$a \equiv b \mod n$ — relación

$a, b \in \mathbb{Z}$

$n \in \mathbb{N}^*$

$x \bmod n$ $\quad x \in \mathbb{Z}$ $\quad a \,\%\, b$ en Python

↑ resto de la división de x por n

$10 \equiv 22 \mod 3$ relación

$15 \mod 3 = 0$

3.2.21

$a = q \cdot n + r \qquad r - a = (-q) \cdot n$

a) 3.2.20 d) $\Rightarrow$ $a \equiv \underbrace{(a \bmod n)}_{r} \mod n$

$b \equiv (b \bmod n) \mod n$

3.2.20 f) $\Rightarrow$ $a+b \equiv \big((a \bmod n) + (b \bmod n)\big) \mod n$

3.2.20 e) $\Rightarrow$ $(a+b) \bmod n = \big((a \bmod n) + (b \bmod n)\big) \bmod n$

$(37 + 53) \bmod 3 = (37 \bmod 3 + 53 \bmod 3) \bmod 3$

$1 + 2$

$90 \bmod 3 = 0$

$3 \bmod n = 0$ ✓

$(47 \cdot 128) \bmod 3$

$(47 \bmod 3 \cdot 128 \bmod 3) \bmod 3 = (2 \cdot 2) \bmod 3 = 1$

$137728 \bmod 17$

$22^{22} \bmod 9 = (22 \bmod 9)^{22} \bmod 9$

$= 4^{22} \bmod 9$

$= 16^{11} \bmod 9$

$= 7^{11} \bmod 9$

$= (7^6 \cdot 7^5) \bmod 9$

$2^k \bmod n$

$= (2 \bmod n)^k \bmod n$

$$= (49^3 \cdot 7^4 \cdot 7^1) \bmod 9$$

$$= (4^3 \cdot 4^2 \cdot 7) \bmod 9$$

3.2.12

b) $(123\,456\,789 \cdot 987\,654\,321) \bmod 11 =$ 3.2.21

$$\Big((123\,456\,789 \bmod 11) \cdot (987\,654\,321 \bmod 11)\Big) \bmod 11 =$$

$5 \qquad 5$

$$25 \bmod 11 = 3$$

$$35^{34} \bmod 11 = (35 \bmod 11)^{34} \bmod 11$$

$$= 2^{34} \bmod 11$$

$$= (2^{10} \cdot 2^{10} \cdot 2^{10} \cdot 2^{4}) \bmod 11$$

$$= (((1024 \bmod 11)^{3} \cdot 5) \bmod 11$$

1

$$= 5$$

·	0	1	2	3	4	5	6	
0	0	0	0	0	0	0	0	
1	0	1	2	3	4	5	6	
2	0	2	4	6	1	3	5	
3	0	3	6	2	5	1	4	
4	0							
5	0							
6	0							

Table de multiplication mod 7

×	0	1	2	3	
0	0	1	2	3	
1	1	2	3	0	
2	2	3	0	1	
3	3	0	1	2	

Calculer mod 4