Resolución de ecuaciones modulares usando el Método de Blankinship

Identidad de Bezout Si a y n son números enteros no nulos ambos entonces $\exists\, u, v \in \mathbb{Z}$ tales que $mcd(a,n) = a \cdot u + n \cdot v$

Por tanto:

$$mcd(a,n) = 1 \;\Leftrightarrow\; \exists\, u, v \in \mathbb{Z} \text{ tales que } au + nv = 1$$

Por otro lado, sabemos que

$$ax \equiv b \pmod{n} \text{ tiene solución en } x \Leftrightarrow mcd(a,n) | b$$

- Si $mcd(a,n) = 1$ la solución es única y además, si encontramos u y v tales que $au + nv = 1$ entonces u es una solución particular de la ecuación $ax \equiv 1 \pmod{n}$.
- Si $mcd(a,n) = d > 1$ y $d|b$ su solución es cualquier $x \equiv x_0 + \dfrac{t \cdot n}{d} \pmod{n}$, $t = 0, 1, \ldots, d-1$ donde x_0 es una solución particular en la ecuación equivalente a la primera $a/d \equiv b/d \pmod{n/d}$

Dados dos números a y n queremos expresar a su máximo común divisor como una combinación lineal de ellos $au + nv = mcd(a,b)$.

Método de Blankinship

Para ello consideraremos el sistema compatible y determinado de ecuaciones

$$\begin{cases} 1 \cdot x + 0 \cdot y &= a \\ 0 \cdot x + 1 \cdot y &= n \end{cases}$$

cuya única solución es $x = a$ e $y = n$.

Además, usaremos el **algoritmo de Euclides**

$$\begin{array}{r|l} D & d \\ r & c \end{array} \qquad \Rightarrow D = d \cdot c + r \Rightarrow r = D - d \cdot c$$

A partir de la expresión anterior en la que obtenemos el resto como una combinación lineal del dividendo y el divisor, usaremos operaciones elementales por fila para obtener sistemas equivalentes, en su forma matricial, en los que los restos r_i estén en la última columna.

Finalizamos el proceso cuando llegamos a una matriz con un cero en la última columna.

$$\begin{cases} u \cdot x + v \cdot y &= mcd(a,n) \\ -n \cdot x + a \cdot y &= 0 \end{cases}$$

En ese caso tendremos en la fila correspondiente el mcd y los coeficientes u y v de la combinación lineal

Resuelve la ecuación modular: $1323x \equiv 1 \pmod{85085}$

Partimos del sistema $\begin{cases} 1 \cdot x + 0 \cdot y &= 1323 \\ 0 \cdot x + 1 \cdot y &= 85085 \end{cases}$ que tiene como soluciones $x = 1323$ e $y = 85085$. Su forma matricial es:

Paso 0

$$\begin{pmatrix} 1 & 0 & 1323 \\ 0 & 1 & 85085 \end{pmatrix}$$

$\begin{array}{r|l} 8\ 5\ 0\ 8\ 5 & 1\ 3\ 2\ 3 \\ \hline 5\ 7\ 0\ 5 & 6\ 4 \\ 4\ 1\ 3 & \end{array}$ $\Rightarrow 85085 = 64 \cdot 1323 + 413 \Rightarrow 85085 - 64 \cdot 1323 = 413 \Rightarrow$ Restamos a la segunda fila 64 veces la primera

Paso 1

$$\begin{pmatrix} 1 & 0 & 1323 \\ -64 & 1 & 413 \end{pmatrix}$$

$\begin{array}{r|l} 1\ 3\ 2\ 3 & 4\ 1\ 3 \\ \hline 8\ 4 & 3 \end{array}$ $\Rightarrow 1323 = 3 \cdot 413 + 84 \Rightarrow 1323 - 3 \cdot 413 = 84 \Rightarrow$ Restamos a la primera fila 3 veces la segunda

Paso 2

$$\begin{pmatrix} 193 & -3 & 84 \\ -64 & 1 & 413 \end{pmatrix}$$

$\begin{array}{r|l} 4\ 1\ 3 & 8\ 4 \\ \hline 7\ 7 & 4 \end{array}$ $\Rightarrow 413 = 4 \cdot 84 + 77 \Rightarrow 413 - 4 \cdot 84 = 77 \Rightarrow$ Restamos a la segunda fila 4 veces la primera

Paso 3

$$\begin{pmatrix} 193 & -3 & 84 \\ -836 & 13 & 77 \end{pmatrix}$$

$\begin{array}{r|l} 8\ 4 & 7\ 7 \\ \hline 7 & 1 \end{array}$ $\Rightarrow 84 = 1 \cdot 77 + 7 \Rightarrow 84 - 1 \cdot 77 = 7 \Rightarrow$ Restamos a la primera fila 1 veces la segunda

Paso 4

$$\begin{pmatrix} 1029 & -16 & 7 \\ -836 & 13 & 77 \end{pmatrix}$$

$\begin{array}{r|l} 7\ 7 & 7 \\ \hline 0\ 7 & 1\ 1 \\ 0 & \end{array}$ $\Rightarrow 77 = 11 \cdot 7 + 0 \Rightarrow 77 - 11 \cdot 7 = 0 \Rightarrow$ Restamos a la segunda fila 11 veces la primera

Paso 5

$$\begin{pmatrix} 1029 & -16 & 7 \\ -12155 & 189 & 0 \end{pmatrix}$$

Obtenemos el sistema equivalente al primero de ecuaciones:

$$\begin{cases} (1029) \cdot x + (-16) \cdot y & = 7 \\ (-12155) \cdot x + (189) \cdot y & = 0 \end{cases}$$

En consecuencia

$$(1029) \cdot 1323 + (-16) \cdot 85085 = 7 \Rightarrow \begin{cases} mcd(1323, 85085) & = 7 \\ u & = 1029 \end{cases}$$

No tiene solución ya que el mcd(a,n) no es 1

Resuelve la ecuación modular: $1323x \equiv 49 \pmod{85085}$

$\begin{array}{r|l} 4\ 9 & 7 \\ \hline 0 & 7 \end{array}$ $\Rightarrow 49 = 7 \cdot 7$

En este caso, mcd(a,n) (por el apartado anterior) divide a b. La ecuación anterior es equivalente a resolver $189x \equiv 7 \pmod{12155}$. Resolvamos primero la ecuación $189x \equiv 1 \pmod{12155}$

Paso 0

$$\begin{pmatrix} 1 & 0 & 189 \\ 0 & 1 & 12155 \end{pmatrix}$$

$\begin{array}{r|l} 1\ 2\ 1\ 5\ 5 & 1\ 8\ 9 \\ \hline 8\ 1\ 5 & 6\ 4 \\ \hline 5\ 9 & \end{array}$ $\Rightarrow 12155 = 64 \cdot 189 + 59 \Rightarrow 12155 - 64 \cdot 189 = 59 \Rightarrow$ Restamos a la segunda fila 64 veces la primera

Paso 1

$$\begin{pmatrix} 1 & 0 & 189 \\ -64 & 1 & 59 \end{pmatrix}$$

$\begin{array}{r|l} 1\ 8\ 9 & 5\ 9 \\ \hline 1\ 2 & 3 \end{array}$ $\Rightarrow 189 = 3 \cdot 59 + 12 \Rightarrow 189 - 3 \cdot 59 = 12 \Rightarrow$ Restamos a la primera fila 3 veces la segunda

Paso 2

$$\begin{pmatrix} 193 & -3 & 12 \\ -64 & 1 & 59 \end{pmatrix}$$

$\begin{array}{r|l} 5\ 9 & 1\ 2 \\ \hline 1\ 1 & 4 \end{array}$ $\Rightarrow 59 = 4 \cdot 12 + 11 \Rightarrow 59 - 4 \cdot 12 = 11 \Rightarrow$ Restamos a la segunda fila 4 veces la primera

Paso 3

$$\begin{pmatrix} 193 & -3 & 12 \\ -836 & 13 & 11 \end{pmatrix}$$

$\begin{array}{r|l} 1\ 2 & 1\ 1 \\ \hline 1 & 1 \end{array}$ $\Rightarrow 12 = 1 \cdot 11 + 1 \Rightarrow 12 - 1 \cdot 11 = 1 \Rightarrow$ Restamos a la primera fila 1 veces la segunda

Paso 4

$$\begin{pmatrix} 1029 & -16 & 1 \\ -836 & 13 & 11 \end{pmatrix}$$

$\begin{array}{r|l} 1\ 1 & 1 \\ \hline 0\ 1 & 1\ 1 \\ \hline 0 & \end{array}$ $\Rightarrow 11 = 11 \cdot 1 + 0 \Rightarrow 11 - 11 \cdot 1 = 0 \Rightarrow$ Restamos a la segunda fila 11 veces la primera

Paso 5

$$\begin{pmatrix} 1029 & -16 & 1 \\ -12155 & 189 & 0 \end{pmatrix}$$

Por tanto

$mcd(189, 12155) = 1$

$u = 1029$

Si x_0 es una solución de $ax \equiv 1 \pmod{n}$, entonces $x_0 \cdot b$ es una solución de la ecuación $ax \equiv b \pmod{n}$. A partir de lo anterior tenemos que:

$1029 \cdot 7 \pmod{12155} \equiv 7203 \pmod{12155} \equiv 7203 \pmod{12155} \Rightarrow x_0 = 7203 \Rightarrow$
$x \equiv 7203, 19358, 31513, 43668, 55823, 67978, 80133 \pmod{85085}$