

Sistemas de congruencias

Por sustitución

Daniel Felipe Triviño

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

El sistema

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

El sistema

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

Con la receta del teorema: $x = 17$.

1. La primera congruencia, como igualdad

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

$$x = 2 + 5k$$

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

2. Sustituir en la segunda congruencia

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

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

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

2. Sustituir en la segunda congruencia

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

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

Una sola incógnita: k .

3. Despejar k

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

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

$$5k \equiv 3 - 2 \equiv 1 \bmod 7$$

Una sola incógnita: k .

3. Despejar k

$$5^{-1} \bmod 7$$

5 y 7 son primos relativos: 5 tiene inverso módulo 7.

3. Despejar k

$$5^{-1} \bmod 7$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

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

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

3. Despejar k

$$5^{-1} \bmod 7$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

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

$$2 = 7 - 5 \times 1$$

$$1 = 5 - 2 \times 2$$

De cada división despejamos el residuo.

3. Despejar k

$$5^{-1} \bmod 7$$

Despejes

$$2 = 7 - 5 \times 1$$

$$1 = 5 - 2 \times 2$$

Sustitución hacia atrás

$$1 = 5 - 2 \times 2$$

$$1 = 5 - (7 - 5 \times 1) \times 2$$

$$1 = 5 \times 3 - 7 \times 2$$

Se empieza por el despeje del 1.

3. Despejar k

$$5^{-1} \bmod 7$$

Despejes

$$2 = 7 - 5 \times 1$$

$$1 = 5 - 2 \times 2$$

Sustitución hacia atrás

$$1 = 5 - 2 \times 2$$

$$1 = 5 - (7 - 5 \times 1) \times 2$$

$$1 = 5 \times 3 - 7 \times 2$$

$$5 \times 3 \equiv 1 \bmod 7$$

$$5^{-1} \bmod 7 = \boxed{3}$$

Módulo 7, el 7 vale 0.

3. Despejar k

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

$$x = 2 + 5k$$

$$5^{-1} \bmod 7 = 3$$

$$2 + 5k \equiv 3 \bmod 7$$

$$5k \equiv 3 - 2 \equiv 1 \bmod 7$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 7$$

Por el inverso: $3 \times 5 \equiv 1$, así que queda k solo.

4. Volver a x

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

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

$$5k \equiv 3 - 2 \equiv 1 \bmod 7$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 7$$

$$k = 3 + 7j$$

$k \equiv 3 \bmod 7$ significa $k = 3 + 7j$ para algún entero j .

4. Volver a x

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

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

$$5k \equiv 3 - 2 \equiv 1 \bmod 7$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 7$$

$$k = 3 + 7j$$

$$x = 2 + 5(3 + 7j) = 17 + 35j$$

$k \equiv 3 \bmod 7$ significa $k = 3 + 7j$ para algún entero j .

4. Volver a x

$$x \equiv 17 \bmod 35$$

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \bmod 7$$

$$5k \equiv 3 - 2 \equiv 1 \bmod 7$$

$$k \equiv 3 \times 1 \equiv 3 \bmod 7$$

$$k = 3 + 7j$$

$$x = 2 + 5(3 + 7j) = 17 + 35j$$

Las dos congruencias quedan en una sola: $x \equiv 17 \bmod 35$.

4. Volver a x

$$x \equiv 17 \pmod{35}$$

$$x = 17$$

$$x = 2 + 5k$$

$$2 + 5k \equiv 3 \pmod{7}$$

$$5k \equiv 3 - 2 \equiv 1 \pmod{7}$$

$$k \equiv 3 \times 1 \equiv 3 \pmod{7}$$

$$k = 3 + 7j$$

$$x = 2 + 5(3 + 7j) = 17 + 35j$$

Las dos congruencias quedan en una sola: $x \equiv 17 \pmod{35}$.

5. Comprobación

$$x \equiv 17 \bmod 35$$

$$x = 17$$

$$17 = 5 \times 3 + 2 \quad \checkmark$$

$$17 = 7 \times 2 + 3 \quad \checkmark$$

Comprobamos cada congruencia del sistema.

Ejemplo 2: tres congruencias

El sistema

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$$

El sistema

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases} \longrightarrow x \equiv 17 \pmod{35}$$

El sistema

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

Se juntan las congruencias de dos en dos.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

Se juntan las congruencias de dos en dos.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \bmod 11$$

Se juntan las congruencias de dos en dos.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \bmod 11$$

$$35k \equiv 10 - 17 \equiv -7 \bmod 11$$

Se juntan las congruencias de dos en dos.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \bmod 11$$

$$35k \equiv 10 - 17 \equiv -7 \bmod 11$$

$$2k \equiv 4 \bmod 11$$

Reducimos módulo 11: $35 \equiv 2$ y $-7 \equiv 4$.

Juntar con la tercera congruencia

$$2^{-1} \bmod 11$$

Reducimos módulo 11: $35 \equiv 2$ y $-7 \equiv 4$.

Juntar con la tercera congruencia

$$2^{-1} \bmod 11$$

$$11 = 2 \times 5 + 1$$

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

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

Juntar con la tercera congruencia

$$2^{-1} \bmod 11$$

$$11 = 2 \times 5 + 1$$

$$1 = 11 - 2 \times 5$$

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

De cada división despejamos el residuo.

Juntar con la tercera congruencia

$$2^{-1} \bmod 11$$

Despejes

$$1 = 11 - 2 \times 5$$

Sustitución hacia atrás

$$1 = 11 - 2 \times 5$$

Se empieza por el despeje del 1.

Juntar con la tercera congruencia

$$2^{-1} \bmod 11$$

Despejes

$$1 = 11 - 2 \times 5$$

Sustitución hacia atrás

$$1 = 11 - 2 \times 5$$

$$2 \times (-5) \equiv 1 \bmod 11$$

$$2^{-1} \bmod 11 = -5 \bmod 11 = \boxed{6}$$

Módulo 11, el 11 vale 0.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

$$2^{-1} \bmod 11 = -5 \bmod 11 = 6$$

$$17 + 35k \equiv 10 \bmod 11$$

$$35k \equiv 10 - 17 \equiv -7 \bmod 11$$

$$2k \equiv 4 \bmod 11$$

$$k \equiv 6 \times 4 \equiv 2 \bmod 11$$

Módulo 11, el 11 vale 0.

Juntar con la tercera congruencia

$$\begin{cases} x \equiv 17 \bmod 35 \\ x \equiv 10 \bmod 11 \end{cases}$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \bmod 11$$

$$35k \equiv 10 - 17 \equiv -7 \bmod 11$$

$$2k \equiv 4 \bmod 11$$

$$k \equiv 6 \times 4 \equiv 2 \bmod 11$$

$$k = 2 + 11j$$

$$x = 17 + 35(2 + 11j) = 87 + 385j$$

Módulo 11, el 11 vale 0.

Juntar con la tercera congruencia

$$x \equiv 87 \bmod 385$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \bmod 11$$

$$35k \equiv 10 - 17 \equiv -7 \bmod 11$$

$$2k \equiv 4 \bmod 11$$

$$k \equiv 6 \times 4 \equiv 2 \bmod 11$$

$$k = 2 + 11j$$

$$x = 17 + 35(2 + 11j) = 87 + 385j$$

Las dos congruencias quedan en una sola: $x \equiv 87 \bmod 385$.

Juntar con la tercera congruencia

$$x \equiv 87 \pmod{385}$$

$$x = 87$$

$$x = 17 + 35k$$

$$17 + 35k \equiv 10 \pmod{11}$$

$$35k \equiv 10 - 17 \equiv -7 \pmod{11}$$

$$2k \equiv 4 \pmod{11}$$

$$k \equiv 6 \times 4 \equiv 2 \pmod{11}$$

$$k = 2 + 11j$$

$$x = 17 + 35(2 + 11j) = 87 + 385j$$

Las dos congruencias quedan en una sola: $x \equiv 87 \pmod{385}$.

Comprobación

$$x \equiv 87 \pmod{385}$$

$$x = 87$$

$$87 = 5 \times 17 + 2 \quad \checkmark$$

$$87 = 7 \times 12 + 3 \quad \checkmark$$

$$87 = 11 \times 7 + 10 \quad \checkmark$$

Comprobamos cada congruencia del sistema.

Por sustitución

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.
2. Se sustituye en la siguiente congruencia y se despeja $m k$.

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.
2. Se sustituye en la siguiente congruencia y se despeja $m k$.
3. Se reduce y se multiplica por el inverso de m : queda k solo.

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.
2. Se sustituye en la siguiente congruencia y se despeja $m k$.
3. Se reduce y se multiplica por el inverso de m : queda k solo.
4. k también se escribe como igualdad y se sustituye: $x \equiv x_0 \pmod{m n}$.

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.
2. Se sustituye en la siguiente congruencia y se despeja $m k$.
3. Se reduce y se multiplica por el inverso de m : queda k solo.
4. k también se escribe como igualdad y se sustituye: $x \equiv x_0 \pmod{m n}$.
5. Si hay más congruencias, se repite con la siguiente.

Por sustitución

1. $x \equiv a \pmod{m}$ se escribe $x = a + m k$.
2. Se sustituye en la siguiente congruencia y se despeja $m k$.
3. Se reduce y se multiplica por el inverso de m : queda k solo.
4. k también se escribe como igualdad y se sustituye: $x \equiv x_0 \pmod{m n}$.
5. Si hay más congruencias, se repite con la siguiente.

Los dos métodos necesitan módulos primos relativos entre sí.