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) $7a + 11b = 10$ ii) $20a + 16b = 36$ iii) $39a - 24b = 6$ iv) $1555a - 300b = 11$

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 gastando exactamente 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) $78X \equiv 30\ (12126)$

5. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.

6. 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.

7. Hallar todas las soluciones $(x, y) \in \mathbb{Z}^2$ de la ecuación

   $$110x + 250y = 100$$

   que satisfacen simultáneamente que $37^2 \mid (x - y)^{4321}$.

8. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(2a - 3 : 4a^2 + 10a - 10) \neq 1$.

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:

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

11. 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) $\begin{cases} 15\,a \equiv 10 & (35) \\ 21\,a \equiv 15 & (8) \\ 18\,a \equiv 24 & (30) \end{cases}$

12. i) 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.

    ii) 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.

13. En un depósito se almacenan latas de gaseosa. El viernes por la noche, un empleado realizó un control de inventario y observó que:

    - Al poner las latas en cajas de 12 unidades sobraban 4.
    - Al poner las latas en cajas de 63 unidades sobraban 43.
    - Había por lo menos 12.600 latas y no más de 13.000, pero no tomó nota de la cantidad exacta.

    ¿Cuántas latas de gaseosa había en el depósito el viernes por la noche?

14. Hallar los posibles restos de dividir a un entero a por 238 sabiendo que $a^2 \equiv 21\ (238)$.

Pequeño Teorema de Fermat

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

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

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

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

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

    ii) $5^{86}X \equiv 3\ (89)$

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. Sea $a \in \mathbb{Z}$ coprimo con 561. Probar que $a^{560} \equiv 1\ (561)$.
    (Un número $n \in \mathbb{N}$ se dice un *seudoprimo o número de Carmichael* si satisface el Pequeño Teorema de Fermat sin ser primo, es decir, si a es un entero coprimo con n, entonces $a^{n-1} \equiv 1 \pmod{n}$. Estos números se llaman así por Robert Carmichael, matemático estadounidense, 1879-1967. En 1994 se probó finalmente que hay infinitos números de Carmichael).

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

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

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

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

24. Hallar todos los primos $p \in \mathbb{N}$ que satisfacen:

    i) $2p \mid 38^{2p^2-p-1} + 3p + 171$

    ii) $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

25. Hallar los posibles restos de dividir a un entero a por 44 sabiendo que $(a^{760} + 11a + 10 : 88) = 2$.

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

26. Escribir las tablas de suma y producto en $\mathbb{Z}/m\mathbb{Z}$ para $m = 5$ y 8. ¿Alguno de estos anillos es un cuerpo?

27. 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 en $\mathbb{Z}/m\mathbb{Z}$ para $m = 2$, 3, 4, 9 y 11. ¿Cuántos hay en cada caso?

    ii) Sea $p \in \mathbb{N}$ primo. 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 $\mathbb{Z}/p\mathbb{Z}$.

28. 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 $\{\overline{a}^n : n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\overline{0}\}$.

29. 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. 25 Práctica 4). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?

30. *Test de Primalidad de Wilson:*
    El objetivo de este ejercicio es probar que si $n \in \mathbb{N}$ es distinto de 1, entonces

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

    i) Verificar que $3! \not\equiv -1\,(4)$ y 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 $(p-1)! \equiv -1 \pmod{p}$.

    (Este test de primalidad debe su nombre al matemático inglés John Wilson, 1741-1793, pero era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matemático italiano Joseph-Louis Lagrange en 1771).