

## 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:

i)  $\begin{cases} a \equiv 0 \pmod{8} \\ a \equiv 2 \pmod{5} \\ a \equiv 1 \pmod{21} \end{cases}$

ii)  $\begin{cases} a \equiv 3 \pmod{10} \\ a \equiv 2 \pmod{7} \\ a \equiv 5 \pmod{9} \end{cases}$

iii)  $\begin{cases} a \equiv 1 \pmod{6} \\ a \equiv 2 \pmod{20} \\ a \equiv 3 \pmod{9} \end{cases}$

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:

i)  $\begin{cases} 3a \equiv 4 \pmod{5} \\ 5a \equiv 4 \pmod{6} \\ 6a \equiv 2 \pmod{7} \end{cases}$

ii)  $\begin{cases} 3a \equiv 1 \pmod{10} \\ 5a \equiv 3 \pmod{6} \\ 9a \equiv 1 \pmod{14} \end{cases}$

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

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.

25. *La función  $\varphi$  de Euler* (por el matemático suizo Leonhard Euler, 1707-1783, quién introdujo esta función en 1760) es la función  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definida como

$$\varphi(n) = \#\{m \in \mathbb{N} : m \leq n \text{ y } (m : n) = 1\},$$

es decir  $\varphi(n)$  cuenta la cantidad de números menores (o iguales) que  $n$  que son coprimos con  $n$ . Por ejemplo  $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \dots$

i) Sea  $p$  un primo. Probar que  $\varphi(p) = p - 1$  y que  $\varphi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}$ ,  $\forall k \in \mathbb{N}$ .

ii) Sean  $p$  y  $q$  dos primos distintos. Probar que  $\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1)$ .

iii) Probar que si  $n = pq$  con  $p$  y  $q$  primos desconocidos, y uno además de  $n$  conoce  $\varphi(n)$  entonces puede recuperar con facilidad quiénes son  $p$  y  $q$ .

*Nota:* Resulta que la función  $\varphi$  también cumple que  $\varphi(mn) = \varphi(m)\varphi(n)$  si  $m, n \in \mathbb{N}$  son coprimos (se puede probar por ejemplo usando el Teorema Chino del Resto). Esto permite calcular  $\varphi(n)$ ,  $\forall n \in \mathbb{N}$ , dada la factorización de  $n$  en números primos!

$$\text{Si } n = p_1^{k_1} \cdots p_r^{k_r}, \text{ entonces } \varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}) = (p_1 - 1)p_1^{k_1-1} \cdots (p_r - 1)p_r^{k_r-1}.$$

Nadie sabe hasta la fecha calcular  $\varphi(n)$  en general de una forma más económica que utilizando la factorización. Esto es un factor esencial del que depende la seguridad del sistema criptográfico RSA!

### 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  $\mathbb{Z}/m\mathbb{Z}$ .
- 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?
  - Probar que si  $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$  son cuadrados, entonces  $\bar{a} \cdot \bar{b}$  es un cuadrado también.
  - 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 también en  $\mathbb{Z}/m\mathbb{Z}$  y  $\bar{a}^{-1}$  es un cuadrado también.
  - Sea  $p$  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.** *Test de primalidad de Wilson*, por el matemático 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

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

- Probar que si  $n$  es compuesto, entonces  $(n-1)! \equiv 0 \pmod{n}$ . ¿Qué implicación se prueba con esto?
  - Sea  $p$  un primo positivo. Se recuerda que  $\mathbb{Z}/p\mathbb{Z}$  es un cuerpo. Probar que  $\bar{a} = \bar{a}^{-1}$  en  $\mathbb{Z}/p\mathbb{Z}$  si y solo si  $\bar{a} = \pm \bar{1}$ . Deducir que  $(p-1)! \equiv -1 \pmod{p}$ .
- 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.** *El problema del logaritmo discreto.* Sea  $p$  un número primo y sea  $\bar{g} \in \mathbb{Z}/p\mathbb{Z}$  tal que

$$\{\bar{g}^k; 0 \leq k < p-1\} = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$$

(se puede probar que un tal  $\bar{g}$  siempre existe, se llama *generador* de  $\mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$ , c.f. por ejemplo Ej. 29(i)): para  $p = 7$  se puede tomar  $\bar{g} = \bar{3}$ . ¿Quién se puede elegir para  $p = 11$ ?

- Probar que si  $\bar{g}^k = \bar{a} \in \mathbb{Z}/p\mathbb{Z}$  con  $0 \leq k < p-1$ , entonces  $g^n \equiv a \pmod{p} \iff n \equiv k \pmod{p-1}$ .

- ii) Dado  $\bar{a} \in \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$ , el problema del logaritmo discreto consiste en determinar cuál es el  $k$  con  $0 \leq k < p - 1$  tal que  $\bar{g}^k = \bar{a}$  en  $\mathbb{Z}/p\mathbb{Z}$ . Ese  $k$  siempre existe por ser  $\bar{g}$  un generador. En ese caso,  $k$  se llama el *logaritmo discreto* de  $a$  (en base  $g$  módulo  $p$ ) y se nota

$$k = \log_g(a) \pmod{p}.$$

O sea  $k = \log_g(a) \pmod{p} \Leftrightarrow 0 \leq k < p - 1$  y  $g^k \equiv a \pmod{p}$ .

Calcular  $\log_3(4) \pmod{7}$ ,  $\log_3(5) \pmod{7}$  y  $\log_3(12) \pmod{17}$ .

- iii) Para el taller: armar un programa que calcule  $\log_g(a) \pmod{p}$  dados  $p$  primo,  $g$  generador de  $\mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$  y  $a$ . No se conoce ningún algoritmo eficiente para calcular logaritmos discretos en general: un importante problema abierto es ¿Existe un algoritmo polinomial para calcular el logaritmo discreto en una computadora clásica? (donde esto significa que la cantidad de operaciones "bit" que realiza el algoritmo tiene que ser a lo sumo polinomial en la cantidad de bits del primo  $p$ ).

**31.** *El algoritmo de intercambio de clave de Diffie-Hellman, 1976.* Este es un algoritmo para que dos personas Alice y Bob, puedan intercambiar una clave secreta sin que ningún espía pueda determinar cuál es, aún oyendo las comunicaciones entre Alice y Bob. Se basa en lo difícil que es calcular el logaritmo discreto de un número módulo un primo  $p$  (se usan primos de 300 dígitos al menos).

- i) Alice y Bob concuerdan públicamente en un primo  $p$  (grande) y en  $g \in \mathbb{Z}$  tal que

$$\{\bar{g}^k; 0 \leq k < p - 1\} = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$$

(hay algoritmos que calculan un tal  $g$  en forma más rápida que intentar con todos los elementos de  $\mathbb{Z}/p\mathbb{Z}$ ).

Por ejemplo para fijar ideas  $p = 23$  y  $g = 5$ .

- ii) Alice elije secretamente un número  $k$ , y le manda públicamente a Bob el número  $\bar{A} = \bar{g}^k$  en  $\mathbb{Z}/p\mathbb{Z}$ , y Bob elije secretamente un número  $j$ , y le manda públicamente a Alice el número  $\bar{B} = \bar{g}^j$  en  $\mathbb{Z}/p\mathbb{Z}$ . Por ejemplo si Alice elije el 6 y Bob elije el 15, se tiene  $\bar{A} = \bar{5}^6 = \bar{8}$ , y  $\bar{B} = \bar{5}^{15} = \bar{19}$  en  $\mathbb{Z}/23\mathbb{Z}$ .
- iii) Alice calcula  $\bar{B}^k$  y Bob calcula  $\bar{A}^j$  en  $\mathbb{Z}/p\mathbb{Z}$ , y resulta que estos dan el mismo elemento  $\bar{s} \in \mathbb{Z}/p\mathbb{Z}$ , con  $1 \leq s \leq p - 1$ . Tal  $s$  es la clave secreta que Alice y Bob compartirán. Aquí  $\bar{19}^6 = \bar{2} = \bar{8}^{15}$  en  $\mathbb{Z}/23\mathbb{Z}$ , o sea  $s = 2$ .

Justificar por qué siempre da el mismo  $s$ , y explicar por qué con los datos  $p$ ,  $g$ ,  $\bar{A}$  y  $\bar{B}$  un espía no puede encontrar  $s$  fácilmente.