

Elementos de Matemáticas

Victoria Torroja Rubio

9/10/2024-

Índice general

1. Teoría de Números	2
1.1. División Euclídea	3
1.2. Máximo Común Divisor	4
1.3. Números Primos	6
1.4. Congruencias	9

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 X .

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). Sean $m, n \in \mathbb{Z}$, 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, $r_1 = r_2$. \square

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 divide 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 . \square

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:

$$r_{t-2} = r_{t-1} q_t + r_t, \quad 0 < r_t < r_{t-1}$$

$$r_{t-1} = r_t q_{t+1} + 0.$$

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

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 esta 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 . \square

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

1

Ejemplo 1. Hallamos el máximo común divisor de 26 y 382. Tenemos que:

$$382 = 26 \cdot 14 + 18$$

$$26 = 18 \cdot 1 + 8$$

$$18 = 8 \cdot 2 + 2$$

$$8 = 2 \cdot 4 + 0.$$

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

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

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 (Mínimo Común Múltiplo). Consideramos $m, n \in \mathbb{Z}$ no nulos. Decimos que $l = \text{mcm}(m, n)$, o l es el mínimo 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,

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

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 . \square

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. \square

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,

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

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 . \square

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 $m|b$. \square

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 $p|b$. \square

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

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

Entonces $p \mid a_i$ 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 . \square

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 $p_1 \mid n$. Por el teorema anterior tenemos que $p_1 \mid (a_1 \cdot a_2 \cdots a_k)$, y por tanto, $p_1 \mid a_i$. 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. \square

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 $i \in \{1, 2, \dots, r\}$ 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 múltiplo.

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

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

$$\begin{aligned} m \cdot n &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \cdot (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}) \\ &= p_1^{\alpha_1 + \beta_1} \cdots p_r^{\alpha_r + \beta_r} = p_1^{\delta_1 + \gamma_1} \cdots p_r^{\delta_r + \gamma_r} \\ &= (p_1^{\gamma_1} \cdots p_r^{\gamma_r}) \cdot (p_1^{\delta_1} \cdots p_r^{\delta_r}) = \text{mcd}(m, n) \cdot \text{mcm}(m, n). \end{aligned}$$

2

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

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

Ejemplo 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,

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

Ejemplo 3.

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

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.

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

²Estamos 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

$$a \equiv b \pmod{m},$$

si y solo si $a - b$ es múltiplo de n . Es decir, a y b tienen el mismo resto al dividirlos 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. \square

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

(i) $a \equiv a \pmod{n}$.

(ii) Si $a \equiv b \pmod{n}$, entonces $b \equiv a \pmod{n}$.

(iii) Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces, $a \equiv c \pmod{n}$.

(iv) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces

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

(v) Si $a \equiv b \pmod{n}$, entonces

$$a + k \equiv b + k \pmod{n} \quad \text{y} \quad a \cdot k \equiv b \cdot k \pmod{n}.$$

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

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

(ii) Si $a \equiv b \pmod{n}$, 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 $b \equiv a \pmod{n}$.

(iii) Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, tenemos que

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

Por tanto,

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

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

(iv) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, 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, $a + c \equiv b + d \pmod{n}$.

Similarmente,

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

Por tanto, $ac \equiv b d \pmod{n}$.

(v) Si $a \equiv b \pmod{n}$, tenemos que

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

Por tanto, $a + k \equiv b + k \pmod{n}$.

Similarmente,

$$a - b = \lambda n \iff k(a - b) = k(\lambda n) \iff a \cdot k - b \cdot k = (k\lambda)n \iff a \cdot k \equiv b \cdot k \pmod{n}.$$

(vi) Si $a \equiv b \pmod{n}$,

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

Por tanto, $a^m \equiv b^m \pmod{n}$.

□

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

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

Donde a, b y m están dados. ^a

^aTenemos que ver si la congruencia tiene solución, cuántas tiene y dónde están.

Proposición 1.4. Si tenemos una congruencia lineal $ax \equiv b \pmod{m}$. Si α es una solución de la misma, entonces todo $\beta \equiv \alpha \pmod{m}$ es también solución de la congruencia. ^a

^aEsto nos permite reducir las posibles soluciones a los elementos de \mathbb{Z}_m .

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

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

Por otra parte, si $\beta \equiv \alpha \pmod{m}$, tenemos que

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

Entonces,

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

Por otro lado,

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

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

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

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

Ejemplo 4. $2x \equiv 1 \pmod{4}$. 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 5. $2x \equiv 2 \pmod{8}$. 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 6. $4x \equiv 4 \pmod{8}$. Comprobamos con los elementos de \mathbb{Z}_8 . Funcionan el 1, 3, 5 y el 7.

Ejemplo 7. (a) $12427 \pmod{10}$. 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 $12427 \equiv 7 \pmod{10}$.

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

$$12112 \times 347 \pmod{3} \Rightarrow 12112 \times 347 \equiv 2 \pmod{3}.$$

Por lo que $12112 \times 347 \equiv 2 \pmod{3}$.

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

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

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

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

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

Teorema 1.13. Sean $a, b, m \in \mathbb{Z}$ con $m > 0$, y sea $d = \text{mcd}(a, m)$. Entonces, la congruencia lineal: $ax \equiv b \pmod{m}$ 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, $b \equiv auk \pmod{m}$. Por la propiedad simétrica, $auk \equiv b \pmod{m}$. 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 $a\alpha \equiv b \pmod{m}$, 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 $a = a_1d$, $b = b_1d$ y $m = m_1d$. Entonces, sabemos que

$$a_1dx \equiv b_1d \pmod{m_1d}.$$

Por tanto,

$$a_1dx - b_1d = km_1d.$$

Por tanto,

$$a_1x - b_1 = km_1 \iff a_1x \equiv b_1 \pmod{m_1}.$$

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,

$$\alpha, \alpha + m_1, \alpha + 2m_1, \dots$$

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

Ejemplo 8. $51x \equiv 27 \pmod{123}$

(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: $17x \equiv 9 \pmod{41}$. 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,

$$9 \equiv -9 \cdot 12 \cdot 17 \pmod{41} \iff 17(-9 \cdot 12) \equiv 9 \pmod{41}.$$

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

$$x \equiv -108 + 3 \cdot 41 \equiv 15 \pmod{41}.$$

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

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

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

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

Ejemplo 9. $17x \equiv 5 \pmod{13}$. 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 $17 \cdot (-15) \equiv 5 \pmod{13}$, por lo que la solución será $x \equiv -15 \equiv 11 \pmod{13}$.

Ejemplo 10. $66x \equiv 42 \pmod{168}$. 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:

$$11x \equiv 7 \pmod{28}.$$

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 $11 \cdot (-35) \equiv 7 \pmod{28}$, por lo que las soluciones serán,

$$x \equiv -35 \pmod{28} \Rightarrow x \equiv 21 \pmod{168}.$$

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 $\text{mcd}(m, n) = 1$, tenemos que $n \mid \lambda$, 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 $a_1 x \equiv b_1 \pmod{m}$ y $a_2 x \equiv b_2 \pmod{n}$, 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:

$$a_1 x \equiv b_1 \pmod{m} \quad \text{y} \quad a_2 x \equiv b_2 \pmod{n},$$

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

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

$$mu + nv = 1.$$

Tomamos módulos en esta expresión:

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

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

$$\alpha_1 nv + \alpha_2 mu \equiv \alpha_2 \pmod{n}.$$

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

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

$$\therefore \alpha_1 nv + \alpha_2 mu \equiv \alpha_1 \pmod{m}.$$

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 \mathbb{Z}_m , α y β son congruentes módulo m . Por la transitividad tenemos que

$$\alpha \equiv \beta \pmod{m}.$$

Similarmente,

$$\alpha \equiv \beta \pmod{n}.$$

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} . \square

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

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

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

Ejemplo 11. $x \equiv 4 \pmod{8}$ y $x \equiv -1 \pmod{15}$. 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, $\alpha \equiv 44 \pmod{120}$.

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

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

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

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

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

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 $\text{mcd}(a_i, m_i) = 1$, $\forall i = 1, 2, \dots, n$ 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. \square

Ejemplo 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 $x \equiv \alpha \pmod{12 \cdot 7}$. Cogemos la anterior y una de las otras dos restantes para obtener $x \equiv \beta \pmod{12 \cdot 7 \cdot 5}$. 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:

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

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:

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

3

³En 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 $a_1 \equiv b_1 \pmod{m_1}$ y α_2 es solución de la congruencia $a_2 x \equiv b_2 \pmod{m_2}$, entonces la solución de ambas congruencias será $\alpha \equiv \alpha_2 u m_1 + \alpha_1 v m_2 \pmod{m_1 \cdot m_2}$ (u y v proceden de la Identidad de Bézout).

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

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

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. \square

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

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

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

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

\square

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 $n_1, \dots, n_k \in \mathbb{Z}^+$ 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, \dots, 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 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 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

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

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

$$\exists c, a \cdot c = 1 \pmod{n}, \quad 1 \leq c < n.$$

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

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

Ejemplo 14. $777^{-1} \pmod{1009}$. Queremos resolver la congruencia $777x \equiv 1 \pmod{1009}$. Calculamos la identidad de Bézout para obtener:

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

Ejemplo 15. Calculamos $5^{28575} \pmod{17}$. En primer lugar, intentamos aplicar el teorema de Euler. Vemos que $\text{mcd}(5, 17) = 1$, por lo que lo podemos aplicar. Entonces, tenemos que

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

Además, tenemos que

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

Por otro lado tenemos que

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

Por tanto,

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

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

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

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

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

Ejemplo 16. (i) Para calcular $41^5 \pmod{43}$, tenemos en cuenta que $41 \equiv -2 \pmod{43}$, por tanto,

$$41^5 \equiv (-2)^5 \equiv -32 \equiv 11 \pmod{43}.$$

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

$$11^2 \equiv 121 \equiv 36 \pmod{85}$$

$$11^3 \equiv 11^2 \cdot 11 \equiv 36 \cdot 11 \equiv 56 \pmod{85}$$

$$11^4 \equiv 11^3 \cdot 11 \equiv 56 \cdot 11 \equiv 21 \pmod{85}$$

$$11^5 \equiv 11^4 \cdot 11 \equiv 21 \cdot 11 \equiv 61 \pmod{85}$$

$$11^6 \equiv 11^5 \cdot 11 \equiv 61 \cdot 11 \equiv 76 \pmod{85}.$$

Entonces tenemos que

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

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

$$a^4 \equiv (a^2)^2 \pmod{n}$$

$$a^8 \equiv (a^4)^2 \pmod{n}$$

$$a^{16} \equiv (a^8)^2 \pmod{n}$$

$$a^{32} \equiv (a^{16})^2 \pmod{n}.$$

Ejemplo 17. En el ejemplo anterior sería:

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