

Sistemas de congruencias

Cuando los módulos no son primos relativos

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

¿Qué estamos buscando?

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$\text{mcd}(8, 12) = 4$: no son primos relativos.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$x \equiv 3 \bmod 8$: 3 11 19 27 35 43 51 59 67 75 83 91

Los candidatos entre 0 y 95.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$x \equiv 3 \pmod{8}$: 3 11 19 27 35 43 51 59 67 75 83 91

Los candidatos entre 0 y 95.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$



4 soluciones entre 0 y 95, cada 24.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

4 soluciones entre 0 y 95, cada 24.

1. La primera congruencia, como igualdad

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$x \equiv a \bmod m$ significa $x = a + m k$ para algún entero k .

2. Sustituir en la segunda congruencia

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

Donde dice x , va $a + m k$.

2. Sustituir en la segunda congruencia

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

Una sola incógnita: k .

3. Despejar k

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

Una sola incógnita: k .

3. Despejar k

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$\text{mcd}(8, 12) = 4$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

8 no tiene inverso módulo 12: $\text{mcd}(8, 12) = 4$.

3. Despejar k

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

$$\text{mcd}(8, 12) = 4$$

$$12 \mid 8k - 4$$

$$\iff 3 \mid 2k - 1$$

8 no tiene inverso módulo 12: $\text{mcd}(8, 12) = 4$.

3. Despejar k

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 7 \bmod 12 \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

$$2k \equiv 1 \bmod 3 \quad \div 4$$

$$\text{mcd}(8, 12) = 4$$

$$12 \mid 8k - 4$$

$$\iff 3 \mid 2k - 1$$

Se divide todo entre 4: el coeficiente, el lado derecho y el módulo.

3. Despejar k

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \pmod{12}$$

$$8k \equiv 7 - 3 \equiv 4 \pmod{12}$$

$$2k \equiv 1 \pmod{3} \quad \div 4$$

$$\text{mcd}(8, 12) = 4$$

$$12 \mid 8k - 4$$

$$\iff 3 \mid 2k - 1$$

$$4 \mid 4 \quad \checkmark$$

Se divide todo entre 4: el coeficiente, el lado derecho y el módulo.

3. Despejar k

$$2^{-1} \bmod 3$$

Se divide todo entre 4: el coeficiente, el lado derecho y el módulo.

3. Despejar k

$$2^{-1} \bmod 3$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

Euclides: $\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$.

3. Despejar k

$$2^{-1} \bmod 3$$

$$3 = 2 \times 1 + 1$$

$$1 = 3 - 2 \times 1$$

$$2 = 1 \times 2 + 0$$

De cada división despejamos el residuo.

3. Despejar k

$$2^{-1} \bmod 3$$

Despejes

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

Se empieza por el despeje del 1.

3. Despejar k

$$2^{-1} \bmod 3$$

Despejes

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$2 \times (-1) \equiv 1 \bmod 3$$

$$2^{-1} \bmod 3 = -1 \bmod 3 = \boxed{2}$$

Módulo 3, el 3 vale 0.

3. Despejar k

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$$x = 3 + 8k$$

$$2^{-1} \pmod{3} = -1 \pmod{3} = 2$$

$$3 + 8k \equiv 7 \pmod{12}$$

$$8k \equiv 7 - 3 \equiv 4 \pmod{12}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

Por el inverso: $2 \times 2 \equiv 1$, así que queda k solo.

4. Volver a x

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \pmod{12}$$

$$8k \equiv 7 - 3 \equiv 4 \pmod{12}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$k \equiv 2 \pmod{3}$ significa $k = 2 + 3j$ para algún entero j .

4. Volver a x

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \pmod{12}$$

$$8k \equiv 7 - 3 \equiv 4 \pmod{12}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$$x = 3 + 8(2 + 3j) = 19 + 24j$$

$k \equiv 2 \pmod{3}$ significa $k = 2 + 3j$ para algún entero j .

4. Volver a x

$$x \equiv 19 \bmod 24$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

$$2k \equiv 1 \bmod 3$$

$$k \equiv 2 \times 1 \equiv 2 \bmod 3$$

$$k = 2 + 3j$$

$$x = 3 + 8(2 + 3j) = 19 + 24j$$

Las dos congruencias quedan en una sola: $x \equiv 19 \bmod 24$.

4. Volver a x

$$x \equiv 19 \bmod 24$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \bmod 12$$

$$8k \equiv 7 - 3 \equiv 4 \bmod 12$$

$$2k \equiv 1 \bmod 3$$

$$k \equiv 2 \times 1 \equiv 2 \bmod 3$$

$$k = 2 + 3j$$

$$x = 3 + 8(2 + 3j) = 19 + 24j$$

La solución es única módulo $\text{mcm}(8, 12) = 24$, no módulo 96.

4. Volver a x

$$x \equiv 19 \pmod{24}$$

$$x = 19$$

$$x = 3 + 8k$$

$$3 + 8k \equiv 7 \pmod{12}$$

$$8k \equiv 7 - 3 \equiv 4 \pmod{12}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$$x = 3 + 8(2 + 3j) = 19 + 24j$$

La solución es única módulo $\text{mcm}(8, 12) = 24$, no módulo 96.

5. Comprobación

$$x \equiv 19 \bmod 24$$

$$x = 19$$

$$19 = 8 \times 2 + 3 \checkmark$$

$$19 = 12 \times 1 + 7 \checkmark$$

Comprobamos cada congruencia del sistema.

Ejemplo 2: sin solución

El sistema

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$\text{mcd}(10, 15) = 5.$$

Por sustitución

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x = 4 + 10k$$

$$\text{mcd}(10, 15) = 5.$$

Por sustitución

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x = 4 + 10k$$

$$4 + 10k \equiv 7 \bmod 15$$

$$\text{mcd}(10, 15) = 5.$$

Por sustitución

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x = 4 + 10k$$

$$4 + 10k \equiv 7 \bmod 15$$

$$10k \equiv 7 - 4 \equiv 3 \bmod 15$$

$$\text{mcd}(10, 15) = 5.$$

Por sustitución

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x = 4 + 10k$$

$$4 + 10k \equiv 7 \bmod 15$$

$$10k \equiv 7 - 4 \equiv 3 \bmod 15$$

$$\text{mcd}(10, 15) = 5$$

$$5 \nmid 3 \quad \times$$

10 no tiene inverso módulo 15.

Por sustitución

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x = 4 + 10k$$

$$4 + 10k \equiv 7 \bmod 15$$

$$10k \equiv 7 - 4 \equiv 3 \bmod 15$$

$$\text{mcd}(10, 15) = 5$$

$$5 \nmid 3 \quad \times$$

No hay solución.

¿Por qué no hay solución?

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x \equiv 4 \bmod 10$$

4 14 24 34 44 54 64 74 84

$$x \equiv 7 \bmod 15$$

7 22 37 52 67 82

Las dos listas nunca coinciden.

¿Por qué no hay solución?

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x \equiv 4 \bmod 10 \quad \quad \quad 4 \quad 14 \quad 24 \quad 34 \quad 44 \quad 54 \quad 64 \quad 74 \quad 84$$

$$x \equiv 7 \bmod 15 \quad \quad \quad 7 \quad \quad 22 \quad \quad 37 \quad \quad 52 \quad \quad 67 \quad \quad 82$$

$$x \equiv 4 \bmod 10 \implies x \equiv 4 \bmod 5$$

Los dos módulos son múltiplos de 5.

¿Por qué no hay solución?

$$\begin{cases} x \equiv 4 \bmod 10 \\ x \equiv 7 \bmod 15 \end{cases}$$

$$x \equiv 4 \bmod 10 \quad 4 \quad 14 \quad 24 \quad 34 \quad 44 \quad 54 \quad 64 \quad 74 \quad 84$$

$$x \equiv 7 \bmod 15 \quad 7 \quad 22 \quad 37 \quad 52 \quad 67 \quad 82$$

$$x \equiv 4 \bmod 10 \implies x \equiv 4 \bmod 5$$

$$x \equiv 7 \bmod 15 \implies x \equiv 2 \bmod 5$$

$$4 \not\equiv 2 \bmod 5$$

Las dos congruencias se contradicen módulo 5.

¿Cuándo hay solución?

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases} \text{ tiene solución} \iff \text{mcd}(m, n) \mid b - a$$

¿Cuándo hay solución?

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases} \text{ tiene solución} \iff \text{mcd}(m, n) \mid b - a$$

$$\text{mcd}(8, 12) = 4 \mid 7 - 3 = 4 \checkmark$$

$$\text{mcd}(10, 15) = 5 \nmid 7 - 4 = 3 \times$$

¿Cuándo hay solución?

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases} \text{ tiene solución} \iff \text{mcd}(m, n) \mid b - a$$

$$\text{mcd}(8, 12) = 4 \mid 7 - 3 = 4 \checkmark$$

$$\text{mcd}(10, 15) = 5 \nmid 7 - 4 = 3 \times$$

Si la tiene, es única módulo $\text{mcm}(m, n)$

Con módulos primos relativos, el mínimo común múltiplo es el producto.

Ejemplo 3: tres congruencias

El sistema

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 3 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

Se juntan de dos en dos.

Las dos primeras

$$\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 1 + 6k$$

Se juntan de dos en dos.

Las dos primeras

$$\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \bmod 8$$

Se juntan de dos en dos.

Las dos primeras

$$\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \bmod 8$$

$$6k \equiv 3 - 1 \equiv 2 \bmod 8$$

Se juntan de dos en dos.

Las dos primeras

$$\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \bmod 8$$

$$6k \equiv 3 - 1 \equiv 2 \bmod 8$$

$$3k \equiv 1 \bmod 4 \quad \div 2$$

$$\text{mcd}(6, 8) = 2$$

$$2 \mid 2 \quad \checkmark$$

Se juntan de dos en dos.

Las dos primeras

$$3^{-1} \bmod 4$$

Se juntan de dos en dos.

Las dos primeras

$$3^{-1} \bmod 4$$

$$4 = 3 \times 1 + 1$$

$$3 = 1 \times 3 + 0$$

Euclides: $\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$.

Las dos primeras

$$3^{-1} \bmod 4$$

$$4 = 3 \times 1 + 1$$

$$1 = 4 - 3 \times 1$$

$$3 = 1 \times 3 + 0$$

De cada división despejamos el residuo.

Las dos primeras

$$3^{-1} \bmod 4$$

Despejes

$$1 = 4 - 3 \times 1$$

Sustitución hacia atrás

$$1 = 4 - 3 \times 1$$

Se empieza por el despeje del 1.

Las dos primeras

$$3^{-1} \bmod 4$$

Despejes

$$1 = 4 - 3 \times 1$$

Sustitución hacia atrás

$$1 = 4 - 3 \times 1$$

$$3 \times (-1) \equiv 1 \bmod 4$$

$$3^{-1} \bmod 4 = -1 \bmod 4 = \boxed{3}$$

Módulo 4, el 4 vale 0.

Las dos primeras

$$\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$3^{-1} \bmod 4 = -1 \bmod 4 = 3$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \bmod 8$$

$$6k \equiv 3 - 1 \equiv 2 \bmod 8$$

$$3k \equiv 1 \bmod 4$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 4$$

Módulo 4, el 4 vale 0.

Las dos primeras

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 3 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \pmod{8}$$

$$6k \equiv 3 - 1 \equiv 2 \pmod{8}$$

$$3k \equiv 1 \pmod{4}$$

$$k \equiv 3 \times 1 \equiv 3 \pmod{4}$$

$$k = 3 + 4j$$

$$x = 1 + 6(3 + 4j) = 19 + 24j$$

Módulo 4, el 4 vale 0.

Las dos primeras

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 1 + 6k$$

$$1 + 6k \equiv 3 \bmod 8$$

$$6k \equiv 3 - 1 \equiv 2 \bmod 8$$

$$3k \equiv 1 \bmod 4$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 4$$

$$k = 3 + 4j$$

$$x = 1 + 6(3 + 4j) = 19 + 24j$$

Las dos congruencias quedan en una sola: $x \equiv 19 \bmod 24$.

Con la tercera

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 19 + 24k$$

Las dos congruencias quedan en una sola: $x \equiv 19 \bmod 24$.

Con la tercera

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \bmod 9$$

Las dos congruencias quedan en una sola: $x \equiv 19 \bmod 24$.

Con la tercera

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \bmod 9$$

$$24k \equiv 4 - 19 \equiv -15 \bmod 9$$

Las dos congruencias quedan en una sola: $x \equiv 19 \bmod 24$.

Con la tercera

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \bmod 9$$

$$24k \equiv 4 - 19 \equiv -15 \bmod 9$$

$$6k \equiv 3 \bmod 9$$

Reducimos módulo 9: $24 \equiv 6$ y $-15 \equiv 3$.

Con la tercera

$$\begin{cases} x \equiv 19 \pmod{24} \\ x \equiv 4 \pmod{9} \end{cases}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \pmod{9}$$

$$24k \equiv 4 - 19 \equiv -15 \pmod{9}$$

$$6k \equiv 3 \pmod{9}$$

$$2k \equiv 1 \pmod{3} \quad \div 3$$

$$\text{mcd}(6, 9) = 3$$

$$3 \mid 3 \quad \checkmark$$

Reducimos módulo 9: $24 \equiv 6$ y $-15 \equiv 3$.

Con la tercera

$$2^{-1} \bmod 3$$

Reducimos módulo 9: $24 \equiv 6$ y $-15 \equiv 3$.

Con la tercera

$$2^{-1} \bmod 3$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

Euclides: $\text{dividendo} = \text{divisor} \times \text{cociente} + \text{residuo}$.

Con la tercera

$$2^{-1} \bmod 3$$

$$3 = 2 \times 1 + 1$$

$$1 = 3 - 2 \times 1$$

$$2 = 1 \times 2 + 0$$

De cada división despejamos el residuo.

Con la tercera

$$2^{-1} \bmod 3$$

Despejes

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

Se empieza por el despeje del 1.

Con la tercera

$$2^{-1} \bmod 3$$

Despejes

$$1 = 3 - 2 \times 1$$

Sustitución hacia atrás

$$1 = 3 - 2 \times 1$$

$$2 \times (-1) \equiv 1 \bmod 3$$

$$2^{-1} \bmod 3 = -1 \bmod 3 = \boxed{2}$$

Módulo 3, el 3 vale 0.

Con la tercera

$$\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 4 \bmod 9 \end{cases}$$

$$x = 19 + 24k$$

$$2^{-1} \bmod 3 = -1 \bmod 3 = 2$$

$$19 + 24k \equiv 4 \bmod 9$$

$$24k \equiv 4 - 19 \equiv -15 \bmod 9$$

$$6k \equiv 3 \bmod 9$$

$$2k \equiv 1 \bmod 3$$

$$k \equiv 2 \times 1 \equiv 2 \bmod 3$$

Módulo 3, el 3 vale 0.

Con la tercera

$$\begin{cases} x \equiv 19 \pmod{24} \\ x \equiv 4 \pmod{9} \end{cases}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \pmod{9}$$

$$24k \equiv 4 - 19 \equiv -15 \pmod{9}$$

$$6k \equiv 3 \pmod{9}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$$x = 19 + 24(2 + 3j) = 67 + 72j$$

Módulo 3, el 3 vale 0.

Con la tercera

$$x \equiv 67 \bmod 72$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \bmod 9$$

$$24k \equiv 4 - 19 \equiv -15 \bmod 9$$

$$6k \equiv 3 \bmod 9$$

$$2k \equiv 1 \bmod 3$$

$$k \equiv 2 \times 1 \equiv 2 \bmod 3$$

$$k = 2 + 3j$$

$$x = 19 + 24(2 + 3j) = 67 + 72j$$

Las dos congruencias quedan en una sola: $x \equiv 67 \bmod 72$.

Con la tercera

$$x \equiv 67 \pmod{72}$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \pmod{9}$$

$$24k \equiv 4 - 19 \equiv -15 \pmod{9}$$

$$6k \equiv 3 \pmod{9}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$$x = 19 + 24(2 + 3j) = 67 + 72j$$

$$\text{mcm}(6, 8, 9) = 72.$$

Con la tercera

$$x \equiv 67 \pmod{72}$$

$$x = 67$$

$$x = 19 + 24k$$

$$19 + 24k \equiv 4 \pmod{9}$$

$$24k \equiv 4 - 19 \equiv -15 \pmod{9}$$

$$6k \equiv 3 \pmod{9}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \times 1 \equiv 2 \pmod{3}$$

$$k = 2 + 3j$$

$$x = 19 + 24(2 + 3j) = 67 + 72j$$

$$\text{mcm}(6, 8, 9) = 72.$$

Comprobación

$$x \equiv 67 \bmod 72$$

$$x = 67$$

$$67 = 6 \times 11 + 1 \checkmark$$

$$67 = 8 \times 8 + 3 \checkmark$$

$$67 = 9 \times 7 + 4 \checkmark$$

Comprobamos cada congruencia del sistema.

En resumen

En resumen

1. Al despejar $m k \equiv b - a \pmod n$, se calcula $d = \text{mcd}(m, n)$.

En resumen

1. Al despejar $m k \equiv b - a \pmod n$, se calcula $d = \text{mcd}(m, n)$.
2. Si d no divide a $b - a$: no hay solución.

En resumen

1. Al despejar $m k \equiv b - a \pmod n$, se calcula $d = \text{mcd}(m, n)$.
2. Si d no divide a $b - a$: no hay solución.
3. Si lo divide: se divide todo entre d y se sigue igual.

En resumen

1. Al despejar $m k \equiv b - a \pmod n$, se calcula $d = \text{mcd}(m, n)$.
2. Si d no divide a $b - a$: no hay solución.
3. Si lo divide: se divide todo entre d y se sigue igual.
4. La solución es única módulo $\text{mcm}(m, n)$, no módulo $m n$.