

Problema 1. Calcular el resto de dividir :

- (a) 1986^{2061} por 7, (b) 1654^{1255} por 23, (c) 293^{1767} por 7, (d) 6^{2000} por 11
 (e) $(1843)^{138648568243871569}$ por 11

Problema 2. Hallar las dos últimas cifras de 7^{5448} .

Problema 3. Demuestra que 1241 es un divisor de $8^{72} - 1$

Problema 4. Sea p un número primo impar, Demuestra que sólo son inversos de sí mismos en \mathbb{Z}_p $\bar{1}$ y $\overline{p-1}$.

Problema 5. Encontrar el menor resto no negativo de $1! + 2! + 3! + \dots + 10!$ módulo cada uno de los siguientes enteros a) 3, b) 11, c) 4, d) 23

Problema 6. Encontrar el menor resto no negativo de $1! + 2! + 3! + \dots + 100!$ módulo cada uno de los siguientes enteros a) 2, b) 7, c) 12, d) 25

Problema 7. Encontrar el menor resto no negativo de:
 6! Módulo 7, (b) 10! Módulo 11, (c) 12! Modulo 13, (d) 16! Modulo 17.

Problema 8. Demuestra que:
 (a) 437 es divisor de $18! + 1$, (b) 11 es divisor de $10! + 1$

Problema 9. Encontrar los restos de la división euclídea en los siguientes casos:
 (a) $16!$ dividido por 19, (b) $5!25!$ dividido por 31, (c) $8*9*10*11*12$ por 7
 (d) $8*9*10*11*12*13$ por 7 (e) $3^{99999999}$ dividido por 17

Problema 10. Encuentra el resto de dividir $40!$ por 1763.

Problema 11. Demostrar que $3^{10} \equiv 1 \pmod{11^2}$

Problema 12. Se considera la expansión en base 7 de 3^{100} :
 (a) Encuentra el último dígito, (b) Encuentra los dos últimos dígitos.

Problema 13. Demuestra que si p es un número primo impar, se verifica
 $2(p-3)! \equiv -1 \pmod{p}$

Problema 14. Demuestra que si n es un entero compuesto con $n \neq 4$, se verifica que
 $(n-1)! \equiv 0 \pmod{n}$

Problema 15. Demuestra que $a^{12}-1$ es divisible por 35 si $\text{mcd}(a, 35) = 1$

Problema 16. Demuestra que a^6-1 es divisible por 168 si $\text{mcd}(a, 42) = 1$

Problema 17. Demuestra que 42 es divisor de $n^7 - n$, para todo entero positivo n .

Problema 18. Demuestra que 30 es divisor de $n^9 - n$, para todo entero positivo n .

Problema 19. Si p es un número primo impar, demuestra que

$$1^p + 2^p + 3^p + \dots + (p-1)^p \equiv 0 \pmod{p}$$

Problema 20. Demuestra que si p es número primo y, a y b son enteros no divisibles por p , con $a^p \equiv b^p \pmod{p}$, se verifica $a^p \equiv b^p \pmod{p^2}$.

Problema 21. Demostrar que si p y q son dos primos distintos, se verifica que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

Problema 22. Demuestra que si p es primo y $p \equiv 3 \pmod{4}$, se verifica que

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$$

Problema 23. Encontrar los inversos de los números dados en los cuerpos que se indican:

(a) 3, 5, 8 en \mathbf{Z}_{13} , (b) 3, 6, 9, 10 en \mathbf{Z}_{11} , (c) 3, 4, 2, en \mathbf{Z}_5 , (d) 3, 11, 15, 22 en \mathbf{Z}_{23} .

Problema 24. Resolver los siguientes sistemas de congruencia:

$$\begin{aligned} \text{(a)} \quad & \begin{cases} x + 2y + 3z \equiv 1 \pmod{7} \\ x + 2y + 4z \equiv 1 \pmod{7} \\ x + 4y + 6z \equiv 1 \pmod{7} \end{cases}, & \text{(b)} \quad & \begin{cases} 3x + y + 3z \equiv 1 \pmod{5} \\ x + 2y + 4z \equiv 2 \pmod{5} \\ 4x + 3y + 2z \equiv 3 \pmod{5} \end{cases}, \\ \text{(c)} \quad & \begin{cases} x + 2y + 3z \equiv 1 \pmod{7} \\ x + 2y + 5z \equiv 1 \pmod{7} \\ x + 4y + 6z \equiv 1 \pmod{7} \end{cases}, & \text{(d)} \quad & \begin{cases} x + 2y + 3z \equiv 1 \pmod{11} \\ x + 2y + 5z \equiv 1 \pmod{11} \\ x + 4y + 6z \equiv 1 \pmod{11} \end{cases}, \\ \text{(e)} \quad & \begin{cases} 3x + y + 3z \equiv 1 \pmod{7} \\ x + 2y + 4z \equiv 2 \pmod{7} \\ 4x + 3y + 2z \equiv 3 \pmod{7} \end{cases}, & \text{(f)} \quad & \begin{cases} 3x + y + 3z \equiv 1 \pmod{13} \\ x + 2y + 4z \equiv 2 \pmod{13} \\ 4x + 3y + 2z \equiv 3 \pmod{13} \end{cases} \end{aligned}$$

Problema 25. (*Residuos cuadráticos*) Un entero a se dice residuo cuadrático módulo n si $\text{mcd}(a, n) = 1$ y la ecuación

$$x^2 \equiv a \pmod{n}$$

posee solución. Por ejemplo, en \mathbf{Z}_{11} , los residuos cuadráticos son 1, 3, 4, 5 y 9.

Sea $n = 4$, p^k , $2p^k$ (p primo impar). Demostrar que a es residuo cuadrático si, y sólo si, $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$

Problema 26. Sea p un primo impar y $\text{mcd}(a, p) = 1$. Demostrar que a es residuo cuadrático módulo p si $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ y que a no es residuo cuadrático módulo p si $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Problema 27. Sea p un primo impar y $\text{mcd}(a, p) = 1$. Demostrar que la ecuación $x^2 \equiv a \pmod{p}$ tiene o dos soluciones o ninguna módulo p .

Problema 28. Demostrar que en \mathbf{Z}_p (p primo impar) hay tantos residuos cuadráticos como no residuos cuadráticos.

Problema 29. Demostrar que la ecuación $X^2 + 1 \equiv 0 \pmod{p}$ tiene solución si, y sólo si, $p = 2$ o $p \equiv 1 \pmod{4}$.