

SOLUCIONES ARITMÉTICA MODULAR

1a) 2 1b) 0 1c) 1 1d) 6 2a) 1 2b) 24

3) Cualquier entero $n > 5$ se escribe en la forma $6k+r$ para algún $k \geq 1$ y $r=0,1,2,3,4$ o 5 , en el caso particular de ser n primo, dicho resto no podrá ser 0 , ni 2 , ni 4 (n sería divisible por 2), ni 3 (n sería divisible por 3), así tenemos que n será congruente con 1 o 5 módulo 6 .

4) Observemos que $10 \equiv -1 \pmod{11}$, así $10^n \equiv (-1)^n \pmod{11}$ y por tanto tenemos $x = 10^n x_n + \dots + 10 x_1 + x_0 \equiv (-1)^n x_n + \dots + x_2 - x_1 + x_0 \pmod{11}$.

$1213141516171819 \equiv 36 \equiv 3 \pmod{11}$ no divisible por 11

$192837465564738291 \equiv 0 \pmod{11}$ divisible por 11

5) Trabajando módulo 11 obtenemos que $2+x \equiv 0 \pmod{11}$, de donde $x=9$.

6) Los ejemplos pueden ser 2 y 3 , 2 y 4 , 3 y 5 respectivamente. En \mathbf{Z}_7 no se puede dar este hecho, ya que todos los elementos no nulos son invertibles por ser todos primos con 7 (ya que 7 es primo).

7) En \mathbf{Z}_6 son 1 y 5 . En \mathbf{Z}_7 son $1, 2, 3, 4$ y 5 . En \mathbf{Z}_8 son $1, 3, 5$ y 7 . En \mathbf{Z}_{18} son $1, 5, 7, 11, 13$ y 17 .

8a) 2 8b) 3 8c) 7 8d) 5 8e) 6 8f) 13 8g) 7 8h) 8

9) $3^{47} \equiv 3^3 \equiv 9 \pmod{23}$ $6^{592} \equiv 6^2 \equiv 36 \equiv 3 \pmod{11}$

10) $3^{15} \equiv 3^{-1} \equiv 6 \pmod{17}$ $15^{90} \equiv 2^{90} \equiv 2^6 \equiv 3 \cdot 4 \equiv 12 \pmod{13}$

11) Trabajando módulo 9 tenemos que $n^3 + (n+1)^3 + (n+2)^3 \equiv r^3 + (r+1)^3 + (r+2)^3 \pmod{9}$ donde r es el resto de dividir n por 9 . Ahora bien, si calculamos $r^3 \pmod{9}$ para cada posible resto $r=0,1,2,3,4,5,6,7,8$ obtenemos $0,1,-1,0,1,-1,0,1,-1$, de donde sea cual sea r sale $r^3 + (r+1)^3 + (r+2)^3 \equiv 0 \pmod{9}$.

14) Queremos determinar el menor entero positivo X con $X \equiv -1 \pmod{m}$ para $m=2, \dots, 10$, así X será de la forma $9 \cdot 8 \cdot 7 \cdot 5 \cdot K - 1$ para algún entero K . De este modo $X=2519$ ($K=1$).

15a) $x \equiv 5, 11 \pmod{12}$ 15b) no tiene solución 15c) $x \equiv 6 \pmod{7}$

15d) $x \equiv 3, 8, 13 \pmod{15}$

16) 0 y 436