Taller ProgComp: Track Matemática

Arimética Modular

Gabriel Carmona Tabja

Universidad Técnica Federico Santa María,
Università di Pisa

April 15, 2024

Part I

Aritmética Modular

Operaciones

Suma modular

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Operaciones

Suma modular

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Resta modular

$$(a - b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

Operaciones

Suma modular

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Resta modular

$$(a - b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

Multiplicación modular

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

OPERACIONES

Suma modular

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Resta modular

$$(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

Multiplicación modular

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

División modular

$$(a/b) \bmod m = ((a \bmod m)/(b \bmod m)) \bmod m$$

Operaciones

Suma modular

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Resta modular

$$(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

Multiplicación modular

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

División modular

$$(a/b) \bmod m = ((a \bmod m)/(b \bmod m)) \bmod m$$

¿Seguro?

Precauciones

- Números negativos

$$((a \bmod m) + m) \bmod m$$

- División, esta no funciona con lo puesto antes
  - ¿Cómo hacemos la división una operación que sirva con el modúlo?

Part II

Pequeño Teorema de Fermat

FUNCIÓN TOTIENT

Definición Coprimos

Dos enteros x e y son coprimos si su máximo común divisor es igual a 1.

Función Totient

Definición Coprimos

Dos enteros x e y son coprimos si su máximo común divisor es igual a 1.

Definición Función Totient

La función totient sobre n o $\varphi(n)$, corresponde a la cantidad de números enteros positivos menores que n que son coprimos con n.

Ejemplo

$$\varphi(12) = 4$$

Los coprimos son: 1, 5, 7 y 11

Pequeño Teorema de Fermat (Fermatito)

Teorema

Si p y a son enteros coprimos, entonces:

$$a^{\varphi(p)} \equiv 1 (\mathrm{mod}\ p)$$

Inverso modular

$$\frac{1}{a} = a^{-1}$$

Inverso modular

$$\frac{1}{a} = a^{-1}$$

Usamos Fermatito:

$$a^{\varphi(p)} \cdot a^{-1} \equiv 1 \cdot a^{-1} (\bmod p)$$
$$a^{\varphi(p)-1} \equiv a^{-1} (\bmod p)$$

Inverso modular

$$\frac{1}{a} = a^{-1}$$

Usamos Fermatito:

$$a^{\varphi(p)} \cdot a^{-1} \equiv 1 \cdot a^{-1} \pmod{p}$$
$$a^{\varphi(p)-1} \equiv a^{-1} \pmod{p}$$

Pero, si p es primo, $\varphi(p) = p - 1$, entonces;

$$a^{p-2} \equiv a^{-1} \pmod{p}$$

TIP: Primos comunes en ProgComp son $p = 10^9 + 7$ o $p = 10^9 + 9$.

División modular

$$(a/b) \bmod m = ((a \bmod m) \cdot (b^{-1} \bmod m)) \bmod m$$
$$(a/b) \bmod m = ((a \bmod m) \cdot (b^{p-2} \bmod m)) \bmod m$$

División modular

División modular

$$(a/b) \bmod m = ((a \bmod m) \cdot (b^{-1} \bmod m)) \bmod m$$
$$(a/b) \bmod m = ((a \bmod m) \cdot (b^{p-2} \bmod m)) \bmod m$$

Ahora solo nos falta saber elevar de manera eficiente :).
Spoiler: Exponienciación Binaria.

References I