Elementos de Matemáticas

Victoria Torroja Rubio

9/10/2024-

Índice general

Capítulo 1

Teoría de Números

Definición 1.1. R es una relación de orden sobre un conjunto E si:

(i) R es reflexiva.

$$\forall x \in E,\ xRx.$$

(ii) R es transitiva.

$$\forall x, y, z \in E,\ xRy \wedge yRz \Rightarrow xRz.$$

(iii) R es antisimétrica.

$$\forall x, y \in E\ xRy \wedge yRx \Rightarrow x = y.$$

Definición 1.2. R es una relación de orden total si R es una relación de orden y

$$\forall x, y \in E,\ xRy \vee yRx.$$

Teorema 1.1 (Principio de la buena ordenación)**.** Todo subconjunto no vacío $S \subset \mathbb{N}$ contiene un primer elemento, i.e.

$$\exists a \in \mathbb{N}, a \in S, \forall b \in S,\ a \leq b.$$

Definición 1.3. Sea R una relación de orden sobre E. Decimos que R es una **buena ordenación** si para cada subconjunto no vacío X de E existe un elemento $a \in X$ tal que a está relacionado con todos los elementos de Y.

Es decir, la relación en $\mathbb{N}$ definida como $a \leq b$ es una buena ordenación (por el Principio de la buena ordenación). Sin embargo, esto no se cumple en $\mathbb{Z}$, pues puedo tomar subconjuntos en el que no exista un menor número (el subconjunto de los números negativos). Sin embargo, se cumple que

$$\forall a \in \mathbb{Z},\ \{m \in \mathbb{Z}\ : a \leq m\}$$

está bien ordenado con la relación definida anteriormente.

Teorema 1.2. Todo buen orden es total.

Definición 1.4 (Relación de divisibilidad)**.** Si $m, n \in \mathbb{Z}$, decimos que m divide a n, es decir, $m|n$, si existe un número entero d tal que $n = m \cdot d$.

La relación de divisibilidad en $\mathbb{N}$ es una relación de orden **no total** (Considera dos números primos distintos, por ejemplo 3 y 5, 3 no divide a 5 y 5 no divide a 3). En $\mathbb{Z}$ no es una relación de orden, pues no se cumple la condición antisimétrica. Para demostrar esto, considera $a \in \mathbb{Z}$ y $-a \in \mathbb{Z}$, entonces tenemos que $a|-a$ y $-a|a$, pero $a \neq -a$ si $a \neq 0$.

1.1. División Euclídea

Teorema 1.3 (División Euclídea)**.** Seam $m, n \in \mathbb{Z}$, con $m \neq 0$. Entonces existen $q, r \in \mathbb{Z}$ únicos tales que

$$n = mq + r, \quad 0 \leq r < |m|.$$

Denominamos a q el cociente y a r el resto.

Demostración. Primero demostraremos la existencia.

(i) Sea $m > 0$.

Sea $S = \{mx - n \ : \ x \in \mathbb{Z}\}$. S tiene números positivos, por lo que existe un mínimo $mt-n > 0$. Entonces tenemos que

$$m(t-1) - n \leq 0 \Rightarrow 0 \leq n - m(t-1).$$

Por tanto,

$$0 \leq n - m(t-1) = \underbrace{n - mt}_{<0} + m < m.$$

Sea $q = t - 1$ y $r = n - m(t-1)$, entonces:

$$n = m(t-1) + n - m(t-1) = mq + r.$$

Esto también se puede demostrar por reducción al absurdo. Nos tenemos que dar cuenta de que para cualquier $q \in \mathbb{Z}$ tenemos que

$$n = mq + (n - mq).$$

La idea es encontrar un $q \in \mathbb{Z}$ que satisfazca la hipótesis para r.

Si consideramos el conjunto $S_0 = \{n - mx \ : \ x \in \mathbb{Z} \wedge n - mx \geq 0\}$. Dado que $S_0 \subset \mathbb{N}$ y $S_0 \neq \emptyset$, podemos encontrar un menor elemento $r = n - mq$ con $q \in \mathbb{Z}$. Entonces, está claro que $r \geq 0$ dado que $r \in S_0$. Si $r \geq m$ tenemos que:

$$0 \leq r - m = n - mq - m = n - m(q+1) = r - m < r.$$

Por tanto, $n - m(q+1)$ sería un elemento de S_0 menor que r, lo cual es una contradicción.

(ii) Si $m < 0$, entonces $-m > 0$ y aplicamos el razonamiento anterior.

Ahora demostramos la unicidad. Suponemos que hay dos cocientes y dos restos,

$$n = mq_1 + r_1 = mq_2 + r_2.$$

Además, suponemos que $q_1 \neq q_2$, por lo que $|q_1 - q_2| \geq 1$. También sabemos que

$$|m\,(q_1 - q_2)\,| = |m|\,|q_1 - q_2| \geq |m|\,.$$

Por otra parte,

$$|m\,(q_1 - q_2)\,| = |r_1 - r_2| < |m|\,.$$

Por tanto tenemos una contradicción, y debe ser que $q_1 = q_2$ y, consecuentemente, $r_1 = r_2$. □

1.2. Máximo Común Divisor

Definición 1.5 (Máximo Común Divisor)**.** Sean $n, m \in \mathbb{Z}$, con $n, m \neq 0$, tenemos que $d = \text{mcd}\,(m, n)$ $(d > 0)$ si

- d divida a a y b
- cualquier otro divisor común de a y b divide a d

Teorema 1.4. Si $m, n \neq 0$ y $m, n \in \mathbb{Z}$, entonces:

(i) Existe algún $\text{mcd}\,(m, n) = d$

(ii) El máximo común divisor es único

(iii) Identidad de Bézout

$$\exists u, v \in \mathbb{Z},\ d = mu + nv.$$

Demostración. **(i)** Esto queda demostrado en la primera parte de la demostración para el Teorema 1.5.

(ii) Si existen dos máximos comunes divisores, d_1 y d_2, tenemos que $d_1|d_2$ y $d_2|d_1$. Por tanto, al tratarse de dos números positivos que se dividen mutuamente ha de ser el caso que $d_1 = d_2$.

(iii) En primer lugar, es obvio que $r_1 = n - mq_1$. Similarmente, $r_2 = m - r_1q_2 = m - (n - mq_1)\,q_2 = -q_2n + m\,(1 + q_1q_2)$. Este proceso lo podemos repetir hasta r_t.

□

Teorema 1.5 (Algoritmo de Euclides)**.** Tenemos $m, n \neq 0$ y $m, n \in \mathbb{Z}$. Si $n > m$, por el Teorema 1.3 tenemos que existen $q_1, r_1 \in \mathbb{Z}$ tales que

$$n = mq_1 + r_1, \quad 0 \leq r_1 < |m|\,.$$

También podemos poner:

$$m = r_1 q_2 + r_2, \quad 0 < r_2 < r_1.$$

En la posición i:

$$r_i = r_{i+1} q_{i+2} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1}.$$

En algún momento vamos a tener:

$$\begin{aligned} r_{t-2} &= r_{t-1} q_t + r_t, \quad 0 < r_t < r_{t-1} \\ r_{t-1} &= r_t q_{t+1} + 0. \end{aligned}$$

Entonces, $\operatorname{mcd}(m, n) = r_t$.

Demostración. Tenemos que cada resto siempre va a ser menor que el módulo del divisor y, además, cada resto va a ser menor que el anterior. Por está razón, llegará un momento en el que el resto sea 0 (en, como mucho, $|m|$ etapas).

Vamos a comprobar que r_t es el máximo común divisor. De la última ecuación tenemos que $r_t | r_{t-1}$. De manera similar, $r_{t-1} | r_{t-2}$, y así sucesivamente hasta llegar a concluir que r_t divide a n y a m. Suponemos que j también divide a m y n. Entonces, de la primera ecuación obtenemos que j divide a r_1, de la segunda obtenemos que j divide a r_2 y así sucesivamente hasta llegar al hecho de que j divide a r_t. □

Lema 1.1. Si $a, b \in \mathbb{Z}$ son no nulos y $a > b$ tenemos que

$$a = bc + r.$$

Cualquier divisor común de a y b es también divisor de r y cualquier divisor común de b y r lo es también de a.

Además, si $r \geq 1$, se cumple que $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$.

[1]

Ejemplo 1.1. Hallamos el máximo común divisor de 26 y 382. Tenemos que:

$$\begin{aligned} 382 &= 26 \cdot 14 + 18 \\ 26 &= 18 \cdot 1 + 8 \\ 18 &= 8 \cdot 2 + 2 \\ 8 &= 2 \cdot 4 + 0. \end{aligned}$$

Por tanto, el primer resto no nulo es 2 y el máximo común divisor de 26 y 382 es 2.

[1] Esto está demostrado en los ejercicios de Matemáticas Básicas y nos ayuda a demostrar el Algoritmo de Euclídes.

Calculamos la identidad de Bézout para estos dos números:

$$\begin{aligned} 2 &= 18 - 2 \cdot 8 \\ &= 18 - (2 \cdot (26 - 18)) \\ &= (382 - 26 \cdot 14) - (2 \cdot (26 - 18)) \\ &= 3 \cdot 382 - 44 \cdot 26. \end{aligned}$$

Aquí nos podemos dar cuenta de que **la Identidad de Bézout no es única**, pues podemos escribir:

$$\begin{aligned} 2 &= 3 \cdot 382 + (-44) \cdot 26 \\ &= 3 \cdot 382 + 382 \cdot 26 \cdot k - 382 \cdot 26 \cdot k + (-44) \cdot 26 \\ &= 382 \cdot (3 + 26k) + 26 \cdot (-44 - 382k)\,. \end{aligned}$$

Definición 1.6 (Mímimo Común Múlitplo)**.** Consideramos $m, n \in \mathbb{Z}$ no nulos. Decimos que $l = \operatorname{mcm}(m, n)$, o l es el mímimo común múltiplo de m y n si:

- ambos lo dividen.
$$m|l \quad \text{y} \quad n|l.$$
- divide a cualquier entero t al que m y n dividen.
$$m|t \ \wedge \ n|t \ \Rightarrow l|t.$$

Teorema 1.6. Si $a, b \in \mathbb{Z}$ no nulos,

$$\operatorname{mcd}(a, b) \cdot \operatorname{mcm}(a, b) = |a \cdot b|\,.$$

1.3. Números Primos

Definición 1.7. Un **número primo** es todo entero $p > 1$ cuyos únicos divisores son 1 y p. A los números no primos se les llama **compuestos**.

Proposición 1.1. Todo número natural $n > 1$ tiene algún divisor primo.

Demostración. Lo demostramos por inducción sobre n. Esto claramente se cumple para $n = 2$, pues $2|2$. Si $n > 2$, asumimos que $\forall k,\ k \leq n - 1$ tiene algún divisor primo. Si n es primo, hemos ganado. Si n es compuesto, es divisible por $t \in \mathbb{N}$ con $t \neq 1$ y $t \neq n$. Por tanto, como $t < n$, t tiene algún divisor primo, que será también divisor de n. □

Proposición 1.2. Todo número natural $n > 1$ se puede expresar como producto de primos.

Demostración. Lo hacemos por reducción al absurdo. Asumimos que existe algún $n \in \mathbb{N}$ que no es producto de primos. Definimos

$$S = \{x \in \mathbb{N} \ : \ x \text{ no es producto de primos}\} \subset \mathbb{N}.$$

Asumimos que k es el elemento más pequeño en S. Entonces k se puede expresar como $k = a \cdot b$ con $a, b \neq k$ y $a, b < k$. Entonces, como a y b son menores que k tenemos que a y b son producto de primos, esto nos da una contradicción.

También se puede demostrar por inducción. Sabemos que se cumple para $n = 2$ pues $2 = 2 \cdot 1$. Si $n > 2$ y asumimos que se cumple para todos los números $k \leq n - 1$. Si n es primo hemos ganado. Si n no es primo, tenemos que n es compuesto y, consecuentemente, $n = a \cdot b$ con $a, b \neq n$ y $a, b < n$. Por tanto, a y b se puede expresar como producto de primos porque son menores que n y, consecuentemente, n se puede expresar como producto de primos. □

Teorema 1.7 (Teorema de Euclides)**.** El conjunto de números primos es infinito.

Demostración. Supongamos que el conjunto de números primos fuera finito, es decir,

$$P = \{p_1, p_2, \ldots, p_n\}.$$

Entonces tomamos $k = 1 + p_1 \cdot p_2 \cdots p_n$. Ningún $p_i \in P$ divide a k, pero k tiene que tener algún divisor primo, por tanto tiene que ser alguno que no está en P. □

Teorema 1.8. Si $a, b \in \mathbb{Z} - \{0\}$ y $m \in \mathbb{Z} - \{0\}$ primo con a. Si m divide a $a \cdot b$ entonces m divide a b.

Demostración. Tenemos que como m es primo con a, entonces $\text{mcd}\,(a, m) = 1$. Aplicando la identidad de Bézout, sabemos que $\exists u, v \in \mathbb{Z}$ tales que

$$1 = mu + av.$$

Además, si multiplicamos por b tenemos que

$$b = bmu + abv.$$

Como $m|m$ y $m|ab$, tenemos que $m|b$. □

Teorema 1.9. Sean $a, b \in \mathbb{Z}$ y p un número primo. Si p divide a $a \cdot b$ entonces $p|a$ o $p|b$.

Demostración. Si $p|a$ hemos ganado. Sin pérdida de generalidad, si p no divide a a, tenemos que $\text{mcd}\,(p, a) = 1$. Por el teorema anterior, debe darse que $p|b$. □

Corolario 1.1. Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ y p primo, tal que

$$p| \prod_{i=1}^{n} a_i.$$

Entonces $p|a_i$ para algún i.

Demostración. Esto se puede demostrar por inducción fuerte. El caso inicial es el teorema anterior. Asumimos que si esto se sostiene para $k \leq n-1$. Si cogemos el producto de n números que es divisible entre p, tenemos que

$$\prod_{i=1}^{n} a_i = a_n \cdot \prod_{i=1}^{n-1} a_i.$$

Por la hipótesis de inducción, tenemos que p divide a a_n o p divide a $a_{n-1} \cdot a_{n-2} \cdots a_1$. Por la hipótesis de inducción, p divide a algún a_i. □

Teorema 1.10. Sea $n > 1$ y $n \in \mathbb{Z}$. La expresión de n como producto de primos es única (salvo el orden).

Demostración. Sabemos que el teorema es cierto para $n = 2$. Asumimos que n es el número más pequeño para el que hay factorizaciones distintas en números primos. Entonces,

$$n = a_1 \cdot a_2 \cdots a_k = p_1 \cdot p_2 \cdots p_l.$$

Sabemos que $p_1|n$. Por el teorema anterior tenemos que $p_1| (a_1 \cdot a_2 \cdots a_k)$, y por tanto, $p_1|a_i$. Como a_i también es primo, tenemos que $a_i = p_1$. Si dividimos entre ambos números nos quedamos con

$$p_2 \cdot p_3 \cdots p_l = a_1 \cdot a_2 \cdots a_{i-1} \cdot a_{i+1} \cdots a_k.$$

Entonces, estas dos factorizaciones son distintas, pero $p_2 \cdot p_3 \cdots p_l < n$, que contradice nuestra hipótesis inicial de que n era el número más pequeño con factorizaciones distintas. □

Definición 1.8. Se dice que $m, n \in \mathbb{Z}$ no nulos son **primos entre sí** cuando $\text{mcd}\,(m, n) = 1$.

Corolario 1.2. Si m y n son coprimos, tenemos que

$$\text{mcm}\,(m, n) = |m \cdot n|\,.$$

Sabemos que todo número entero se puede escribir como una factorización de primos. Es decir, si $n \in \mathbb{Z}$,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad p_1 < p_2 < \cdots < p_r.$$

Para otro $m \in \mathbb{Z}$,

$$m = p_1^{\beta_1} \cdot p_2 \beta_2 \cdots p_r^{\beta_r}.$$

Con $\alpha_i, \beta_i \geq 0$. Para cada $i \in \{1, 2, \ldots, r\}$ denotamos:

$$\gamma_i = \min \alpha_i, \beta_i \quad \text{y} \quad \delta_i = \max \{\alpha_i, \beta_i\}.$$

Vamos a calcular el máximo común divisor y el mínimo común múlitplo.

- $\operatorname{mcd}(m, n) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$
- $\operatorname{mcm}(m, n) = p_1^{\delta_1} \cdots p_r^{\delta_r}$

Además sabemos que $\delta_i + \gamma_i = \alpha_i + \beta_i$.

$$m \cdot n = (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \cdot \left(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}\right)$$

$$= p_1^{\alpha_1+\beta_1} \cdots p_r^{\alpha_r+\beta_r} = p_1^{\delta_1+\gamma_1} \cdots p_r^{\delta_r+\gamma_r}$$

$$= (p_1^{\gamma_1} \cdots p_r^{\gamma_r}) \cdot \left(p_1^{\delta_1} \cdots p_r^{\delta_r}\right) = \operatorname{mcd}(m, n) \cdot \operatorname{mcm}(m, n).$$

[2]

Definición 1.9 (Función de Euler)**.** Sea $n \in \mathbb{Z}$ con $n \neq 0$.

$$\varphi(n) = |\{t \in \mathbb{N} \,:\, 1 \leq t \leq n,\ \operatorname{mcd}(n, t) = 1\}|.$$

Ejemplo 1.2. Tenemos que $\varphi(1) = 1$, además $\varphi(2) = 1$. Para $\varphi(3)$, tenemos que 1 y 2 son coprimos con 3, por lo que $\varphi(3) = 2$. $\varphi(4) = 2$, $\varphi(5) = 4$.

Teorema 1.11. Si p es primo y $k \in \mathbb{Z}^+$. Entonces,

$$\varphi\left(p^k\right) = p^k - p^{k-1}.$$

Ejemplo 1.3.

$$\varphi\left(5^3\right) = 5^3 - 5^2.$$

1.4. Congruencias

Definición 1.10 (Relación de equivalencia)**.** Una relación R en un conjunto E es una relación que verifica:

(i) R es reflexiva.

$$\forall x \in E,\ xRx.$$

(ii) R es simétrica.

$$\forall x, y \in R,\ xRy \Rightarrow yRx.$$

[2]Estamos asumiendo, sin pérdida de generalidad, que $n, m \in \mathbb{N}$, o que son enteros positivos.

(iii) R es transitiva.

$$\forall x, y, z \in R,\ xRy \wedge yRz \Rightarrow xRz.$$

Definición 1.11 (Relación de congruencia módulo n)**.** Si $m \in \mathbb{Z}^+$ decimos que a y b están relacionados por una relación de equivalencia módulo m

$$a \equiv b \mod m,$$

si y solo si $a - b$ es múltiplo de n. Es decir, a y b tienen el mismo resto al dividirlas por m.

Teorema 1.12. La relación de congruencia es una relación de equivalencia en $\mathbb{Z}$. Las clases de equivalencia son los restos al dividir por m.

Demostración. Queda demostrado con las primeras tres propiedades de la siguiente proposición. □

Proposición 1.3 (Propiedades de las congruencias)**.** Si $n > 1$, $n \in \mathbb{N}$ y $a, b, c, d, k \in \mathbb{Z}$.

(i) $a \equiv a \mod n$.

(ii) Si $a \equiv b \mod n$, entonces $b \equiv a \mod n$.

(iii) Si $a \equiv b \mod n$ y $b \equiv c \mod n$, entonces, $a \equiv c \mod n$.

(iv) Si $a \equiv b \mod n$ y $c \equiv d \mod n$, entonces

$$a + c \equiv b + d \mod n \quad \text{y} \quad a \cdot c \equiv b \cdot d \mod n.$$

(v) Si $a \equiv b \mod n$, entonces

$$a + k \equiv b + k \mod n \quad y \quad a \cdot k \equiv b \cdot k \mod n.$$

(vi) Si $a \equiv b \mod n$, entonces $a^m \equiv b^m \mod n$ con $m \in \mathbb{Z}^+$.

Demostración. **(i)** Tenemos que $a - a = 0 = 0 \cdot n$ para $\forall n \in \mathbb{N}$. Por tanto, $a \equiv a \mod n$.

(ii) Si $a \equiv b \mod n$, tenemos que $a - b = n\lambda$ con $\lambda \in \mathbb{Z}$, entonces, $b - a = -n\lambda = (-\lambda)\, n$. Tenemos que $-\lambda \in \mathbb{Z}$, por lo que $b \equiv a \mod n$.

(iii) Si $a \equiv b \mod n$ y $b \equiv c \mod n$, tenemos que

$$a - b = n\lambda_1 \quad \text{y} \quad b - c = n\lambda_2.$$

Por tanto,

$$a - c = n\left(\lambda_1 + \lambda_2\right).$$

Como $\lambda_1 + \lambda_2 \in \mathbb{Z}$, tenemos que $a \equiv c \mod n$.

(iv) Si $a \equiv b \mod n$ y $c \equiv d \mod n$, tenemos que

$$a - b = \lambda_1 n \quad \text{y} \quad c - d = \lambda_2 n.$$

Por tanto,

$$a + c - (b + d) = n(\lambda_1 + \lambda_2).$$

Consecuentemente, $a + c \equiv b + d \mod n$.

Similarmente,

$$\begin{aligned} ac &= (\lambda_1 n + b)(\lambda_2 n + d) \\ &= \lambda_1\lambda_2 n^2 + \lambda_1 dn + \lambda_2 bn + bd \\ \iff ac - bd &= n(\lambda_1\lambda_2 n + \lambda_1 d + \lambda_2 b). \end{aligned}$$

Por tanto, $ac \equiv bd \mod n$.

(v) Si $a \equiv b \mod n$, tenemos que

$$a - b = \lambda n \iff (a + k) - (b + k) = \lambda n.$$

Por tanto, $a + k \equiv b + k \mod n$.

Similarmente,

$$a - b = \lambda n \iff k(a - b) = k(\lambda n) \iff a \cdot k - b \cdot k = (k\lambda) n \iff a \cdot k \equiv b \cdot k \mod n.$$

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

$$a^m - b^m = (a - b)\left(a^{m-1} + a^{m-2}b + \cdots + b^{m-1}\right) = \lambda n \cdot \left(a^{m-1} + a^{m-2}b + \cdots + b^{m-1}\right).$$

Por tanto, $a^m \equiv b^m \mod n$.

□

Definición 1.12 (Congruencia lineal)**.** Si $a, b, m \in \mathbb{Z}$ con $m > 0$, tenemos una congruencia lineal si:

$$ax \equiv b \mod m.$$

Donde a, b y m están dados. [a]

[a] Tenemos que ver si la congruencia tiene solución, cuántas tiene y dónde están.

Proposición 1.4. Si tenemos una congruencia lineal $ax \equiv b \mod m$. Si α es una solución de la misma, entonces todo $\beta \equiv \alpha \mod m$ es también solución de la congruencia. [a]

[a] Esto nos permite reducir las posibles soluciones a los elementos de $\mathbb{Z}_m$.

Demostración. Sea α una solución de la congruencia lineal $ax \equiv b \mod m$. Por definición,

$$\exists \lambda \in \mathbb{Z},\ a\alpha - b = \lambda m.$$

Por otra parte, si $\beta \equiv \alpha \mod m$, tenemos que

$$\exists \mu \in \mathbb{Z},\ \beta - \alpha = \mu m \Rightarrow \alpha = \beta - \mu m.$$

Entonces,

$$\alpha a - b = a\left(\beta - \mu m\right) - b = \lambda m.$$

Por otro lado,

$$a\beta - b = \lambda m + a\mu m = \left(\lambda + a\mu\right) m.$$

Entonces, β es solución de la congruencia lineal $ax \equiv b \mod m$. □

Definición 1.13. Definimos el conjunto de las clases de equivalencia $a \equiv b \mod n$como $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\} = \{0, 1, 2, \ldots, n-1\}.$$

Ejemplo 1.4. $2x \equiv 1 \mod 4$. Esta congruencia lineal no tiene soluciones porque

$$2x - 1 = 4k$$

es imposible, pues $\forall x \in \mathbb{Z},\ 2x - 1$ es impar. Las posibles soluciones son $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Si comprobamos con $x \in \mathbb{Z}_4$, ningún valor funciona. Por tanto, no tiene solución.

Ejemplo 1.5. $2x \equiv 2 \mod 8$. Comprobamos con las posibles soluciones, que están en el conjunto $\mathbb{Z}_8$. Tenemos que 1 y 5 son soluciones pues

$$2 \cdot 1 - 2 = 0 \cdot 8 \quad \text{y} \quad 2 \cdot 5 - 2 = 1 \cdot 8.$$

Ejemplo 1.6. $4x \equiv 4 \mod 8$. Comprobamos con los elementos de $\mathbb{Z}_8$. Funcionan el 1, 3, 5 y el 7.

Ejemplo 1.7. **(a)** $12427 \mod 10$. Sabemos que

$$12427 = 7 + 2 \cdot 10 + 4 \cdot 10^2 + 2 \cdot 10^3 + 1 \cdot 10^4.$$

Entonces, el resto de esta división entre 10 será 7, por lo que $12427 \equiv 7 \mod 10$.

(b) $12112 \times 347 \mod 3$. Sabemos que $12112 \equiv 1 \mod 3$ y $347 \equiv 2 \mod 3$. Por tanto,

$$12112 \times 347 \mod 3 \Rightarrow 12112 \times 347 \equiv 2 \mod 3.$$

Por lo que $12112 \times 347 \equiv 2 \mod 3$.

(c) $22^{1327} \mod 21$. Sabemos que $22 \equiv 1 \mod 21$, entonces,

$$22^{1327} \equiv 1^{1327} = 1 \mod 21.$$

(d) $10^{123} \mod 8$. Sabemos que $10 \equiv 2 \mod 8$, entonces

$$10^{123} \equiv 2^{123} = \left(2^3\right)^{41} = 8^{41} \mod 8.$$

$$\therefore 10^{123} \equiv 0 \mod 8.$$

Teorema 1.13. Sean $a, b, m \in \mathbb{Z}$ con $m > 0$, y sea $d = \text{mcd}\,(a, m)$. Entonces, la congruencia lineal: $ax \equiv b \mod m$ tiene solución si y solo si $d|b$ y, en este caso, el número de soluciones $\mathbb{Z}_m$ es d.

Demostración. **(i)** Suponemos que $d = \text{mcd}\,(a, m)\,|b$, es decir, $\exists k \in \mathbb{Z}$ tal que $b = dk$. Como $d = \text{mcd}\,(a, m)$ sabemos que $\exists u, v \in \mathbb{Z}$ tales que

$$d = au + mv \quad \text{Identidad de Bézout.}$$

Entonces, tenemos que

$$b = dk = (au + mv)\,k = auk + mvk \Rightarrow b - auk = mvk.$$

Es decir, $b \equiv auk \mod m$. Por la propiedad simétrica, $auk \equiv b \mod n$. Si $x = uk$, es solución de la congruencia.

(ii) Asumimos que existe una solución α, por lo que $\exists \lambda \in \mathbb{Z}$ tal que $a\alpha - b = \lambda m$. Por tanto

$$b = a\alpha - \lambda m.$$

Como $d = \text{mcd}\,(a, m)$, $d|a$ y $d|m$. Entonces, $d|b$ (por la ecuación anterior).

En cuanto al número de soluciones, si $d = 1 = \text{mcd}\,(a, m)$, vamos a asumir que existen dos soluciones, $\alpha, \beta \in \mathbb{Z}$. Tenemos que $a\alpha \equiv b \mod m$, por lo que $a\alpha - b$ es múltiplo de m y $a\beta - b$ también. Si restamos las dos ecuaciones, tenemos que

$$a\alpha - a\beta = a\,(\alpha - \beta) \quad \text{múltiplo de } m\ .$$

Además, como $d = 1$, tenemos que a es primo con m, tenemos que $\alpha - \beta$ es múltiplo de m. Es decir, $m|\alpha - \beta$. Sin embargo, $\alpha - \beta \in \mathbb{Z}_m$. Por tanto, $\alpha - \beta = 0$ y $\alpha = \beta$.

Si $d > 1$ y $d|b$, tenemos que $a = a_1 d$, $b = b_1 d$ y $m = m_1 d$. Entonces, sabemos que

$$a_1 dx \equiv b_1 d \mod m_1 d.$$

Por tanto,

$$a_1 dx - b_1 d = k m_1 d.$$

Por tanto,

$$a_1 x - b_1 = k m_1 \iff a_1 x \equiv b_1 \mod m_1.$$

Además, sabemos que $\text{mcd}\,(a_1, m_1) = 1$. Por tanto, estamos en el caso anterior, que nos dice que $\exists \alpha \in \mathbb{Z}_{m_1}$ que es única. Las soluciones serán,

$$\alpha,\ \alpha + m_1,\ \alpha + 2m_1,\ \ldots.$$

Es decir, las soluciones tienen la forma $\alpha + (d-1)\,m_1$. □

Ejemplo 1.8. $51x \equiv 27 \mod 123$

(1) $\text{mcd}\,(51, 123) = 3$. Además, $3|27$, por lo que tiene solución y, en concreto, tiene 3 soluciones.

(2) Construimos la congruencia auxiliar: $17x \equiv 9 \mod 41$. Sabemos que esta congruencia tiene solución única. Sea $a_1 = 17$ y $m_1 = 41$. Encontramos la identidad de Bézout para ellos:

$$1 = 41 \cdot 5 + 17 \cdot (-12).$$

Multiplicamos todo por 9,

$$9 = 9 \cdot 5 \cdot 41 - 9 \cdot 12 \cdot 17.$$

Tomamos módulo 41,

$$9 \equiv -9 \cdot 12 \cdot 17 \mod 41 \iff 17(-9 \cdot 12) \equiv 9 \mod 41.$$

Es decir, $x \equiv -9 \cdot 12 = 108 \mod 41$. Otra solución será,

$$x \equiv -108 + 3 \cdot 41 \equiv 15 \mod 41.$$

A partir de aquí, podemos deducir el resto de soluciones:

$$\alpha_1 = 15 \quad \text{o} \quad \alpha \equiv 15 \mod 41.$$

$$\alpha_2 = 15 + 41 = 56.$$

$$\alpha_3 = 15 + 2 \cdot 41 = 97.$$

Ejemplo 1.9. $17x \equiv 5 \mod 13$. Tenemos que $\text{mcd}(17, 13) = 1$, por lo que tendremos sólo una solución. Encontramos la identidad de Bézout:

$$1 = (-3) \cdot 17 + 4 \cdot 13.$$

$$\therefore 5 = (-15) \cdot 17 + 20 \cdot 13.$$

Por tanto, tenemos que $17 \cdot (-15) \equiv 5 \mod 13$, por lo que la solución será $x \equiv -15 \equiv 11 \mod 13$.

Ejemplo 1.10. $66x \equiv 42 \mod 168$. Tenemos que $d = \text{mcd}(66, 168) = 6$, y $6|42$, por lo que esta congruencia lineal va a tener 6 soluciones en $\mathbb{Z}_{168}$. Encontramos la congruencia auxiliar:

$$11x \equiv 7 \mod 28.$$

Hallamos la identidad de Bézout para $\text{mcd}(11, 28) = 1$:

$$1 = 2 \cdot 28 + (-5) \cdot 11.$$

$$\therefore 7 = 14 \cdot 28 + (-35) \cdot 11.$$

Por todo ello, tenemos que $11 \cdot (-35) \equiv 7 \mod 28$, por lo que las soluciones serán,

$$x \equiv -35 \mod 28 \Rightarrow x \equiv 21 \mod 168.$$

Sumamos múltiplos de 28 hasta obtener 6 soluciones.

Proposición 1.5. Si m y n son primos entre sí, entonces $[x]_m \cap [x]_n = [x]_{mn}$.

Demostración. **(i)** Si $x \in \mathbb{Z}$ y $m, n \in \mathbb{N}$ siempre tenemos la inclusión

$$[x]_{mn} \subset [x]_m \cap [x]_n .$$

En efecto, si $y \in [x]_{mn}$, tenemos que existe $\lambda \in \mathbb{Z}$ tal que

$$y - x = \lambda mn.$$

Por tanto, tenemos que y es congruente con x módulo n y módulo m.

(ii) Si m, n son primos entre sí y $y \in [x]_m \cap [x]_n$, tenemos que existen $\lambda, \mu \in \mathbb{Z}$ tales que

$$y - x = \lambda m = \mu n.$$

Como $\operatorname{mcd}(m, n) = 1$, tenemos que $n|\lambda$, por lo que $\lambda = \lambda_1 n$. Por tanto,

$$y - x = \lambda m = \lambda_1 mn.$$

Por tanto, $y \in [x]_{mn}$.

□

Observación 1.1. Si $a_1 x \equiv b_1 \mod m$ y $a_2 x \equiv b_2 \mod n$, y α es solución de cada una de las congruencias, cada $\beta \in [\alpha]_{mn}$ es también solución.

Teorema 1.14. Sean m y n primos entre sí, con $m, n \in \mathbb{Z}$. Si cada una de las congruencias lineales:

$$a_1 x \equiv b \mod m \quad \text{y} \quad a_2 x \equiv b_2 \mod n,$$

tiene solución, existe una solución común a las dos congruencias en $\mathbb{Z}_{mn}$. Además, si $\operatorname{mcd}(a_1, m) = \operatorname{mcd}(a_2, n) = 1$, tenemos que la solución es única en $\mathbb{Z}_{mn}$.

Demostración. Consideramos dos soluciones, α_1 y α_2. Consideramos $x \equiv \alpha_1 \mod m$ y $x \equiv \alpha_2$ mód n. Vamos a ver que tienen soludión común en $\mathbb{Z}_{mn}$. Sabemos que $\operatorname{mcd}(m, n) = 1$. Por tanto, $\exists u, v \in \mathbb{Z}$ tales que

$$mu + nv = 1.$$

Tomamos módulos en esta expresión:

$$nv \equiv 1 \mod m \quad \text{y} \quad mu \equiv 1 \mod n.$$

Vamos a ver que $\alpha_1 nv + \alpha_2 mu$ es una solución para cada una de las congruencias. Consideramos

$$\alpha_1 nv + \alpha_2 mu = \alpha_1 nv + \alpha_2 (1 - nv) = \alpha_2 + n(\alpha_1 v - \alpha_2 v).$$

Si hacemos módulo n, tenemos que

$$\alpha_1 nv + \alpha_2 mu \equiv \alpha_2 \mod n.$$

Por tanto, va a ser una solución de la segunda congruencia. Similarmente,

$$\alpha_1 nv + \alpha_2 mu = \alpha_1 (1 - mu) + \alpha_2 mu = \alpha_1 + m(\alpha_2 u - \alpha_1 u).$$

$$\therefore \alpha_1 nv + \alpha_2 mu \equiv \alpha_1 \mod m.$$

Por tanto, $\alpha_1 nv + \alpha_2 mu$ es solución de ambos sistemas. Como $[\alpha]_n \cap [\alpha]_m = [\alpha]_{mn}$, tenemos que $\beta \in [\alpha]_{mn}$ es solución del sistema.

Ahora demostramos la unicidad. Sean $\alpha, \beta \in \mathbb{Z}_{mn}$ son soluciones del sistema de congruencias. Por ser soluciones de la primera, y tener está única solución en Z_m, α y β son congruentes módulo m. Por la transitividad tenemos que

$$\alpha \equiv \beta \mod m.$$

Similarmente,

$$\alpha \equiv \beta \mod n.$$

Por tanto, tenemos que $\alpha \in [\beta]_m \cap [\beta]_n = [\beta]_{mn}$. Por tanto, $\alpha = \beta$, por se ambos números elementos de $\mathbb{Z}_{mn}$. □

Corolario 1.3. Tenemos $m, n \in \mathbb{Z}$ y m, n primos entre sí. Entonces las congruencias

$$x \equiv b_1 \mod m \quad \text{y} \quad x \equiv b_2 \mod n$$

tiene solución única en $\mathbb{Z}_{mn}$.

Ejemplo 1.11. $x \equiv 4 \mod 8$ y $x \equiv -1 \mod 15$. Tenemos que $\text{mcd}(8, 15) = 1$. La identidad Bézout es:

$$1 = 2 \cdot 8 + (-1) \cdot 15.$$

La solución común estará en $\mathbb{Z}_{120}$. Tenemos que la solución será

$$\alpha = \alpha_1 \cdot 2 \cdot 8 + \alpha_2 \cdot (-1) \cdot 15 = (-1) \cdot 2 \cdot 8 + 4 \cdot (-1) \cdot 15 = -76.$$

Para que sea positiva le sumamos múltiplos de 120, es decir, $\alpha \equiv 44 \mod 120$.

Teorema 1.15 (Teorema Chino del resto)**.** Sean $n_1, \ldots, n_k \in \mathbb{Z}^+$, primos entre sí 2 a 2. Si cada una de las congruencias lineales $a_i x \equiv b_i \mod n_i$ tiene solución, entonces existe una solución común a todas ellas en $\mathbb{Z}_{n_1 \cdots n_k}$.

Demostración. Ya hemos demostrado el caso $n = 2$. Asumimos que es cierto para $n-1$ congruencias, entonces las primeras $n-1$ congruencias tendrán solución común, a la que llamaremos α. También cualquier solución de la congruencia

$$x \equiv \alpha \mod m_1 \cdots m_{n-1},$$

es solución de las primeras $n-1$ congruencias. Ahora podemos considerar el siguiente sistema de congruencias:

$$\begin{cases} x \equiv \alpha \mod m_1 \cdots m_{n-1} \\ a_n x \equiv b_n \mod m_n \end{cases}.$$

Como $m_1 \cdots m_{n-1}$ y m_n son primos entre sí, el sistema de congruencias tiene solución común, que es de todo el sistema. La unicidad de las soluciones en el caso de que $\text{mcd}\,(a_i, m_i) = 1,\ \forall i = 1, 2, \ldots, n$ se puede demostrar también por inducción de la siguiente manera: la solución α de las $n-1$ primeras congruencias del sistema es única, como la de la n-ésima también lo es. □

Ejemplo 1.12.

$$\begin{cases} 5x \equiv 6 & \text{mód } 12 \\ 2x \equiv 5 & \text{mód } 7 \\ 3x \equiv 1 & \text{mód } 5 \end{cases}.$$

Primero tenemos que ver que los módulos son primos entre sí dos a dos.

$$\text{mcd}\,(12, 7) = \text{mcd}\,(5, 7) = \text{mcd}\,(12, 5) = 1.$$

Cada congruencia tiene solución.

$$\begin{cases} x \equiv \alpha_1 & \text{mód } 12 \\ x \equiv \alpha_2 & \text{mód } 7 \\ x \equiv \alpha_3 & \text{mód } 5 \end{cases}.$$

Cogemos dos congruencias y las resolvemos para obtener $x \equiv \alpha \mod 12 \cdot 7$. Cogemos la anterior y una de las otras dos restantes para obtener $x \equiv \beta \mod 12 \cdot 7 \cdot 5$. Obtenemos las siguientes soluciones:

$$\begin{cases} x \equiv 6 & \text{mód } 12 \\ x \equiv 6 & \text{mód } 7 \\ x \equiv 2 & \text{mód } 5 \end{cases}.$$

Cogemos las dos primeras congruencias:

$$1 = 3 \cdot 12 + (-5) \cdot 7.$$

Sabemos que la solución será de la forma:

$$\alpha \equiv 6 \cdot 3 \cdot 12 + 6 \cdot (-5) \cdot 7 \equiv 6 \quad \text{mód } 84.$$

Ahora resolvemos el siguiente sistema de congruencias:

$$\begin{cases} x \equiv 2 & \text{mód } 5 \\ x \equiv 6 & \text{mód } 84 \end{cases}.$$

Tenemos que

$$1 = 17 \cdot 5 - 84.$$

Por tanto, la solución tendrá la forma:

$$\beta \equiv 6 \cdot 17 \cdot 5 - 2 \cdot 84 \equiv -334 \equiv 342 \quad \text{mód } 420.$$

[3]

[3] En la solución de un sistema de dos congruencias, se multiplica la solución de cada congruencia de forma cruzada, es decir, si α_1 es solución de $a_1 \equiv b_1 \mod m_1$ y α_2 es solución de la congruencia $a_2 x \equiv b_2 \mod m_2$, entonces la solución de ambas congruencias será $\alpha \equiv \alpha_2 u m_1 + \alpha_1 v m_2 \mod m_1 \cdot m_2$ (u y v proceden de la Identidad de Bézout).

Definición 1.14 (Función de Euler)**.** Si $n \in \mathbb{Z}$,

$$\varphi(n) = |t \in \mathbb{N},\ 1 \leq t \leq n,\ \operatorname{mcd}(t,n) = 1|.$$

Proposición 1.6. Si p es primo, tenemos que

$$\varphi(p) = p - 1.$$

Demostración. Es trivial, pues todos los números menores a p serán coprimos con p, pues p es primo. □

Proposición 1.7. Si p es primo y $k > 1$,

$$\varphi\left(p^k\right) = p^k - p^{k-1}.$$

Demostración. Tenemos que el número de números de 1 a p^k que tienen a p como divisor serán $\dfrac{p^k}{p}$. Por tanto, el número de números que no tienen a p como divisor será:

$$p^k - p^{k-1}.$$

□

Teorema 1.16. Si a y b son primos entre sí, entonces

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Corolario 1.4. Si $n_1, \ldots, n_k \in \mathbb{Z}^+$ y primos entre sí (2 a 2), entonces

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k).$$

Corolario 1.5. Si $n > 2$ con $n \in \mathbb{Z}$ y $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ ($p_1, \ldots, p_k$ primos). Entonces tenemos que

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Demostración. Por una proposición anterior, tenemos que

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).$$

Aplicando el corolario anterior:

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}).$$

Entonces tenemos que,

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

□

Ejemplo 1.13. $\varphi(151200)$. Si factorizamos 151200 en sus factores primos tenemos que:

$$151200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7.$$

Entonces:

$$\varphi(151200) = 151200 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2^8 \cdot 3^3 \cdot 5 = 34560.$$

Teorema 1.17 (Teorema de Euler)**.** Si a y n son primos entre sí, entonces $a^{\varphi(n)} \equiv 1 \mod n$.

Corolario 1.6 (Pequeño Teorema de Fermat)**.** Si p es primo y a no es múltiplo de p, entonces $a^{p-1} \equiv 1 \mod p$.

Teorema 1.18 (Inversa módulo n)**.** Si $1 \leq a \leq n$ y $\operatorname{mcd}(a, n) = 1$, entonces a tiene inverso módulo n. Es decir,

$$\exists c,\ a \cdot c = 1 \mod n, \quad 1 \leq c < n.$$

Si $\operatorname{mcd}(a, n) \neq 1$, a no tiene inversa módulo n. Para averiguar la inversa tenemos que resolver esta congruencia:

$$ac \equiv 1 \mod n \begin{cases} a^{-1} \equiv c \mod n \\ \operatorname{mcd}(a, n) = 1 \end{cases}.$$

Ejemplo 1.14. $777^{-1} \mod 1009$. Queremos resolver la congruencia $777x \equiv 1 \mod 1009$. Calculamos la identidad de Bézout para obtener:

$$1 = -274 \cdot 777 + 211 \cdot 1009 \Rightarrow x \equiv -274 \equiv 735 \mod 1009.$$

Ejemplo 1.15. Calculamos $5^{28575} \mod 17$. En primer lugar, intentamos aplicar el teorema de Euler. Vemos que $\operatorname{mcd}(5, 17) = 1$, por lo que lo podemos aplicar. Entonces, tenemos que

$$\varphi(17) = 16.$$

Además, tenemos que

$$5^{28575} \equiv 5^{16\cdot 1785+15} \equiv 5^{15} \mod 17.$$

Por otro lado tenemos que

$$5^{16} \equiv 5^{15} \cdot 5 \equiv 1 \mod 17.$$

Por tanto,

$$5^{15} \equiv 5^{-1} \mod 17.$$

Para calcular $5^{-1} \mod 17$ tenemos que resolver la congruencia $5x \equiv 1 \mod 17$. Para ello hacemos la identidad de Bézout:

$$1 = 7 \cdot 5 - 2 \cdot 17 \Rightarrow x \equiv 5^{-1} \equiv 7 \mod 17.$$

$$\therefore 5^{28575} \equiv 7 \mod 17.$$

Teorema 1.19 (Propiedad exponencial de las congruencias)**.** Si $a \equiv b \mod n$ con $k \in \mathbb{N}$, entonces $a^k \equiv b^k \mod n$.

Ejemplo 1.16. (i) Para calcular $41^5 \mod 43$, tenemos en cuenta que $41 \equiv -2 \mod 43$, por tanto,

$$41^5 \equiv (-2)^5 \equiv -32 \equiv 11 \mod 43.$$

(ii) Calculamos $11^{13} \mod 85$. Iteramos:

$$\begin{aligned}
11^2 &\equiv 121 \equiv 36 \mod 85 \\
11^3 &\equiv 11^2 \cdot 11 \equiv 36 \cdot 11 \equiv 56 \mod 85 \\
11^4 &\equiv 11^3 \cdot 11 \equiv 56 \cdot 11 \equiv 21 \mod 85 \\
11^5 &\equiv 11^4 \cdot 11 \equiv 21 \cdot 11 \equiv 61 \mod 85 \\
11^6 &\equiv 11^5 \cdot 11 \equiv 61 \cdot 11 \equiv 76 \mod 85.
\end{aligned}$$

Entonces tenemos que

$$11^{13} \equiv 11^6 \cdot 11^6 \cdot 11 \equiv 76 \cdot 76 \cdot 11 \equiv 63536 \equiv 41 \mod 85.$$

Teorema 1.20 (Procedimiento sistemático)**.** Sea $k \in \mathbb{N}$ suma de potencias de 2. Es decir,

$$\begin{aligned}
a^4 &\equiv \left(a^2\right)^2 \mod n \\
a^8 &\equiv \left(a^4\right)^2 \mod n \\
a^{16} &\equiv \left(a^8\right)^2 \mod n \\
a^{32} &\equiv \left(a^{16}\right)^2 \mod n.
\end{aligned}$$

Ejemplo 1.17. En el ejemplo anterior sería:

$$11^{13} = 11^8 \cdot 11^4 \cdot 11 = \left(11^4\right)^2 \cdot 11^4 \cdot 11.$$

Ejemplo 1.18. Este es un ejemplo de un ejercicio de examen.

(a) Hallar el menor número natural n para que la congruencia $329x \equiv 729 + n \mod 1222$ tenga solución.

Para que la congruencia tenga solución tiene que darse que $\mcd(329, 122) \mid 729 + n$. Tenemos que $\mcd(329, 1222) = 47$. Entonces tenemos que

$$729 + n \equiv 0 \mod 47.$$

Además, tenemos que $729 \equiv 40 \mod 47$, por lo que

$$n \equiv -40 \mod 47 \Rightarrow n \equiv 7 \mod 47.$$

(b) Resolver la congruencia para el valor de n obtenido en **(a)**.

Resolvemos la congruencia $329x \equiv 799 \mod 1222$. Hallamos la congruencia auxiliar:

$$7x \equiv 17 \mod 26.$$

Con la identidad de Bézout, tenemos que $1 = 3 \cdot 26 + (-11)\,7$, así

$$17 = 51 \cdot 26 + (-187)\,7 \Rightarrow x \equiv 21 + 26k \mod 1222,\ 0 \leq k \leq 47.$$

1.5. Aplicaciones

1.5.1. Dígitos de control

Definición 1.15 (La letra del D.N.I.)**.** La letra del D.N.I. se obtiene dividiendo el número del D.N.I. entre 23 y luego traduciendo cada uno de los 23 posibles restos a una letra predeterminada [a] .

[a] Hay una tabla.

Ejemplo 1.19. La letra que corresponde al D.N.I. 12345678 es la Z, pues el resto de este número entre 23 es 14.

Definición 1.16 (Los dígitos de control.)**.** Tenemos cuatro dígitos de control. El primero es la última cifra del número que se obtiene sumando los productos de las cifras número de serie del soporte, respectivamente, por 7,3,1,7,3,1,7,3,1, una vez convertidas las tres primeras letras según la tabla.
El en caso del segundo, se procede como en el caso anterior para el campo de la fecha de nacimiento.
Para el tercer número se hace lo mismo solo que en este caso para la fecha de vencimiento.
Para el último número, se hace lo mismo para la concatenación de los campos 3, 4, 5, 7, 8, 10 y 11 (sustituyendo las letras por números según la tabla).

Definición 1.17 (Número de registro personal de los funcionarios.)**.** Está formado por el número de su D.N.I.y dos cifras más. La primera es el resto del número anterior entre 7 (entonces estará entre 0 y 6). La segunda es este mismo resto más dos.

1.5.2. Criptografía

Consiste en transformar un mensaje claro en otro cifrado (cifrar) y en reconvertir el mensaje cifrado en mensaje claro (descifrar). Existen varios procedimientos.

Definición 1.18 (Procedimiento aditivo.)**.** La clave del cifrado es un número b que se suma a cada uno de los del mensaje. Para obtener números entre 0 y 36 se obtiene el resto módulo 37 de la suma del número original más b. El receptor debe conocer b y no tiene más que restar b módulo 37 para descifrar el mensaje.

Ejemplo 1.20. Vamos a cifrar el mensaje 'EL 1 A LAS 3' con la clave aditiva $b = 17$. Primero traducimos cada carácter a su valor numérico según la tabla:

$$14\ 21\ 36\ 1\ 36\ 10\ 36\ 21\ 10\ 28\ 36\ 3.$$

Su codificación será:

$$31\ 1\ 16\ 18\ 16\ 27\ 16\ 1\ 27\ 8\ 16\ 20.$$

Según la tabla, esto se traduce en 'V1GIGRG1RGK'.

Definición 1.19 (Procedimiento multiplicativo.)**.** Es lo mismo que el anterior solo que en vez de sumar se multiplica por un factor a. Es decir, el cifrado de la conversión numérica de cada carácter será $ma \mod 37$. Para que el cifrado sea biyectivo es necesario que todas las congruencias lineales $ax \equiv y \mod 37$ tengan una única solución para cualquier $y \in \mathbb{Z}_{37}$. Esto ocurre sí y solo sí

$$\operatorname{mcd}(a, 37) = 1.$$

Para descifrar el mensaje se considera a^{-1}, inverso de a en $\mathbb{Z}_{37}$. Así,

$$(ma)\, a^{-1} \equiv m \mod 37.$$

[a]

[a] Es decir, el número buscado m es el resto de dividir $(ma)\, a^{-1}$ entre 37.

Ejemplo 1.21. Vamos a cifrar el mensaje anterior: 'El 1 A LAS 3', con la clave multiplicativa $a = 7$. Su traducción venía dada en el ejemplo anterior y su codificación será:

$$24\ 36\ 30\ 7\ 30\ 33\ 30\ 36\ 33\ 11\ 30\ 21.$$

Esto se traduce en 'O U7UXU XBUL'. Ahora, el receptor debe multiplicar la cadena numérica por el inverso de 7 en $\mathbb{Z}_{37}$, que es 16. Así obtenemos la cadena

$$384\ 576\ 480\ 112\ 480\ 528\ 480\ 576'; 528\ 176\ 480\ 336,$$

cuyos restos módulo 37 constituyen la cadena original.

Definición 1.20 (Procedimiento exponencial)**.** Se quiera cifrar un número m, se elevará este a un exponente k y el resultado se reducirá módulo n, siendo k y n números naturales elegidos convenientemente.

Teorema 1.21. Sean $n, t \in \mathbb{N}$ tales que

$$t \equiv 1 \mod (\varphi(n)).$$

Dado $m \in \mathbb{N}$ si se verifica alguna de las siguientes hipótesis

- m y n son primos entre sí.
- n es primo.
- n es producto de dos primos distintos.

entonces,

$$m^t \equiv m \mod n.$$

Observación 1.2. Este resultado se utiliza para encriptar de la siguiente manera: se elige n primo o producto de dos primos distintos, se calcula $\varphi(n)$, se toma k primo con $\varphi(n)$ y se calcula j, el inverso de k en $\mathbb{Z}_{\varphi(n)}$. De esta manera,

$$kj \equiv 1 \mod \varphi(n).$$

Suponiendo que el emisor y el receptor conocen k y j, el emisor mandará el mensaje codificado que es r, el resto de la división de k^k entre n. Para descodificar, teniendo en cuenta que

$$m^{kj} \equiv m \mod n,$$

el receptor calculará

$$r^j \equiv \left(m^k\right)^j \equiv m^{jk} \equiv m \mod n.$$

Así se recupera el mensaje original m. [4]

Definición 1.21 (Procedimiento RSA)**.** Se da un par (n, k). Cada letra se traduce a su número correspondiente a y se calcula $a^k \mod n$. El resultado del cifrado es un número, no se vuelve a traducir a letras. Ahora, para descifrar es necesario calcular j, el inverso de k módulo $\varphi(n)$.

[4] Este procedimiento solo es válido si $m < n$.

A continuación, se eleva cada número del cifrado a j módulo n.

Ejemplo 1.22. Hacemos un ejemplo con la palabra 'ADN' y la clave $(n, k) = (55, 3)$. Tenemos que los números correspondientes son 10 13 23. Elevamos cada uno de los números a 3 mód 55 obteniendo el resultado 10 52 12. Ahora, para descifrar, calculamos el inverso de $k = 3$ módulo $\varphi(n) = \varphi(55) = 40$. En este caso, obtenemos que $j = 27$. Así, elevando cada uno de los elementos del cifrado a $j = 27$ módulo 55 obtenemos la configuración inicial 10 13 23, es decir, las letras 'ADN'.

Capítulo 2

Grupos de simetrías. Mosaicos.

Objetivo: Estudiar y clasificar todas las formas posibles de cubrir el plano con copias idénticas de una 'ficha' o 'pieza' (tesela) de manera períodica: mosaicos.

Herramientas: Estudio de los movimientos en el plano que preservan la teselación.

Elementos matemáticos:

- Grupo - Subgrupo
- Grupo de movimento en el plano
- Simetrías

Aplicaciones:

- Retículos
- 17 grupos cristalográficos planos

2.1. Grupos. Isomorfismos y homomorfismos de grupos.

Definición 2.1 (Grupo)**.** Se define como **grupo** al par ordenado $(G, \cdot)$ formado por un conjutno G y una operación interna

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\to a \cdot b. \end{aligned}$$

tales que

(1) La operación es asociativa.

$$\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)\,.$$

(2) Existe un elemento neutro.

$$\exists e \in G, \forall a \in G,\ e \cdot a = a \cdot e = a.$$

(3) Existe el inverso.

$$\forall a \in G, \exists a^{-1} \in G\ a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Si se cumple también la propiedad conmutativa:

$$\forall a, b \in G,\ a \cdot b = b \cdot a,$$

se denomina grupo conmutativo o **abeliano**.

Ejemplo 2.1. (1) $(\mathbb{Z}, +)$ es un grupo abeliano.

(2) $(\mathbb{Q}, \cdot)$ no es un grupo pues $0 \in \mathbb{Q}$ no tiene inverso.

(3) $(\mathbb{Q}^*, \cdot)$ es un grupo abeliano.

(4) Tenemos que $(2\mathbb{Z} + 1, +)$ no es un grupo, pues la suma de dos números impares es un número par. Similarmente, $(2\mathbb{Z} + 1, \cdot)$ no es un grupo por la ausencia de inversos.

(5) El conjunto de las matrices 2×2 es un grupo abeliano con la suma. $(M_{2\times 2}, +)$ es un grupo abeliano.

(6) El conjunto de las matrices $n \times n$ con $\det \neq 0$, $(M_{n\times n}, \cdot)$, es un grupo abeliano. En concreto, en el caso de las matrices 2×2, recibe el nombre de **grupo general lineal de orden 2** y se denota como $\mathrm{GL}(2, \mathbb{R})$ o $\mathrm{GL}(2)$.

(7) El conjunto de matrices 2×2, $(M_{2\times 2}, \cdot)$, con $\det = 1$ es un grupo y se denomina **grupo especial lineal**: $\mathrm{SL}(2)$.

(8) El conjunto de matrices ortogonales $(A^T = A^{-1})$ es un grupo al que se denomina **grupo ortogonal**: $\mathrm{O}(2)$.

(9) Las matrices ortogonales con $\det = 1$ se denomina **grupo especial ortogonal**: $\mathrm{SO}(n)$.

(10) $(\mathbb{Z}_n, +)$ con $n \in \mathbb{N}$ forma un grupo abeliano.

(11) Si p es primo, $(\mathbb{Z}_p, \cdot)$ también es un grupo abeliano.

Proposición 2.1. Sea $(G, \cdot)$ un grupo.

(1) Propiedades cancelativas por la derecha y por la izquierda de un grupo:

$$a \cdot c = b \cdot c \Rightarrow a = b$$
$$c \cdot a = c \cdot b \Rightarrow a = b.$$

(2) El elemento neutro de un grupo es único.

(3) Cada elemento de un grupo tiene un único inverso.

(4) Si $a \in G$, entonces $\left(a^{-1}\right)^{-1} = a$.

(5) Si $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

(6) Son equivalentes:

(a) $(G, \cdot)$ es un grupo abeliano.

(b) $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}, \forall a, b \in G$.

Demostración. **(1)** Como $(G, \cdot)$ es un grupo, tenemos que si $a, b, c \in G$, existe $c^{-1} \in G$ tal que

$$a \cdot c = b \cdot c \iff a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \iff a \cdot e = b \cdot e \iff a = b.$$

Similarmente,

$$c \cdot a = c \cdot b \iff c^{-1} \cdot c \cdot a = c^{-1} \cdot c \cdot b \iff e \cdot a = e \cdot b \iff a = b.$$

(2) Sean $e, e' \in G$ dos elementos neutros de $(G, \cdot)$. Entonces, tenemos que

$$e = e \cdot e' = e' \cdot e = e'.$$

(3) Si $a \in G$, sean $b, c \in G$ dos inversos de a. Entonces tenemos que

$$a \cdot b = a \cdot c = e.$$

Por **(1)** tenemos que $b = c$. Otra manera de demostrarlo es:

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c.$$

(4)

$$\left(a^{-1}\right)^{-1} \cdot a^{-1} = e.$$

Como el inverso de a^{-1} es a y el inverso es único, tenemos que $a = \left(a^{-1}\right)^{-1}$.

(5) Tenemos que

$$(a \cdot b) \cdot \left(b^{-1} \cdot a^{-1}\right) = a \cdot \left(b^{-1} \cdot b\right) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e.$$

Como el inverso de $a \cdot b$ es $(a \cdot b)^{-1}$, y el inverso es único, tenemos que $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

(6) Si es un grupo abeliano, se cumple la propiedad conmutativa y con el resultado **(5)** la demostración es trivial. Recíprocamente, si $\forall a, b \in G$ tenemos que

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

tenemos que

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

Por la propiedad **(1)** tenemos que $a \cdot b = b \cdot a$, por lo que se cumple la propiedad conmutativa y es un grupo abeliano.

□

2.2. Subgrupo. Grupos finitos. Orden

Definición 2.2. Sea $(G, \cdot)$ un grupo y sea $H \subset G$. Se dice que H es un subgrupo de G, y se escribe $H \leq G$, si $(H, \cdot)$ es un grupo.

Ejemplo 2.2. **(i)** Tenemos que $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

(ii) $\mathrm{SO}(n) \leq \mathrm{SL}(n) \leq \mathrm{GL}(n)$.

Definición 2.3. Si $x \in G$ con $(G, \cdot)$ grupo, $n \in \mathbb{Z}$, denotamos a

$$x^n = \begin{cases} \underbrace{x \cdots x}_{n \text{ veces}} \text{ si } n > 0 \\ e \text{ si } n = 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ veces}} \text{ si } n < 0 \end{cases}.$$

El conjunto $\langle x \rangle = \{x^n \ : \ n \in \mathbb{Z}\}$ es un subgrupo abeliano de G. Es un subgrupo generado por el elemento x. Si $\exists x \in G$, $G = \langle x \rangle$ se denomina **grupo cíclico** .

Definición 2.4 (Orden)**.** Si G es un grupo finito, se llama **orden** de G a $|G|$, es decir, al número de elementos de G. Si G no es un conjunto finito diremos que tiene **orden infinito**. Si $x \in G$, el orden de x es: $\mathrm{ord}(x) = |\langle x \rangle|$.

Observación 2.1. El orden de un elemento x, si es finito, es el menor entero positivo n tal que $x^n = e$.

Proposición 2.2. Sea H un subconjunto no vacío de un grupo $(G, \cdot)$. Entonces, $H \leq G$ si y solo si $\forall x, y \in H$ se tiene que $x \cdot y^{-1} \in H$.

Demostración. **(i)** Es trivial, pues si $x, y \in H$, como $H \leq G$, tenemos que $\exists y^{-1} \in H$ y $x \cdot y^{-1} \in H$.

(ii) Recíprocamente, tenemos que la operación interna está cerrada. La propiedad asociativa se cumple porque se $(G, \cdot)$ es un grupo. Por definición, tenemos que si $x, y \in H$ entonces, $x \cdot y^{-1} \in H$. Podemos coger $x \cdot x^{-1} = e \in H$. Así, H contiene al elemento neutro. Similarmente, como $e, x \in H$, tenemos que $e \cdot x^{-1} = x^{-1} \in H$. Por lo que podemos encontrar inversos para todos los elementos de H.

□

Proposición 2.3. Si $H_1 \leq G$ y $H_2 \leq G$, entonces $H_1 \cap H_2 \leq G$.

Demostración. Tenemos que ver que $\forall x, y \in H_1 \cap H_2 \Rightarrow x \cdot y^{-1} \in H_1 \cap H_2$. Si $x, y \in H_1 \cap H_2$, tenemos que $x, y \in H_1$ y $x, y \in H_2$. Así, como $H_1, H_2 \leq G$, tenemos que $y^{-1} \in H_1 \cap H_2$ y $x \cdot y^{-1} \in H_1 \cap H_2$. □

Proposición 2.4. Si $(G, \cdot)$ es un grupo finito y $x \in G$, el orden de x coincide con el menor entero positivo k tal que $x^k = e$. Además,

$$\langle x \rangle = \left\{ x, x^2, x^3, \ldots, x^k = e \right\}.$$

Ejemplo 2.3. Consideramos el grupo $(\mathbb{Z}_6, +) = \{0, 1, 2, 3, 4, 5\}$. Entonces, tenemos que

$$\begin{aligned}
&\langle 0 \rangle = \{0\} \Rightarrow \operatorname{ord}(0) = 1 \\
&\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} \Rightarrow \operatorname{ord}(1) = 6 \\
&\langle 2 \rangle = \{2, 4, 0\} \Rightarrow \operatorname{ord}(2) = 3 \\
&\langle 3 \rangle = \{3, 0\} \Rightarrow \operatorname{ord}(3) = 2 \\
&\langle 4 \rangle = \{4, 2, 0\} \Rightarrow \operatorname{ord}(4) = 3 \\
&\langle 5 \rangle = \{5, 4, 3, 2, 1, 0\} \Rightarrow \operatorname{ord}(5) = 6.
\end{aligned}$$

2.3. Isomorfismos de grupos

Definición 2.5 (Isomorfismo)**.** Sean $(G, \cdot), (G', *)$ grupos. Se dice que $f : G \to G'$ es un **isomorfismo** (de grupos) si es biyectiva y

$$\forall x, y \in G,\ f(x \cdot y) = f(x) * f(y).$$

Si G es isomorfo a G', lo escribirmos $G \cong G'$.

Ejemplo 2.4. $f : (\mathbb{R}, +) \to \left(\mathbb{R}^+, \cdot\right)$ con $f : x \to e^x$.

Proposición 2.5. Si $G \cong G'$, entonces

(a) G y G' tienen el mismo cardinal.

(b) Si e y e' son, respectivamente, los elementos neutros de G y G',

$$f(e) = e' \quad \text{y} \quad f^{-1}(e') = e.$$

Además, $f\left(x^{-1}\right) = (f(x))^{-1}$.

(c) Si $H \leq G$, $f(H) \leq G'$.

(d) Si $x \in G$, $\operatorname{ord}(x) = \operatorname{ord}(f(x))$.

(e) Si G es abeliano, entonces G' también lo es.

Demostración. **(a)** Es trivial, puesto que tiene que un isomorfismo es biyectivo por definición.

(b) Tenemos que $\forall x \in G$,

$$f(x) = f(x \cdot e) = f(x) * f(e).$$

De esta manera,

$$e' = (f(x))^{-1} * f(x) = (f(x))^{-1} * f(x) * f(e) = e' * f(e) = f(e).$$

Similarmente, tenemos que

$$f(x) * f\left(x^{-1}\right) = f\left(x \cdot x^{-1}\right) = f(e) = e'.$$

Así, tenemos que $f\left(x^{-1}\right) = (f(x))^{-1}$. El hecho que $f^{-1}(e') = e$ se deriva de que f es una biyección.

(c) Sea $H \leq G$. Entonces si $f(x), f(y) \in f(H)$ tenemos que

$$f(x)(f(y))^{-1} = f\left(x \cdot y^{-1}\right) \in f(H),$$

pues $x \cdot y^{-1} \in H$.

(d) Tenemos que $f(\langle x \rangle) \leq G'$ y además,

$$f(x^n) = (f(x))^n.$$

Por tanto,

$$\operatorname{ord}(x) = |\langle x \rangle| = |f(\langle x \rangle)| = |\langle f(x) \rangle| = \operatorname{ord}(f(x)).$$

(e) Si G es abeliano, $\forall x, y \in G$ tenemos que $x \cdot y = y \cdot x$. Así,

$$f(x \cdot y) = f(x) * f(y) \quad \text{y} \quad f(y \cdot x) = f(y) * f(x)$$

$$\therefore f(x) * f(y) = f(y) * f(x).$$

□

Definición 2.6 (Homomorfismo)**.** Se dice que $(G, \cdot) \to (G', *)$ es **homomorfismo** si $\forall x, y \in G$, $f(x \cdot y) = f(x) * f(y)$.

Ejemplo 2.5. La siguiente aplicación es homomorfismo pero no isomorfismo.

$$\begin{aligned} f : (\mathrm{GL}(n), \cdot) &\to (\mathbb{R}/\{0\}, \cdot) \\ M_{n\times n} &\to \det(M_{n\times n}). \end{aligned}$$

Si $A, B \in \mathrm{GL}(n)$, entonces $f(A \cdot B) = f(A) \cdot f(B)$, pues $\det(A \cdot B) = \det(A) \cdot \det(B)$.

Definición 2.7 (Núcleo e imagen)**.** Sea e' el elemento neutro de G'. El **núcleo** de f se define de la siguiente manera:

$$\mathrm{Ker}\,(f) = \{x \in G \ : \ f(x) = e'\}\,.$$

Se define **imagen** de f al conjunto

$$\mathrm{Im}\,(f) = (f(x) \in G' \ : \ x \in G)\,.$$

Ejemplo 2.6. En la aplicación del ejemplo anterior tenemos que $\mathrm{Ker}\,(f) = \mathrm{SL}\,(n)$ e $\mathrm{Im}\,(f) = \mathbb{R}/\{0\}$.