Matemática Discreta

Mariam Cobalea

Universidad de Málaga
Dpto. de Matemática Aplicada

Tema 2: Teoría de números

- 2.1 Aritmética entera.
  - Introducción: Axiomática de $\mathbb{Z}$.
  - Algoritmo de la división de dos números enteros. Divisibilidad.
  - Máximo Común Divisor. Algoritmo de Euclides.
  - Algoritmo extendido de Euclides: Identidad de Bezout.
  - Primos. Teorema fundamental de la aritmética.
  - Ecuaciones Diofánticas.
- 2.2 Aritmética modular.
  - Congruencia módulo m . Propiedades.
  - Aritmética de las congruencias.
  - Congruencias lineales. Teoremas de Euler y Fermat.
  - Sistemas de congruencias. Teorema chino de los restos. Generalización.
  - Aplicaciones de las congruencias:
    - Restos potenciales.
    - Criterios de divisibilidad.

Tema 2: Teoría de números

- Congruencia módulo m . Propiedades.
- Aritmética de las congruencias.
- Congruencias lineales. Teoremas de Euler y Fermat.
- Sistemas de congruencias. Teorema chino de los restos. Generalización.
- Aplicaciones de las congruencias:
  - Restos potenciales.
  - Criterios de divisibilidad.

2.2 Aritmética Modular

Congruencia módulo m

- El lenguaje de las congruencias es muy útil en Teoría de números.
- Este lenguaje fué introducido al final del siglo $XVIII$ por Gauss (1777-1855).

Definición (Congruencia módulo m)

Sean los enteros $a, b, m \in \mathbb{Z}$, *tales que* $m > 1$. *Se dice que* a *es* ***congruente*** *con* b ***módulo*** m *si y sólo si* $m \mid (a - b)$.
Se denota $a \equiv b \pmod{m}$

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

Ejemplos

(1) $23 \equiv 17 \pmod{3}$, ya que $23 - 17 = 6 = 2 \cdot 3$

(2) $-12 \equiv 14 \pmod{13}$, ya que $-12 - 14 = -26 = (-2)13$

2.2 Aritmética Modular

Congruencia módulo m

Las congruencias surgen a menudo en la vida diaria:

- Los relojes trabajan (mód 12) ó (mód 24) para las horas y (mód 60) para los minutos y segundos.
- Los calendarios trabajan (mód 7) para los días de la semana y (mód 12) para los meses.
- Los odómetros trabajan (mód 100,000)

Ejercicio Demuestra que en años no bisiestos el mes de Enero coincide con el mes de Octubre y que en años bisiestos Enero coincide con Julio.

Aritmética Modular

Congruencia módulo m

Teorema

Sean los enteros $a, b, m \in \mathbb{Z}$, *tales que* $m > 1$. *Se verifica:*

$$a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z},\ a = b + km$$

Demostración:

$$a \equiv b \pmod{m} \iff m|(a-b)$$

$$\iff \exists k \in \mathbb{Z},\ a - b = mk$$

$$\iff \exists k \in \mathbb{Z},\ a = b + mk$$

2.2 Aritmética Modular

Propiedades de las congruencias

Teorema

Los enteros $a, b \in \mathbb{Z}$ *son congruentes módulo* m *si y sólo si tienen el mismo resto al dividirse entre* m .

Demostración: Ejercicio

Ejemplo

2.2 Aritmética Modular

Propiedades de las congruencias

Teorema

Sea $m \in \mathbb{Z},\ m > 1$. *Entonces cada entero* $x \in \mathbb{Z}$ *es congruente módulo* m *exactamente con uno de los siguientes enteros:* $0, 1, \ldots, m-1$.

Demostración: Dados $x \in \mathbb{Z},\ m > 1$, por el algoritmo de la división

$$\exists!\ \ q, r,\ x = qm + r,\ 0 \leq r < m$$

Por lo tanto,

$$x \equiv r \pmod{m}, \quad \text{con} \quad r \in \{0, 1, \ldots, m-1\}$$

Esta propiedad del conjunto de enteros $\{0, 1, \ldots, m-1\}$ pueden tenerla otros subconjuntos de $\mathbb{Z}$.

2.2 Aritmética Modular

Aritmética de las congruencias

Ejercicio Sean los enteros $a, b, m \in \mathbb{Z}$, con $m > 1$ tales que

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

Demuestra que si m' es un divisor de m , entonces $a \equiv b \pmod{m'}$

Solución:

$$\left.\begin{array}{l} a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z}, a - b = km \\ m' | m \iff \exists j \in \mathbb{Z},\ jm' = m \end{array}\right\} \iff a - b = kjm'$$

Por lo tanto,

$$m' | (a - b) \iff a \equiv b \pmod{m'}$$

Ejemplo

$$\left.\begin{array}{l} 18 \equiv 6 \pmod{12} \\ 4 | 12 \end{array}\right\} \Longrightarrow 18 \equiv 6 \pmod{4}$$

Aritmética Modular

Propiedades de las congruencias

Teorema

Sean los enteros $a, b, c, m \in \mathbb{Z}$ *, con* $m > 1$ *. La congruencia* **módulo** m *verifica las propiedades:*

Reflexiva: $a \equiv a \pmod{m}$

Simétrica: $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$

Transitiva: $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

Demostración: Ejercicio

2.2 Aritmética Modular

Propiedades de las congruencias

- Del teorema anterior se deduce que la **congruencia módulo** m es una **relación de equivalencia** definida en $\mathbb{Z}$. Por tanto, establece una **partición** en $\mathbb{Z}$.
- Las clases de equivalencia definidas por la relación de congruencia módulo m se denotan $[a]_m$ y el conjunto cociente, es decir, el conjunto formado por todas las clases de equivalencia se denota $\mathbb{Z}_m = \mathbb{Z}_{/\equiv_m}$.
- Cada clase $[a]_m$ contendrá todos los enteros que son mutuamente congruentes módulo m .
- Teniendo en cuenta las propiedades vistas anteriormente, el conjunto $\mathbb{Z}_m$ tiene exactamente m elementos.

2.2 Aritmética Modular

Propiedades de las congruencias

Ejemplo: Las cuatro clases de equivalencia de la congruencia módulo 4 son:

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

$$\mathbb{Z}_4 = \left\{[0]_4, [1]_4, [2]_4, [3]_4\right\}$$

- Las relación de congruencia entre números se pueden expresar más brevemente usando las clases de equivalencia:

$$a \equiv b \pmod{m} \iff [a]_m = [b]_m$$

Ejemplo:

$22 = 2 + 5 \cdot 4 \iff 22 \equiv 2 \pmod{5} \iff [22]_5 = [2]_5$

Teorema (Aritmética de las congruencias (I))

Sean $a, b, c, m \in \mathbb{Z}$, $m > 1$ *tales que* $a \equiv b \pmod{m}$. *Entonces:*

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $a \cdot c \equiv b \cdot c \pmod{m}$

Ejemplos Ya que $17 \equiv 3 \pmod{7}$, tenemos que:

- $22 = 17 + 5 \equiv 3 + 5 = 8 \pmod{7}$
- $17 - 4 = 13 \equiv 3 - 4 = -1 \pmod{7}$
- $17 \cdot 2 = 34 \equiv 3 \cdot 2 \pmod{7}$

Hemos visto que al sumar, restar o multiplicar ambos lados de una congruencia se preserva la congruencia.

¿Qué sucederá cuando dividimos ambos lados de la congruencia por un número?

¿Se conserva la congruencia?

Ejemplo $2 \cdot 9 \equiv 2 \cdot 3 \pmod{12}$, pero $9 \not\equiv 3 \pmod{12}$.

Con este ejemplo comprobamos que **no** se preserva la congruencia al dividir ambos lados por un entero.

Sin embargo, el siguiente teorema nos enseña cómo se pueden **simplificar** las congruencias.

Teorema (Aritmética de las congruencias (II))

Sean $a, b, c, d, m \in \mathbb{Z}$, $m > 1$, $mcd(c, m) = d$. *Si* $a \cdot c \equiv b \cdot c \pmod{m}$, *entonces* $a \equiv b \pmod{\left(\frac{m}{d}\right)}$

$$\left.\begin{array}{rcl} a \cdot c & \equiv & b \cdot c \pmod{m} \\ d & = & mcd(c, m) \end{array}\right\} \Longrightarrow a \equiv b \pmod{\left(\frac{m}{d}\right)}$$

Ejemplo Simplifica: $18x \equiv 42 \pmod{45}$.

$$18 = 6 \cdot 3, \quad 42 = 6 \cdot 7, \quad mcd(6, 45) = 3$$

$$18x \equiv 42 \pmod{45} \Longrightarrow 3x \equiv 7 \pmod{15}$$

Demostración:

$$a \cdot c \equiv b \cdot c \pmod{m} \iff \exists k \in \mathbb{Z}, \quad a \cdot c - b \cdot c = km \qquad (1)$$

Dividiendo ambos lados de (1) por d , tenemos

$$(a - b)\left(\frac{c}{d}\right) = k\left(\frac{m}{d}\right)$$

De aquí, por ser coprimos $\left(\frac{c}{d}\right)$ y $\left(\frac{m}{d}\right)$, se sigue que

$$\left(\frac{m}{d}\right) \Big| (a - b)$$

Por tanto,

$$a \equiv b \pmod{\left(\frac{m}{d}\right)}$$

Corolario

Sean $a, b, c, m \in \mathbb{Z}$, $m > 1$ *con* $mcd(c, m) = 1$. *Si* $a \cdot c \equiv b \cdot c \pmod{m}$, *entonces* $a \equiv b \pmod{m}$.

Ejemplo

$$18x \equiv 42 \pmod{47} \implies 3x \equiv 7 \pmod{47}$$

Ejercicio Sean los enteros $a, b, m \in \mathbb{Z}$, $m > 1$ tales que $a \equiv b \pmod{m}$.
Demuestra que si e es un divisor común de a, b y m , entonces

$$\left(\frac{a}{e}\right) \equiv \left(\frac{b}{e}\right) \pmod{\left(\frac{m}{e}\right)}$$

Solución:

Por ser e un divisor común de a, b y m , existen $a', b', m' \in \mathbb{Z}$ tales que

$$a = ea', \qquad b = eb', \qquad m = em'$$

Sabemos que $a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z}, a - b = km$.
Luego,

$$ea' - eb' = kem' \iff a' - b' = km' \iff \left(\frac{a}{e}\right) \equiv \left(\frac{b}{e}\right) \pmod{\left(\frac{m}{e}\right)}$$

Ejemplo

$$\left.\begin{array}{l} 66 \equiv 30 \pmod{18} \\ 2|66,\ 2|30,\ 2|18 \end{array}\right\} \implies 33 \equiv 15 \pmod{9}$$

$$\left.\begin{array}{l} 33 \equiv 15 \pmod{9} \\ 3|33,\ 3|15,\ 3|9 \end{array}\right\} \implies 11 \equiv 5 \pmod{3}$$

Teorema (Aritmética básica de las congruencias (III))

Sean $a, b, c, d, m \in \mathbb{Z}$, $m > 1$. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces:*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $a \cdot c \equiv b \cdot d \pmod{m}$

Ejemplos

$$\left.\begin{array}{rcll} 18 & \equiv & 6 & \pmod{12} \\ -2 & \equiv & 10 & \pmod{12} \end{array}\right\} \implies \left\{\begin{array}{llcll} (1) & 18 + (-2) & \equiv & 6 + 10 & \pmod{12} \\ (2) & 18 - (-2) & \equiv & 6 - 10 & \pmod{12} \\ (3) & 18 \cdot (-2) & \equiv & 6 \cdot 10 & \pmod{12} \end{array}\right\}$$

Demostración

➢ La demostración del teorema anterior es una simple comprobación:

$$\left.\begin{array}{l} a = b + m \cdot k_1 \\ c = d + m \cdot k_2 \end{array}\right\} \implies \left\{\begin{array}{l} a + c = b + d + m(k_1 + k_2) \\ a - c = b - d + m(k_1 - k_2) \\ a \cdot c = b \cdot d + m(d \cdot k_1 + b \cdot k_2) \end{array}\right.$$

- Este teorema justifica que las siguientes operaciones en $\mathbb{Z}_m$ están bien definidas

$$[a]_m +_m [b]_m = [a + b]_m \qquad [a]_m \cdot_m [b]_m = [a \cdot b]_m$$

- Estas propiedades permitirán trabajar más eficientemente con congruencias.

Corolario

Si $a \equiv b \pmod{m}$, *entonces* $a^k \equiv b^k \pmod{m}$.

Demostración: Se puede demostrar aplicando reiteradamente el teorema anterior y usando inducción.

También se puede dar una demostración directa, como hacemos a continuación.

- Por ser $a \equiv b \pmod{m}$, tenemos que m es un divisor de $a - b$.
- Por otra parte, sabemos que para todo $k \in \mathbb{Z}^+$

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$$

- Así, m también es divisor de $a^k - b^k$.
- Por tanto, $a^k \equiv b^k \pmod{m}$.

Ejemplo Encuentra el resto de dividir 795^{25} entre 11.

Solución:

- Ya que $795 \equiv 3 \pmod{11}$, se tiene que $795^{25} \equiv 3^{25} \pmod{11}$.
- Luego basta determinar el resto de dividir 3^{25} entre 11.
- Por otra parte, sabemos que $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1$
- Aplicando el teorema

$$3^2 \equiv -2 \pmod{11} \implies 3^4 \equiv 4 \pmod{11}$$
$$\implies 3^8 \equiv 5 \pmod{11}$$
$$\implies 3^{16} \equiv 3 \pmod{11}$$

- Así, $3^{25} \equiv 3 \cdot 5 \cdot 3 \pmod{11}$
- Por lo tanto, $795^{25} \equiv 1 \pmod{11}$.

¿Cómo combinar congruencias de dos números con diferentes módulos?

Teorema

Sean $a, b, m_1, m_2, \ldots, m_k$ *enteros, con* $m_1, m_2, \ldots, m_k$ *positivos.*
Si $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, *entonces*

$$a \equiv b \pmod{m.c.m.(m_1, \ldots, m_k)}$$

Demostración:

- Ya que $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, sabemos que $m_1 | (a-b)$, $m_2 | (a-b), \ldots$, $m_k | (a-b)$.
- De aquí se deduce que $\text{mcm}(m_1, \ldots, m_k) | (a-b)$.
- Por consiguiente,

$$a \equiv b \pmod{(m.c.m.(m_1, \ldots, m_k))}$$

Corolario

Sean $a, b, m_1, m_2, \ldots, m_k$ *enteros, tales que* $m_1, m_2, \ldots, m_k$ *son primos relativos dos a dos. Si* $a \equiv b \pmod{m_1}$, $\ldots, a \equiv b \pmod{m_k}$, *entonces*

$$a \equiv b \pmod{m_1 \cdots m_k}$$

Demostración:

- Por ser $m_1, \ldots, m_k$ primos relativos, $mcm(m_1, \ldots, m_k) = m_1 \cdot m_2 \cdot m_k$.
- Por tanto, por el teorema anterior

$$a \equiv b \pmod{m_1 \cdots m_k}$$

.

Definición

Una congruencia de la forma

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

donde x *es un entero desconocido, se llama* ***congruencia lineal de una variable***.

- En primer lugar, observamos que si $x = x_0$ es una solución de la congruencia $ax \equiv b \pmod{m}$, y si $x_1 \equiv x_0 \pmod{m}$, entonces $ax_1 \equiv ax_0 \equiv b \pmod{m}$, por lo que x_1 es también una solución.
- De ahí, si un elemento de una clase de congruencia módulo m es una solución, entonces todos los miembros de esa clase son soluciones.
- Por tanto, podemos preguntarnos cuántas de las m clases de congruencia módulo m son soluciones.

El siguiente teorema nos enseña cuando tiene solución una congruencia lineal de una variable y, si la tiene, nos dice exactamente cuantas soluciones hay en $\mathbb{Z}_m$.

Teorema (Brahmagupta)

Sean a, b *y* m *enteros con* $m > 1$ *y* $mcd(a, m) = d$.

- *Si* $d \not| b$, *entonces* $ax \equiv b \pmod{m}$ *no tiene solución.*
- *Si* $d|b$, *entonces* $ax \equiv b \pmod{m}$ *tiene exactamente* d *soluciones en* $\mathbb{Z}_m$.

Demostración:

- El entero x es una solución de $ax \equiv b \pmod{m}$ si y sólo si hay un entero k tal que $ax - mk = b$.
- Y tomando $y = -k$, nos queda la ecuación diofántica $ax + my = b$.
- Por el teorema de existencia de soluciones de tales ecuaciones, sabemos que si $d \not| b$, dicha ecuación no tiene solución;
- mientras que si $d|b$ hay infinitas soluciones dadas por

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t, \quad t \in \mathbb{Z}$$

  donde $x = x_0$ e $y = y_0$ es una solución particular de la ecuación.
- Y estos valores de x dados son las soluciones de la congruencia lineal.

Demostración: (cont.)

- Para determinar cuántas soluciones hay en $\mathbb{Z}_m$, buscamos la condición que describe cuando dos de las soluciones $x_1 = x_0 + \left(\frac{m}{d}\right)t_1$ y $x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ son congruentes módulo m.
- Si estas soluciones son congruentes

$$x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \pmod{m}$$

- entonces $t_1 \equiv t_2 \pmod{d}$
- Esto muestra que un conjunto completo de soluciones módulo m se obtiene tomando $x = x_0 + \left(\frac{m}{d}\right)t$, donde t toma los valores en $\{0, 1, \ldots, d-1\}$.

2.2 Aritmética Modular

Congruencias Lineales

Dada una congruencia lineal

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

encontramos todas las soluciones aplicando el teorema anterior.

1. Estudiamos si tiene soluciones enteras, comprobando si $mcd(a, m) = d$ es un divisor de b
2. Hallamos una **solución particular**: x_0 resolviendo la ecuación diofántica $ax + my = b$
3. Damos las d soluciones a partir de la solución particular

$$x_0 + t(\frac{m}{d}), \quad t \in \{0, 1, ..., d-1\}$$

2.2 Aritmética Modular

Congruencias Lineales

Ejemplo Resuelve la congruencia lineal $9x \equiv 12 \pmod{15}$

Solución:

1. Estudiamos si tiene soluciones enteras,

$$\left.\begin{array}{rcl} mcd(9, 15) & = & 3 \\ 3 & | & 12 \end{array}\right\}$$

   Luego $9x \equiv 12 \pmod{15}$ tiene 3 soluciones en $\mathbb{Z}_{15}$

2. La convertimos en una ecuación diofántica

$$9x \equiv 12 \pmod{15} \implies 9x + 15y = 12 \implies 3x + 5y = 4$$

   Hallamos una **solución particular**: x_0

$$mcd(3, 5) = 1 = 3 \cdot 2 + 5 \cdot (-1) \implies 4 = 3 \cdot 8 + 5 \cdot (-4) \implies x_0 = 8$$

2.2 Aritmética Modular

Congruencias Lineales

Ejemplo $9x \equiv 12 \pmod{15}$

Solución:(cont.)

3. Damos las 3 soluciones en $\mathbb{Z}_{15}$ a partir de la solución particular

$$4 = 3 \cdot 8 + 5 \cdot (-4)$$

   La solución general es $x = 8 + t(\frac{15}{3}), \quad t \in \{0, 1, 2\}$ que incluye enteros de las siguientes clases de equivalencia:

$$[8]_{15}, \quad [13]_{15}, \quad [18]_{15} = [3]_{15}$$

2.2 Aritmética Modular

Congruencias Lineales

Ejemplo $4x \equiv 10 \pmod{30}$

Solución:

1. Estudiamos si tiene soluciones enteras,

$$\left.\begin{array}{rcl} mcd(4, 30) & = & 2 \\ 2 & | & 10 \end{array}\right\}$$

   Luego $4x \equiv 10 \pmod{30}$ tiene 2 soluciones en $\mathbb{Z}_{30}$

2. La convertimos en una ecuación diofántica

$$4x \equiv 10 \pmod{30} \implies 4x + 30y = 10 \implies 2x + 15y = 5$$

   Hallamos una **solución particular**: x_0,

$$mcd(2, 15) = 1 = 2 \cdot 8 + 15 \cdot (-1) \implies 5 = 2 \cdot 40 + 15 \cdot (-5) \implies x_0 = 40$$

Ejemplo $4x \equiv 10 \pmod{30}$
Solución:(cont.)

3. Damos las 2 soluciones módulo 30 a partir de la solución particular

$$5 = 2 \cdot 40 + 15 \cdot (-5)$$

La solución general es $x = 40 + \frac{30}{2}t, \quad t \in \{0, 1\}$ que incluye enteros de las siguientes clases de equivalencia:

$$[40]_{30} = [10]_{30} \qquad [40 + 15]_{30} = [25]_{30}$$

Ahora consideramos congruencias de la forma

$$ax \equiv 1 \pmod{m}$$

Por el teorema anterior existe solución si y sólo si $mcd(a, m) = 1$.

Definición (Inverso módulo m)

Sea $a \in \mathbb{Z}$, tal que $mcd(a, m) = 1$. Un **inverso** *de a módulo m es un $x \in \mathbb{Z}$ que verifica*

$$ax \equiv 1 \pmod{m}$$

- Si $[a]_m[b]_m = [1]_m$, escribimos $[b]_m = [a]_m^{-1}$.

Ejemplo Halla el inverso de la clase $[6]_{17}$.
Solución:

- La clase $[6]_{17}$ tiene inverso, ya que $mcd(6, 17) = 1$.
- Para calcularlo, resolvemos la congruencia $6x \equiv 1 \pmod{17}$.
- Para ello, la convertimos en una ecuación diofántica

$$6x \equiv 1 \pmod{17} \implies 6x + 17y = 1$$

- Hallamos una **solución particular**: x_0,

$$mcd(6, 17) = 1 = 6(3) + 17(-1) \implies x_0 = 3$$

- La solución de $6x \equiv 1 \pmod{17}$ es $x \equiv 3 \pmod{17}$.
- Luego $[6]_{17}^{-1} = [3]_{17}$
- Análogamente,

$$6 \cdot 3 \equiv 1 \pmod{17} \implies [3]_{17}^{-1} = [6]_{17}$$

- Si existe inverso de a módulo m , podemos resolver directamente cualquier congruencia $ax \equiv b \pmod{m}$.
- Sea $\hat{a}$ un inverso de a módulo m :

$$a\hat{a} \equiv 1 \pmod{m}$$

- Entonces, si $ax \equiv b \pmod{m}$, podemos multiplicar ambos miembros de esta congruencia por $\hat{a}$ para encontrar que

$$\hat{a} \cdot (ax) \equiv \hat{a} \cdot b \pmod{m}$$

- Así,

$$x \equiv \hat{a} \cdot b \pmod{m}$$

- En este caso, la congruencia lineal tiene **solución única** en $\mathbb{Z}_m$.

Ejemplo Resuelve la congruencia lineal $6x \equiv 5 \pmod{17}$

Solución:

$$6x \equiv 5 \pmod{17}$$

$$[6]_{17}[x]_{17} = [5]_{17}$$

$$[6]_{17}^{-1}[6]_{17}[x]_{17} = [6]_{17}^{-1}[5]_{17}$$

$$[1]_{17}[x]_{17} = [3]_{17}[5]_{17}$$

$$[x]_{17} = [15]_{17}$$

Ejemplo Resuelve la congruencia lineal $7x \equiv 23 \pmod{31}$

Solución:

1. Hallamos $[7]_{31}^{-1}$, resolviendo la congruencia lineal $7x \equiv 1 \pmod{31}$
   - Para ello, la convertimos en una ecuación diofántica
     $$7x \equiv 1 \pmod{31} \implies 7x + 31y = 1$$
   - Hallamos una **solución particular**: x_0,
     $$mcd(7, 31) = 1 = 7(9) + 31(-2) \implies x_0 = 9,\ y_0 = -2$$
   - Por lo tanto, $[7]_{31}^{-1} = [9]_{31}$
2. Multiplicamos por el inverso en ambos lados de la congruencia lineal

$$7x \equiv 23 \pmod{31}$$
$$[7]_{31}[x]_{31} = [23]_{31} = [-8]_{31}$$
$$[7]_{31}^{-1}[7]_{31}[x]_{31} = [7]_{31}^{-1}[-8]_{31}$$
$$[1]_{31}[x]_{31} = [9]_{31}[-8]_{31}$$
$$[x]_{31} = [-72]_{31} = [21]_{31}$$

- En el ejemplo anterior, $\text{mcd}(a, m) = 1$. Si no fuera 1, también podremos resolver la congruencia usando el inverso, pero necesitaremos simplificar.

Ejemplo Resuelve $12x \equiv 14 \pmod{34}$.

Solución: Ya que $\text{mcd}(12, 34) = 2$, esta congruencia lineal tiene **dos** soluciones módulo 34.

$$\begin{aligned} 12x &\equiv 14 \pmod{34} \\ 6x &\equiv 7 \pmod{17} \\ [6]_{17}[x]_{17} &= [7]_{17} \\ [6]_{17}^{-1}[6]_{17}[x]_{17} &= [6]_{17}^{-1}[7]_{17} \\ [1]_{17}[x]_{17} &= [3]_{17}[7]_{17} \\ [x]_{17} &= [21]_{17} = [4]_{17} \end{aligned}$$

$\Leftarrow$ $\boxed{\begin{array}{c} 12x = 14 + 34k \\ \Updownarrow \\ 6x = 7 + 17k \end{array}}$

Por lo tanto, las dos soluciones módulo 34 son: $[4]_{34}$ y $[4 + 17]_{34} = [21]_{34}$.

Ejemplo Resuelve $12x \equiv 14 \pmod{34}$.

Solución:

- Ya que $\text{mcd}(12, 34) = 2$, esta congruencia lineal tiene **dos** soluciones módulo 34.
- Simplificando la congruencia por $\text{mcd}(12, 34) = 2$, se obtiene una congruencia con solución única
  $$12x \equiv 14 \pmod{34} \implies 6x \equiv 7 \pmod{17}$$
- Hallamos un inverso de 6 módulo m y multiplicamos a ambos lados
  $$3 \cdot 6x \equiv 3 \cdot 7 \pmod{17}$$
- La solución será $x \equiv 21 \pmod{17}$
- Por lo tanto, las dos soluciones módulo 34 son:
  $$[21]_{34} \quad \text{y} \quad [21 + 17]_{34} = [4]_{34}.$$

2.2 Aritmética Modular

Método de resolución de una congruencia lineal $ax \equiv b \pmod{m}$

1. Se calcula $d = \mathrm{mcd}(a, m)$.
2. Se comprueba si d es un divisor de b .
   - **i)** Si d no es un divisor de b , entonces no hay solución.
   - **ii)** Si d es un divisor de b , entonces hay d soluciones en $\mathbb{Z}_m$.
3. Para encontrar las soluciones en el caso **ii)**, se simplifica la congruencia por d ; así obtenemos la congruencia de solución única en $\mathbb{Z}_{\frac{m}{d}}$

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

4. Se halla el inverso de $\frac{a}{d}$ en $\mathbb{Z}_{\frac{m}{d}}$.
5. Se multiplica en ambos lados de la congruencia, lo que nos da una solución c para x .
6. Las soluciones de la congruencia inicial son

$$[c]_m,\ [c + \frac{m}{d}]_m,\ \ldots [c + \frac{m}{d} \cdot (d-1)]_m$$

2.2 Aritmética Modular

Método de resolución de una congruencia lineal $ax \equiv b \pmod{m}$

Ejemplo Resuelve $6x \equiv 12 \pmod{21}$.

Solución:

1. Hallamos $\mathrm{mcd}(6, 21) = 3$
2. Ya que $3 \mid 12$, existen 3 soluciones en $\mathbb{Z}_{21}$.
3. Se simplifica la congruencia

$$6x \equiv 12 \pmod{21} \implies 2x \equiv 4 \pmod{7}$$

4. Se halla el inverso de 2 en $\mathbb{Z}_7$

$$\mathrm{mcd}(2, 7) = 1 = 2 \cdot (-3) + 7 \cdot 1$$

5. Se multiplica por el inverso

$$2x \equiv 4 \pmod{7} \implies (-3) \cdot 2x \equiv (-3) \cdot 4 \pmod{7}$$

6. Las soluciones de la congruencia inicial son

$$[-12]_{21} = [9]_{21};\ [-12 + \frac{21}{3}]_{21} = [-5]_{21} = [16]_{21};\ [-12 + \frac{21}{3} \cdot 2]_{21} = [2]_{21}$$

2.2 Aritmética Modular

Método de resolución de una congruencia lineal $ax \equiv b \pmod{m}$

Ejemplo Resuelve $432x \equiv 12 \pmod{546}$.

Solución:

1. Hallamos $\mathrm{mcd}(432, 546) = 6$
2. Ya que $6 \mid 546$, existen 6 soluciones en $\mathbb{Z}_{546}$.
3. Se simplifica la congruencia

$$432x \equiv 12 \pmod{546} \implies 72x \equiv 2 \pmod{91}$$

4. Se halla el inverso de 72 en $\mathbb{Z}_{91}$

$$\mathrm{mcd}(72, 91) = 1 = 72 \cdot (-24) + 91 \cdot 19$$

5. Se multiplica por el inverso para obtener la solución $\pmod{91}$

$$72x \equiv 2 \pmod{91} \implies (-24) \cdot 72x \equiv (-24) \cdot 2 \pmod{91}$$
$$\implies x \equiv -48 \pmod{91} \implies x \equiv 43 \pmod{91}$$

2.2 Aritmética Modular

Método de resolución de una congruencia lineal $ax \equiv b \pmod{m}$

Ejemplo Resuelve $432x \equiv 12 \pmod{546}$.

Solución: (cont.)

5. La solución módulo 91 es $x \equiv 43 \pmod{91}$.
6. Las soluciones de la congruencia inicial son

$$[43]_{546};\qquad [43 + 91]_{546} = [134]_{546};$$

$$[43 + 91 \cdot 2]_{546} = [225]_{546};\qquad [43 + 91 \cdot 3]_{546} = [316]_{546};$$

$$[43 + 91 \cdot 4]_{546} = [407]_{546};\qquad [43 + 91 \cdot 5]_{546} = [498]_{546}$$

Ejercicio

Sea p primo. El entero positivo a es su propio inverso módulo p si y sólo si $a \equiv 1 \pmod{p}$ ó bien $a \equiv -1 \pmod{p}$.

$$[a]_p^{-1} = [a]_p \iff \left\{ \begin{array}{rcl} a & \equiv & 1 \pmod{p} \\ a & \equiv & -1 \pmod{p} \end{array} \right\}$$

Definición

*La **función de Euler** $\Phi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ se define como: $\Phi(n)$ es el número de enteros positivos no superiores a n que son coprimos con n .*

Ejemplo

n	1	2	3	4	5	6	7	8	9	10	11	12
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Teorema (Propiedades de Φ)

1. *Si p es primo, entonces $\Phi(p) = p - 1$.*
2. *Si p es primo, entonces $\Phi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$.*
3. *Si m y n son coprimos, entonces $\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$.*
4. *Si $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, entonces*
$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

Ejemplo

- $\Phi(13) = 13 - 1 = 12$
- $\Phi(91) = \Phi(13 \cdot 7) = \Phi(13) \cdot \Phi(7) = 12 \cdot 6 = 72$
- $\Phi(600) = \Phi(2^3 \cdot 3 \cdot 5^2) = 600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 160$

Teorema (Euler)

Sea $m \in \mathbb{Z}^+, m > 1$ y sea $a \in \mathbb{Z}$ tal que $mcd(a, m) = 1$.
Entonces $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Ejemplo Para $m = 14$, sabemos que $\Phi(14) = \Phi(7)\Phi(2) = 6$.
Si tomamos $a = 3$, el teorema anterior establece que $3^6 \equiv 1 \pmod{14}$, lo que comprobamos fácilmente:

$$3^6 = 3^3 \cdot 3^3 = 27 \cdot 27 \equiv (-1) \cdot (-1) \equiv 1 \pmod{14}$$

Ahora podemos hallar el resto de dividir 3^{50} entre 14.
Teniendo en cuenta que

$$50 = 6 \cdot 8 + 2$$

podemos expresar

$$3^{50} = (3^6)^8 \cdot 3^2$$

Luego

$$3^{50} = (3^6)^8 \cdot 3^2 \equiv 1 \cdot 9 \pmod{14}$$

Corolario (Fermat)

Si $a \in \mathbb{Z}^+$ *y* p *es primo tal que* $p \nmid a$, *entonces* $a^{p-1} \equiv 1 \pmod{p}$.

Ejemplo Halla el resto de la división de 29^{92} entre 11.

Solución: Tomamos $p = 11$ y $a = 29$. Ya que $11 \nmid 29$, el teorema de Fermat nos asegura que $29^{10} \equiv 1 \pmod{11}$.

Teniendo en cuenta que $92 = 10 \cdot 9 + 2$, podemos expresar

$$29^{92} = (29^{10})^9 \cdot 29^2$$

Luego

$$29^{92} = (29^{10})^9 \cdot 29^2 \equiv 1^9 \cdot 29^2 \pmod{11}$$

Ahora sólo queda determinar el resto de la división de 29^2 entre 11.

Ya que $29 \equiv 7 \pmod{11}$, se tiene que $29^2 \equiv 7^2 \pmod{11}$.

Por lo tanto,

$$29^{92} \equiv 5 \pmod{11}$$

Ejercicio Usa el teorema de Fermat para hallar el resto de dividir 795^{25} entre 11.

Ejercicios En los apartados siguientes, calcula el menor entero positivo x que verifique la relación:

$a)$ $4^{30} \equiv x \pmod{19}$ $\quad b)$ $3^{201} \equiv x \pmod{22}$

$c)$ $2^{11} \cdot 3^{13} \equiv x \pmod{7}$ $\quad d)$ $6^{592} \equiv x \pmod{11}$

El teorema de Euler también se usa para encontrar inversos (mód m).

Si a y m son coprimos, sabemos que

$$a \cdot a^{\Phi(m)-1} = a^{\Phi(m)} \equiv 1 \pmod{m}$$

Por lo tanto, $a^{\Phi(m)-1}$ es un inverso de a módulo m .

Ejemplo Aplicamos el teorema de Euler para $a = 2$ y $m = 9$

$$m.c.d.(2, 9) = 1, \quad \Phi(9) = 6$$

$$2^{\Phi(9)} \equiv 1 \pmod{9} \implies 2 \cdot 2^5 \equiv 1 \pmod{9}$$

$$\implies [2]_9^{-1} = [2^5]_9 = [32]_9 = [5]_9$$

- Como hemos estudiado anteriormente, podemos usar el inverso módulo m para resolver congruencias lineales.
- Para resolver $ax \equiv b \pmod{m}$, donde $mcd(a, m) = 1$, multiplicamos ambos lados de esta congruencia por $a^{\Phi(m)-1}$ para obtener

$$a^{\Phi(m)-1} \cdot ax \equiv a^{\Phi(m)-1} \cdot b \pmod{m}$$

- Por lo tanto, las soluciones son aquellos enteros x tales que

$$x \equiv a^{\Phi(m)-1} \cdot b \pmod{m}$$

Ejemplo $2x \equiv 8 \pmod 9$

$$x \equiv 2^{\Phi(9)-1} \cdot 8 \pmod 9$$

$$x \equiv 5 \cdot 8 \pmod 9$$

$$x \equiv 4 \pmod 9$$

Ejemplo $2x \equiv 7 \pmod{11}$

$$\Phi(11) = 10, \quad [2]_{11}^{-1} = 2^{\Phi(11)-1} = [2]_{11}^{9} = [6]_{11}$$

$$x \equiv 2^{\Phi(11)-1} \cdot 7 \pmod{11}$$

$$x \equiv 6 \cdot 7 \pmod{11}$$

$$x \equiv 9 \pmod{11}$$

Ejercicio Sea n un entero positivo cualquiera. Demuestra que:

1. si p es primo, entonces $n^p \equiv n \pmod p$.
2. el último dígito de n^5 coincide con el último dígito de n.
3. el entero $n^{13} - n$ es divisible por $2, 3, 5, 7$ y 13 .
4. la cifra de las unidades de n^4 es $0, 1, 5$ ó 6 .
5. si n es impar, la cifra de las unidades de n^4 es 1 ó 5 .

Ahora consideramos sistemas de congruencias con una sola variable, pero diferentes módulos.Tales sistemas surgieron en la antigua China para dar respuesta a preguntas como:

- ¿Cuál es el número que al dividirse entre 3 da por resto 1, al dividirse entre 5 da por resto 2 y al dividirse entre 7 da por resto 3?

Para determinar dicho número hemos de resolver el sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

Teorema (Teorema chino del resto)

Sean $m_1, m_2, \ldots, m_k$ *enteros positivos mayores que 1, coprimos dos a dos y* $b_1, b_2, \ldots, b_k$ *enteros cualesquiera. El sistema de congruencias*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

tiene solución única módulo $M = m_1 \cdot m_2 \cdots m_k$.

Demostración: Construimos la solución y así probamos su existencia.

- En primer lugar, planteamos los sistemas

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_2} \\ \vdots \\ x_1 \equiv 0 \pmod{m_k} \end{cases} \quad \begin{cases} x_2 \equiv 0 \pmod{m_1} \\ x_2 \equiv 1 \pmod{m_2} \\ \vdots \\ x_2 \equiv 0 \pmod{m_k} \end{cases} \quad \cdots \quad \begin{cases} x_k \equiv 0 \pmod{m_1} \\ x_k \equiv 0 \pmod{m_2} \\ \vdots \\ x_k \equiv 1 \pmod{m_k} \end{cases}$$

- Si resolvemos estos sistemas, encontraremos un x_i para cada $i : 1, 2, \ldots, k$
- Con las soluciones de estos sistemas formamos

$$x = b_1 \cdot x_1 + b_2 \cdot x_2 + \cdots + b_k \cdot x_k$$

- Entonces, $x \equiv b_i \pmod{m_i}$, para cada $i : 1, 2, \ldots, k$.
- Por lo tanto, x será solución del sistema de congruencias inicial.

Demostración: (cont.)

- Podemos resolver el sistema (1) considerando $M_1 = m_2 \cdot m_3 \cdots m_k = \dfrac{M}{m_1}$.
- Al ser los módulos coprimos dos a dos, M_1 y m_1 también son coprimos.
- Por lo que existen $s_1, t_1 \in \mathbb{Z}$ tales que $s_1 \cdot M_1 + t_1 \cdot m_1 = 1$.
- De aquí,

$$s_1 \cdot M_1 \equiv 0 \pmod{M_1} \quad \text{y} \quad s_1 \cdot M_1 \equiv 1 \pmod{m_1}$$

- Así, obtenemos un entero $x_1 = s_1 \cdot M_1$ tal que

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_2} \\ \vdots \\ x_1 \equiv 0 \pmod{m_k} \end{cases} \Longrightarrow \begin{cases} b_1 \cdot x_1 \equiv b_1 \pmod{m_1} \\ b_1 \cdot x_1 \equiv 0 \pmod{m_2} \\ \vdots \\ b_1 \cdot x_1 \equiv 0 \pmod{m_k} \end{cases}$$

Demostración: (cont.)

- Procediendo de manera análoga en el sistema (2), determinamos $s_2, t_2 \in \mathbb{Z}$ tales que

$$s_2 \cdot M_2 + t_2 \cdot m_2 = 1$$

- Y, así, obtenemos un entero $x_2 = s_2 \cdot M_2$ que verificará

$$\begin{cases} x_2 \equiv 0 \pmod{m_1} \\ x_2 \equiv 1 \pmod{m_2} \\ x_2 \equiv 0 \pmod{m_3} \\ \vdots \\ x_2 \equiv 0 \pmod{m_k} \end{cases} \Longrightarrow \begin{cases} b_2 \cdot x_2 \equiv 0 \pmod{m_1} \\ b_2 \cdot x_2 \equiv b_2 \pmod{m_2} \\ b_2 \cdot x_2 \equiv 0 \pmod{m_3} \\ \vdots \\ b_2 \cdot x_2 \equiv 0 \pmod{m_k} \end{cases}$$

Demostración: (cont.)

- Continuamos resolviendo todos los sistemas $(3), \ldots, (k)$ y obtenemos enteros x_3 , . . . , x_k tales que

$$\begin{cases} b_3 \cdot x_3 \equiv 0 \pmod{m_1} \\ b_3 \cdot x_3 \equiv 0 \pmod{m_2} \\ b_3 \cdot x_3 \equiv b_3 \pmod{m_3} \\ \vdots \\ b_3 \cdot x_3 \equiv 0 \pmod{m_k} \end{cases} \quad \cdots \quad \begin{cases} b_k \cdot x_k \equiv 0 \pmod{m_1} \\ b_k \cdot x_k \equiv 0 \pmod{m_2} \\ b_k \cdot x_k \equiv 0 \pmod{m_3} \\ \vdots \\ b_k \cdot x_k \equiv b_k \pmod{m_k} \end{cases}$$

- Con las soluciones de estos sistemas formamos

$$x = b_1 \cdot x_1 + b_2 \cdot x_2 + \cdots + b_k \cdot x_k$$

que es solución del sistema de congruencias inicial.

Demostración: (cont.)

- Ahora, supongamos que x' es otra solución, esto es, para cada $i : 1, 2, \ldots, k$

$$x' \equiv b_i \pmod{m_i}$$

- Entonces, para cada $i : 1, 2, \ldots, k$ se verifica

$$x - x' \equiv 0 \ (mod\ m_i)$$

- De donde, $x - x'$ es un múltiplo de cada m_i .
- Luego, $x - x'$ también será un múltiplo del mínimo común múltiplo de $m_1, m_2, \ldots, m_k$.
- Pero, ya que los módulos son coprimos dos a dos, su mcm es el producto

$$M = m_1 \cdot m_2 \cdots m_k$$

Ejemplo Resuelve el sistema de congruencias

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

Solución:

1. Comprobamos que los módulos son coprimos dos a dos

$$\text{mcd}(3,5) = 1 = \text{mcd}(3,7) = \text{mcd}(5,7)$$

2. Planteamos los sistemas auxiliares:

$$\left\{\begin{array}{rcll} x_1 & \equiv & 1 & (\text{mód } 3) \\ x_1 & \equiv & 0 & (\text{mód } 5) \\ x_1 & \equiv & 0 & (\text{mód } 7) \end{array}\right\} \quad \left\{\begin{array}{rcll} x_2 & \equiv & 0 & (\text{mód } 3) \\ x_2 & \equiv & 1 & (\text{mód } 5) \\ x_2 & \equiv & 0 & (\text{mód } 7) \end{array}\right\} \quad \left\{\begin{array}{rcll} x_3 & \equiv & 0 & (\text{mód } 3) \\ x_3 & \equiv & 0 & (\text{mód } 5) \\ x_3 & \equiv & 1 & (\text{mód } 7) \end{array}\right\}$$

(1) (2) (3)

Ejemplo Resuelve el sistema de congruencias

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

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(1)\left\{\begin{array}{rcll} x_1 & \equiv & 1 & (\text{mód } 3) \\ x_1 & \equiv & 0 & (\text{mód } 5) \\ x_1 & \equiv & 0 & (\text{mód } 7) \end{array}\right\} \qquad \begin{array}{c} M = 3 \cdot 5 \cdot 7 = 105, \\ m_1 = 3,\ M_1 = m_2 \cdot m_3 = 35 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$mcd(35, 3) = 1 = (-1) \cdot 35 + 12 \cdot 3 \implies (-1) \cdot 35 = 1 + (-12) \cdot 3$$

Por lo tanto, $x_1 = (-1) \cdot 35 = -35$ es una solución del sistema (1).

Ejemplo Resuelve el sistema de congruencias

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

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(2)\left\{\begin{array}{rcll} x_2 & \equiv & 0 & (\text{mód } 3) \\ x_2 & \equiv & 1 & (\text{mód } 5) \\ x_2 & \equiv & 0 & (\text{mód } 7) \end{array}\right\} \qquad \begin{array}{c} M = 3 \cdot 5 \cdot 7 = 105, \\ m_2 = 5,\ M_2 = m_1 \cdot m_3 = 21 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$mcd(21, 5) = 1 = 1 \cdot 21 + (-4) \cdot 5 \implies 1 \cdot 21 = 1 + 4 \cdot 5$$

Por lo tanto, $x_2 = 1 \cdot 21 = 21$ es una solución del sistema (2).

Ejemplo Resuelve el sistema de congruencias

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

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(3)\left\{\begin{array}{rcll} x_3 & \equiv & 0 & (\text{mód } 3) \\ x_3 & \equiv & 0 & (\text{mód } 5) \\ x_3 & \equiv & 1 & (\text{mód } 7) \end{array}\right\} \qquad \begin{array}{c} M = 3\cdot 5\cdot 7 = 105, \\ m_3 = 7,\ M_3 = m_1\cdot m_2 = 15 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$mcd(15,7) = 1 = 1\cdot 15 + (-2)\cdot 7 \implies 1\cdot 15 = 1 + 2\cdot 7$$

Por lo tanto, $x_3 = 1\cdot 15 = 15$ es una solución del sistema (3).

Ejemplo Resuelve el sistema de congruencias

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

Solución:

4. Con las soluciones de estos sistemas formamos

$$x = (-1)\cdot 35 + 2\cdot 21 + 3\cdot 15 = -35 + 42 + 45 = 52$$

La solución del sistema es:

$$\{x \in \mathbb{Z} \mid x = 52 + 105t,\ t \in \mathbb{Z}\} = [52]_{105}$$

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución:

1. Comprobamos que los módulos son coprimos dos a dos

$$\text{mcd}(11,8) = 1 = \text{mcd}(11,15) = \text{mcd}(8,15)$$

2. Planteamos los sistemas auxiliares:

$$\left\{\begin{array}{rcll} x_1 & \equiv & 1 & (\text{mód } 11) \\ x_1 & \equiv & 0 & (\text{mód } 8) \\ x_1 & \equiv & 0 & (\text{mód } 15) \end{array}\right\} \quad \left\{\begin{array}{rcll} x_2 & \equiv & 0 & (\text{mód } 11) \\ x_2 & \equiv & 1 & (\text{mód } 8) \\ x_2 & \equiv & 0 & (\text{mód } 15) \end{array}\right\} \quad \left\{\begin{array}{rcll} x_3 & \equiv & 0 & (\text{mód } 11) \\ x_3 & \equiv & 0 & (\text{mód } 8) \\ x_3 & \equiv & 1 & (\text{mód } 15) \end{array}\right\}$$

(1) (2) (3)

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(1)\left\{\begin{array}{rcll} x_1 & \equiv & 1 & (\text{mód } 11) \\ x_1 & \equiv & 0 & (\text{mód } 8) \\ x_1 & \equiv & 0 & (\text{mód } 15) \end{array}\right\} \qquad \begin{array}{c} M = 11\cdot 8\cdot 15 = 1320, \\ m_1 = 11,\ M_1 = m_2\cdot m_3 = 120 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$\text{mcd}(120,11) = 1 = (-1)\cdot 120 + 11\cdot 11 \implies (-1)\cdot 120 = 1 + (-11)\cdot 11$$

Por lo tanto, $x_1 = (-1)\cdot 120 = -120$ es una solución del sistema (1).

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(2)\left\{\begin{array}{rcll} x_2 & \equiv & 0 & (\text{mód } 11) \\ x_2 & \equiv & 1 & (\text{mód } 8) \\ x_2 & \equiv & 0 & (\text{mód } 15) \end{array}\right\} \qquad \begin{array}{c} M = 11 \cdot 8 \cdot 15 = 1320, \\ m_2 = 8,\ M_2 = m_1 \cdot m_3 = 165 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$\text{mcd}(165, 8) = 1 = (-3) \cdot 165 + 62 \cdot 8 \implies (-3) \cdot 165 = 1 + (-62) \cdot 8$$

Por lo tanto, $x_2 = (-3) \cdot 165 = -495$ es una solución del sistema (2).

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución:

3. Hallamos las soluciones de cada uno de estos sistemas auxiliares

$$(3)\left\{\begin{array}{rcll} x_3 & \equiv & 0 & (\text{mód } 11) \\ x_3 & \equiv & 0 & (\text{mód } 8) \\ x_3 & \equiv & 1 & (\text{mód } 15) \end{array}\right\} \qquad \begin{array}{c} M = 11 \cdot 8 \cdot 15 = 1320, \\ m_3 = 15,\ M_3 = m_1 \cdot m_2 = 88 \end{array}$$

Ya que los módulos son coprimos dos a dos,

$$\text{mcd}(88, 15) = 1 = 7 \cdot 88 + (-41) \cdot 15 \implies 7 \cdot 88 = 1 + 41 \cdot 15$$

Por lo tanto, $x_3 = 7 \cdot 88 = 616$ es una solución del sistema (3).

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución:

4. Con las soluciones de estos sistemas formamos

$$x = 3 \cdot (-120) + 6 \cdot (-495) + (-1) \cdot 616 = -3946$$

La solución del sistema es:

$$\{x \in \mathbb{Z} \mid x = -3946 + 1320t,\ t \in \mathbb{Z}\} = [-3946]_{1320} = [14]_{1320}$$

Podemos resolver los sistemas de congruencias de otra manera.

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{rcll} x & \equiv & 3 & (\text{mód } 11) \\ x & \equiv & 6 & (\text{mód } 8) \\ x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

Solución: Podemos escribir el sistema de la forma

$$\left\{\begin{array}{rrcll} i) & x & \equiv & 6 & (\text{mód } 8) \\ ii) & x & \equiv & 3 & (\text{mód } 11) \\ iii) & x & \equiv & -1 & (\text{mód } 15) \end{array}\right\}$$

y usamos las propiedades de las congruencias para resolverlo por sustitución.

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{llll} i) & x & \equiv & 6 \pmod 8 \\ ii) & x & \equiv & 3 \pmod{11} \\ iii) & x & \equiv & -1 \pmod{15} \end{array}\right\}$$

Solución:

- Partimos de la ecuación $i)$

  $i)\ x \equiv 6 \pmod 8 \iff \exists j \in \mathbb{Z} \mid x = 6 + 8j$

- Sustituimos esta expresión de x en la ecuación $ii)$

$$6 + 8j \equiv 3 \pmod{11}$$

y se resuelve la congruencia lineal que resulta

$$6+8j \equiv 3 \pmod{11} \implies 8j \equiv -3 \pmod{11}$$

$$\implies (-3)j \equiv (-3) \pmod{11}$$

$$\implies j \equiv 1 \pmod{11} \implies \exists t \in \mathbb{Z} \mid j = 1 + 11t$$

Solución:

- Se sustituye este valor de j en la expresión de x

$$x = 6 + 8j = 6 + 8(1 + 11t) = 14 + 88t$$

- Para que x verifique la ecuación $iii)$, se debe cumplir

$$14 + 88t \equiv -1 \pmod{15}$$

- Ahora resolvemos esta congruencia lineal

$$14 + 88t \equiv -1 \pmod{15} \implies 88t \equiv -15 \pmod{15}$$

$$\implies 88t \equiv 0 \pmod{15} \implies t \equiv 0 \pmod{15}$$

$$\implies \exists r \in \mathbb{Z} \mid t = 15r$$

Ejemplo Resuelve el sistema de congruencias

$$\left\{\begin{array}{llll} i) & x & \equiv & 6 \pmod 8 \\ ii) & x & \equiv & 3 \pmod{11} \\ iii) & x & \equiv & -1 \pmod{15} \end{array}\right\}$$

Solución:

- Por último, se sustituye este valor de t en la expresión de x

$$x = 6 + 8j = 6 + 8(1 + 11t) = 14 + 88t = 14 + 88(15r) = 14 + 1320r$$

- Por lo tanto, la solución del sistema es $[14]_{1320}$.

- El teorema chino del resto asegura la existencia de solución para un sistema de congruencias lineales con módulos **coprimos** dos a dos.
- Para los sistemas en los que los módulos **no** sean coprimos dos a dos necesitamos estudiar condiciones de existencia de soluciones.
- El siguiente resultado establece condiciones necesarias y suficientes para afirmar que un sistema de dos congruencias lineales tiene solución.
- Este resultado se puede generalizar para sistemas con más ecuaciones.

Teorema (Generalización del teorema chino del resto)

Sean m_1, m_2 *enteros estrictamente mayores que 1, sea* $d = \text{mcd}(m_1, m_2)$ *y* $M = \text{mcm}(m_1, m_2)$. *Entonces, el sistema*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}$$

tiene solución si y sólo si $b_1 \equiv b_2 \pmod{d}$. *En tal caso, la solución es única módulo* $M = \text{mcm}(m_1, m_2)$.

Demostración:

➢ Si $x = b_1 + k_1 m_1$ y $x = b_2 + k_2 m_2$, entonces

$$b_1 - b_2 = k_2 m_2 - k_1 m_1$$

➢ Por tanto, $d = \text{mcd}(m_1, m_2)$ divide a $b_1 - b_2$.

Ejemplo Resuelve (si es posible) el sistema de congruencias:

$$\left\{ \begin{array}{rcrl} x & \equiv & 1 & (\text{mód } 4) \\ x & \equiv & 5 & (\text{mód } 12) \\ x & \equiv & -3 & (\text{mód } 16) \end{array} \right\}$$

Solución:

1. En primer lugar, se usa el teorema para determinar si existe solución. Ya que,
   - $\text{mcd}(4, 12) = 4$ es divisor de $1 - 5 = -4$
   - $\text{mcd}(4, 16) = 4$ es divisor de $1 - (-3) = 4$
   - $\text{mcd}(12, 16) = 4$ es divisor de $5 - (-3) = 8$

   podemos asegurar que existe solución módulo $\text{mcm}(4, 12, 16) = 48$
2. Hallamos la solución usando sustitución.

Ejemplo Resuelve (si es posible) el sistema de congruencias:

$$\left\{ \begin{array}{rcrl} i) \ x & \equiv & 1 & (\text{mód } 4) \\ ii) \ x & \equiv & 5 & (\text{mód } 12) \\ iii) \ x & \equiv & -3 & (\text{mód } 16) \end{array} \right\}$$

Solución:

- Para hallar la solución, partimos de la ecuación $i)$

  $i) \ x \equiv 1 \pmod{4} \iff \exists j \in \mathbb{Z} \mid x = 1 + 4j$
- Sustituimos esta expresión de x en la ecuación $ii)$

  $$1 + 4j \equiv 5 \pmod{12}$$

  y se resuelve esta congruencia lineal

  $$1 + 4j \equiv 5 \pmod{12} \implies 4j \equiv 4 \pmod{12}$$

  $$\implies j \equiv 1 \pmod{3}$$

  $$\implies \exists t \in \mathbb{Z} \mid j = 1 + 3t$$

Solución:

- Se sustituye este valor de j en la expresión de x

  $$x = 1 + 4j = 1 + 4(1 + 3t) = 5 + 12t$$
- Para que x verifique la ecuación $iii)$, se debe cumplir

  $$5 + 12t \equiv -3 \pmod{16}$$
- Ahora resolvemos esta congruencia lineal

  $$5 + 12t \equiv -3 \pmod{16} \implies 12t \equiv -8 \pmod{16}$$

  $$\implies 12t \equiv 24 \pmod{16} \implies 3t \equiv 6 \pmod{4}$$

  $$\implies t \equiv 2 \pmod{4} \implies \exists r \in \mathbb{Z} \mid t = 2 + 4r$$

Ejemplo Resuelve (si es posible) el sistema de congruencias

$$\left\{\begin{array}{rrcrl} i) & x & \equiv & 1 & (\text{mód } 4) \\ ii) & x & \equiv & 5 & (\text{mód } 12) \\ iii) & x & \equiv & -3 & (\text{mód } 16) \end{array}\right\}$$

Solución:

- Por último, se sustituye este valor de t en la expresión de x

$$x = 1 + 4j = 1 + 4(1 + 3t) = 5 + 12t = 5 + 12(2 + 4r) = 29 + 48r$$

- Por lo tanto, la solución del sistema es $[29]_{48}$.

Ejercicio Resuelve (cuando sea posible) los sistemas:

$$a) \left\{\begin{array}{l} x \equiv 5 \ (\text{mód } 6) \\ x \equiv 3 \ (\text{mód } 10) \\ x \equiv 8 \ (\text{mód } 15) \end{array}\right. \qquad b) \left\{\begin{array}{l} x \equiv 2 \ (\text{mód } 14) \\ x \equiv 10 \ (\text{mód } 30) \\ x \equiv 6 \ (\text{mód } 21) \end{array}\right.$$

$$c) \left\{\begin{array}{ll} 3x + 9 \equiv 8x + 12 & (\text{mód } 16) \\ x \equiv 11^{954} & (\text{mód } 20) \end{array}\right.$$