3. ARITMÉTICA MODULAR

3.1. Congruencias de números enteros

Definición de congruencia
Dado un número entero fijo $p > 1$ y dos números enteros cualesquiera $a, b \in \mathbb{Z}$, se dice que a es **congruente con** b **módulo** p, y se indica $a \equiv b \pmod{p}$, si $p \mid (a - b)$.
Es fácil ver que $a \equiv b \pmod{p}$ si y sólo si coinciden los restos de dividir los números a y b por p, que se llaman **residuos módulo** p. En módulo p los posibles residuos son: 0, 1, 2, ..., $p - 1$.

Propiedades
La relación de congruencia módulo $p > 1$ verifica las siguientes propiedades:

1. Reflexiva: $a \equiv b \pmod{p}$, para todo $a \in \mathbb{Z}$.
2. Simétrica: $a \equiv b \pmod{p} \implies b \equiv a \pmod{p}$.
3. Transitiva: $a \equiv b \pmod{p}$ y $b \equiv c \pmod{p} \implies a \equiv c \pmod{p}$.

Por verificar estas tres propiedades, se dice que la relación de congruencia es una relación de equivalencia.

Relación de equivalencia
Se llama **relación de equivalencia** sobre un conjunto A a cualquier relación R entre sus elementos que verifica las siguientes tres propiedades:

1. Reflexiva: aRa, para cualquier $a \in A$.
2. Antisimétrica: si aRb entonces bRa.
3. Transitiva: si aRb y bRc, entonces aRc.

Una relación de equivalencia R sobre un conjunto A produce una partición del conjunto en subconjuntos disjuntos, llamados **clases de equivalencia**, cada uno de ellos formados por elementos que están relacionados entre sí. Esta partición se representa por A/R y se llama **conjunto cociente**.

El conjunto $\mathbb{Z}_p$
Cada clase del conjunto cociente de $\mathbb{Z}$ por la relación de congruencia módulo p está formada por todos los números enteros con el mismo residuo módulo p. Puesto que hay p posibles residuos habrá p clases distintas, cada una de ellas asociada a un residuo r, $0 \leq r \leq p - 1$, y que se representa por $[r]_p$, $\overline{r}_p$ ó $\overline{r}$ si no hay lugar a error. El conjunto de todas las clases se representa por $\mathbb{Z}_p$, es decir:

$$\mathbb{Z}_p = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\right\} \quad \text{donde} \quad \overline{r} = \{a \in \mathbb{Z} : a \equiv r \pmod{p}\} = \{np + r : n \in \mathbb{Z}\}$$

Ejercicios

1. Estudia si son ciertas las siguientes congruencias:
   (a) $2 \equiv 4 \pmod{2}$; **(b)** $13 \equiv -2 \pmod{5}$; **(c)** $15 \equiv 3 \pmod{3}$; **(d)** $20 \equiv 4 \pmod{7}$.
2. Describe los conjuntos $\mathbb{Z}_2$ y $\mathbb{Z}_5$.
3. Demuestra que si $n \geq 5$ es primo, entonces $n \equiv 1 \pmod{6}$ ó $n \equiv 5 \pmod{6}$, es decir, $n \in \overline{1}_6$ ó $n \in \overline{5}_6$.

Soluciones y/o sugerencia a los ejercicios
1. **(a)** Cierta; **(b)** Cierta; **(c)** Cierta; **(d)** No es cierta.
2. $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$, $\mathbb{Z}_5 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$.
3. Prueba que los número congruentes con 0, 2, 3 y 4 no son primos.

3. ARITMÉTICA MODULAR

3.2. Residuos de operaciones aritméticas

Residuos de operaciones aritméticas
Dado un número entero $p > 1$, si $a \equiv \alpha \pmod{p}$ y $b \equiv \beta \pmod{p}$, entonces:

$$(a+b) \equiv (\alpha+\beta) \pmod{p} \qquad ab \equiv \alpha\beta \pmod{p} \qquad a^b \equiv \alpha^b \pmod{p}$$

¡Ojo!: No es cierto, en general, que $a^b \equiv \alpha^\beta \pmod{p}$.

Simplificación de congruencias de productos

- Si $\mathrm{mcd}(c,p) = 1$ entonces: $ac \equiv bc \pmod{p} \implies a \equiv b \pmod{p}$
- En general: $ac \equiv bc \pmod{p} \implies a \equiv b \pmod{\frac{p}{\mathrm{mcd}(c,p)}}$

Criterios de divisibilidad
Si $n = a_k a_{k-1} \dots a_2 a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$, con $0 \le a_i \le 9$, entonces:

- n es divisible por 2 si y sólo si a_0 es divisible por 2.
- n es divisible por 3 si y sólo si $\sum_{i=0}^{k} a_i$ es divisible por 3.
- n es divisible por 4 si y sólo si $a_1 a_0 = 10a_1 + a_0$ es divisible por 4 ($\iff$ $2a_1 + a_0$ es divisible por 4).
- n es divisible por 5 si y sólo si a_0 es divisible por 5 ($\iff$ $a_0 = 0$ ó $a_0 = 5$).
- n es divisible por 9 si y sólo si $\sum_{i=0}^{k} a_i$ es divisible por 9.
- n es divisible por 11 si y sólo si $\sum_{i=0}^{k} (-1)^i a_i$ es divisible por 11.

Regla del nueve
El producto de números naturales debe verificar la siguiente regla, conocida como **regla del nueve**:

$$\begin{cases} n = a_k a_{k-1} \dots a_2 a_1 a_0 = \sum_{i=0}^{k} a_i 10^i \ , \ \text{ con } 0 \le a_i \le 9 \\ m = b_l b_{l-1} \dots b_2 b_1 b_0 = \sum_{i=0}^{l} b_i 10^i \ , \ \text{ con } 0 \le b_i \le 9 \end{cases} \implies n \cdot m \equiv \sum_{i=0}^{k} a_i \cdot \sum_{i=0}^{l} b_i \pmod{9}$$

Ejercicios

1. Halla el residuo módulo 7 del resultado de las siguientes operaciones sin realizarlas:
   (a) $2419 + 987$; **(b)** $2345 + 214 \cdot 432$.
2. Comprueba si $N = 1213141516171819$ y $M = 192837465564738291$ son divisibles por 11.
3. ¿Qué cifra falta en la igualdad $14! = 871782\_1200$?
4. Usa la regla del nueve para qué dos de las siguientes operaciones son falsas. ¿Qué se puede decir de la otra?
   (a) $5783 \cdot 40162 = 233256846$; **(b)** $9787 \cdot 1258 = 12342046$; **(c)** $8901 \cdot 5743 = 52018443$.
5. ¿Qué dígito falta en la operación: $7987354243 \cdot 9284576563 = 741592020049\_6406809$?

Soluciones y/o sugerencia a los ejercicios
1. **(a)** 4; **(b)** 6.
2. N no y M si.
3. 9.
4. **(a)** Falsa; **(b)** Falsa; **(c)** La regla del nueve no implica falsedad, luego puede estar bien.
5. 3.

3. ARITMÉTICA MODULAR

3.3. Aritmética en $\mathbb{Z}_p$

Operaciones en $\mathbb{Z}_p$

La compatibilidad de la congruencia con la suma y el producto de números enteros permite definir en $\mathbb{Z}_p$ las operaciones suma y producto, para cada $0 \leq a, b < p$, como:

$$\textbf{Suma: } \overline{a} + \overline{b} = \overline{a+b} \qquad\qquad \textbf{Producto: } \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Divisores de cero

Se llaman **divisores de cero** a cualesquiera $\overline{a}, \overline{b} \in \mathbb{Z}_p$, con $\overline{a} \neq \overline{0} \neq \overline{b}$, tales que $\overline{a} \cdot \overline{b} = \overline{0}$. Es fácil ver que:

$$\text{Existen divisores de cero en } \mathbb{Z}_p \iff p \text{ no es primo (es compuesto)}$$

Elementos inversibles

Se dice que $\overline{a} \in \mathbb{Z}_p$ es un **elemento inversible** ó **unidad** si existe $\overline{b} \in \mathbb{Z}_p$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, y se indica $\overline{a}^{-1} = \overline{b}$ y a^{-1} para referirse a cualquier elemento de la clase.
Es fácil ver que para cualquier $p > 1$ existen elementos inversibles. Se representa por U_p al conjunto de todos los elementos inversibles de $\mathbb{Z}_p$.

Estructura de U_p

- $\overline{a} \in U_p \iff \text{mcd}(a, p) = 1$
  En consecuencia, si p es primo: $U_p = \mathbb{Z}_p - \{\overline{0}\}$.
- Si $\overline{a}, \overline{b} \in U_p$ entonces: $\overline{a} \cdot \overline{b} \in U_p$, $\overline{a}^{-1} \in U_p$, y $\overline{a} \cdot U_p = U_p$.

Ejercicios

1. Construye las tablas de sumar y multiplicar en $\mathbb{Z}_2$, $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

2. Halla los divisores de cero y los elementos inversibles en $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ y $\mathbb{Z}_{15}$.

3. Halla los siguientes inversos:
(a) de $\overline{6}$ en $\mathbb{Z}_{17}$; **(b)** de $\overline{3}$ en $\mathbb{Z}_{10}$; **(c)** de $\overline{5}$ en $\mathbb{Z}_{12}$; **(d)** de $\overline{7}$ en $\mathbb{Z}_{16}$; **(e)** de $\overline{5}$ en $\mathbb{Z}_{13}$; **(f)** de $\overline{777}$ en $\mathbb{Z}_{1009}$.

4. **(a)** Demuestra que todos los elementos de $\mathbb{Z}_{11} - \{\overline{0}\}$, excepto $\overline{1}$ y $\overline{10}$, se pueden agrupar de dos en dos de manera que cada uno de ellos es el inverso del otro.
(b) Demuestra que $10! \equiv -1 \pmod{11}$.
(c) Demuestra que si p es primo los únicos elementos de $\mathbb{Z}_p$ que coinciden con su inverso son $\overline{1}$ y $\overline{p-1}$.
(d) Demuestra que si p es primo entonces $(p-1)! \equiv -1 \pmod{p}$ (Teorema de Wilson, 1770).
(e) Halla, sin calculadora, el resto de dividir $15!$ por 17.

Soluciones y/o sugerencia a los ejercicios

1. Las tablas que se obtienen al sumar y multiplicar todos sus elementos entre sí.

2. $\mathbb{Z}_6 : \begin{cases} \text{Divisores de cero: } \overline{2} \text{ y } \overline{3},\ \overline{3} \text{ y } \overline{4}. \\ \text{Inversibles: } \overline{1}^{-1} = \overline{1},\ \overline{5}^{-1} = \overline{5}. \end{cases}$; $\mathbb{Z}_8 : \begin{cases} \text{Divisores de cero: } \overline{2} \text{ y } \overline{4},\ \overline{4} \text{ y } \overline{4},\ \overline{4} \text{ y } \overline{6}. \\ \text{Inversibles: } \overline{1}^{-1} = \overline{1},\ \overline{3}^{-1} = \overline{3},\ \overline{5}^{-1} = \overline{5},\ \overline{7}^{-1} = \overline{7}. \end{cases}$;

$\mathbb{Z}_7 : \begin{cases} \text{Divisores de cero: no hay.} \\ \text{Inversibles: } \overline{1}^{-1} = \overline{1},\ \overline{2}^{-1} = \overline{4},\ \overline{3}^{-1} = \overline{5},\ \overline{4}^{-1} = \overline{2},\ \overline{5}^{-1} = \overline{3},\ \overline{6}^{-1} = \overline{6}. \end{cases}$;

$\mathbb{Z}_{15} : \begin{cases} \text{Divisores de cero: } \overline{3} \text{ y } \overline{5},\ \overline{3} \text{ y } \overline{10},\ \overline{5} \text{ y } \overline{6},\ \overline{5} \text{ y } \overline{9},\ \overline{5} \text{ y } \overline{12},\ \overline{6} \text{ y } \overline{10},\ \overline{9} \text{ y } \overline{10},\ \overline{10} \text{ y } \overline{12}. \\ \text{Inversibles: } \overline{1}^{-1} = \overline{1},\ \overline{2}^{-1} = \overline{8},\ \overline{4}^{-1} = \overline{4},\ \overline{7}^{-1} = \overline{13},\ \overline{8}^{-1} = \overline{2},\ \overline{11}^{-1} = \overline{11},\ \overline{13}^{-1} = \overline{7},\ \overline{14}^{-1} = \overline{14}. \end{cases}$.

3. **(a)** $\overline{3}$; **(b)** $\overline{7}$; **(c)** $\overline{5}$; **(d)** $\overline{7}$; **(e)** $\overline{8}$; **(f)** $\overline{735}$.

4. **(a)** Se hallan los inversos de todos y se agrupan. **(b)** Usa las agrupaciones obtenidas en el apartado anterior. **(c)** Se impone la condición de que un elemento coincide con su inverso. **(d)** Utiliza en mismo argumento que en (b). **(e)** Utiliza el teorema de Wilson.

3. ARITMÉTICA MODULAR

3.4. Residuos de potencias

Cálculo residuos de potencias
Para calcular el residuo de $x = 233^{46}$ módulo 22 se puede proceder como sigue:

1. En primer lugar, puesto que $233 \equiv 13 \pmod{22}$: $x = 233^{46} \equiv 13^{46} \pmod{22}$.
2. Se expresa el exponente en base 2: $46 = 101110_2 = 2^5 + 2^3 + 2^2 + 2^1 = 2 + 4 + 8 + 32$.
3. Se calcula el residuo de la potencia a partir de los residuos que tienen por exponente las potencias de 2:

$$\begin{cases} 13^2 = 169 \equiv 15 \pmod{22} \\ 13^4 = \left(13^2\right)^2 \equiv 15^2 = 225 \equiv 5 \pmod{22} \\ 13^8 = \left(13^4\right)^2 \equiv 5^2 = 25 \equiv 3 \pmod{22} \\ 13^{16} = \left(13^8\right)^2 \equiv 3^2 = 9 \equiv 9 \pmod{22} \\ 13^{32} = \left(13^{16}\right)^2 \equiv 9^2 = 81 \equiv 15 \pmod{22} \end{cases} \implies 13^{46} = 13^2 13^4 13^8 13^{32} \equiv 15{\cdot}5{\cdot}3{\cdot}15 = 3375 \equiv 9 \pmod{22}$$

4. El residuo de la potencia pedida es: $x = 233^{46} \equiv 9 \pmod{22}$.

Función de Euler
Para cada número natural n, se define la función de Euler $\Phi(n)$ como el número de naturales menores que n relativamente primos con n, es decir:

$$\Phi(n) = |\{x \in \mathbb{N} \,:\, 1 \leq x \leq n \text{ y } \operatorname{mcd}(x, n) = 1\}|$$

donde $|A|$ es el cardinal o número de elementos del conjunto A. Para los primeros números naturales, la función de Euler es:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Propiedades

1. Para cualquier número entero $p > 1$: $\Phi(p) = |U_p|$.
2. Si p es primo, entonces: $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3. Si $\operatorname{mcd}(a, b) = 1$, entonces: $\Phi(ab) = \Phi(a)\Phi(b)$.
4. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, con cada p_i primo, entonces: $\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$.

Teorema de Euler
Si $\operatorname{mcd}(a, p) = 1$, entonces: $a^{\Phi(p)} \equiv 1 \pmod{p}$.

Teorema de Fermat
Si p es primo y no es divisor a, entonces: $a^{p-1} \equiv 1 \pmod{p}$.

Ejercicios

1. Calcula el último dígito de las siguientes potencias: 6^{20}, 7^{93} y 23^{189}.
2. Calcula el resto de de las siguientes divisiones:
   (a) $7^{512} : 11$; **(b)** $3^{47} : 23$; **(c)** $3^{15} : 17$; **(d)** $125^{4577} : 13$; **(e)** $11^{954} : 20$; **(f)** $\left(140^{1221} + 28^{753}\right) : 13$.
3. Calcula el residuo de 84^{1234} en los módulos 2, 5 y 7.

4. Comprueba que $2^{340} \equiv 1 \pmod{11}$ y $2^{340} \equiv 1 \pmod{31}$, y concluye que $2^{340} \equiv 1 \pmod{341}$.

5. Realiza en $\mathbb{Z}_{203}$ la siguiente operación: $\overline{5} + \overline{5} \cdot \overline{4}^{169} \cdot \overline{17}^{-1}$.

6. Demuestra que para cualquier $n \in \mathbb{Z}$ las últimas cifras de n y n^5 son iguales.

Soluciones y/o sugerencia a los ejercicios
1. 6, 7 y 3.
2. **(a)** 5; **(b)** 4; **(c)** 6; **(d)** 8; **(e)** 1; **(f)** 4. **3.** 0, 1 y 0.
4. Comprueba que son ciertas las dos primeras afirmaciones, y úsalas para obtener la última.
5. $\overline{42}$.
6. Consecuencia de que, por el teorema de Fermat, si $0 \leq a \leq 9$ entonces $a^4 \equiv 1 \pmod{10}$.

3. ARITMÉTICA MODULAR

3.5. Ecuaciones lineales de congruencias

Ecuaciones lineales de congruencias
Se llama **ecuación lineal de congruencias** a cualquier ecuación de la forma $ax \equiv b \pmod{p}$, donde $a, b \in \mathbb{Z}$ y $p > 1$, y se llama **solución** a cualquier $x \in \mathbb{Z}$ que verifica la ecuación.

Resolución
La condición necesaria y suficiente para que la ecuación en congruencias $ax \equiv b \pmod{p}$ tenga solución en x es que la ecuación $ax + py = b$ tenga solución en x e y, y esta ecuación tiene solución si y sólo si $\text{mcd}(a, p) \mid b$. Por tanto:

$$ax \equiv b \pmod{p} \text{ tiene solución en } x \iff \text{mcd}(a, p) \mid b$$

Para resolver la ecuación se procede según el caso:

- Si $\text{mcd}(a, p) = 1$, es solución cualquier $x \equiv a^{-1}b \pmod{p}$, donde a^{-1} es el inverso de a módulo p.
  La solución es única en $\mathbb{Z}_p$.
- Si $\text{mcd}(a, p) = d > 1$, con $d \mid b$, es solución cualquier:

  $$x \equiv x_0 + \frac{tp}{d} \pmod{p}\ , \quad t = 0, 1, 2, \ldots, d-1$$

  donde x_0 es una solución particular de x en la ecuación diofántica $ax + py = b$.
  La ecuación tiene exactamente d soluciones en $\mathbb{Z}_p$.

Ejercicios

1. Hallar todas las soluciones enteras de las ecuaciones:
   (a) $5x + 2 \equiv 5 \pmod{7}$; **(b)** $3x + 4 \equiv 5 \pmod{6}$; **(c)** $12x \equiv 9 \pmod{27}$; **(d)** $8x \equiv 12 \pmod{28}$;
   (e) $5x \equiv 1 \pmod{11}$; **(f)** $4x \equiv 3 \pmod{7}$; **(g)** $5x \equiv 7 \pmod{15}$.
2. Resuelve las siguientes ecuaciones:
   (a) $66x = 42$ en $\mathbb{Z}_{168}$; **(b)** $21x = 18$ en $\mathbb{Z}_{30}$; **(c)** $35x = 42$ en $\mathbb{Z}_{49}$.

Soluciones y/o sugerencia a los ejercicios
1. **(a)** $x = 7k + 2$, $k \in \mathbb{Z}$; **(b)** No tiene solución; **(c)** $x \equiv 3, 12, 21 \pmod{27}$; **(d)** $x \equiv 5, 12, 19, 26 \pmod{28}$; **(e)** $x \equiv 9 \pmod{11}$; **(f)** $x \equiv 6 \pmod{7}$; **(g)** No tiene solución.
2. **(a)** $x \equiv 21, 49, 77, 105, 133, 161 \pmod{168}$; **(b)** $x \equiv 3, 13, 23 \pmod{30}$; **(c)** $x \equiv 3, 10, 17, 24, 31, 38, 45 \pmod{49}$.

3. ARITMÉTICA MODULAR

3.6. Sistemas lineales de congruencias

Sistemas lineales de congruencias

Se llama **sistema lineal de congruencias** a un conjunto de ecuaciones del tipo: $(\star)$ $\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \quad \vdots \\ x \equiv a_n \pmod{p_n} \end{cases}$

Teorema chino del resto

Si $a_i, p_i \in \mathbb{Z}$ con $p_i > 1$ y $\text{mcd}(p_i, p_j) = 1$ (primos entre sí) para $i \neq j$, entonces el sistema de congruencias $(\star)$ tiene solución única en $\mathbb{Z}_p$ con $p = p_1 p_2 \dots p_n$.
Además, la solución es:

$$x \equiv \left(a_1 q_1 \frac{p}{p_1} + a_2 q_2 \frac{p}{p_2} + \ldots + a_n q_n \frac{p}{p_n} \right) \pmod{p}$$

donde q_i es tal que $q_i \frac{p}{p_i} \equiv 1 \pmod{p_i}$, $1 \leq i \leq n$.

Ejercicios

1. **(a)** ¿Qué enteros dan resto 1 al dividirlos por 2 y por 3?
(b) ¿Qué enteros divisibles por 5 dan resto 1 al dividirlos por 3?

2. Halla un número natural cuyos restos al dividirlo por 3, 4, 5 y 6 sean, respectivamente, 2, 3, 4 y 5. (Brahmegupta, siglo VII)

3. Resuelve los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$ **(b)** $\begin{cases} x \equiv 2 \pmod{5} \\ 2x \equiv 1 \pmod{7} \\ 3x \equiv 4 \pmod{11} \end{cases}$ **(c)** $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 1 \pmod{6} \end{cases}$

4. Encuentra los números enteros n tales que $n + 1$ es múltiplo de 3, $n + 3$ es múltiplo de 4 y $n + 5$ es múltiplo de 7.

5. Sabiendo que $\text{mcd}(b, 561) = 1$, justifica las siguientes afirmaciones:
(a) El número b verifica que: $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.
(b) El número b verifica que: $b^{560} \equiv 1 \pmod{3}$, $b^{560} \equiv 1 \pmod{11}$ y $b^{560} \equiv 1 \pmod{17}$.
(c) El número b verifica que: $b^{560} \equiv 1 \pmod{561}$.

6. Resuelve los siguientes sistemas de congruencias:

(a) $\begin{cases} 120x \equiv 180 \pmod{450} \\ 24x \equiv 76 \pmod{100} \end{cases}$ **(b)** $\begin{cases} 4x \equiv 11 \pmod{15} \\ 10x \equiv 8 \pmod{12} \end{cases}$ **(c)** $\begin{cases} 168x \equiv 24 \pmod{220} \\ 56x \equiv 40 \pmod{68} \end{cases}$

7. Unos piratas encuentran en una isla desierta un cofre repleto de monedas de oro, en el que no caben más de 1000. Si los 5 cabecillas del grupo se reparten equitativamente el tesoro les sobra 1 moneda, si incluyen a los oficiales en el reparto son 13 y les sobran 6 monedas, y si incluyen a los 18 miembros de la tripulación les sobran 9 monedas. ¿Cuántas monedas contiene el cofre?

8. Una banda de 17 piratas se reúne para repartirse un cofre con más de 100 monedas de oro, sobrando 1 moneda después del reparto. En la consiguiente pelea, muere un pirata y vuelve a hacerse el reparto sobrando de nuevo 1 moneda. ¿Cuál es menor número de monedas que puede contener el cofre?
Supongamos que la solución anterior es el número real de monedas en el cofre y que la historia continúa: siempre que sobran monedas en el reparto hay pelea y muere un pirata. ¿Cuántos piratas quedarán vivos cuando en el reparto no sobre ninguna moneda?

9. Se reparten cuatro bolsas iguales de caramelos entre tres grupos de niños. En el primer grupo, que tiene cinco niños, se reparten dos bolsas y sobra un caramelo. En el segundo grupo, de seis niños, se reparte una bolsa y sobran dos caramelos. En el tercer grupo, de siete niños, se reparte una bolsa y sobran tres caramelos. Sabiendo que el número total de caramelos no llega a 500, ¿cuántos caramelos contiene cada bolsa?

10. Un distribuidor de equipos informáticos efectuó un pedido de entre 1000 y 1500 equipos a un fabricante que se los envió en contenedores completos con capacidad para 68 equipos cada uno. El distribuidor los repartió a los diferentes puntos de venta usado furgonetas con capacidad para 20 equipos, dejando 32 equipos sin repartir en el almacén. ¿Cuántos equipos pidió el distribuidor a la fábrica?

11. Se dispone de una cantidad par de monedas, menor que 600, que se quieren disponer en filas. Si se ordenan en filas de 17 monedas, sobran 8. Si se consideran únicamente la mitad de las monedas iniciales y se ordenan en filas de 7 monedas, sobran 3. ¿Cuántas monedas hay? ¿Es única la solución?

Soluciones y/o sugerencia a los ejercicios

1. **(a)** $x = 6k + 1$, $k \in \mathbb{Z}$; **(b)** $x = 15k + 10$, $k \in \mathbb{Z}$.
2. $60k - 1$, $k \geq 1$.
3. **(a)** $x \equiv 23 \pmod{105}$; **(b)** $x \equiv 137 \pmod{385}$; **(c)** No tiene solución.
4. $x \equiv 65 \pmod{84}$.
5. **(a)** Aplica el teorema de Fermat; **(b)** Consecuencia inmediata de (a); **(c)** Consecuencia inmediata de (b).
6. **(a)** No tiene solución; **(b)** $x \equiv 14 \pmod{30}$; **(c)** $x \equiv 8 \pmod{935}$.
7. 71 monedas.
8. 273 monedas. 13 piratas.
9. 38 caramelos.
10. 1292 equipos.
11. 76, 314 o 552 monedas.

3. ARITMÉTICA MODULAR

3.7. Dígitos de control

Los **dígitos de control**, que se utilizan para detectar errores en la transmisión de datos.

Número de identificación fiscal: NIF
El **número de identificación fiscal (NIF)** está formado por el número del documento nacional de identidad (DNI), formado por 8 dígitos, seguido de una letra del alfabeto.
Para encontrar la letra del alfabeto asociada al DNI con número $N = n_1n_2n_3n_4n_5n_6n_7n_8$ se procede así:

1. Se halla el resíduo de N módulo 23: $N \equiv x \pmod{23}$.
2. Se determina la letra correspondiente a x en la siguiente identificación:

$$\begin{array}{llllllll} 0 \to \mathrm{T} & 3 \to \mathrm{A} & 6 \to \mathrm{Y} & 9 \to \mathrm{D} & 12 \to \mathrm{N} & 15 \to \mathrm{S} & 18 \to \mathrm{H} & 21 \to \mathrm{K} \\ 1 \to \mathrm{R} & 4 \to \mathrm{G} & 7 \to \mathrm{F} & 10 \to \mathrm{X} & 13 \to \mathrm{J} & 16 \to \mathrm{Q} & 19 \to \mathrm{L} & 22 \to \mathrm{E} \\ 2 \to \mathrm{W} & 5 \to \mathrm{M} & 8 \to \mathrm{P} & 11 \to \mathrm{B} & 14 \to \mathrm{Z} & 17 \to \mathrm{V} & 20 \to \mathrm{C} & \end{array}$$

3. Si $x \to \mathrm{X}$, el número de NIF es: $n_1n_2n_3n_4n_5n_6n_7n_8\mathrm{X}$.

El NIF detecta si ha habido errores, y permite recuperar un dígito perdido en la transmisión, siempre que se sepa el lugar que ocupa.

El número ISBN
El **ISBN (International Standard Book Number)** es un número de 10 cifras que identifica de forma única cualquier libro editado en el mundo. Un organismo internacional (http://www.isbn.org) marca las directrices sobre este número. Sus 10 cifras están estructuradas en cuatro bloques, XX-XXX-XXXX-X, donde:

- El primero es el indicador geográfico. A España le corresponde el 84.
- El segundo bloque corresponde a la editorial.
- El tercer número corresponde al libro (dentro de su editorial).
- El último bloque lo constituye un dígito de control. En el ISBN $x_1x_2 - x_3x_4x_5 - x_6x_7x_8x_9 - x_{10}$ el último dígito es:
$$x_{10} \equiv (x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9) \pmod{11}$$
teniendo en cuenta que cuando $x_{10} = 10$ se sustituye por la letra X.

Así, por ejemplo, el ISBN 84-316-3311-5 corresponde al libro de Matemática Discreta de N.L. Biggs (3311) publicado en España (84) por la editorial Vicens-Vives (316) con dígito de control:

$$8 + 2 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 5 \cdot 6 + 6 \cdot 3 + 7 \cdot 3 + 8 \cdot 1 + 9 \cdot 1 = 115 \equiv 5 \pmod{11}$$

El dígito de control permite detectar errores y recuperar un dígito perdido en la transmisión, siempre que se sepa el lugar que ocupa.

Número de cuenta corriente
En **número de cuenta corriente** consta de 20 dígitos distribuidos en la siguiente estructura:

$$\mathrm{E_1E_2E_3E_4 - O_1O_2O_3O_4 - XY - C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}}$$

donde los cuatro primeros dígitos identifican la entidad, los cuatro siguientes la oficina, los dos siguientes son dígitos de control y los diez últimos identifican la cuenta. Los dígitos de control controlan el primero a la oficina y la entidad y el segundo al número de cuenta, y se calculan como sigue:

$$\mathrm{X} \equiv (7\mathrm{E_1} + 3\mathrm{E_2} + 6\mathrm{E_3} + \mathrm{E_4} + 2\mathrm{O_1} + 4\mathrm{O_2} + 8\mathrm{O_3} + 5\mathrm{O_4}) \pmod{11}$$
$$\mathrm{Y} \equiv (10\mathrm{C_1} + 9\mathrm{C_2} + 7\mathrm{C_3} + 3\mathrm{C_4} + 6\mathrm{C_5} + \mathrm{C_6} + 2\mathrm{C_7} + 4\mathrm{C_8} + 8\mathrm{C_9} + 5\mathrm{C_{10}}) \pmod{11}$$

poniendo, en ambos casos, un 1 cuando el resultado es 10.

Ejercicios

1. Verifica que el NIF correspondiente a tu DNI es el correcto. Si cambias alguno de sus dígitos, ¿cuál sería la letra correspondiente?

2. Por un error de transmisión se ha recibido la siguiente información sobre el NIF de una persona: 213_5427 Z. ¿Cuál es el número que falta?

Soluciones y/o sugerencia a los ejercicios

1. Calcula la letra que corresponde a tu DNI y verifica que es la que aparece en tu NIF.
2. El número 6.

3. ARITMÉTICA MODULAR

3.8. Criptografía

La **criptografía** se ocupa del problema de cifrar (encriptar) y descifrar (desencriptar) mensajes para su transmisión secreta, pudiendo ser:

- **Criptografía simétrica:** cuando se utiliza la misma clave para cifrar y descifrar.
  El principal problema de la criptografía simétrica es que para descifrar es necesario conocer la clave con la que se ha cifrado y, por tanto, hay que enviar la clave junto con el mensaje, pudiendo ser interceptado y descifrado fácilmente.
- **Criptografía asimétrica:** cuando se utilizan claves distintas para cifrar y descifrar.
  En la criptografía asimétrica la clave que se utiliza para cifrar puede ser pública siempre que la clave para descifrar sea privada, es decir, conocida simplemente por el destinatario, ni siquiera por el remitente.

Dos ejemplos de criptografía simétrica son los cifrados de Cesar y los cifrados lineales. Un ejemplo de de criptografía asimétrica son los cifrados de clave pública (RSA).

Codificación del alfabeto
En criptografía, cada letra del alfabeto (y el espacio) se puede codificar con dos dígitos según la siguiente tabla:

$\sqcup = 00$	$\mathrm{D} = 04$	$\mathrm{H} = 08$	$\mathrm{L} = 12$	$\mathrm{O} = 16$	$\mathrm{S} = 20$	$\mathrm{W} = 24$
$\mathrm{A} = 01$	$\mathrm{E} = 05$	$\mathrm{I} = 09$	$\mathrm{M} = 13$	$\mathrm{P} = 17$	$\mathrm{T} = 21$	$\mathrm{X} = 25$
$\mathrm{B} = 02$	$\mathrm{F} = 06$	$\mathrm{J} = 10$	$\mathrm{N} = 14$	$\mathrm{Q} = 18$	$\mathrm{U} = 22$	$\mathrm{Y} = 26$
$\mathrm{C} = 03$	$\mathrm{G} = 07$	$\mathrm{K} = 11$	$\tilde{\mathrm{N}} = 15$	$\mathrm{R} = 19$	$\mathrm{V} = 23$	$\mathrm{Z} = 27$

Cifrados de Cesar
El **cifrado de Cesar** con **clave** $k \geq 1$ cifra los mensajes sumando k en módulo 28 al código numérico de cada letra. Para descifrar el mensaje se realiza la operación inversa, es decir, se resta k en módulo 28 al código numérico de cada una de las letras recibidas.
Hay tantos cifrados de Cesar como valores posibles de k, es decir, 28. Por tanto, son códigos fáciles de romper, ya que habría que hacer un máximo de 28 pruebas hasta obtener un mensaje comprensible.

Ejemplo
Para cifrar el texto JULIO CESAR con clave $k = 3$:

$$\begin{array}{lcl} \text{JULIO CESAR} & \Longleftrightarrow & 10-22-12-09-16-00-03-05-20-01-19 \\ & & \Downarrow \quad \text{(se suma 3 en módulo 28)} \\ & & 13-25-15-12-19-03-06-08-23-04-22 \Longleftrightarrow \mathbf{MX\tilde{N}LRCFHVDU} \end{array}$$

El mensaje a enviar sería **MXÑLRCFHVDU**, que se descifraría así:

$$\begin{array}{lcl} \mathbf{MX\tilde{N}LRCFHVDU} & \Longleftrightarrow & 13-25-15-12-19-03-06-08-23-04-22 \\ & & \Downarrow \quad \text{(se resta 3 en módulo 28)} \\ & & 10-22-12-09-16-00-03-05-20-01-19 \Longleftrightarrow \text{JULIO CESAR} \end{array}$$

Cifrados lineales
Es una variante sobre los cifrados de Cesar. El **cifrado lineal** con **clave** (a, b) cifra los mensajes aplicando al código numérico de cada letra la transformación lineal:

$$n \longrightarrow m \equiv an + b \pmod{28}$$

Para descifrar el mensaje se realiza la operación inversa:

$$m \longrightarrow n \equiv a^{-1}(m - b) \pmod{28}$$

por lo que hay que tener en cuenta que a debe tener inverso en $\mathbb{Z}_{28}$, es decir, ha de ser primo con 28.
En consecuencia, el número cifrados lineales distintos es $\Phi(28)\cdot 28 = 12\cdot 28 = 336$. Estos cifrados son algo más difíciles de romper que los de Cesar, pero relativamente fáciles de romper con ordenador, ya que habría que hacer un máximo de 336 pruebas hasta obtener un mensaje comprensible.

Ejemplo
Para cifrar el texto JULIO CESAR con el cifrado lineal de clave $(3,1)$:

$$\begin{array}{rcl} \text{JULIO CESAR} & \Longleftrightarrow & 10-22-12-09-16-00-03-05-20-01-19 \\ & & \Downarrow \quad \text{(se aplica la operación } 3n+1 \text{ en módulo 28)} \\ & & 03-11-09-00-21-01-10-16-05-04-02 \quad \Longleftrightarrow \quad \textbf{CKI TAJOEDB} \end{array}$$

El mensaje a enviar sería **CKI TAJOEDB**, que se descifraría, teniendo en cuenta que $3^{-1} = 19$ en $\mathbb{Z}_{28}$, así:

$$\begin{array}{rcl} \textbf{CKI TAJOEDB} & \Longleftrightarrow & 03-11-09-00-21-01-10-16-05-04-02 \\ & & \Downarrow \quad \text{(se aplica la operación } 19(m-1) \text{ en módulo 28)} \\ & & 10-22-12-09-16-00-03-05-20-01-19 \quad \Longleftrightarrow \quad \text{JULIO CESAR} \end{array}$$

Ejercicios

1. Utiliza el cifrado de Cesar con clave $k = 7$ para cifrar y descifrar el mensaje: "VAMOS A CENAR EN CASA".
2. Utiliza el cifrado lineal con clave $(5,3)$ para cifrar y descifrar el mensaje: "VAMOS A CENAR EN CASA".
3. Utiliza el cifrado lineal con clave $(3,0)$ para cifrar el mensaje: "HOLA A TODOS".

Soluciones y/o sugerencia a los ejercicios
1. CHSVZGHGJLTHYGLTGJHZH
2. JHNBUCHCQARHPCARCQHUH
3. WSHC C GSLSD

3. ARITMÉTICA MODULAR

3.9. Cifrado de clave pública: RSA

El **cifrado de clave pública RSA** fue desarrollado en 1978 por R.L. Rivest, A. Shamir y L. Adleman, debiendo su nombre a las iniciales de sus autores.

El método completo RSA
El proceso completo de cifrado y descifrado de un mensaje consta de los pasos que se enumeran a continuación y que se realizan, como ejemplo con el mensaje "El código".

1. El mensaje se reagrupa en bloques de letras de igual longitud r, llamadas **palabras**.
   Si $r = 2$: **EL CODIGO** $\Longrightarrow$ EL $-$ ⊔C $-$ OD $-$ IG $-$ O⊔

2. Usando la codificación del alfabeto dada en 2.8, cada palabra se codifica como un número de 2^r dígitos, llamado también **palabra**.

$$\text{EL} - \sqcup\text{C} - \text{OD} - \text{IG} - \text{O}\sqcup \quad \Longrightarrow \quad 0512 - 0003 - 1604 - 0907 - 1600$$

3. La **clave pública**, llamada así porque puede ser conocida por cualquier persona, está formada por una pareja de enteros positivos (n, e) elegidos de tal forma que:

   - n sea primo con cualquier palabra del texto, lo que se garantiza si cualquier divisor primo de n es mayor que la mayor palabra posible del texto. En la práctica, se elige $n = pq$ como el producto de dos números primos mayores que la mayor palabra del texto.
   - e sea primo con $\Phi(n) = (p-1)(q-1)$.

   En el ejemplo que estamos considerando, la mayor palabra del texto es 2727, dos números primos mayores que esta palabra son $p = 2729$ y $q = 2741$, y entonces $n = pq = 2729 \cdot 2741 = 7480189$. En este caso, $\Phi(n) = (p-1)(q-1) = 2728 \cdot 2740 = 7474720$ y, puesto que $\Phi(n)$ no es divisible por 3, se puede elegir $e = 3$. En consecuencia, se elige y publica la clave pública $(7480189, 3)$.

4. La **clave privada**, llamada así porque sólo es conocida por el receptor del mensaje, está formada por la pareja de enteros positivos (n, d), donde n es el mismo de la clave pública y $d = e^{-1} \pmod{\Phi(n)}$, cuya existencia queda garantizada al ser e primo con $\Phi(n)$.
   En el ejemplo, $d = 3^{-1} \pmod{7474720} = 4983147$, y la clave privada es $(7480189, 4983147)$.

5. **El cifrado:** cada palabra N se cifra como $C = N^e \pmod{n}$.
   En el ejemplo:

$$\begin{aligned}
N = 0512 &\Longrightarrow C = 0512^3 \pmod{7480189} = 7054515\\
N = 0003 &\Longrightarrow C = 0003^3 \pmod{7480189} = 27\\
N = 1604 &\Longrightarrow C = 1604^3 \pmod{7480189} = 5212725\\
N = 0907 &\Longrightarrow C = 0907^3 \pmod{7480189} = 5603932\\
N = 1600 &\Longrightarrow C = 1600^3 \pmod{7480189} = 4336617
\end{aligned}$$

   El mensaje cifrado a enviar sería: **7054515 − 27 − 5212725 − 5603932 − 4336617**

6. **El descifrado:** cada palabra recibida C se descifra como $N = C^d \pmod{n}$, ya que, al ser $ed + \alpha\Phi(n) = 1$ para algún $\alpha \in \mathbb{Z}$ y $N^{\Phi(n)} \equiv 1 \pmod{n}$ (por ser n primo con cualquier palabra N del texto), se tiene que:

$$C^d \pmod{n} = N^{ed} \pmod{n} = N^{ed} \left(N^{\Phi(n)}\right)^{\alpha} \pmod{n} = N^{ed+\alpha\Phi(n)} \pmod{n} = N \pmod{n}$$

En el ejemplo:

$$\begin{aligned}
C = 7054515 &\implies N = 7054515^{4983147} \pmod{7480189} = 512\\
C = 27 &\implies N = 27^{4983147} \pmod{7480189} = 3\\
C = 5212725 &\implies N = 5212725^{4983147} \pmod{7480189} = 1604\\
C = 5603932 &\implies N = 5603932^{4983147} \pmod{7480189} = 907\\
C = 4336617 &\implies N = 4336617^{4983147} \pmod{7480189} = 1600
\end{aligned}$$

Puesto que $r = 2$, cada palabra debe tener $2^2 = 4$ dígitos, por lo que para obtener el mensaje hay que completar las palabra con los ceros necesarios hasta obtener los cuatro dígitos, y decodificarla:

$$0512 - 0003 - 1604 - 0907 - 1600 \implies \text{EL} - \sqcup\text{C} - \text{OD} - \text{IG} - \text{O}\sqcup \implies \textbf{EL CODIGO}$$

Seguridad del método

Puesto que la clave pública (n, e) es conocida por todos, la seguridad del método de cifrado RSA consiste en la privacidad de la clave privada (n, d), es decir, del número d y, puesto que $d = e^{-1} \pmod{\Phi(n)}$, la seguridad radica en la dificultad de obtener $\Phi(n) = (p-1)(q-1)$, que en última instancia radica en la dificultad de obtener la descomposición $n = pq$. Si los números primos p y q se eligen suficientemente grandes, el problema de descomposición de n es prácticamente imposible en la actualidad.

El método de trabajo

Para enviarse mensajes cifrados un grupo indeterminado de personas, cada una de ellas publica sus claves (n_i, e_i), $i \geq 1$, manteniendo en secreto su clave privada (n_i, d_i). Cuando i quiere enviar un mensaje a j lo cifra con la clave privada de j, y el mensaje sólo lo podrá descifrar j (que es el único que conoce la clave privada correspondiente).

Ejercicios

1. Tomando $r = 1$, encuentra la clave privada correspondiente a la clave pública $(899, 11)$.
2. Cifra y descifra el mensaje "Es un secreto" con $r = 1$ y clave pública $(899, 11)$.

Soluciones y/o sugerencia a los ejercicios

1. $(n, d) = (899, 611)$.
2. Mensaje cifrado: $738 - 7 - 0 - 296 - 443 - 0 - 7 - 738 - 44 - 723 - 738 - 229 - 605$.