

EXAMEN – LUNES 17 DE JULIO DE 2023 (SOLUCIONES)

Ejercicio 1.

- a) Si  $a$  y  $b$  son enteros no nulos entonces existen enteros  $x, y$  tales que  $ax + by = \text{mcd}(a, b)$ .
- b) Lema de Euclides: si  $a|bc$  y  $\text{mcd}(a, b) = 1$  entonces  $a|c$ . Usando la identidad de Bezout, existen  $x, y \in \mathbb{Z}$  tales que  $ax + by = 1$ , luego  $a|acx + bcy = c$ .
- c) Si  $\sqrt[3]{4} \in \mathbb{Q}$  entonces existen  $a, b \in \mathbb{Z}$  no nulos y coprimos tales que  $\sqrt[3]{4} = \frac{a}{b} \Leftrightarrow \sqrt[3]{4}b = a \Leftrightarrow 4b^3 = a^3$ , pero esto implica que  $a$  debe ser par (ya que  $4b^3$  lo es). Sea  $a = 2c$  con  $c \in \mathbb{Z}$ , entonces  $4b^3 = a^3 = 8c^3$  de donde  $b^3 = 2c^3$  y por lo tanto  $b$  debe ser par (pues  $2c^3$  lo es). Pero esto es una contradicción ya que  $a$  y  $b$  no pueden ser ambos pares por ser coprimos.

Ejercicio 2.

- a) Por la identidad de Bezout sabemos que existen  $x'_0, y'_0 \in \mathbb{Z}$  tales que  $ax'_0 + by'_0 = 1$  (que pueden hallarse usando el Algoritmo de Euclides Extendido). Luego  $(x_0, y_0) = (cx'_0, cy'_0)$  verifica  $ax_0 + by_0 = c$ . Si  $x, y \in \mathbb{Z}$  verifican  $ax + by = c$  entonces  $ax + by = ax_0 + by_0$ , de donde  $a(x - x_0) = b(y_0 - y)$ . Luego  $b|a(x - x_0)$  y dado que  $\text{mcd}(a, b) = 1$ , por el Lema de Euclides tenemos  $b|x - x_0$ , por lo tanto existe  $t \in \mathbb{Z}$  tal que  $x - x_0 = bt$ . Por otra parte,  $b(y_0 - y) = a(x - x_0) = abt$  de donde  $y_0 - y = at$ .  
Despejando  $x, y$  obtenemos  $\begin{cases} x = x_0 + bt; \\ y = y_0 - at. \end{cases}$  con  $t \in \mathbb{Z}$ . Recíprocamente, si  $x = x_0 + bt$  e  $y = y_0 - at$  con  $t \in \mathbb{Z}$  entonces  $ax + by = a(x_0 + bt) + b(y_0 - at) = (ax_0 + by_0) + abt - bat = c + 0 = c$ .
- b) Si  $(x, y) = (3 + 13t, 4 + 18t)$  con  $t \in \mathbb{Z}$  entonces  $18x - 13y = 18(3 + 13t) - 13(4 + 18t) = 18 \cdot 3 - 13 \cdot 4 = 2$ . Luego  $(x, y) \in S \Rightarrow 18x - 13y = 2$ . Recíprocamente, si  $(x, y)$  es solución de la diofántica  $18x - 13y = 2$ , como  $(x_0, y_0) = (3, 4)$  es una solución particular de  $18x - 13y = 2$  entonces por la parte a tenemos que  $(x, y) = (3 + 13t, 4 + 18t)$  con  $t \in \mathbb{Z}$  y por lo tanto  $(x, y) \in S$ .
- c) Como  $(x, y) \in S$  entonces  $x = 3 + 13t, y = 4 + 18t$  con  $t \in \mathbb{Z}$ .  
Luego  $(*) \begin{cases} x \equiv 1 \pmod{18}, \\ y \equiv 2 \pmod{13}. \end{cases} \Leftrightarrow \begin{cases} 3 + 13t \equiv 1 \pmod{18}, \\ 4 + 18t \equiv 2 \pmod{13}. \end{cases} \Leftrightarrow \begin{cases} 13t \equiv -2 \pmod{18}, \\ 18t \equiv -2 \pmod{13}. \end{cases}$   
Para despejar  $t$  primero debemos calcular  $13^{-1} \pmod{18}$  y  $18^{-1} \pmod{13}$  y para ello basta encontrar una solución particular de la diofántica  $13s + 18t = 1$ . Usamos el AEE:  $18 = 1 \cdot 13 + 5$ ,  $13 = 2 \cdot 5 + 3$ ,  $5 = 1 \cdot 3 + 2$ ,  $3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5 = 2 \cdot 13 - 5 \cdot (18 - 13) = 7 \cdot 13 - 5 \cdot 18 \Rightarrow 13^{-1} \pmod{18} = 7$  y  $18^{-1} \pmod{13} = -5$ .  
 $(*) \Leftrightarrow \begin{cases} t \equiv (-2) \cdot 7 \equiv -14 \equiv 4 \pmod{18}, \\ t \equiv (-2) \cdot (-5) \equiv 10 \pmod{13}. \end{cases} \Leftrightarrow t \equiv 4 \cdot 7 \cdot 13 - 10 \cdot 5 \cdot 18 = -536 \equiv 166 \pmod{234}$ .  
Luego los  $(x, y) \in S$  que verifican  $(*)$  son  $\begin{cases} x = 3 + 13(166 + 234k) = 2161 + 3042k, \\ y = 4 + 18(166 + 234k) = 2992 + 4212k \end{cases}$  con  $k \in \mathbb{Z}$ .

### Ejercicio 3.

- a) Como  $\frac{n}{d} > 1$  es entero, entonces tiene algún divisor primo  $p$  (Teorema Fund. de la Aritmética). Luego  $\frac{n}{d} = pm$  con  $m \in \mathbb{Z}$ , o equivalentemente  $\frac{n}{p} = dm$ . Esto último implica  $d \mid \frac{n}{p}$ .
- b) i) Consideramos la división con resto,  $n = o(g) \cdot k + r$  con  $0 \leq r < o(g)$ . Luego  $e = g^n = (g^{o(g)})^k \cdot g^r = g^r$ . Pero por definición de orden resulta  $r = 0$  y por lo tanto  $o(g) \mid n$ .
- ii) Sea  $d = o(g)$ . Por la parte i tenemos que  $d \mid n$ . Si  $d < n$  entonces por la parte a tenemos que  $d \mid \frac{n}{p}$  para algún primo  $p$ . Pero  $g^d = e$  implica  $g^{\frac{n}{p}} = e$  contradiciendo la hipótesis. Luego  $d = n$ .
- c) Como 47 es primo y  $1 < g < 46$  resulta que  $\text{mcd}(g, 47) = 1$  y por lo tanto  $\bar{g} \in U(47)$ . Por Fermat-Euler resulta  $\bar{g}^{46} = \bar{1}$  en  $U(47)$ . Por la parte bii, para ver que  $o(\bar{g}) = 46$  basta chequear que  $\bar{g}^{23} \neq \bar{1}$  y que  $\bar{g}^2 \neq \bar{1}$  en  $U(47)$ . Como  $47 \nmid g^{23} - 1$  tenemos  $\bar{g}^{23} \neq \bar{1}$ . Como 47 es primo,  $0 < g - 1 < 45$  y  $2 < g + 1 < 47$  entonces  $47 \nmid (g - 1)(g + 1) = g^2 - 1$  (pues no divide a ninguno de los factores), luego  $\bar{g}^2 \neq \bar{1}$ . Por bii, tenemos que  $\bar{g}^{46} = \bar{1}$  en  $U(47)$  y por lo tanto  $g$  es raíz primitiva módulo 47.

### Ejercicio 4.

- a) Alicia elige dos primos grandes  $p$  y  $q$  y con ellos calcula  $n = pq$  y  $\varphi(n) = (p-1)(q-1)$ . Luego elige al azar  $e : 1 < e < \varphi(n)$  tal que  $\text{mcd}(e, \varphi(n)) = 1$  y publica su clave pública  $(n, e)$  (conservando en secreto los primos  $p$  y  $q$ ). Luego usando el Algoritmo de Euclides, Alicia calcula  $d$  tal que  $de \equiv 1 \pmod{\varphi(n)}$  (pues conoce  $\varphi(n)$ ). Si Bob quiere enviarle un mensaje  $x$  a Alicia entonces lo encripta via  $x \mapsto x^e \pmod{n}$  y le envía el mensaje encriptado. Alicia al recibir el mensaje encriptado  $y = x^e \pmod{n}$ , lo desencripta<sup>1</sup> via  $y \mapsto y^d \pmod{n}$ . Si conseguimos factorizar  $n = pq$  entonces podemos calcular  $\varphi(n) = (p-1)(q-1)$  y calcular  $d$ , el inverso de  $e$  módulo  $\varphi(n)$  usando el AEE (y por lo tanto desencriptar todos los mensajes que le son enviados a Alicia). Este es la única forma conocida de conseguir  $d$  a partir de la clave pública  $(n, e)$ . Luego la seguridad de este criptosistema se basa en la dificultad de factorizar números grandes (no se conocen algoritmos eficientes para factorizar números grandes en computadoras clásicas y se conjetura que no los hay).
- b) Si los primos  $p$  y  $q$  están muy próximos entonces podemos factorizar  $n$  via el método de Fermat que consiste en ir chequeando si  $n + s^2$  es un cuadrado perfecto para  $s = 1, 2, 3, \dots$ . Observar que si  $n + s^2 = t^2$  entonces  $n = t^2 - s^2 = (t-s)(t+s)$  y conseguimos factorizar  $n$ . Como  $n = pq = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2$  entonces  $n + (\frac{p-q}{2})^2$  es un cuadrado perfecto, lo que significa que el Método de Fermat lleva a lo sumo  $\frac{|p-q|}{2}$  pasos (donde cada paso consiste en chequear si un número es un cuadrado perfecto).

---

<sup>1</sup>Se puede probar que la función de desencriptado y encriptado son inversas una de la otra pero no lo pide aquí.