamos que la suma está bien definida: por (1), sumando ambas expresiones, $a - a' + b - b' = (c + c')n$, o lo que es lo mismo,

$$a + b - (a' + b') = (c + c')n,$$

es decir, $a + b \equiv a' + b' \pmod{n}$ y por tanto $\overline{a + b} = \overline{a' + b'}$.

(ii). Veamos que el producto está bien definida: por (1), $a = a' + cn$ y $b = b' + c'n$ por tanto, si multiplicamos ambas expresiones,

$$ab = a'b' + a'c'n + b'cn + cc'n^2 = a'b' + (a'c' + b'c + cc'n)n.$$

Por tanto $ab \equiv a'b' \pmod{n}$ y por tanto $\overline{ab} = \overline{a'b'}$.

(iii). Todas estas propiedades son ahora triviales:

- Propiedades de la suma:
  - Asociativa: $\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{y + z} = \overline{x + (y + z)} = \overline{(x + y) + z} = \overline{x + y} + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}$.
  - Conmutativa: $\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}$.
  - Elemento neutro: $\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}$.
  - Elemento opuesto: $\overline{x} + \overline{-x} = \overline{0}$.
- Propiedades del producto:
  - Asociativa: $\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{y \cdot z} = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot y} \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}$
  - Conmutativa: $\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x}$.
  - Elemento Neutro: $\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}$.
- Propiedades conjuntas (distributiva):

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot (\overline{y + z}) = \overline{x \cdot (y + z)} = \overline{x \cdot y + x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}.$$

Lo que demuestra la proposición. Se dice que $(\mathbb{Z}_n, +)$ es un grupo abeliano por cumplir las 4 primeras propiedades. Se dice que $(\mathbb{Z}_n, +, \cdot)$ es un anillo unitario por cumplir todas las propiedades anteriores. ■

Corolario 4 *Sea $n \in \mathbb{N}$ y sean $a, b, c, d, x \in \mathbb{Z}$, $y \in \mathbb{N}$. Supongamos que $a \equiv b \pmod n$ y $c \equiv d \pmod n$. Entonces,*

(i) $a + c \equiv b + d \pmod n$ $\qquad$ (ii) $a \cdot c \equiv b \cdot d \pmod n$.

(iii) $x \cdot a \equiv x \cdot b \pmod n$. $\qquad$ (iv) $a^y \equiv b^y \pmod n$.

Nota: Se ha demostrado que si estamos trabajando en el anillo de congruencias modulo n cuando multiplicamos o sumamos número podemos cambiar cualquiera de ellos por un congruente (modulo n) suyo. Así, en $\mathbb{Z}_{11}$ tenemos:

$$(213 \cdot 543) + 1113 \equiv (4 \cdot 4) + 2 = 18 \equiv 7 \pmod{11}$$

En cambio no podemos cambiar por números congruentes las potencias (los exponentes nos dicen cuantas veces hay que multiplicar un elemento):

$$2^{12} \not\equiv 2^1 \pmod{11}$$

Ejemplos A Veamos las tablas de sumar y multiplicar de $\mathbb{Z}_6$:

$+$	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

$\bullet$	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

Nota: En estos conjuntos de números ocurren cosas extrañas: Por ejemplo, en $\mathbb{Z}_6$, $\overline{2}\,\overline{3} = \overline{0}$, por lo que el producto de números no nulos puede ser cero.

Definición 5 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$). Diremos que $\overline{a} \in \mathbb{Z}_n$ **es inversible en** $\mathbb{Z}_n$ si existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1} = \overline{b} \cdot \overline{a}$

Proposición 6 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$) y sea $\overline{a} \in \mathbb{Z}_n$. Entonces, $\overline{a}$ es inversible en $\mathbb{Z}_n$ si y solo si $\text{m. c. d}(a, n) = 1$. Es más, en este caso, existe un único $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1} = \overline{b} \cdot \overline{a}$, llamado **el inverso de $\overline{a}$ en** $\mathbb{Z}_n$, que se denotará usualmente por $\overline{a}^{-1}$.

✓ **Demo:** Supongamos que $\overline{a}$ es inversible en $\mathbb{Z}_n$, entonces existe $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a}\,\overline{b} = \overline{1}, \qquad \text{es decir,} \quad ab \equiv 1 \pmod n$$

o lo que es lo mismo $ab - 1 = cn$. Por tanto, $ab + (-c)n = 1$, luego $\text{m. c. d}(a, n) = d$ divide a 1, lo que implica $\text{m. c. d}(a, n) = 1$. Por otro lado, si $\text{m. c. d}(a, n) = 1$, aplicando el Teorema de Bezout existen $r, s \in \mathbb{Z}$ tales que $ar + cn = 1$ o lo que es lo mismo, $ar - 1 = -sn$, $(ar \equiv 1 \pmod n)$ es decir, $\overline{a}\,\overline{r} = \overline{ar} = \overline{1}$.

Por último, si $\overline{b}, \overline{b}'$ son inversos para $\overline{a}$,

$$\overline{b} = \overline{b}\,\overline{1} = \overline{b}(\overline{a}\,\overline{b}') = (\overline{b}\,\overline{a})\overline{b}' = \overline{1}\,\overline{b}' = \overline{b}'.$$

Lo que demuestra la unicidad. ■

Corolario 7 Sea $\mathbb{Z}_n$ el anillo de congruencias módulo n (con $n \in \mathbb{N}$). Entonces, las siguientes condiciones son equivalentes:

(i) Todo elemento no nulo de $\mathbb{Z}_n$ es inversible.

(ii) n es un número primo.

(iii) Para todo par de elementos no nulos $\overline{a}, \overline{b}$ de $\mathbb{Z}_n$, $\overline{a}\ \overline{b} \neq \overline{0}$.

Demo: (ii) $\Longrightarrow$ (i). Por el resultado anterior, si n es primo, para todo $0 < k < n$, $\mathrm{m.\,c.\,d}(n,k) = 1$ y por tanto $\overline{k}$ es inversible en $\mathbb{Z}_n$.

(i) $\Longrightarrow$ (ii). Supongamos que todo elemento no nulo de $\mathbb{Z}_n$ es inversible. Entonces, para todo $k \in \mathbb{N}$, $0 < k < n$, se tiene que $\mathrm{m.\,c.\,d}(k,n) = 1$. Por tanto n no es divisible por ningún k tal que $0 < k < n$. Así, n es primo.

(i) $\Longrightarrow$ (iii). Sean $\overline{a}, \overline{b} \in \mathbb{Z}_n$ tales que $\overline{a}\ \overline{b} = \overline{0}$. Si $\overline{a} = \overline{0}$ no hay nada que demostrar, por tanto supongamos $\overline{a} \neq \overline{0}$. Entonces, $\overline{a}$ es inversible en $\mathbb{Z}_n$, sea $\overline{a}^{-1} \in \mathbb{Z}_n$ y por tanto,

$$\overline{0} = \overline{a}^{-1} \cdot \overline{0} = \overline{a}^{-1}(\overline{a}\ \overline{b}) = (\overline{a}^{-1}\ \overline{a})\overline{b} = \overline{1}\overline{b}$$

(iii) $\Longrightarrow$ (ii). Por reducción al absurdo, supongamos que n no es primo. Entonces existen $a, b \in \mathbb{Z}$, $1 < a, b < n$ tales que $n = ab$. Pero entonces $\overline{a}, \overline{b}$ son no nulos y $\overline{a}\ \overline{b} = \overline{n} = \overline{0}$, una contradicción. ■

Teorema 8 (Teorema de Fermat(chico)) *Sea $p, x \in \mathbb{N}$ con p un número primo y $\mathrm{m.\,c.\,d}(p,x) = 1$. Entonces $x^{p-1} \equiv 1 \pmod{p}$.*

Demo: Sea $\overline{x} \in \mathbb{Z}_p$. Como $\mathrm{m.\,c.\,d}(p,x) = 1$, $\overline{x}$ es inversible en $\mathbb{Z}_p$, sea $\overline{y}$ su inverso. En estas condiciones tenemos que la aplicación $\Psi_x : \mathbb{Z}_p \to \mathbb{Z}_p$ definida por $\Psi_x(\overline{a}) = \overline{x}\ \overline{a}$ es inversible con inversa Ψ_y. Por tanto,

$$\mathbb{Z}_p = \operatorname{Im} \Psi_x = \{\overline{x}\ \overline{1}, \overline{x}\ \overline{2}, \ldots, \overline{x}\ \overline{p-1}\}$$

Luego $\prod_{k=1}^{p-1} \overline{k} = \prod_{k=1}^{p-1} \overline{x}\ \overline{k} = \overline{x}^{p-1} \prod_{k=1}^{p-1} \overline{k}$. Por último, como $\prod_{k=1}^{p-1} \overline{k}$ es un elemento no nulo de $\mathbb{Z}_p$, multiplicando por su inverso, $\overline{x}^{p-1} = \overline{1}$ es decir, $x^{p-1} \equiv 1 \pmod{p}$. ■

Podemos encontrar una generalización de este teorema para cualquier número Natural, es el llamado Teorema de Euler:

Definición 9 Se define la **función de Euler** como $\varphi : \mathbb{N} \to \mathbb{N}$ definida por:

$$\varphi(n) = \#\{a \in \mathbb{N} \mid 1 \leq a \leq n,\ \mathrm{m.\,c.\,d}(a,n) = 1\}$$

Por ejemplo, $\varphi(10) = 4$ o si p es un número primo, $\varphi(p) = p - 1$.

Proposición 10 $\varphi(n)$ coincide con el número de elementos inversibles en $\mathbb{Z}_n$

Proposición 11 (Ejercicio) Sea $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler. Entonces

(i) Si p es un número primo y $r \in \mathbb{N}$, entonces $\varphi(p^r) = p^r(1 - \frac{1}{p}) = p^r - p^{r-1}$.

(ii) Si $n, m \in \mathbb{Z}$ con $\mathrm{m.\,c.\,d}(n,m) = 1$, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.

(iii) Si $n \in \mathbb{Z}$, $(n \neq 0, 1, -1)$ se factoriza como producto de primos $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, entonces

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Teorema 12 (Teorema de Euler) *Sean* $n, x \in \mathbb{N}$ *con* $\text{m. c. d}(n, x) = 1$. *Entonces* $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Demo: La demostración es muy similar a la demostración del teorema de Fermat. Consideremos Δ el conjunto de los elementos inversibles de $\mathbb{Z}_n$. Sea $\overline{x} \in \mathbb{Z}_n$. Como $\text{m. c. d}(n, x) = 1$, $\overline{x}$ es inversible en $\mathbb{Z}_p$, sea $\overline{y}$ su inverso. En estas condiciones tenemos que la aplicación $\Psi_x : \Delta \to \Delta$ definida por $\Psi_x(\overline{a}) = \overline{x}\,\overline{a}$, está bien definida, y es inversible con inversa Ψ_y. Por tanto,

$$\Delta = \text{Im}\,\Psi_x = \{\overline{x}\,\overline{a} \mid \overline{a} \in \Delta\}$$

Luego $\prod_{a\in\Delta} \overline{a} = \prod_{a\in\Delta} \overline{x}\,\overline{a} = \overline{x}^{\varphi(n)} \prod_{a\in\Delta} \overline{a}$. Por último, como $\prod_{a\in\Delta} \overline{a}$ es un elemento inversible de $\mathbb{Z}_p$, multiplicando por su inverso, $\overline{x}^{\varphi(n)} = \overline{1}$ o lo que es lo mismo, $x^{\varphi(n)} \equiv 1 \pmod{n}$. ■

3.2. Sistemas de ecuaciones en congruencias

Ejemplos B Estudiemos ahora ecuaciones en los anillos de congruencias $\mathbb{Z}_n$. Supongamos que queremos encontrar las soluciones de la ecuación

$$\overline{3}\overline{x} = \overline{5} \quad \text{en } \mathbb{Z}_6. \tag{1}$$

o lo que es lo mismo, $3x \equiv 5 \pmod{6}$. En estos momentos la única posibilidad que tenemos es comprobar, sustituyendo, si tiene o no tiene soluciones:

$$\begin{aligned} &3 \cdot 0 \equiv 0 \pmod{6}, \quad 3 \cdot 1 \equiv 3 \pmod{6}, \quad 3 \cdot 2 \equiv 0 \pmod{6}, \\ &3 \cdot 3 \equiv 3 \pmod{6}, \quad 3 \cdot 4 \equiv 0 \pmod{6}, \quad 3 \cdot 5 \equiv 3 \pmod{6} \end{aligned}$$

luego no tiene soluciones. Sin embargo, la ecuación

$$\overline{6}x = \overline{4} \quad \text{en } \mathbb{Z}_8. \tag{2}$$

tiene por soluciones $x = 2$ y $x = 6$:

$$\begin{aligned} &6 \cdot 0 \equiv 0 \pmod{8}, \quad 6 \cdot 1 \equiv 6 \pmod{8}, \quad 6 \cdot 2 \equiv 4 \pmod{8}, \\ &6 \cdot 3 \equiv 2 \pmod{8}, \quad 6 \cdot 4 \equiv 0 \pmod{8}, \quad 6 \cdot 5 \equiv 6 \pmod{8}, \\ &6 \cdot 6 \equiv 4 \pmod{8}, \quad 6 \cdot 7 \equiv 2 \pmod{8}, \end{aligned}$$

Nota: Observar que, "simplificando" la ecuación anterior por 2, $\overline{3}x = \overline{2}$, tiene una única solución $x = 6$ (luego $x = 2$ ha dejado de ser solución!!).

Proposición 13 Sean $n_1, n_2, \ldots, n_k, r, s, u, v, n, m \in \mathbb{Z}$ elementos no nulos.

(i) Supongamos que para cada $i \in \{1, 2, \ldots, k\}$, $\text{m. c. d}(s, n_i) = 1$ y sea $m = \prod_{i=1}^{k} n_i$. Entonces $\text{m. c. d}(s, m) = 1$.

(ii) Si s divide a uv, y $\mathrm{m.\,c.\,d}(s,u)=1$, entonces s divide a v.

(iii) Si ${}^{n}|_{s}$ y ${}^{m}|_{s}$ con $\mathrm{m.\,c.\,d}(n,m)=1$, entonces ${}^{nm}|s$

(iv) Si $\mathrm{m.\,c.\,d}(n,m)=d$, y sean n' y m' tales que $n=n'd$ y $m=m'd$. Entonces $\mathrm{m.\,c.\,d}(n',m')=1$.

✓ **Demo:** (i) Sea $d=\mathrm{m.\,c.\,d}(s,m)$. Por reducción al absurdo, supongamos que $d>1$. Entonces podemos factorizar d como producto de primos. Sea p uno de los primos que aparece en la factorización de d. Tenemos entonces que d divide a s y de divide a $m=\prod_{i=1}^{k} n_i$. Luego por la proposición 13 (Pag. 35) existe un k tal que p divide a n_k (si un primo p divide a un producto de números, entonces divide a alguno de ellos). Pero entonces (${}^{p}|_{s}$ y ${}^{p}|_{n_k}$), p divide a $\mathrm{m.\,c.\,d}(s,n_k)=1$, una contradicción. Por tanto $d=1$.

(ii) Si $\mathrm{m.\,c.\,d}(s,u)=1$ y $vu=\gamma s$, por Bezout existen $\alpha,\beta\in\mathbb{Z}$ tales que $\alpha s+\beta u=1$. Si multiplicamos ahora por v,

$$v=\alpha sv+\beta uv=\alpha sv+\gamma s=(\alpha v+\gamma)s$$

Lo que demuestra que s divide a v.

(iii) Por hipótesis $s=\alpha m$ y $s=\beta n$. Aplicando el Teorema de Bezout, existen $x,y\in\mathbb{Z}$ tales que $xn+ym=1$. Por tanto, multiplicando esta igualdad por s obtenemos

$$s=sxn+sym=\alpha mxn+\beta nym=(\alpha x+\beta y)nm$$

Por tanto s es divisible por nm.

(iv) Por el teorema de existencia del máximo común divisor, existen $r,s\in\mathbb{Z}$ tales que

$$d=rn+sm=rn'd+sm'd=(rn'+sm')d.$$

Aplicando ahora la ley de simplificación en $\mathbb{Z}$ tenemos que $rn'+sm'=1$, por lo que por el Teorema de Bezout, $\mathrm{m.\,c.\,d}(n'.m')=1$. ■

Nota: Podemos pensar en una ecuación $\overline{a}\cdot x=\overline{b}$ en $\mathbb{Z}_n$, el anillo de congruencias módulo n, con $n\in\mathbb{N}$, o podemos pensar en la ecuación en congruencias $ax\equiv b\pmod n$. En ambos casos se trata del mismo problema, en el primero las soluciones serán elementos de $\mathbb{Z}_n$ (con lo que con dar un representante de cada solución es suficiente. En el segundo tenemos que dar todos los elementos de $\mathbb{Z}$ que verifican la ecuación, que no es más que cualquier representante de las soluciones en $\mathbb{Z}_n$: Así,

- La ecuación $\overline{3}\cdot x=\overline{4}$ en $\mathbb{Z}_5$ tiene por solución $x=\overline{3}\in\mathbb{Z}_5$.
- La ecuación $3x\equiv 4\pmod 5$ tiene por solución el conjunto

$$S=\{\cdots,-12,-7,-2,3,8,13,\cdots\}.$$

Que no es más que el conjunto definido por $\overline{3}$.

Trabajaremos indistintamente con una ecuación que con otra. Cuando se hable sobre el numeró de soluciones de alguna de estas ecuaciones nos estaremos refiriendo al número de soluciones en $\mathbb{Z}_n$ (ya que en $\mathbb{Z}$ o no tiene soluciones o son infinitas)

Teorema 14 Sean $n\in\mathbb{N}$ y $a,b\in\mathbb{Z}$. Entonces las siguientes condiciones son equivalentes:

(i) La ecuación $ax\equiv b\pmod n$ tiene solución.

(ii) El máximo común divisor de a y n divide a b.

Es más, el número de soluciones de la ecuación (en $\mathbb{Z}_n$) es exactamente el $\mathrm{m.\,c.\,d}(a, n)$.

✓ **Demo:** Denotemos por $d = \mathrm{m.\,c.\,d}(a, n)$. Supongamos que $s \in \mathbb{Z}$ es solución de la ecuación

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

Entonces existe $\alpha \in \mathbb{Z}$ tal que $as - b = \alpha n$. Por tanto $b = as - \alpha n$. Ahora, como a y n son divisibles por d (esto es por definición), b es divisible por d.

Supongamos ahora que b es divisible por d, $b = \beta d$. Por el Teorema 6 (Pag. 31) existen $r, s \in \mathbb{Z}$ tales que $d = ra + sn$. Si multiplicamos por β en esta igualdad obtenemos que $b = \beta d = \beta(ra + sn)$, lo que implica que $\beta ra - b = \beta sn$, o lo que es lo mismo, $a(\beta r) \equiv b \pmod{n}$, es decir, βr es solución de la ecuación.

Demostremos ahora el además: Supongamos que la ecuación $ax \equiv b \pmod{n}$ tiene solución, sea s una solución de la ecuación. Por lo anterior sabemos que $d = \mathrm{m.\,c.\,d}(a, n)$ divide a b. Sean $\alpha, \gamma \in \mathbb{Z}$ tales que $n = \gamma d$, $a = \alpha d$. Veamos que $s + \gamma$ es también solución de la ecuación.

$$a(s + \gamma) = as + a\gamma \equiv b + a\gamma = b + \alpha d\gamma = b + \alpha n \equiv b \pmod{n}$$

Luego para todo $k \in \mathbb{N}$, $s + k\gamma$ es solución. Como nos estamos preocupando de las soluciones módulo n, la solución $s + d\gamma = s + n \equiv s \pmod{n}$ por lo que k toma los valores $0 \leq k \leq d - 1$. Por tanto, como mucho tenemos las siguientes d soluciones

$$\{s, s + \gamma, s + 2\gamma, \ldots, s + (d - 1)\gamma\}$$

Observar que todas son distintas, módulo n, ya que si

$$0 \leq t_1 < t_2 \leq d - 1 \text{ y } s + t_1\gamma \equiv s + t_2\gamma \pmod{N},$$

entonces $0 \leq (t_2 - t_1)\gamma \leq t_2\gamma < d\gamma = n$ y por tanto como $(t_2 - t_1)\gamma = \dot{n}$ (es múltiplo de n) éste tiene que ser cero, una contradicción, $t_1 = t_2$.

Por último, si s' es solución del sistema, $a(s' - s) \equiv 0 \pmod{n}$ y por tanto $a(s' - s) = \tau n$ dividiendo en esta igualdad por d obtenemos

$$d\alpha(s' - s) = a(s' - s) = \tau n = \tau\gamma d$$

por lo que $\alpha(s' - s) = \tau\gamma$ y como $\mathrm{m.\,c.\,d}(\alpha, \gamma) = 1$, por la proposición anterior, γ divide a $s' - s$ por lo que $s' - s = \xi\gamma$ y por tanto $s' = s + \xi\gamma$ es una de las soluciones anteriores. ■

El siguiente resultado nos va a permitir calcular más fácilmente las soluciones de una ecuación en congruencias cuando el número de soluciones (En $\mathbb{Z}_n$) es mayor que 1:

Proposición 15 (Ejercicio) *Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Supongamos que $1 < \mathrm{m.\,c.\,d}(a, n) = d$ y que d divide a b. Tenemos entonces que $a = da'$, $n = dn'$ y $b = db'$. Entonces el conjunto de soluciones en $\mathbb{Z}$ de las siguientes ecuaciones coincide*

$$ax \equiv b \pmod{n} \qquad a'x \equiv b' \pmod{n'}$$

✔ **Demo:** Sea $s \in \mathbb{Z}$ una solución de $ax \equiv b \pmod{n}$. Entonces $as - b = \dot{n}$, por lo que existe $\alpha \in \mathbb{Z}$ tal que $as - b = \alpha n$. Es decir, $a'dx - db' = \alpha dn'$. Si simplificamos ahora por d tenemos que $a'x - b' = \alpha n'$, lo que demuestra que s es solución de la ecuación $a'x \equiv b' \pmod{n'}$.

Sea $s \in \mathbb{Z}$ una solución de $a'x \equiv b' \pmod{n'}$. Entonces existe $\beta \in \mathbb{Z}$ tal que $a's - b' = \beta n'$. Si multiplicamos ahora esta igualdad por d tenemos, $a'dx - db' = \alpha dn'$. Es decir, $as - b = \beta n$, lo que demuestra que s es solución de la ecuación $ax \equiv b \pmod{n}$. ■

Nota: La proposición anterior es muy útil a la hora de resolver ecuaciones en congruencias: Resuelve la ecuación en congruencias

$$4x \equiv 4 \pmod{8}$$

Como $\text{m. c. d}(4, 8) = 4$ y 4 divide a 4, esta ecuación tiene solución, es más, modulo 8 el número de soluciones es 4. Por la proposición anterior, esta ecuación tiene las mismas soluciones en $\mathbb{Z}$ que la ecuación

$$x \equiv 1 \pmod{2}$$

que claramente es el conjunto

$$\{1 + 2k, \quad k \in \mathbb{Z}\}.$$

Por tanto las soluciones distintas en $\mathbb{Z}_8$ son $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ ($\overline{9}$ ya coincide con $\overline{1}$ en $\mathbb{Z}_8$).

Teorema 16 Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$ y $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Supongamos que $\text{m. c. d}(n_i, n_j) = 1$ para todo $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$. Entonces el sistema de ecuaciones:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Tiene solución. Es más, ésta es única modulo $m = \prod_{i=1}^{k} n_i$.

✔ **Demo:** Vamos a dar una demostración constructiva, lo que nos servirá para resolver casos concretos. Construimos k y resolvemos k ecuaciones en congruencias independientes: sean $m_i = m/n_i$ y consideremos las ecuaciones (independientes)

$$m_i x \equiv a_i \pmod{n_i} \qquad \text{para,} \quad i = \{1, 2, \ldots, k\}$$

Sea s_r solución de la ecuación r-esima ecuación, $m_r x \equiv a_r \pmod{n_r}$. Veamos que $s = \sum_{i=1}^{k} m_i s_i$ es solución de nuestro sistema.

$$s = \sum_{i=1}^{k} m_i s_i \equiv m_r s_r \equiv a_r \pmod{n_r} \quad \text{para todo } r \in \{1, 2, \ldots, k\}$$

Supongamos ahora que s y s' son soluciones del sistema. Entonces como $s \equiv a_i \pmod{n_i}$ y $s' \equiv a_i \pmod{n_i}$,

$$s - s' \equiv 0 \pmod{n_i}. \tag{1}$$

Por último, veamos, aplicando un proceso de inducción, que $s - s'$ es divisible por m: si $k = 1$ no tenemos nada que demostrar, por (1), $s - s'$ es divisible por n_1. Supongamos que

el resultado es cierto para $k-1$ y demostrémoslo para k: por hipótesis $s-s'$ es divisible por $\prod_{1=1}^{k-1} n_i$ y por (1) $s-s'$ es divisible por n_k. Luego como $\mathrm{m.c.d}(\prod_{1=1}^{k-1} n_i, n_k) = 1$, por la proposición anterior, $s-s'$ es divisible por $(\prod_{1=1}^{k-1} n_i)n_k = m$, lo que demuestra el teorema. ■

★ Los ejercicios del 22 al 39 de este tema pueden servirte para comprobar si has asimilado las nociones de esta sección.