

Congruencias

1. Criterios de divisibilidad: Sea $n \in \mathbb{N}$.
 - a) Demuestra que n es divisible por 7 si y sólo si al separar la cifra correspondiente a las unidades, multiplicarla por 2 y restarla de las cifras restantes la diferencia es un múltiplo de 7.
 - b) Demuestra que n es divisible por 13 si y sólo si al separar la cifra correspondiente a las unidades, multiplicarla por 9 y restarla de las cifras restantes la diferencia es un múltiplo de 13.
 - c) Demuestra que n es divisible por 17 si y sólo si al separar la cifra correspondiente a las unidades, multiplicarla por 5 y restarla de las cifras restantes la diferencia es un múltiplo de 17.
 - d) Demuestra que n es divisible por 19 si y sólo si al separar la cifra correspondiente a las unidades, multiplicarla por 2 y sumarla a las cifras restantes la suma es un múltiplo de 19.
 - e) Demuestra que n es divisible por 23 si y sólo si al separar la cifra correspondiente a las unidades, multiplicarla por 7 y sumarla a las cifras restantes la suma es un múltiplo de 23.
 - f) Demuestra que n es divisible por 11 si y sólo si la suma de las cifras en las posiciones pares menos la suma de las cifras en las posiciones impares es un múltiplo de 11.
2. Criterios de divisibilidad en otras bases.
 - a) Demuestra que n es divisible por 2 (resp. 3) si y sólo si su última cifra al escribirlo en base 6 es múltiplo de 2 (resp. 3).
 - b) Demuestra que para todo $k \in \mathbb{N}$, n es divisible por 2^k (resp. 3^k) si y sólo si sus k últimas cifras en base 6 forman un número divisible por 2^k (resp. 3^k).
 - c) Demuestra que n es divisible por 5 si y sólo si la suma de sus cifras en base 6 es divisible por 5.
 - d) Demuestra que n es divisible por 7 si y sólo si la suma de sus cifras (en base 6) en posiciones pares menos la suma de sus cifras en posiciones impares es divisible por 7.
 - e) Demuestra que n es divisible por 11 si y sólo si, en base 6, al separar la cifra correspondiente a las unidades, multiplicarla por 2 y sumarla a las cifras restantes la suma es un múltiplo de 11.
 - f) Encuentra un criterio de divisibilidad por n en base b , cuando $n|b$.
 - g) Encuentra un criterio de divisibilidad por n en base b , cuando $n|b - 1$.
 - h) Encuentra un criterio de divisibilidad por n en base b , cuando $n|b + 1$.
3. Sea $(\mathbb{Z}/n\mathbb{Z})^\times$ el subconjunto de los elementos invertibles (respecto a la multiplicación) de $\mathbb{Z}/n\mathbb{Z}$. Demuestra que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ es un grupo.
 - a) Calcula $(\mathbb{Z}/7\mathbb{Z})^\times$ e indique cuál es el inverso multiplicativo de cada uno de sus elementos.
 - b) Haz lo mismo con $(\mathbb{Z}/8\mathbb{Z})^\times$.
 - c) Calcula los inversos de 13 y -15 en $\mathbb{Z}/23\mathbb{Z}$ y $\mathbb{Z}/31\mathbb{Z}$.
 - d) Demuestra que la ecuación $13x = 2$ tiene solución única en $\mathbb{Z}/23\mathbb{Z}$. Indicar cuál es.
4. Sea $p \in \mathbb{N}$ un primo.
 - a) Demuestra que p divide al número combinatorio $\binom{p}{k}$ para cada valor de k con $1 \leq k \leq p - 1$.
 - b) Demuestra $a^p + b^p \equiv (a + b)^p \pmod{p}$.
 - c) ¿Es cierto alguno de los apartados anteriores si p no es primo?
5. Demuestra que existen infinitos naturales no representables como suma de tres cuadrados.

6. Demostrar que si $n > 1$ y $(n - 1)! + 1 \equiv 0 \pmod{n}$ entonces n es primo.

7. Escribe una sola congruencia que sea equivalente al sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{7}, \end{cases}$$

y resuélvela.

8. Probar que $n^7 - n$ es divisible entre 42, para cualquier entero n .

9. Probar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero para todo n .

10. Demuestra que $2222^{5555} + 5555^{2222}$ es divisible por 7.

11. Calcula el resto que queda al dividir 3^{2023} entre 11.

12. Resuelve los sistemas de congruencias:

$$a) \begin{cases} x \equiv -5 \pmod{77} \\ x \equiv 17 \pmod{143} \end{cases} \qquad b) \begin{cases} x \equiv 7 \pmod{8} \\ x \equiv 3 \pmod{12} \end{cases}$$

Sean $n, b \in \mathbb{N}$ con $b \neq 1$. Se dice que n es *pseudoprimo en base b* si es compuesto y $b^{n-1} \equiv 1 \pmod{n}$. Se dice que n es un *número de Carmichael* si n es un pseudoprimo en base b para todo b coprimo con n . Recientemente, se ha demostrado que existen infinitos números de Carmichael (Alford, Granville, Pomerance 1992).

13. Probar que 15 es un pseudo-primo en base 4, que 28 es un pseudo-primo en base 9 y que 91 es un pseudo-primo en base 3.

14. Sea $n \in \mathbb{N}$ impar compuesto y sea $\text{mcd}(b, n) = 1$.

a) Sea p un divisor primo de n y escribamos $n = pm$. Probar que si n es un pseudo-primo en base b entonces $b^{m-1} \equiv 1 \pmod{p}$.

b) Demostrar que ningún entero de la forma $n = 3p$, con $p > 3$ primo, puede ser un pseudo-primo en bases 2, 5 ni 7.

c) Demostrar que ningún entero de la forma $n = 5p$, con $p > 5$ primo, puede ser un pseudo-primo en bases 2, 3 ni 7.

d) Probar que 91 es el menor pseudo-primo (impar) en base 3.

15. Demostrar que no existen números de Carmichael pares, o sea, que para todo n par existe b tal que $\text{mcd}(b, n) = 1$ y $b^{n-1} \not\equiv 1 \pmod{n}$.

16. Demostrar que si n es un pseudo-primo en base 2, entonces $N = 2^n - 1$ también es un pseudo-primo en base 2. Esto demuestra que existen infinitos pseudo-primos en base 2 (esta construcción es de Malo 1903).