Aplicaciones de Aritmética modular
El pequeño teorema de Fermat

Sergio A. Carrillo
sacarrillot@unal.edu.co

Congruencias

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}^+$. Recordemos que

$$a \equiv_m b \qquad \text{sii} \qquad m|(a-b) \qquad \text{sii} \qquad \exists k \in \mathbb{Z}, a = b + km.$$

$\equiv_m$ es una relación de equivalencia sobre $\mathbb{Z}$ y sus clases se pueden escribir como

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

Además hay compatibilidad con las operaciones: si $a \equiv b \,(\text{mod } m)$ y $c \equiv d \,(\text{mod } m)$, entonces

$$a + c \equiv b + d \,(\text{mod } m), \qquad ac \equiv bd \,(\text{mod } m).$$

Ejemplos: últimos dígitos

Calcular el último dígito de 2^{2025}. Esto equivale a reducir este valor módulo 10.

$$\begin{aligned} 2^0 &\equiv 1 \pmod{10}, & 2^1 &\equiv 2 \pmod{10}, & 2^2 &\equiv 4 \pmod{10}, \\ 2^3 &\equiv 8 \pmod{10}, & 2^4 &\equiv 6 \pmod{10}, & 2^5 &\equiv 2 \pmod{10}, \\ 2^6 &\equiv 4 \pmod{10}, & 2^7 &\equiv 8 \pmod{10}, & 2^8 &\equiv 6 \pmod{10}. \end{aligned}$$

De aquí observamos que $2^{4n+1} \equiv 2 (\text{mod } 10)$, para todo $n \geq 0$ y por tanto, como $2025 = 506 \cdot 4 + 1$, entonces

$$2^{2025} = 2^{506 \cdot 4 + 1} \equiv 2 (\text{mod } 10).$$

Exponenciación modular rápida

El algoritmo para calcular efectivamente $a^n(\mod m)$, funciona de la siguiente manera:

1. Escriba en binario a n.
2. Calcule sucesivamente las potencias $a, a^2, a^4, a^8, \ldots$ hasta alcanzar la máxima potencia de 2 que aparece en la expansión binaria de n. En cada cálculo reduzca módulo m.
3. Finalmente multiplique los $a^{(2^j)} \mod m$, para aquellos j que aparezcan en la expansión de n.

Ejemplo

Calcular $5^{23} \mod 1001$.

1. $n = 23 = 10111_2 = 2^4 + 2^2 + 2^1 + 2^0$.
2. Calculamos

$$\begin{aligned} 5^2 &= 25 \mod 1001, \\ 5^4 &= 25^2 \equiv 625 \mod 1001, \\ 5^8 &= 625^2 = 390625 \equiv 235 \mod 1001, \\ 5^{16} &= 235^2 = 55225 \equiv 170 \mod 1001. \end{aligned}$$

3. $5^{23} = 5^{2^4+2^2+2^1+2^0} = 5^{2^4} \cdot 5^{2^2} \cdot 5^{2^1} \cdot 5^{2^0} \equiv 170 \cdot 625 \cdot 25 \cdot 5 \equiv 983 \mod 1001$.

Calcule ahora los 3 últimos dígitos de 3^{1000}. **Respuesta**: 001.

Ejemplos

- $7 \mid 3^{2n+1} + 2^{n+2}$, para todo $n \in \mathbb{N}$.
- $a^5 \equiv a \pmod{30}$, para todo $a \in \mathbb{Z}$.

Como $30 = 6 \cdot 5$ basta mostrar que $a^5 \equiv a \pmod{6}$ y $a^5 \equiv a \pmod{5}$. Puede emplear la factorización:

$$a^5 - a = a(a^4 - 1) = a(a^2 - 1)(a^2 + 1) = a(a - 1)(a + 1)(a^2 + 1).$$

Criterios de divisibilidad

¿Por qué un número es par si y solo si su último dígito es $0, 2, 4, 6, 8$? En base decimal un número se escribe como

$$n = a_k 10^k + \cdots + a_1 10 + a_0, \quad a_j \in \{0, 1, \ldots, 9\}.$$

Si $j \geq 1$, $10^j \equiv 0 (\text{mod } 2)$ y $10^j \equiv 0 (\text{mod } 10)$. Por tanto,

$$n \equiv a_0 (\text{mod } 2), \qquad n \equiv a_0 (\text{mod } 10).$$

Tomando módulo 5 obtenemos

$$n \equiv a_0 (\text{mod } 5).$$

Así n es divisible por 5 si y solo si $a_0 = 0$ ó 5.

División por 3 y 11

Tomando módulo 3, como $10 \equiv 3 (\text{mod } 3)$, obtenemos

$$n \equiv a_k + \cdots + a_1 + a_0 \, (\text{mod } 3).$$

Así n es divisible por 3 si y solo si la suma de los dígitos de n es divisible por 3.

Tomando módulo 11, como $10 \equiv -1 (\text{mod } 11)$, obtenemos

$$n \equiv a_0 - a_1 + \cdots + (-1)^k a_k \, (\text{mod } 11).$$

Así n es divisible por 11 si y solo si la suma alternada de sus dígitos es divisible por 11.

Estructura de grupo

$(\mathbb{Z}/m\mathbb{Z}, +)$ es un grupo abeliano, donde sumar clases se hace de forma natural, módulo m. Por ejemplo, $[1] + [m-1] = [0]$. Sin embargo, para la multiplicación puede pasar que $[a][b] = [0]$ con $[a] \neq [0]$ y $[b] \neq 0$. Observe las tablas para $m = 6$.

+	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

·	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

Inversos multiplicativos

Recordemos por la identidad de Bezout que $\gcd(a,b) = 1$ si y solo si existen $s, t \in \mathbb{Z}$ con $as + bt = 1$. Esto significa que $as \equiv 1 (\text{mod } b)$. La recíproca es idéntica. Así tenemos que:

Proposición

Dado $m \in \mathbb{N}^+$, $a \in \mathbb{Z}$ tiene inverso multiplicativo módulo m si y solo si $\gcd(a,m) = 1$.

Corolario

Si p es primo, entonces $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ es un grupo abeliano.

Aquí $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\} = \{[1], [2], \ldots, [p-1]\}$.

Ejemplos

- Hacer la tabla de multiplicación de $\mathbb{Z}/5\mathbb{Z}$. ¿Qué grupo de orden 4 se obtiene?
- Resolver la congruencia $2x \equiv 5 (\text{mod } 11)$.
- (Lema de Euclides) Si p es primo y $p|(ab)$, entonces $p|a$ ó $p|b$. Esto significa que si $ab \equiv_p 0$, entonces $a \equiv_p 0$ ó $b \equiv_p 0$.

  Demostrar que si $x^2 \equiv_p 1$, entonces $x \equiv_p 1$ ó $x \equiv_p -1$.

Tres congruencias relativas a primos

Sea p primo y $a, b \in \mathbb{Z}$.

Proposición (The freshman's dream)

$$(a+b)^p \equiv a^p + b^p \,(\text{mod } p).$$

Teorema (Pequeño teorema de Fermat)

$$a^p \equiv a(\text{mod } p).$$

Además si $\gcd(a,p) = 1$, *entonces* $a^{p-1} \equiv 1(\text{mod } p)$.

Proposición (Teorema de Wilson)

$$(p-1)! \equiv -1 \,(\text{mod } p).$$