ABRIL 30 CLASE 5

MÓDULO 3

ARITMÉTICA MÓDULAR

① ¿Que es el módulo en los números enteros?

Ej) $17\%3=2$ → $\begin{array}{c|c} 17 & 3 \\ \hline (2) & 5 \end{array}$

↓ mate

$17 \equiv 2 \pmod 3$ → $\mathbb{Z}_3 = \{0, 1, 2\}$

En general $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

$a \equiv b \pmod n$ → $n \mid a-b$

$37 \equiv 1 \pmod 9$ → $9 \mid 37-1$ → $9 \mid 36$ ✓

$68 \equiv 13 \pmod{11}$ → $11 \mid 68-13$ → $11 \mid 55$ ✓ Pero 13 no esta en $\mathbb{Z}_{11}$

$12 \equiv -2 \pmod 7$ → $7 \mid 12-(-2)$ → $7 \mid 14$ ✓ Pero -2 no esta en $\mathbb{Z}_7$

pertenece

$39 \equiv 6 \pmod{11}$ $6 \in \mathbb{Z}_{11}$

$17 \equiv 5 \pmod 6$ $5 \in \mathbb{Z}_6$

$25 \equiv 7 \pmod 9$ $7 \in \mathbb{Z}_9$

NOTA: El módulo en c++ es solo sacar el resto.

En c++ ¿Cual es el resultado de imprimir $(-25\%3)$?

Imprime -1 que es correcto, pues $-25 \equiv -1 \pmod 3$

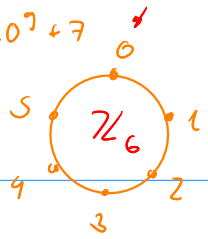
$3 \mid -25-(-1) = -24$

Pero $-1 \notin \mathbb{Z}_3$ entonces la respuesta correcta es $\mathbb{Z}_{//}$

↳ $+3 = (2)$

NOTA: En PYTHON $-25\%3 = (2)$

Ej: Obtener la respuesta $\mod m = 10^7 + 7$



OPERACIONES

a) Sumar

$$(a+b)\,\%\,m = \big((a\,\%\,m) + (b\,\%\,m)\big)\,\%\,m$$

b) Restar

$$(a-b)\,\%\,m = \Big\{\big[\big((a\,\%\,m) - (b\,\%\,m)\big)\,\%\,m\big] + m\Big\}\,\%\,m$$

LO NORMAL — LO CORRECTO

c) Multiplicar

$$(a*b)\,\%\,m = \big((a\,\%\,m) * (b\,\%\,m)\big)\,\%\,m$$

d) ¿Dividir?

En reales

$$\frac{372}{3} = 124 \rightarrow \left(\frac{372}{3}\right) \bmod 5$$

$$372 \cdot 3^{-1} = 124 \rightarrow (372 \cdot 3^{-1}) \pmod 5$$

3^{-1}: inverso multiplicativo de 3

$3 \cdot \frac{1}{3} = 1$

$$372 \pmod 5 \cdot 3^{-1} \pmod 5$$

$$2 \cdot 2 \pmod 5$$

$$4 \pmod 5$$

En $\mathbb{Z}_5$: $0, 1, 2, 3, 4$

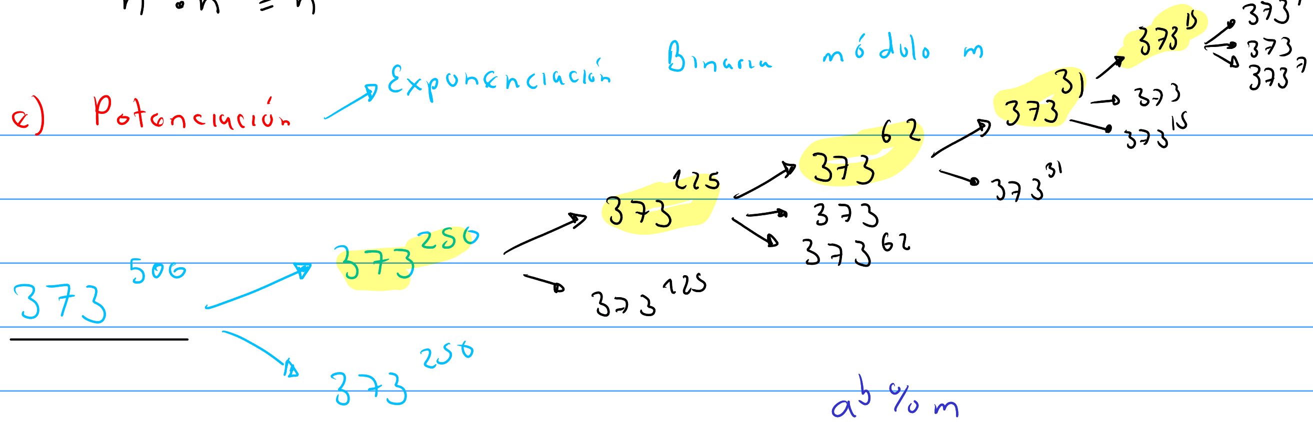
3^{-1}

$3 \cdot 2 = 6 \equiv 1 \pmod 5$

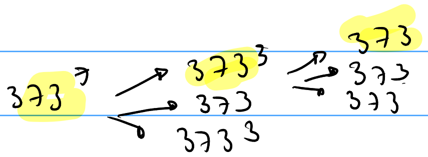
NOTA: Los inversos modulares no entran en ICI, mas sin embargo es un problema interesante de estudiar pues no todos los $\mathbb{Z}_n$ tienen inversos modulares.

$n^a \cdot n^b = n^{a+b}$

e) Potenciación → Exponenciación Binaria módulo m



$a^b \% m$




```
ll elevar (ll a, ll b, ll m){
    if(b==1) return (a%m);
    ll res = elevar(a, b/2, m);
    res =((res%m)*(res%m))%m;

    if(b%2==0) return res;
    else return ((res%m)*(a%m))%m;
}
```