Matemática Discreta I

Tema 3. Aritmética modular

Luis Magdalena Layos
luis.magdalena@upm.es

Departamento de Matemática Aplicada a las TIC
E.T.S. Ingenieros Informáticos
Universidad Politécnica de Madrid

Grado en Ciencia de Datos e Inteligencia Artificial
Grado en Matemáticas e Informática
Curso 2020/21

Contenidos

Congruencias enteras

Definición

Dados $m \in \mathbb{N}$ y $a, b \in \mathbb{Z}$, se dice que **a es congruente con b** módulo m si y sólo si $m \mid (a-b)$. Se denota por $a \equiv b \pmod{m}$. Denominamos a m módulo de la congruencia.

Ejemplos

Por ejemplo $83 \equiv 2 \pmod{9}$, ya que $9 \mid 83 - 2 = 81$.
De igual forma $59 \equiv 4 \pmod{5}$ puesto que $5 \mid 59 - 4 = 55$.

Proposición

La relación de congruencia módulo m es una relación de equivalencia para todo $m \in \mathbb{N}$:

- Reflexiva: $\forall a \in \mathbb{Z}, a \equiv a \pmod{m}$ ya que $m \mid (a-a) = 0$.
- Simétrica: $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$, ya que $m \mid (a-b) \Leftrightarrow m \mid (b-a)$.
- Transitiva: $\forall a, b, c \in \mathbb{Z}$, si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.

$$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow m \mid (a-b) \\ b \equiv c \pmod{m} \Rightarrow m \mid (b-c) \end{array}\right\} \Rightarrow m \mid (a-b+b-c) = (a-c) \Rightarrow a \equiv c \pmod{m}$$

Congruencias enteras

Proposición

Dado $m \in \mathbb{N}$ se cumple que:

- $a \equiv b \pmod{m} \iff \exists q, q', r \in \mathbb{Z} \mid a = m \cdot q + r, b = m \cdot q' + r,$ con $0 \leq r < m$.
- Para todo $a \in \mathbb{Z}$ existe $r \in \{0, 1, \ldots, m-1\}$ tal que $a \equiv r \pmod{m}$.

Definiciones

- Se denomina **Clase de congruencias** módulo m al conjunto $[r]_m = \{a \in \mathbb{Z} \mid a \equiv r \pmod{m}\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \text{ con } a = m \cdot q + r\}$.
- Al resto de la división entera con divisor m se le denomina **residuo** módulo m.
- Denominamos **conjunto de mínimos residuos no negativos** módulo m al conjunto de las clases de congruencias módulo m, y lo representamos por $\mathbb{Z}_m$:

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

Proposición

$\mathbb{Z}_m$ es el conjunto cociente de $\mathbb{Z}$ por la relación de congruencia módulo m.

Compatibilidad con suma y producto en $\mathbb{Z}$

Teorema

La relación de congruencia es compatible con la suma y el producto en $\mathbb{Z}$.
Sean $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$, con $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, se cumple que:

- $(a + c) \equiv (b + d) \pmod{m}$.
- $(a \cdot c) \equiv (b \cdot d) \pmod{m}$.
- $(a^c) \equiv (b^c) \pmod{m}$.

Demostración.

Al ser $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, $a = b + k_1 m$ y $c = d + k_2 m$, con $k_1, k_2 \in \mathbb{Z}$.
Por tanto $(a + c) = (b + d) + (k_1 + k_2)m$, con $k_1 + k_2 \in \mathbb{Z}$, y $(a + c) \equiv (b + d) \pmod{m}$.
Por otro lado $ac = bd + (bk_2 + dk_1 + k_1 k_2 m)m$ con $(bk_2 + dk_1 + k_1 k_2 m) \in \mathbb{Z}$, por lo que $(a \cdot c) \equiv (b \cdot d) \pmod{m}$.

Finalmente $(a^c) = (b + k_1 m)^c = \binom{c}{0} b^c + \binom{c}{1} b^{c-1}(k_1 m) + \ldots + \binom{c}{c} (k_1 m)^c$, siendo múltiplos de m todos los sumandos salvo el primero, con lo que $(a^c) \equiv (b^c) \pmod{m}$. □

Observación: En general no se cumple que $(a^c) \equiv (b^d) \pmod{m}$.

Compatibilidad con suma y producto en $\mathbb{Z}$

Proposición

Sean $m \in \mathbb{N}$ y $a_i, b_i \in \mathbb{Z} \forall i \in \{1, 2, 3, \ldots, k\}$. Si $a_i \equiv b_i \pmod{m} \forall i \in \{1, 2, 3, \ldots, k\}$, entonces:

- $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$.
- $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$.

Observación: El resultado previo nos indica que el resto de la suma es congruente con la suma de restos y el resto del producto es congruente con el producto de restos.

Ejemplos

- Como $1234567 \equiv 7 \pmod{10}$ y $90213 \equiv 3 \pmod{10}$, se tiene que $1234567 \cdot 90213 \equiv 21 \equiv 1 \pmod{10}$.
- El resto al dividir 6^{123} entre 5 es igual al resto al dividir 1^{123} entre 5, que es obviamente 1.
- El resto al dividir 7^{123} entre 5 es igual al resto al dividir 2^{123} entre 5, que no es inmediato. Pero observamos que $2^4 \equiv 1 \pmod{5}$ y por tanto $2^{123} = 2^{4 \cdot 30 + 3} = (2^4)^{30} \cdot 2^3 \equiv 2^3 \equiv 3 \pmod{5}$.

Aritmética en $\mathbb{Z}_m$

Definición

En $\mathbb{Z}_m$ definimos dos operaciones binarias internas:

- La suma $(+)$ dada por: $[a]_m + [b]_m = [a+b]_m$.
- El producto $(\cdot)$ dado por: $[a]_m \cdot [b]_m = [a \cdot b]_m$.

Propiedades: En $(\mathbb{Z}_m, +, \cdot)$ se verifican las siguientes propiedades:

- **Asociativa:** $[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m$, $[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m$ para cualesquiera $a, b, c \in \mathbb{Z}$.
- **Conmutativa:** $[a]_m + [b]_m = [b]_m + [a]_m$, $[a]_m[b]_m = [b]_m[a]_m$, para cualesquiera $a, b \in \mathbb{Z}$.
- **Elemento neutro:** Existen $[0]_m$ y $[1]_m \mid \in \mathbb{Z}_m$ tales que $[a]_m + [0]_m = [a]_m$, y $[a]_m[1]_m = [a]_m$, para todo $a \in \mathbb{Z}$.
- **Elemento opuesto:** Para todo $a \in \mathbb{Z}$ existe $[-a]_m \in \mathbb{Z}_m$ tal que $[a]_m + [-a]_m = [0]_m$.
- **Distributiva:** $[a]_m([b]_m + [c]_m) = [a]_m[b]_m + [a]_m[c]_m$, para cualesquiera $a, b, c \in \mathbb{Z}$.

Aritmética en $\mathbb{Z}_m$

Ejemplo

Construir las **tablas** de la suma y el producto en $\mathbb{Z}_5$ **y** $\mathbb{Z}_6$**.**

$Z_5 +$

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

$\mathbb{Z}_5 \cdot$

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

$\mathbb{Z}_6 +$

$+$	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

$\mathbb{Z}_6 \cdot$

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

Aritmética en $\mathbb{Z}_m$

Observación: En general no se cumple la propiedad cancelativa, por ejemplo en $\mathbb{Z}_6$ $[2]_6 \times [1]_6 = [2]_6 \times [4]_6$ pero $[1]_6 \neq [4]_6$.

Proposición

Sea $c \in \mathbb{Z}$ con $[c]_m \neq [0]_m$, si $ac \equiv bc \pmod{m}$ entonces $a \equiv b \pmod{\frac{m}{\mathrm{mcd}(m,c)}}$, o lo que es equivalente, si $[a]_m[c]_m = [b]_m[c]_m$ entonces $[a]_{\frac{m}{\mathrm{mcd}(m,c)}} = [b]_{\frac{m}{\mathrm{mcd}(m,c)}}$.

Corolario.

1. Si $\mathrm{mcd}(m,c) = 1$ y $[c]_m \neq [0]_m$, entonces: $[a]_m[c]_m = [b]_m[c]_m \Rightarrow [a]_m = [b]_m$.
2. Si p es primo, $\mathbb{Z}_p$ tiene la propiedad cancelativa del producto.

Ejemplo

$[10]_{14}[x]_{14} = [6]_{14} \Rightarrow [2]_{14}[5]_{14}[x]_{14} = [2]_{14}[3]_{14} \overset{\mathrm{mcd}(14,2)=2}{\Longrightarrow} [5]_7[x]_7 = [3]_7 = [10]_7 \Rightarrow$
$[5]_7[x]_7 = [5]_7[2]_7 \overset{\mathrm{mcd}(7,5)=1}{\Longrightarrow} [x]_7 = [2]_7$.
Si quisieramos expresar ahora la solución en $\mathbb{Z}_{14}$ debemos darnos cuenta de que $2 \equiv 9 \pmod{7}$, pero $2 \not\equiv 9 \pmod{14}$, por lo que habría dos soluciones en $\mathbb{Z}_{14}$: $[x]_{14} = [2]_{14}, [9]_{14}$.

Aritmética en $\mathbb{Z}_m$

Definiciones

- Se denominan **divisores de cero** en $\mathbb{Z}_m$ a los elementos $[a]_m, [b]_m$ tales que $[a]_m \neq [0]_m \neq [b]_m$ y sin embargo $[a]_m \cdot [b]_m = [0]_m$.
- Se denominan **elementos inversibles** de $\mathbb{Z}_m$ a los elementos $[a]_m$ para los que existe un $[b]_m$ tal que $[a]_m \cdot [b]_m = [1]_m$.

Proposición

- El conjunto $\mathbb{Z}_m$ tendrá divisores de cero si y solo si m es un número compuesto (m no es primo).
- Un elemento $[a]_m \in \mathbb{Z}_m$ será inversible si y solo si $\mathrm{mcd}(a, m) = 1$ (a y m son coprimos).
- Igualmente podemos decir que un elemento $[a]_m \in \mathbb{Z}_m$ será inversible si y solo si existen $b, k \in \mathbb{Z}$ tales que $a \cdot b + k \cdot m = 1$, y podríamos calcular b por el algoritmo de Euclides.
- Si m es primo, todos los elementos de $\mathbb{Z}_m$ son inversibles.

Definición

Si $[a]_m$ es inversible en $\mathbb{Z}_m$ y $[a]_m \cdot [b]_m = [1]_m$, diremos que $[b]_m$ es el inverso de $[a]_m$ en $\mathbb{Z}_m$ y lo denotamos por $[b]_m = [a]_m^{-1}$.

Criterios de divisibilidad

Observación: Dado $n = (a_p \dots a_0)_{10} \in \mathbb{N}$ (representado en base 10) tenemos que $n = \sum_{i=0}^{p} a_i 10^i$, y a partir de las propiedades de la aritmética modular, $[n]_m = \sum_{i=0}^{p} [a_i]_m [10^i]_m$.

Ejemplos

Como $100 \equiv 10 \equiv 1 \pmod 3, 832 \equiv (8 \cdot 1 + 3 \cdot 1 + 2) \equiv 1 \pmod 3$.
Como $100 \equiv 10 \equiv 0 \pmod 5, 832 \equiv (8 \cdot 0 + 3 \cdot 0 + 2) \equiv 2 \pmod 5$.

Además sabemos que si x es divisible por m, $x \equiv 0 \pmod m$. Por tanto x será divisible por m si y solo si $\sum_{i=0}^{p} [a_i]_m [10^i]_m = [0]_m$.

Ejemplos

Como $100 \equiv 4 \pmod 8$ y $10 \equiv 2 \pmod 8, 832 \equiv (8 \cdot 4 + 3 \cdot 2 + 2) \equiv 0 \pmod 8$. Por tanto 832 es divisible por 8.

Criterios de divisibilidad

Proposición

Sea $n = (a_p \dots a_0)_{10} \in \mathbb{N}$ un número natural representado en base 10.

i) $10^i \equiv 0 \pmod 2 \forall i > 0$, $n \equiv a_0 \pmod 2$, luego n es divisible por 2 $\Leftrightarrow a_0$ lo es.

ii) $10^i \equiv 1 \pmod 3 \forall i \geq 0$, $n \equiv \sum_{i=0}^{p} a_i \pmod 3$, luego n es divisible por 3 $\Leftrightarrow \sum_{i=0}^{p} a_i$ lo es.

iii) $10^i \equiv 0 \pmod 4 \forall i > 1$, $n \equiv 10a_1 + a_0 \equiv 2a_1 + a_0 \pmod 4$, luego n es divisible por 4 $\Leftrightarrow 2a_1 + a_0$ lo es. Otra opción sería comprobar si $(a_1 a_0)_{10}$ es divisible por 4.

iv) $10^i \equiv 0 \pmod 5 \forall i > 0$, $n \equiv a_0 \pmod 5$, luego n es divisible por 5 $\Leftrightarrow a_0$ lo es.

v) $10^i \equiv 1 \pmod 9 \forall i \geq 0$, $n \equiv \sum_{i=0}^{p} a_i \pmod 9$, luego n es divisible por 9 $\Leftrightarrow \sum_{i=0}^{p} a_i$ lo es.

vi) $10 \equiv -1 \pmod{11}$, $10^i \equiv -1^i \pmod{11}$, y por tanto $n \equiv \sum_{i=0}^{p} (-1)^i a_i \pmod{11}$, con lo que n es divisible por 11 $\Leftrightarrow \sum_{i=0}^{p} (-1)^i a_i$ lo es.

Prueba del 9 para la multiplicación

Teorema

Sean $x, y, z \in \mathbb{N}$. *Entonces* $xy = z \Leftrightarrow \theta(x)\theta(y) \equiv \theta(z) \pmod 9$, *donde* $\theta((a_p \dots a_0)_{10}) = a_p + a_{p-1} + \cdots + a_1 + a_0$.

Ejemplo

Como $\theta(12)\theta(12) = 9 \not\equiv \theta(145) \pmod 9$ se tiene que $12 \cdot 12 \neq 145$. Por otra parte, como $\theta(12)\theta(12) = 9 \equiv \theta(144) \pmod 9$ es posible que $12 \cdot 12 = 144$ aunque en principio no tiene porque ser así puesto que también se tiene que $\theta(12)\theta(12) = 9 \equiv \theta(135) \pmod 9$.

Observación: La prueba del 9 también se puede utilizar para la recuperación de datos perdidos. Por ejemplo, un dígito perdido en $53928719937 \cdot 376648 = 20312144X06831176$. Como $\theta(53928719937) \equiv 0 \pmod 9$ y $\theta(376648) \equiv 7 \pmod 9$ sabemos que deberá ser $\theta(20312144X06831176) \equiv 0 \pmod 9$. Por tanto $49 + X \equiv 0 \pmod 9$, o lo que es los mismo, $4 + X \equiv 0 \pmod 9$, y como $0 \leq X \leq 9$, solo puede ser $X = 5$.

Observación: El proceso de corrección o recuperación de información se puede hacer de forma general con cualquier congruencia. Por tanto al comprobar que $\theta(12)\theta(12) = 9 \not\equiv \theta(145) \pmod 9$ y ver que tenemos dos opciones de corrección (144 y 135), bastaría ver que $[12]_{10} \cdot [12]_{10} = [144]_{10}$ mientras que $[12]_{10} \cdot [12]_{10} \neq [135]_{10}$.

Unidades en $\mathbb{Z}_m$

Definición

Denominamos **conjunto de Unidades** de $\mathbb{Z}_m$ (representado por U_m) al conjunto de elementos inversibles de $\mathbb{Z}_m$.

$$U_m = \{[a]_m \in \mathbb{Z}_m \mid [a]_m \text{ es inversible}\} = \{[a]_m \in \mathbb{Z}_m \mid \text{mcd}(a, m) = 1\}$$

Ejemplos

$U_{10} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$ con $[1]_{10}^{-1} = [1]_{10}$, $[3]_{10}^{-1} = [7]_{10}$, $[7]_{10}^{-1} = [3]_{10}$, $[9]_{10}^{-1} = [9]_{10}$.
$U_5 = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ con $[1]_5^{-1} = [1]_5$, $[2]_5^{-1} = [3]_5$, $[3]_5^{-1} = [2]_5$, $[4]_5^{-1} = [4]_5$.
En general, si m es primo $U_m = \{[1], [2], [3], \ldots, [m-1]_m\}$.

Propiedades: En $\mathbb{Z}_m$ se verifican las siguientes propiedades:

- Si $[a]_m, [b]_m \in U_m$ entonces $[a]_m[b]_m \in U_m$ y $[a]_m^{-1} \in U_m$.
- Si $[a]_m \in U_m$ entonces $[a]_m \cdot U_m = \{[a]_m \cdot [b]_m \mid [b]_m \in U_m\} = U_m$.

Unidades en $\mathbb{Z}_m$

Proposición

Si m es primo los únicos elementos que coinciden con su inverso son $[1]_m$ y $[m-1]_m$.
Además, en este caso $|U_m| = m - 1$.

Ejemplo

Hallamos los inversos en $\mathbb{Z}_{13}$.
Vemos en primer lugar que al ser 13 primo, $|U_{13}| = 12$.
$U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
Sabemos que $[1]_{13}^{-1} = [1]_{13}$ y que $[12]_{13}^{-1} = [12]_{13}$.
Por otro lado $7 \cdot 2 = -7 \cdot (-2) = 14 \equiv 1 \pmod{13}$, con lo que $[7]_{13}^{-1} = [2]_{13}$, $[2]_{13}^{-1} = [7]_{13}$, $[11]_{13}^{-1} = [6]_{13}$ (ya que $[-2]_{13}^{-1} = [-7]_{13}$) y $[6]_{13}^{-1} = [11]_{13}$.
Además $3 \cdot 9 = -3 \cdot (-9) = 27 \equiv 1 \pmod{13}$, con lo que $[3]_{13}^{-1} = [9]_{13}$, $[9]_{13}^{-1} = [3]_{13}$, $[10]_{13}^{-1} = [4]_{13}$ (ya que $[-3]_{13}^{-1} = [-9]_{13}$) y $[4]_{13}^{-1} = [10]_{13}$.
Y solo nos quedan por emparejar 5 y 8, pero $5 \cdot 8 = 40 \equiv 1 \pmod{13}$, siendo por tanto $[5]_{13}^{-1} = [8]_{13}$, $[8]_{13}^{-1} = [5]_{13}$.

Unidades en $\mathbb{Z}_m$

Observación: Si m no es primo, puede haber elementos distintos de $[1]_m$ y $[m-1]_m$ que coincidan con su inverso (autoinversos). Además, $|U_m| < m-1$ ya que no todos los elementos serán inversibles.

Ejemplo

Hallamos ahora los inversos en $\mathbb{Z}_{15}$.
Al no ser 15 un número primo no todos los elementos de $\mathbb{Z}_{15}$ van a tener inverso, $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$, y sabemos que $[1]_{15}^{-1} = [1]_{15}$ y $[14]_{15}^{-1} = [14]_{15}$.
Como $8 \cdot 2 = -8 \cdot (-2) = 16 \equiv 1 \pmod{15}$, tenemos que $[8]_{15}^{-1} = [2]_{15}$, $[2]_{15}^{-1} = [8]_{15}$, $[13]_{15}^{-1} = [7]_{15}$ y $[7]_{15}^{-1} = [13]_{15}$.
Nos quedan por emparejar 4 y 11, pero $4 \cdot 11 = 44 \equiv -1 \pmod{15}$, con lo que no son inversos.
Sin embargo $4 \cdot 4 = -4 \cdot (-4) = 16 \equiv 1 \pmod{15}$, con lo que $[4]_{15}^{-1} = [4]_{15}$ y $[11]_{15}^{-1} = [11]_{15}$.

Ejemplo

En cambio en $\mathbb{Z}_{14}$ solamente 1 y 13 coinciden con su inverso. $U_{14} = \{1, 3, 5, 9, 11, 13\}$.
Sabemos que $[1]_{14}^{-1} = [1]_{14}$ y $[13]_{14}^{-1} = [13]_{14}$.
Como $3 \cdot 5 = -3 \cdot (-5) = 15 \equiv 1 \pmod{14}$, tenemos que $[3]_{14}^{-1} = [5]_{14}$, $[5]_{14}^{-1} = [3]_{14}$, $[11]_{14}^{-1} = [9]_{14}$ y $[9]_{14}^{-1} = [11]_{14}$. Y todos quedan emparejados.

Unidades en $\mathbb{Z}_m$

Proposición (Teorema de Wilson)

Si p es primo, entonces

$$(p-1)! \equiv (p-1) \pmod{p}$$

Ejemplo

Tomamos $p = 11$.

$(10)! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ y por las propiedades vistas anteriormente sabemos que los únicos elementos que coinciden con su inverso son $[10]_{11}^{-1} = [10]_{11}$ y $[1]_{11}^{-1} = [1]_{11}$.

El resto de elementos se agrupan de dos en dos, siendo mutuamente inversos. $[2]_{11}^{-1} = [6]_{11}$, $[6]_{11}^{-1} = [2]_{11}$, $[3]_{11}^{-1} = [4]_{11}$, $[4]_{11}^{-1} = [3]_{11}$, $[5]_{11}^{-1} = [9]_{11}$, $[9]_{11}^{-1} = [5]_{11}$, $[7]_{11}^{-1} = [8]_{11}$, $[8]_{11}^{-1} = [7]_{11}$.

Por lo tanto $[10!]_{11} = [10]_{11} \cdot [9]_{11} \cdot [8]_{11} \cdot [7]_{11} \cdot [6]_{11} \cdot [5]_{11} \cdot [4]_{11} \cdot [3]_{11} \cdot [2]_{11} \cdot [1]_{11} = [10]_{11} \cdot ([9]_{11} \cdot [5]_{11}) \cdot ([8]_{11} \cdot [7]_{11}) \cdot ([6]_{11} \cdot [2]_{11}) \cdot ([4]_{11} \cdot [3]_{11}) \cdot [1]_{11} = [10]_{11} \cdot [1]_{11} \cdot [1]_{11} \cdot [1]_{11} \cdot [1]_{11} \cdot [1]_{11} = [10]_{11}$.

Y en consecuencia $[10!]_{11} = [10]_{11}$.

Cálculo de Inversos

Ejemplo

El inverso de $[5]_{13}$ es $[8]_{13}$, porque $5 \cdot 8 = 40 = 3 \cdot 13 + 1$.
El inverso de $[7]_{16}$ es $[7]_{16}$, porque $7 \cdot 7 = 49 = 3 \cdot 16 + 1$.

Proposición

Para calcular el inverso de a en $\mathbb{Z}_m$ podemos proceder de la siguiente forma:

- Comprobamos en primer lugar que a es inversible en $\mathbb{Z}_m$, para ello se debe cumplir que $\mathrm{mcd}(a, m) = 1$.
- Si $\mathrm{mcd}(a, m) = 1$ sabemos que existen dos enteros x, y tales que $a \cdot x + m \cdot y = 1$ y por tanto $(a \cdot x) \equiv 1 \ (\mathrm{mód}\ m)$, o lo que es lo mismo, $[a]_m \cdot [x]_m = [1]_m$. En definitiva $[a]_m^{-1} = [x]_m$.
- Por tanto, para calcular el inverso de a en $\mathbb{Z}_m$, bastará con resolver la ecuación diofántica $a \cdot x + m \cdot y = 1$ (una vez comprobado que $\mathrm{mcd}(a, m) = 1$).

Cálculo de Inversos

Ejemplo

Para ver si $[777]_{1009}$ tiene inverso, calculamos primero $\mathrm{mcd}(777, 1009)$ mediante el algoritmo de Euclides:

$$1009 = 1 \cdot 777 + 232, \quad 777 = 3 \cdot 232 + 81, \quad 232 = 2 \cdot 81 + 70, \quad 81 = 70 + 11,$$
$$70 = 6 \cdot 11 + 4, \quad 11 = 2 \cdot 4 + 3, \quad 4 = 1 \cdot 3 + 1$$

por tanto, $\mathrm{mcd}(1009, 777) = 1$ y $[777]_{1009}$ tiene inverso.
Resolvemos a continuación la ecuación diofántica $777 \cdot x + 1009 \cdot y = 1$

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = 3 \cdot (70 - 6 \cdot 11) - 11 = 3 \cdot 70 - 19 \cdot 11 \\ &= 3 \cdot 70 - 19 \cdot (81 - 70) = 22 \cdot 70 - 19 \cdot 81 = 22 \cdot (232 - 2 \cdot 81) - 19 \cdot 81 \\ &= 22 \cdot 232 - 63 \cdot 81 = 22 \cdot 232 - 63 \cdot (777 - 3 \cdot 232) = 211 \cdot 232 - 63 \cdot 777 \\ &= 211 \cdot (1009 - 777) - 63 \cdot 777 = 211 \cdot 1009 - 274 \cdot 777. \end{aligned}$$

siendo $x = -274$ e $y = 211$. Así, $(-274) \cdot 777 = 1 + 211 \cdot 1009$.
Luego $[777]_{1009}^{-1} = [-274]_{1009} = [735]_{1009}$.

La función de Euler

Definición

Se define la función de Euler (representada por ϕ) como la función $\phi : \mathbb{N} \to \mathbb{N}$ que a cada n le hace corresponder el número de naturales, menores que n, que son primos con n.

$$\phi(n) = |\{k \in \mathbb{N} \mid k < n \text{ y } \operatorname{mcd}(k, n) = 1\}|.$$

Propiedades:

- $\phi(m) = |U_m|$.
- Si p es primo entonces $\phi(p^r) = p^r - p^{r-1}$.
- Si $\operatorname{mcd}(a, b) = 1$ entonces $\phi(ab) = \phi(a)\phi(b)$.
- Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ (con p_i números primos distintos) entonces $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right)$.

Ejemplos

$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, \phi(8) = 4, \phi(9) = 6, \ldots$

$\phi(3500) = \phi(2^2 \cdot 5^3 \cdot 7) = \phi(2^2) \cdot \phi(5^3) \cdot \phi(7) = (2^2 - 2) \cdot (5^3 - 5^2) \cdot 6 = 2 \cdot 100 \cdot 6 = 1200.$

Teoremas de Euler y Fermat

Teorema (Teorema de Euler)

Si $[a]_m \in U_m$ *entonces* $[a]_m^{\phi(m)} = [1]_m$*, o lo que es lo mismo, si* $\mathrm{mcd}(a, m) = 1$ *entonces* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración.

Supongamos que $U_m = \{[a_1]_m, [a_2]_m, \ldots, [a_r]_m\}$ (por tanto $\phi(m) = |U_m| = r$).
Sea $[a]_m \in U_m$. Entonces $[a]_m U_m = \{[a]_m[a_1]_m, [a]_m[a_2]_m, \ldots, [a]_m[a_r]_m\} = U_m$ y por tanto $[a_1]_m[a_2]_m \cdots [a_r]_m = ([a]_m[a_1]_m)([a]_m[a_2]_m) \cdots ([a]_m[a_r]_m) = [a]_m^r [a_1]_m[a_2]_m \cdots [a_r]_m$ en $\mathbb{Z}_m$.
Además, como $[a_1]_m[a_2]_m \cdots [a_r]_m$ son inversibles, podemos multiplicar por su inverso y obtenemos que $a^r \equiv 1 \pmod{m}$. □

Teoremas de Euler y Fermat

Teorema (Teorema de Fermat)

Si p es primo y no divide a a, entonces $a^{p-1} \equiv 1 \pmod{p}$.
En particular $2^{p-1} \equiv 1 \pmod{p}$ para todo número primo $p \geq 2$.

Demostración.

Si p es primo y no divide a a entonces $\mathrm{mcd}(a, p) = 1$. Por otra parte, como p es primo se tiene que $\phi(p) = p - 1$. Por tanto $a^{p-1} = a^{\phi(p)} \equiv 1 \pmod{p}$. □

Observación: No es necesario que p sea primo para que $a^{p-1} \equiv 1 \pmod{p}$, basta considerar $341 = 11 \cdot 31$ que verifica que $2^{340} \equiv 1 \pmod{p}$.

Ejemplo

Calculamos el resto de 125^{4577} entre 13.

Vemos en primer lugar que $125 \equiv 8 \pmod{13}$, por tanto $125^{4577} \equiv 8^{4577} \pmod{13}$.
Además, como 13 es primo y 8 no es múltiplo de 13, sabemos que $8^{12} \equiv 1 \pmod{13}$.
Por otro lado $4577 = 12 \times 381 + 5$, con lo que $8^{4577} = (8^{12})^{381} \cdot 8^5 \equiv 1^{381} 8^5 \equiv 8^5 \pmod{13}$.
Además, $8^2 \equiv (-1) \pmod{13}$ y por tanto $8^2 \times 8^2 \equiv 1 \pmod{13}$, y $8^5 \equiv 8 \pmod{13}$.
En definitiva $125^{4577} \equiv 8 \pmod{13}$.

Cálculo de residuos de potencias

Proposición

Dados $a, b, m \in \mathbb{Z}$, sabemos que si $a \equiv \alpha \pmod{m}$, entonces $a^b \equiv \alpha^b \pmod{m}$.
Por otro lado, si $\mathrm{mcd}(\alpha, m) = 1$ sabemos que $\alpha^{\phi(m)} \equiv 1 \pmod{m}$.
Por tanto, si $a \equiv \alpha \pmod{m}$, $\mathrm{mcd}(\alpha, m) = 1$ y $b \equiv \beta \pmod{\phi(m)}$, entonces $a^b \equiv \alpha^\beta \pmod{m}$.

Ejemplo

Calculamos el resto de dividir 261^{142} entre 50, por tanto estamos buscando $[261]^{142}$ en $\mathbb{Z}_{50}$.
En primer lugar vemos que $261 \equiv 11 \pmod{50}$. Además se cumple que $\mathrm{mcd}(50, 11) = 1$ y por tanto $11^{\phi(50)} \equiv 1 \pmod{50}$.
Calculamos ahora $\phi(50)$: $\phi(50) = \phi(2 \cdot 5^2) = \phi(2) \cdot \phi(5^2) = 1 \cdot (5^2 - 5) = 20$, y vemos que $142 \equiv 2 \pmod{20}$.
Agrupando ahora todos los resultados,
$[261]^{142} = [11]^{142} = [11]^{7 \cdot 20 + 2} = ([11]^{20})^7 \cdot [11]^2 = [1] \cdot [121] = [21]$ en $\mathbb{Z}_{50}$.

Ecuaciones en congruencias

Definición

Se denomina ecuación en congruencias a cualquier expresión de la forma:

$$a \cdot x \equiv b \pmod{m}, \text{ con } a, b, x, m \in \mathbb{Z}(m > 1).$$

La ecuación en congruencias $a \cdot x \equiv b \pmod{m}$ tiene solución en x si y solo si existen $x, y \in \mathbb{Z}$ tales que $a \cdot x = b + m \cdot y$, y esto es equivalente a que la ecuación diofántica $a \cdot x + m \cdot y = b$ tenga solución.

Teorema

La ecuación en congruencias $a \cdot x \equiv b \pmod{m}$ tiene solución en x si y solo si $d = \mathrm{mcd}(a, m) \mid b$ en cuyo caso tiene exactamente d soluciones distintas en $\mathbb{Z}_m$ de la forma

$$x = x_1 + \frac{mt}{d}, t = 0, 1, 2, \ldots, d - 1,$$

siendo x_1 una solución particular de la ecuación diofántica $a \cdot x + m \cdot y = b$.

Ecuaciones en congruencias

Demostración.

Por el teorema de solución de ecuaciones diofánticas y la observación anterior, las únicas soluciones posibles son las de la forma $x = x_1 + \frac{mt}{d}$ con $t \in \mathbb{Z}$.

Vamos a ver primero que cualquier solución de éstas es congruente en módulo m a una de las del enunciado. Por el teorema de la división se tiene que $t = qd + r$ con $0 \leq r < d$. Entonces $\frac{mt}{d} = qm + \frac{mr}{d}$ y por tanto $x_1 + \frac{mt}{d} \equiv x_1 + \frac{mr}{d} \pmod{m}$.

Veamos ahora que todas las soluciones del enunciado del teorema son distintas. Supongamos que existen $0 \leq t_1 < t_2 \leq d-1$ tales que $x_1 + \frac{mt_1}{d} \equiv x_1 + \frac{mt_2}{d} \pmod{m}$. Entonces

$$\left(x_1 + \frac{mt_1}{d}\right) - \left(x_1 + \frac{mt_2}{d}\right) = qm.$$

Luego $m(t_1 - t_2) = qmd$ y por tanto $t_1 - t_2 = qd$ y $d \mid t_1 - t_2$ con $0 \leq t_1 < t_2 \leq d-1$, lo que es imposible, siendo por tanto todas las soluciones distintas.

□

Ecuaciones en congruencias

Observación: Dada la ecuación en congruencias $a \cdot x \equiv b \pmod{m}$, si $\mathrm{mcd}(a, m) = 1$ (a y m son coprimos), existirá $[a]_m^{-1}$ y se podrá obtener $[x]_m$ de forma directa ya que:

$$[a]_m \cdot [x]_m = [b]_m \Rightarrow [a]_m^{-1} \cdot [a]_m \cdot [x]_m = [a]_m^{-1} \cdot [b]_m \Rightarrow [x]_m = [a]_m^{-1} \cdot [b]_m.$$

Además, en este caso la solución será única.

Ejemplo

Resolvemos la ecuación $5x \equiv 2 \pmod{11}$.
En primer lugar vemos que $\mathrm{mcd}(5, 11) = 1$.
A continuación obtenemos $[5]_{11}^{-1} = [9]_{11}$ y por tanto $[x]_{11} = [9]_{11} \cdot [2]_{11} = [7]_{11}$.

Ecuaciones en congruencias

Ejercicio

Resuelve la ecuación: $28x = 77$ en $\mathbb{Z}_{637}$ con $0 \leq x < 637$.

Podemos abordar el problema de diversas formas:

- Una primera opción sería resolver directamente la ecuación diofántica $28x - 637y = 77$.
- También podemos simplificar la ecuación (dividir por 7), y resolver la ecuación diofántica $4x - 91y = 11$ (que generará exactamente las mismas soluciones que la anterior).
- Por último podemos considerar la ecuación en congruencias para resolverla utilizando inversos y la propiedad cancelativa.

En todo caso deberemos asegurarnos de que exista solución. Por tanto comprobamos que $mcd(637, 28) = 7 \mid 77$.
La ecuación tendrá infinitas soluciones en $\mathbb{Z}$, que se van a corresponder con 7 soluciones en $\mathbb{Z}_{637}$.

Ecuaciones en congruencias

Vamos a resolver la ecuación en congruencias:
$[28]_{637}[x]_{637} = [77]_{637} \Rightarrow [7]_{637}[4]_{637}[x]_{637} = [7]_{637}[11]_{637}$, y como $mcd(637, 7) = 7$,
$[4]_{91}[x]_{91} = [11]_{91}$.
Ahora necesitamos calcular $[4]_{91}^{-1}$, o lo que es lo mismo, resolver $4x - 91y = 1$.
$91 = 4 \cdot 22 + 3$, $4 = 3 \cdot 1 + 1$ y por tanto, $1 = 4 - 3 = 4 - (91 - 4 \cdot 22) = 4 \cdot 23 - 91$, es decir $[4]_{91}^{-1} = [23]_{91}$.
Multiplicando ahora por el inverso que se ha calculado:
$[23]_{91}[4]_{91}[x]_{91} = [23]_{91}[11]_{91} \Rightarrow [x]_{91} = [253]_{91} = [71]_{91}$.
Y para obtener la solución en $\mathbb{Z}_{637}$, teniendo en cuenta que $\dfrac{637}{91} = 7$, tenemos que generar las 7 soluciones en $\mathbb{Z}_{637}$, que son congruentes con 71 en $\mathbb{Z}_{91}$, por tanto $x = 71 + 91 \cdot k$, con $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
Y considerando que de acuerdo con el enunciado, $0 \leq x < 637$, estas serán todas las soluciones posibles. Por tanto, x podrá tomar los siguientes valores:
$71, 162, 253, 344, 435, 526, 617$.

Sistemas de congruencias

Definición

Se denomina sistema lineal de congruencias a un conjunto de ecuaciones en congruencias de la forma

$$\begin{cases} x \equiv c_1 & (\text{mód } m_1) \\ x \equiv c_2 & (\text{mód } m_2) \\ \quad \vdots & \\ x \equiv c_r & (\text{mód } m_r) \end{cases}$$

con $x, c_i, m_j \in \mathbb{Z}$.

Teorema (Teorema Chino del Resto)

El sistema de congruencias

$$\begin{cases} x \equiv c_1 & (\text{mód } m_1) \\ x \equiv c_2 & (\text{mód } m_2) \\ \quad \vdots & \\ x \equiv c_r & (\text{mód } m_r) \end{cases}$$

donde $\text{mcd}(m_i, m_j) = 1$ *para todo* $i \neq j$*, tiene solución única en* $\mathbb{Z}_m$ *con* $m = m_1 m_2 \cdots m_r$.

Sistemas de congruencias

Demostración.

Tomando $m = \prod_{j=1}^{r} m_j$ vemos como $\mathrm{mcd}\left(m_i, \frac{m}{m_i}\right) = 1$ para todo $i \in \{1, 2, \ldots, r\}$ (ya que $\mathrm{mcd}(m_i, m_j) = 1 \; \forall i \neq j$).

Como consecuencia de ello $\frac{m}{m_i}$ tendrá inverso en $\mathbb{Z}_{m_i}$, cumpliéndose también que $\frac{m}{m_i} \equiv 0 \pmod{m_j} \; \forall i \neq j$ ya que m_j divide a $\frac{m}{m_i}$.

En consecuencia vemos que $c_i \frac{m}{m_i} \left[\frac{m}{m_i}\right]_{m_i}^{-1} \equiv c_i \pmod{m_i}$ y que $c_i \frac{m}{m_i} \left[\frac{m}{m_i}\right]_{m_i}^{-1} \equiv 0 \pmod{m_j}$ si $j \neq i$.

Si tomamos ahora $x_0 = \sum_{i=1}^{r} c_i \frac{m}{m_i} \left[\frac{m}{m_i}\right]_{m_i}^{-1}$, x_0 es solución del sistema inicial, ya que $x_0 \equiv c_i \pmod{m_i} \; \forall i \in \{1, 2, \ldots, r\}$.

Para hallar la solución general observamos que si x_1 es otra solución, entonces $x_0 \equiv x_1 \pmod{m_i}$ para todo $i \in \{1, 2, \ldots, r\}$ y por tanto $m_i \mid (x_0 - x_1)$ y como $\mathrm{mcd}(m_i, m_j) = 1$ para todo $i \neq j$, entonces $m \mid (x_0 - x_1)$, y resulta que $x_1 \equiv x_0 \pmod{m}$. Por lo que la solución general es $x \equiv x_0 \pmod{m}$. □

Sistemas de congruencias

Proposición

Sean $x, y \in \mathbb{Z}$ tales que

$$\begin{aligned} x &\equiv y \pmod{m_1} \\ x &\equiv y \pmod{m_2} \\ &\vdots \\ x &\equiv y \pmod{m_r} \end{aligned}$$

Con $\mathrm{mcd}(m_i, m_j) = 1$ para todo $i \neq j$. Entonces $x \equiv y \pmod{m_1 m_2 \cdots m_r}$.

Sistemas de congruencias

Ejercicio

Resolver (si es que tiene solución) el sistema de congruencias $\left\{ \begin{array}{l} 5x \equiv 6 \pmod{12} \\ 2x \equiv 5 \pmod{7} \\ 3x \equiv 1 \pmod{5} \end{array} \right\}$

Vemos que $m = 12 \cdot 7 \cdot 5 = 420$. Despejamos (eliminamos los coeficientes del primer miembro multiplicando por los inversos) y aplicamos el teorema:

$$\left\{ \begin{array}{l} x \equiv 6 \cdot 5 \equiv 6 \pmod{12} \\ x \equiv 5 \cdot 4 \equiv 6 \pmod{7} \\ x \equiv 1 \cdot 2 \pmod{5} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \frac{m}{12} = 35 \text{ y } [35]_{12}^{-1} = 11 \Rightarrow 35 \cdot 11 \equiv 1 \pmod{12} \\ \frac{m}{7} = 60 \text{ y } [60]_{7}^{-1} = 2 \Rightarrow 60 \cdot 2 \equiv 1 \pmod{7} \\ \frac{m}{5} = 84 \text{ y } [84]_{5}^{-1} = 4 \Rightarrow 84 \cdot 4 \equiv 1 \pmod{5} \end{array} \right.$$

Y la solución será de la forma $x = 6 \cdot \frac{m}{12} \cdot \left[\frac{m}{12}\right]_{12}^{-1} + 6 \cdot \frac{m}{7} \cdot \left[\frac{m}{7}\right]_{7}^{-1} + 2 \cdot \frac{m}{5} \cdot \left[\frac{m}{5}\right]_{5}^{-1}$.

$$\left\{ x = (6 \cdot 35 \cdot 11 + 6 \cdot 60 \cdot 2 + 2 \cdot 84 \cdot 4) = 3702 \equiv 342 \pmod{420} \right.$$

$x = [342]_{420}$ que se corresponde en $\mathbb{Z}$ con $x = 342 + 420t \forall t \in \mathbb{Z}$.

Una consecuencia (inmediata) del teorema Chino del Resto

Observación: Si en una ecuación en congruencias el valor de m es muy alto, se puede simplificar su resolución transformándola en un sistema de congruencias.
Sea $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, con $p_1, \ldots, p_k$ primos distintos.
Entonces, dados $a, b \in \mathbb{Z}$ se tiene que

$$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{p_i^{r_i}}, \text{ para cada } i = 1, \ldots, k.$$

Ejemplo

Consideramos la ecuación $91x \equiv 419 \pmod{440}$.
Puesto que $\mathrm{mcd}(91, 440) = 1$ la congruencia tiene solución.
Como $440 = 2^3 \cdot 5 \cdot 11$, se tiene que

$$91x \equiv 419 \pmod{440} \Leftrightarrow \left\{ \begin{array}{l} 91x \equiv 419 \pmod{8} \\ 91x \equiv 419 \pmod{5} \\ 91x \equiv 419 \pmod{11} \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} 3x \equiv 3 \pmod{8} \\ x \equiv 4 \pmod{5} \\ 3x \equiv 1 \pmod{11} \end{array} \right\} \Leftrightarrow$$

$$\Leftrightarrow \left\{ \begin{array}{l} x \equiv 1 \pmod{8} \\ x \equiv 4 \pmod{5} \\ x \equiv 3^{-1} \equiv 4 \pmod{11} \end{array} \right\} \Leftrightarrow x \equiv 1 \cdot 55 \cdot 7 + 4 \cdot 88 \cdot 2 + 4 \cdot 40 \cdot 8 \pmod{440} \Leftrightarrow$$

$$\Leftrightarrow x \equiv 2369 \pmod{440} \Leftrightarrow x \equiv 169 \pmod{440}.$$

Sistemas de congruencias

Teorema (Teorema Chino del Resto Generalizado)

Sea el sistema de congruencias

$$\begin{cases} x \equiv c_1 & (\text{mód } m_1) \\ x \equiv c_2 & (\text{mód } m_2) \\ \quad \vdots & \\ x \equiv c_r & (\text{mód } m_r) \end{cases}$$

con $m_1, m_2, \ldots m_r \in \mathbb{Z}^+$. *Si* $\text{mcd}(m_i, m_j) \mid (c_i - c_j)$ *para todo* i, j, *el sistema tiene solución única en* $\mathbb{Z}_m$ *con* $m = \text{mcm}(m_1, m_2, \cdots, m_r)$.

Sistemas de congruencias

Ejercicio

Hallar un número natural cuyos restos al dividirlo por 3,4,5 y 6 sean respectivamente 2,3,4 y 5.

Como $\mathrm{mcd}(3,6)=3$ y $\mathrm{mcd}(4,6)=2$ resolveramos primero las tres primeras ecuaciones y comprobaremos si la solución verifica también la otra ecuación. En ese caso, la solución será única en $\mathbb{Z}_60$ puesto que $\mathrm{mcd}(3,4,5,6)=60$.

$$\left\{\begin{array}{ll} x\equiv 2 & (\mathrm{mód}\ 3)\\ x\equiv 3 & (\mathrm{mód}\ 4)\\ x\equiv 4 & (\mathrm{mód}\ 5)\\ x\equiv 5 & (\mathrm{mód}\ 6)\end{array}\right\} \Rightarrow \left\{\begin{array}{ll} x\equiv 2 & (\mathrm{mód}\ 3)\\ x\equiv 3 & (\mathrm{mód}\ 4)\\ x\equiv 4 & (\mathrm{mód}\ 5)\\ \{x\equiv 5 & (\mathrm{mód}\ 6)\end{array}\right\}$$

Tenemos que $\frac{60}{3}=20\equiv 2\ (\mathrm{mód}\ 3)$ y $[20]_3^{-1}=[2]_3$. Por otro lado $\frac{60}{4}=15\equiv 3\ (\mathrm{mód}\ 4)$ y $[15]_4^{-1}=[3]_4$. Y por último $\frac{60}{5}=12\equiv 2\ (\mathrm{mód}\ 5)$ y $[12]_5^{-1}=[3]_5$.
Entonces la posible solución del sistema reducido es:
$x_0=2\cdot 20\cdot 2+3\cdot 15\cdot 3+4\cdot 12\cdot 3=80+135+144=359$, es decir, $[59]$ en $\mathbb{Z}_{60}$.
Comprobamos ahora la cuarta congruencia, y en efecto $59\equiv 5\ (\mathrm{mód}\ 6)$, entonces $[x_0]=[59]$ en $\mathbb{Z}_{60}$ es la solución del sistema inicial.

Teorema Chino del Resto Generalizado

Ejercicio.

Resuelve el sistemas de congruencias $\begin{cases} 4x \equiv 11\,(\text{mód } 15) \\ 10x \equiv 8\,(\text{mód } 12) \end{cases}$

Simplificando y despejando resulta

$$\begin{cases} 4x \equiv 11\,(\text{mód } 15) \Leftrightarrow x \equiv 4^{-1} \cdot 11 \equiv 4 \cdot 11 \equiv 44 \equiv 14\,(\text{mód } 15) \\ 10x \equiv 8\,(\text{mód } 12) \Leftrightarrow 5x \equiv 4\,(\text{mód } 6) \Leftrightarrow x \equiv 5^{-1} \cdot 4 \equiv 5 \cdot 4 \equiv 20 \equiv 2\,(\text{mód } 6) \end{cases}$$

Este sistema tiene solución pues $\text{mcd}(15, 6) = 3 | (14 - 2) = 12$.

Resolvemos:

$$\left.\begin{array}{l} x \equiv 14\,(\text{mód } 3 \cdot 5) \Leftrightarrow \begin{cases} x \equiv 14\,(\text{mód } 3) \Leftrightarrow x \equiv 2\,(\text{mód } 3) \\ x \equiv 14\,(\text{mód } 5) \Leftrightarrow x \equiv 4\,(\text{mód } 5) \end{cases} \\ x \equiv 2\,(\text{mód } 2 \cdot 3) \Leftrightarrow \begin{cases} x \equiv 2\,(\text{mód } 2) \\ x \equiv 2\,(\text{mód } 3) \end{cases} \end{array}\right\} \Rightarrow \begin{cases} x \equiv 2\,(\text{mód } 2) \\ x \equiv 2\,(\text{mód } 3) \\ x \equiv 4\,(\text{mód } 5) \end{cases}$$

Como $\text{mcd}(2, 3) = \text{mcd}(2, 5) = \text{mcd}(3, 5) = 1$, aplicamos el Teorema Chino del Resto:
$x \equiv 2 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 4 \cdot 6 \cdot 1\,(\text{mód } 2 \cdot 3 \cdot 5) \Leftrightarrow x \equiv 74\,(\text{mód } 30) \Leftrightarrow x \equiv 14\,(\text{mód } 30)$.