Álgebra I
Práctica 5 - Números enteros (Parte 2)

Ecuaciones diofánticas y de congruencia

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

i) $5a + 8b = 3$
ii) $7a + 11b = 10$
iii) $24a + 14b = 7$
iv) $20a + 16b = 36$
v) $39a - 24b = 6$
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) $17X \equiv 3\ (11)$ ii) $56X \equiv 28\ (35)$ iii) $56X \equiv 2\ (884)$ iv) $33X \equiv 27\ (45)$

5. Determinar todos los $b \in \mathbb{Z}$ para los cuales existe $a \equiv 4\ (5)$ 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.
i) ¿Existe algún entero a cuyo resto en la división por 15 sea 13 y cuyo resto en la división por 35 sea 22?
ii) ¿Existe algún entero a cuyo resto en la división por 15 sea 2 y cuyo resto en la división por 18 sea 8?

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

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

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

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

13.
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.

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) $7^{13}X \equiv 5\ (11)$

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

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

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

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

18. *Seudoprimos o números de Carmichael (Robert Carmichael, 1879-1967, matemático estadounidense).* Se dice que $n \in \mathbb{Z}$ es un número de Carmichael si satisface el pequeño Teorema de Fermat sin ser primo, es decir, si a es un entero coprimo con n, entonces $a^{n-1} \equiv 1 \pmod{n}$. Probar que 561 es un número de Carmichael. En 1994 se probó finalmente que hay infinitos números de Carmichael, luego de que esta conjetura quedara abierta por muchos años.

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

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

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

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

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

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

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

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 $7\,X^{45} \equiv 1 \pmod{46}$.

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 $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ es un *cuadrado* (en $\mathbb{Z}/m\mathbb{Z}$) si existe $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$ 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 $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ son cuadrados, entonces $\overline{a} \cdot \overline{b}$ es un cuadrado también.

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

iv) Sea p primo positivo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\overline{a}^2 = \overline{b}^2$ entonces $\overline{a} = \overline{b}$ ó $\overline{a} = -\overline{b}$. Deducir que si p es impar, entonces hay exactamente $\dfrac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.

27. Sea p un primo. Probar que en $\mathbb{Z}/p\mathbb{Z}$ vale que $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ (sug: ver Ej. 26 Práctica 3). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?

28. *Test de primalidad de Wilson,* por el mátemático inglés John Wilson, 1741-1793. Este test era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matemático italiano Joseph-Louis Lagrange en 1771. Dice que si $n \in \mathbb{N}$ es distinto de 1, entonces

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ es primo .}$$

i) Probar que si $n \geq 5$ es compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$. ¿Qué implicación se prueba con esto?

ii) Sea p un primo positivo. Se recuerda que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Probar que $\overline{a} = \overline{a}^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\overline{a} = \pm\overline{1}$. Deducir que $(p-1)! \equiv -1 \pmod{p}$.

29. i) Describir el conjunto $\{\overline{3}^n;\ n \in \mathbb{N}\}$ 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 $\overline{a} \in \mathbb{Z}/11\mathbb{Z}$ que cumpla que $\{\overline{a}^n;\ n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\overline{0}\}$.

ii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (7)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 4\ (7)$.

iii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (11)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 9\ (11)$.

iv) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53\ (77)$.