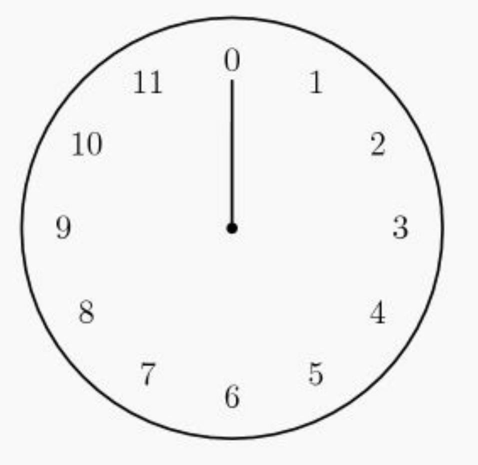
Aritmética Modular

Bach. Rodolfo Mercado Gonzales
Universidad Nacional de Ingeniería

Aritmética modular o de reloj



Las 24 horas del día :

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, **12**, **13**, **14**, 15, 16, 17, 18, ...

El reloj cuenta en módulo 12 :

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, **0**, 1 , 2 , 3 , 4 , 5 , 6 , ...

12 ≡ 0 (mod 12) **13 ≡ 1 (mod 12)**

Relación de Congruencia

Sean $\boldsymbol{a}, \boldsymbol{b}\ y\ \boldsymbol{m}$ números enteros, con $\boldsymbol{m} > \mathbf{0}$, si $\boldsymbol{m} \mid (\boldsymbol{a} - \boldsymbol{b})$ se dice que $\boldsymbol{a}$ es congruente a $\boldsymbol{b}$ módulo $\boldsymbol{m}$.

Se representa de la siguiente manera:

$$\boldsymbol{a} \equiv \boldsymbol{b}\ (\boldsymbol{mod}\ \boldsymbol{m})$$

Relación de Congruencia

Ejemplos:

$$22 \equiv 4 \pmod{9}$$

$$-9 \equiv 31 \pmod{10}$$

$$16 \equiv 30 \pmod{7}$$

Relación de Congruencia

Dos enteros **a** y **b** son congruentes módulo **m** (m es un entero positivo) si el resto de **a** entre **m** es el mismo que el resto de **b** entre **m**.

$$\mathbf{a} \bmod \mathbf{m} = \mathbf{b} \bmod \mathbf{m} \;\leftrightarrow\; \mathbf{a} \equiv \mathbf{b} \pmod{\mathbf{m}}$$

Propiedades de Congruencia

Sean $\boldsymbol{a}, \boldsymbol{b}$ y $\boldsymbol{m}$ números enteros, entonces

- $a \equiv a \pmod{m}$ **reflexiva**
- $a \equiv b \pmod{m} \rightarrow b \equiv a \pmod{m}$ **simétrica**
- $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \rightarrow a \equiv c \pmod{m}$ **transitiva**

Propiedades de Congruencia

- La relación de congruencia para un módulo **m** también es una relación de equivalencia.
- A las clases de equivalencia que se forman se le llaman clases residuales.

$$[\,a\,] = \{\, x \in Z \mid x \equiv a \pmod{m} \,\} \quad , \quad a \in [\,0, m-1]$$

Propiedades de Congruencia

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

$a + b \equiv a \bmod m + b \bmod m \pmod{m}$ **suma**

$a - b \equiv a \bmod m - b \bmod m \pmod{m}$ **resta**

$a * b \equiv a \bmod m * b \bmod m \pmod{m}$ **multiplicación**

$a \wedge b \equiv (a \bmod m) \wedge b \pmod{m}$ **exponenciación**

¿ y para la división ?

Inverso Modular

Dado los enteros **a** y **m**, el inverso modular de **a** módulo **m** es un entero **x**, tal que:

$$a\,x \equiv 1 \pmod{m}$$

x se denota como **a^-1**.

Inverso Modular

Teorema

a tiene inversa módulo **m** $\leftrightarrow$ **gcd(a, m) = 1.**

Inverso Modular

Demostración

$\rightarrow$

$a \,.\, a^{-1} \equiv 1 \pmod{m}$

$a \,.\, a^{-1} = mk + 1$, donde k es un entero

$a \,.\, a^{-1} - mk = 1$

$a \,.\, a^{-1} + m(-k) = 1$

$\gcd(a, m) \mid 1 \rightarrow \gcd(a, m) = 1$

$\leftarrow$

$ax + \mathbf{m}y = 1$

$ax \equiv 1 \pmod{m}$

Inverso Modular

Corolario

Sea $ax \equiv ay \pmod{m}$ y $\text{mcd}(a, m) = 1 \rightarrow x \equiv y \pmod{m}$

Inverso Modular

Teorema

a tiene inversa módulo **m** $\rightarrow$ la clase residual de los inversos es única

Inverso Modular

Demostración

gcd(a, m) = 1

Sean a1 y a2 inversas de a módulo m

$a \cdot a1 \equiv 1 \qquad a \cdot a2 \equiv 1$, aplicando transitividad

$a \cdot a1 \equiv a \cdot a2$

$a1 \equiv a2$

Inverso Modular

¿ Cómo hallamos el inverso modular de a mod m ?

Inverso Modular

Solución Ingenua

Aplicamos brute force en el rango [0, m -1] **O(m)**

Inverso Modular

Solución particular (cuando m es un número primo)

Del pequeño teorema de Fermat : $a \wedge (m-1) \equiv 1 \pmod{m}$, m es primo

Dándole forma $a \ . \ a\wedge(m-2) \equiv 1 \pmod{m}$

$a\wedge{-1} \equiv a\wedge(m-2)$ **O(log m)**

Inverso Modular

Solución

Con el algoritmo extendido de euclides podemos encontrar solución para :

$$\mathbf{a}\, x + \mathbf{m}\, y = \gcd(a, m)$$

Como existe el inverso: $\mathbf{a}\, x + \mathbf{m}\, y = 1$

Sacando módulo: $a\, \mathbf{x} \equiv 1 \pmod{m}$

$$a^{-1} \equiv \mathbf{x} \qquad \mathbf{O(\log \min(a, m))}$$

Inverso Modular

```
ll modularInverse( ll a, ll n ){
    Tuple t = extGcd( a, n );
    ll inverse = ( ( t.x % n ) + n ) % n;
    return inverse;
}
```

Problemas

Hackerearth - Modulo Inverse

Codeforces- Magic Five

Referencias

- **Rosen, K.** - Elementary number theory and its applications.
- **Hackerearth**.- Basic Number Theory 1

¡ Good luck and have fun !