

Álgebra I

Práctica 4- Números enteros (Parte 2)

Ecuaciones diofánticas y de congruencia

1. Determinar, cuando existan, todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen

i) $5a + 8b = 3,$	iii) $24a + 14b = 7,$	v) $39a - 24b = 6,$
ii) $7a + 11b = 10,$	iv) $20a + 16b = 36,$	vi) $1555a - 300b = 11.$
2. Determinar todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen simultáneamente $4 \mid a, 8 \mid b$ y $33a + 9b = 120$.
3. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar con 135 pesos?
4. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia

i) $17X \equiv 3 \pmod{11},$	ii) $56X \equiv 28 \pmod{35},$	iii) $56X \equiv 2 \pmod{884},$	iv) $33X \equiv 27 \pmod{45}.$
------------------------------	--------------------------------	---------------------------------	--------------------------------
5. Determinar todos los $b \in \mathbb{Z}$ para los cuales existe $a \equiv 4 \pmod{5}$ tal que $6a + 21b = 15$.
6. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod{5}$ y $28a + 10b = 26$.
7. Hallar el resto de la división de un entero a por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.
8. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(7a + 1 : 5a + 4) \neq 1$.
9. Describir los valores de $(5a + 8 : 7a + 3)$ en función de los valores de $a \in \mathbb{Z}$.

Teorema chino del resto

10. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

$$\text{i) } \begin{cases} a \equiv 0 \pmod{8} \\ a \equiv 2 \pmod{5} \\ a \equiv 1 \pmod{21} \end{cases} \quad \text{ii) } \begin{cases} a \equiv 3 \pmod{10} \\ a \equiv 2 \pmod{7} \\ a \equiv 5 \pmod{9} \end{cases} \quad \text{iii) } \begin{cases} a \equiv 1 \pmod{6} \\ a \equiv 2 \pmod{20} \\ a \equiv 3 \pmod{9} \end{cases} \quad \text{iv) } \begin{cases} a \equiv 1 \pmod{12} \\ a \equiv 7 \pmod{10} \\ a \equiv 4 \pmod{9} \end{cases}$$

11. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

$$\text{i) } \begin{cases} 3a \equiv 4 \pmod{5} \\ 5a \equiv 4 \pmod{6} \\ 6a \equiv 2 \pmod{7} \end{cases} \quad \text{ii) } \begin{cases} 3a \equiv 1 \pmod{10} \\ 5a \equiv 3 \pmod{6} \\ 9a \equiv 1 \pmod{14} \end{cases} \quad \text{iii) } \begin{cases} 15a \equiv 10 \pmod{35} \\ 21a \equiv 15 \pmod{8} \\ 18a \equiv 24 \pmod{30} \end{cases}$$

12. i) Sabiendo que los restos de la división de un entero a por 3, 5 y 8 son 2, 3 y 5 respectivamente, hallar el resto de la división de a por 120.
 ii) Sabiendo que los restos de la división de un entero a por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de a por 480.
13. i) ¿Existe algún entero a cuyo resto en la división por 15 sea 2 y cuyo resto en la división por 18 sea 8?
 ii) ¿Existe algún entero a cuyo resto en la división por 15 sea 13 y cuyo resto en la división por 35 sea 22?
14. i) Hallar el menor entero positivo a tal que el resto de la división de a por 21 es 13 y el resto de la división de $6a$ por 15 es 9.
 ii) Hallar un entero a entre 60 y 90 tal que el resto de la división de $2a$ por 3 es 1 y el resto de la división de $7a$ por 10 es 8.

Pequeño teorema de Fermat

15. Hallar el resto de la división de a por p en los casos

i) $a = 33^{1427}$, $p = 5$,

ii) $a = 71^{22283}$, $p = 11$,

iii) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$.

16. Resolver en \mathbb{Z} las ecuaciones de congruencia

i) $7^{13}X \equiv 5 \pmod{11}$,

ii) $2^{194}X \equiv 7 \pmod{97}$.

17. Probar que para todo $a \in \mathbb{Z}$ vale

i) $728 \mid a^{27} - a^3$,

ii) $\frac{2a^7}{35} + \frac{a}{7} - \frac{a^3}{5} \in \mathbb{Z}$.

18. Probar que para todo $a \in \mathbb{Z}$ tal que $(a : 561) = 1$ vale $a^{560} \equiv 1 \pmod{561}$.

Los números $n \in \mathbb{N}$ que sin ser primos verifican que si a es un entero coprimo con n , entonces $a^{n-1} \equiv 1 \pmod{n}$ se llaman *seudoprimos* o *números de Carmichael*.

19. Resolver en \mathbb{Z} los siguientes sistemas lineales de ecuaciones de congruencia

i)
$$\begin{cases} 2^{2013}X \equiv 6 \pmod{13} \\ 5^{2013}X \equiv 4 \pmod{7} \\ 7^{2013}X \equiv 2 \pmod{5} \end{cases},$$

ii)
$$\begin{cases} 10^{49}X \equiv 17 \pmod{39} \\ 5X \equiv 7 \pmod{9} \end{cases}.$$

20. Hallar el resto de la división de

i) $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70,

ii) 3^{385} por 400,

iii) $\sum_{i=1}^{1759} i^{42}$ por 56.

21. Hallar todos los $a \in \mathbb{Z}$ tales que

i) $539 \mid 3^{253}a + 5^{44}$,

ii) $a^{236} \equiv 6 \pmod{19}$.

22. Hallar el resto de la división de 2^{2^n} por 13 para cada $n \in \mathbb{N}$.

23. Resolver en \mathbb{Z} la ecuación de congruencia $7X^{45} \equiv 1 \pmod{46}$.

24. Hallar todos los divisores positivos de 25^{70} que sean congruentes a 2 módulo 9 y a 3 módulo 11.

El anillo $\mathbb{Z}/m\mathbb{Z}$

25. Escribir las tablas de suma y producto en $\mathbb{Z}/m\mathbb{Z}$ para $m = 5, 6, 7$ y 8 . ¿Cuáles de estos anillos son cuerpos?

26. Un elemento $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ es un *cuadrado* (en $\mathbb{Z}/m\mathbb{Z}$) si existe $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\bar{a} = \bar{b}^2$ en $\mathbb{Z}/m\mathbb{Z}$.

i) Calcular los cuadrados de $\mathbb{Z}/m\mathbb{Z}$ para $m = 2, 3, 4, 5, 6, 7, 8, 9, 11$ y 13 . ¿Cuántos hay en cada caso?

ii) Probar que si $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ son cuadrados, entonces $\bar{a} \cdot \bar{b}$ también es un cuadrado.

iii) Probar que si \bar{a} es un elemento inversible de $\mathbb{Z}/m\mathbb{Z}$ tal que $\bar{a} = \bar{b}^2$, entonces \bar{b} es inversible en $\mathbb{Z}/m\mathbb{Z}$ y \bar{a}^{-1} es un cuadrado.

- iv) Sea p un primo positivo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\bar{a}^2 = \bar{b}^2$ entonces $\bar{a} = \bar{b}$ ó $\bar{a} = -\bar{b}$. Deducir que si p es impar, entonces hay exactamente $\frac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.
27. Sea p un primo. Probar que en $\mathbb{Z}/p\mathbb{Z}$ vale que $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$, $\forall \bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ (sug: ver Ej. 29 Práctica 3). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?
28. Sea $n \in \mathbb{N}$ distinto de 1.
- Probar que si n es compuesto y distinto de 4, entonces $(n-1)! \equiv 0 \pmod{n}$. ¿Qué pasa para $n = 4$?
 - Sea p un primo positivo. Probar que $\bar{a} = \bar{a}^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\bar{a} = \pm \bar{1}$. Deducir que $(p-1)! \equiv -1 \pmod{p}$. (Sugerencia: calcular $(p-1)!$ en $\mathbb{Z}/p\mathbb{Z}$ agrupando los factores distintos de $\bar{1}$ y $\overline{p-1} = -\bar{1}$ de a pares: \bar{a} con \bar{a}^{-1}).
 - Deducir que $(n-1)! \equiv -1 \pmod{n} \iff n$ es primo (*Teorema de Wilson*).
- 29.
- Describir el conjunto $\{\bar{3}^n; n \in \mathbb{N}\}$ en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/11\mathbb{Z}$. Observar la diferencia que hay en el primer caso con respecto al segundo caso, y hallar si se puede un elemento $\bar{a} \in \mathbb{Z}/11\mathbb{Z}$ que cumpla que $\{\bar{a}^n; n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\bar{0}\}$.
 - Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1 \pmod{7}$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 4 \pmod{7}$.
 - Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1 \pmod{11}$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 9 \pmod{11}$.
 - Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53 \pmod{77}$.
30. Sea p un primo positivo y sea $\bar{g} \in \mathbb{Z}/p\mathbb{Z}$ tal que $\{\bar{g}^k; 0 \leq k < p-1\} = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$.
- Probar que $g^n \equiv 1 \pmod{p} \iff (p-1) \mid n$. Deducir que si $\bar{g}^k = \bar{a} \in \mathbb{Z}/p\mathbb{Z}$ con $0 \leq k < p-1$, entonces $g^n \equiv a \pmod{p} \iff n \equiv k \pmod{p-1}$.
 - Dado $\bar{a} \in \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$, se llama el *logaritmo discreto* de a (en base g módulo p) y se nota $k = \log_g(a) \pmod{p}$ al entero k con $0 \leq k < p-1$ tal que $\bar{g}^k = \bar{a}$ en $\mathbb{Z}/p\mathbb{Z}$. Calcular $\log_3(4) \pmod{7}$, $\log_3(5) \pmod{7}$ y $\log_3(12) \pmod{17}$.