

## Solución segundo parcial

### Ejercicio 1 (18 pts).

- a) Probar que 2 es raíz primitiva módulo 101.
- b) Alicia y Bernardo eligen  $p = 101$ ,  $g = 27$  para intercambiar claves en Diffie-Hellman.
  - i. Bernardo elige  $m = 3$  y Alicia le envía el número  $g^m = 22 \pmod{101}$ . ¿Cuál es la clave  $K$  que acuerdan?
  - ii. ¿Qué número ( $n$ ) eligió Alicia?
- c) Se utiliza el método César afín para encriptar siendo la función de encriptado  $E : \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$ , donde  $E(x) = cx + e$ , con  $K = e28 + c$  escrito en base 28.
  - i. Hallar la función de desencriptar  $D : \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$  explícitamente.
  - ii. Desencriptar *GBZWFÑRJGDSFUB*.

### Solución Ejercicio 1

**a.** Alcanza con ver, por el Ejercicio 1, parte C, del Práctico 8, que  $2^{100/p} \not\equiv 1 \pmod{101}$  para todo primo  $p$  que divide a 100. En efecto

$$\begin{aligned} 2^{100/5} &= 2^{20} = (2^{10})^2 \equiv 14^2 \equiv 95 \pmod{101} \\ 2^{100/2} &= 2^{50} = (2^{10})^5 \equiv 14^5 = (14^2)^2 \cdot 14 \equiv (-6)^2 \cdot 14 \equiv 100 \pmod{101}. \end{aligned}$$

Luego 2 es una raíz primitiva módulo 101.

**b.i.** La clave que acuerdan al utilizar Diffie-Hellman es  $g^{nm} = (g^n)^m = 22^3 = 43 \pmod{101}$ .

**b.ii.** Como  $g = 27 = 2^7 \pmod{101}$  entonces  $g^2 = 2^{14} = 27 \cdot 27 = 22 \pmod{101}$ . Luego como  $g^n = 22 \pmod{101}$ , entonces

$$2^{7n} \equiv 2^{14} \pmod{101}.$$

Luego, usando que 2 es raíz primitiva módulo 101 por la parte anterior y usando el Ejercicio 6 del Práctico 8 (Logaritmo Discreto), de este parcial, se tiene que  $7n \equiv 14 \pmod{100}$ . O sea que  $n = 2$  es solución.

**c.**  $K = 43 = 28 \cdot 1 + 15$ . Por lo que  $e = 1$  y  $c = 15$ .

**c.i.** Sabemos que  $D(x) = c'(x - e) \pmod{28}$  donde  $c'$  es el inverso de  $c$  módulo 28. Luego como  $c = 15$ , se puede probar que  $c' = 15$  (pues

$15 \cdot 15 = 225 = 1 \pmod{28}$ . Y como  $e = 1$ , entonces  $D(x) = 15(x - 1) \pmod{28}$ .

**c.ii.** La descriptación de  $GBZWF\tilde{N}RJGDSFUB$  es *SALVÉ DISCRETA*.

## Ejercicio 2 (15 pts).

- a) Sea  $H$  es un subgrupo no nulo de  $\mathbb{Z}$ .
  - i. Probar que si  $a \in H$  entonces  $na \in H$  para todo entero  $n$ .
  - ii. Sea  $x = \min\{a > 0 : a \in H\}$ . Probar que  $H = x\mathbb{Z} = \{xn : n \in \mathbb{Z}\}$ .
- b) Sean  $x, y \in \mathbb{Z}$ . Probar que  $x\mathbb{Z} \cap y\mathbb{Z} = \text{mcm}(x, y)\mathbb{Z}$ .
- c) Concluir, usando las partes anteriores, que si  $H$  y  $H'$  son dos subgrupos no nulos de  $\mathbb{Z}$  entonces  $H \cap H' \neq 0$ .
- d) Dados  $x, y \in \mathbb{Z}$  probar que el grupo generado por  $x$  e  $y$  es  $\langle x, y \rangle = \text{mcd}(x, y)\mathbb{Z}$ .

### Solución Ejercicio 2

**a.i.** Como  $H$  es un subgrupo de  $\mathbb{Z}$  y  $a \in H$ , entonces  $\langle a \rangle \subset H$ . Pero  $\langle a \rangle = \{na / n \in \mathbb{Z}\} = \underbrace{\{a + a + \cdots + a\}}_{n\text{-veces}} / n \in \mathbb{Z}^+ \cup \{0\} \cup \underbrace{\{(-a) + (-a) + \cdots + (-a)\}}_{(-n)\text{-veces}} / n \in \mathbb{Z}^-$ , y por tanto  $na \in H$  para todo entero  $n$ .

**a.ii.** Sea  $a \in H$ . Como  $x > 0$ , se puede hacer la división entera de  $a$  por  $x$  y obtener

$$a = qx + r \text{ con } q, r \text{ enteros, y } 0 \leq r < x.$$

La parte anterior aplicada a  $x \in H$  implica  $qx \in H$ . Como  $a$  también está en  $H$ , entonces

$$r = a - qx \in H.$$

Y dado que  $x$  es el mínimo elemento positivo de  $H$ ,  $r$  debe ser necesariamente 0. O sea que  $a = qx$ . Luego  $H = \{nx : n \in \mathbb{Z}\}$ .

**b.** La igualdad de conjuntos se sigue de las siguientes equivalencias inmediatas

$$z \in x\mathbb{Z} \cap y\mathbb{Z} \iff x, y | z \iff \text{mcm}(x, y) | z \iff z \in \text{mcm}(x, y)\mathbb{Z}.$$

c. Usando 2)a) se puede afirmar que como  $H$  es no nulo entonces existe  $x > 0$  tal que  $H = \langle x \rangle$ . Lo mismo se puede decir para  $H'$ , es decir al ser no nulo hay un  $y > 0$  tal que  $H' = \langle y \rangle$ . Y ahora usando 2)b) se tiene que  $H \cap H' = mcm(x, y)\mathbb{Z} \neq 0$ .

d. La igualdad de conjuntos se sigue de las siguientes equivalencias inmediatas

$$z \in \langle x, y \rangle \iff z = ax + by \text{ con } a, b \in \mathbb{Z} \iff mcd(x, y) | z \iff z \in mcd(x, y)\mathbb{Z}.$$

### Ejercicio 3 (15 pts).

- a) Sea  $r$  una raíz primitiva módulo  $p$ , con  $p$  primo. Probar que  $r^a \equiv r^b \pmod{p}$  si y solamente si  $a \equiv b \pmod{p-1}$ .
- b) Probar que 2 es raíz primitiva módulo 37.
- c) Calcular  $\log_2 17$ .
- d) Resolver  $13^{5z} \equiv 17 \pmod{37}$ .

### Solución Ejercicio 3

a. ( $\implies$ ) Sean

$$\begin{aligned} a &= q_1(p-1) + s_1 \text{ con } q_1, s_1 \text{ enteros, y } 0 \leq s_1 < p-1 \\ b &= q_2(p-1) + s_2 \text{ con } q_2, s_2 \text{ enteros, y } 0 \leq s_2 < p-1 \end{aligned}$$

las respectivas divisiones enteras de  $a$  y  $b$  entre  $p-1$ . Luego

$$\begin{aligned} r^a &= r^{q_1(p-1)+s_1} = (r^{p-1})^{q_1} \cdot r^{s_1} \equiv r^{s_1} \pmod{p} \\ r^b &= r^{q_2(p-1)+s_2} = (r^{p-1})^{q_2} \cdot r^{s_2} \equiv r^{s_2} \pmod{p} \end{aligned}$$

y como  $r^a \equiv r^b \pmod{p}$ , entonces  $r^{s_1} \equiv r^{s_2} \pmod{p}$ . Luego  $r^{s_1-s_2} \equiv 1 \pmod{p}$ , y por lo tanto  $o(r) | s_1 - s_2$ . Como  $r$  es una raíz primitiva, entonces  $o(r) = p-1$ . Y como  $0 \leq s_1, s_2 < p-1$  entonces  $s_1 = s_2$ .

( $\impliedby$ ) Si  $a \equiv b \pmod{p-1}$  entonces  $a$  y  $b$  dejan el mismo resto al dividirse por  $p-1$ . Luego razonando como en el directo se obtiene  $r^a \equiv r^b \pmod{p}$ .

b. Al igual que en el Ejercicio 1, para ver que 2 es raíz primitiva módulo 37, como  $\phi(37) = 36 = 2^2 \cdot 3^2$ , alcanza con ver que  $2^{36/2}$  y  $2^{36/3}$  no son congruentes con 1 módulo 37. Pero

$$\begin{aligned} 2^{36/2} &= 2^{18} = (2^5)^3 \cdot 2^3 \equiv (-5)^3 \cdot 8 \equiv 36 \pmod{37} \\ 2^{36/3} &= 2^{12} = (2^5)^2 \cdot 2^2 \equiv (-5)^2 \cdot 4 \equiv 26 \pmod{37} \end{aligned}$$

y por tanto 2 es raíz primitiva módulo 37.

c. Como  $2^7 = 128 \equiv 17 \pmod{37}$  entonces  $\log_2 17 = 7$ .

d. Como  $2^{11} = 2048 \equiv 13 \pmod{37}$  entonces

$$(2^{11})^{5z} \equiv 2^7 \pmod{37}.$$

Luego, usando que 2 es raíz primitiva módulo 37 y 3)a), se tiene que  $55z \equiv 7 \pmod{36}$ . Luego  $z = 25$ .

#### Ejercicio 4 (12 pts).

a) Enunciar el test de primalidad de Lucas.

b) Demostrarlo.

#### Solución Ejercicio 4

Fue dado en ambos Teóricos. Ver en el Texto *The Mathematics of Ciphers - Number Theory and RSA Cryptography*, S. C. Coutinho, pág. 151.