

**Ejercicio 1.**

- Enunciar y demostrar la Identidad de Bézout.
- Deducir el Lema de Euclides.
- Hallar todos los  $x \in \mathbb{Z}$  que cumplan:

$$\begin{cases} 5x \equiv 1 & (\text{mód } 47) \\ x \equiv 21^{44} & (\text{mód } 19). \end{cases}$$

**Solución.**

- Teorema.** Dados  $a, b \in \mathbb{Z}$  con  $(a, b) \neq (0, 0)$ , existen  $x, y \in \mathbb{Z}$  tales que  $ax + by = \text{mcd}(a, b)$ .

**Demostración.** Sea  $S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{Z}^+$ . Basta probar que  $d = \text{mcd}(a, b) \in S$ . Por definición  $S \subseteq \mathbb{Z}^+$ , además  $S \neq \emptyset$  pues  $a^2 + b^2 \in S$ . Por el principio del buen orden  $S$  tiene un mínimo que llamamos  $s_0$ . Como  $s_0 \in S$  podemos escribir  $s_0 = ax_0 + by_0$ .

Mostraremos que  $s_0 = d$ , probando ambas desigualdades. En primer lugar como  $d \mid a$  y  $d \mid b$  tenemos que  $d \mid ax_0 + by_0 = s_0$ . Concluimos que  $d \leq s_0$ .

Ahora veremos que  $s_0$  divide a  $a$  y a  $b$ . Por el teorema de división entera existen  $q, r \in \mathbb{Z}$  tales que  $a = qs_0 + r$  con  $0 \leq r < s_0$ . Entonces  $r = a - qs_0 = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$ . Si  $r > 0$  tendríamos  $r \in S$  con  $r < s_0$  lo que contradice que  $s_0$  es el mínimo. Entonces  $r = 0$  y concluimos que  $s_0 \mid a$ .

De la misma forma se prueba que  $s_0 \mid b$ . Entonces  $s_0$  es un divisor común de  $a$  y de  $b$  y concluimos que  $s_0 \leq d$ .

En resumen,  $d = s_0 \in S$  lo que concluye la demostración.  $\square$

- Teorema.** Sean  $a, b, c \in \mathbb{Z}$  con  $\text{mcd}(a, b) = 1$ . Si  $a \mid bc$  entonces  $a \mid c$ .

**Demostración.** Por la identidad de Bézout existen  $x, y \in \mathbb{Z}$  tales que  $ax + by = 1$ . Multiplicando por  $c$  obtenemos  $acx + bcy = c$ . Ahora  $a \mid a$  y por hipótesis  $a \mid bc$ , concluimos que  $a \mid a(cx) + bc(y) = c$ .  $\square$

- Calculando el inverso de 5 módulo 47 encontramos que la primera ecuación equivale a  $x \equiv 19 \pmod{47}$  (en efecto,  $5 \cdot 19 - 2 \cdot 47 = 1$ ).

Para la segunda ecuación observamos que  $21^{44} \equiv 2^{44} \pmod{19}$ . Como 19 es primo y 2 no es múltiplo de 19 tenemos que  $2^{18} \equiv 1 \pmod{19}$  (pequeño Teorema de Fermat) de modo que  $2^{44} \equiv 2^8 \equiv 256 \equiv 9 \pmod{19}$ .

Entonces el sistema es equivalente a

$$\begin{cases} x \equiv 19 & (\text{mód } 47) \\ x \equiv 9 & (\text{mód } 19). \end{cases}$$

Por el Teorema Chino de los restos, el sistema tiene solución única módulo  $19 \cdot 47 = 893$ .

Como *ya sabemos* de la primer parte que  $5 \cdot 19 \equiv 1 \pmod{47}$ , es fácil ver que una solución es  $x = 9 + 10 \cdot (19 \cdot 5) \equiv 66 \pmod{893}$ .

En definitiva la solución es  $\{66 + 893 \cdot k : k \in \mathbb{Z}\}$ .

### Ejercicio 2.

a. Sea  $G$  un grupo y  $g \in G$  un elemento de orden finito.

i) Probar que si  $k \in \mathbb{Z}$  entonces

$$o(g^k) = \frac{o(g)}{\text{mcd}(o(g), k)}.$$

ii) Deducir que  $o(g^k) = o(g)$  si y sólo si  $\text{mcd}(k, o(g)) = 1$ .

b. Sabiendo que el grupo  $U(p)$  de invertibles módulo un primo  $p$  es cíclico, probar que existen  $\varphi(p-1)$  raíces primitivas módulo  $p$ .

### Solución.

a. i) Denotamos  $n = o(g)$ ,  $d = \text{mcd}(n, k)$  y  $m = o(g^k)$ . Podemos escribir  $n = d n'$  y  $k = d k'$  siendo  $n'$  y  $k'$  enteros coprimos. Tenemos que probar que  $m = n'$ .

En primer lugar  $(g^k)^{n'} = g^{k n'} = g^{d k' n'} = g^{n k'} = (g^n)^{k'} = e^{k'} = e$ , entonces  $m \mid n'$ .

Por otro lado,  $(g^k)^m = e$ , entonces  $g^{k m} = e$  y como  $o(g) = n$  se sigue que  $n \mid k m$ . Dividiendo entre  $d$  en ambos lados tenemos que  $n' \mid k' m$  y por el Lema de Euclides  $n' \mid m$ .

En conclusión,  $m \mid n'$  y  $n' \mid m$  por lo tanto  $m = n'$ .

ii) Es claro.

b. Como  $U(p)$  es cíclico, existe un generador  $g \in U(p)$ . Como  $o(g) = p-1$  tenemos que  $U(p) = \{g^1, g^2, \dots, g^{p-1}\}$  siendo estos elementos todos distintos.

Por la parte anterior  $o(g^k) = p-1$  si y sólo si  $\text{mcd}(k, p-1) = 1$ , entonces las raíces primitivas (elementos de orden  $p-1$ ) están en biyección con  $\{k = 1, 2, \dots, p-1 : \text{mcd}(k, p-1) = 1\}$  cuyo cardinal es  $\varphi(p-1)$ .

### Ejercicio 3.

a. i) Probar que 103 es un número primo.

ii) Probar que  $g = 5$  es una raíz primitiva módulo el primo  $p = 103$ .

iii) Sabiendo que  $g^{102} \equiv 1752 \pmod{103^2}$ , probar que  $g$  es una raíz primitiva módulo  $p^2$ .

iv) Probar que  $g$  es una raíz primitiva módulo  $p^k$  para cada  $k > 2$ .

b. i) Describir el método de intercambio de claves de Diffie-Hellman.

ii) Mostrar que en el método Diffie-Hellman ambos participantes llegan a la misma clave.

### Solución.

a. i) Basta con verificar que no es múltiplo de 2, de 3, de 5, o de 7, ya que  $11^2 = 121 > 103$ .

ii) Como 103 es primo  $\varphi(103) = 102 = 2 \cdot 3 \cdot 17$ , y alcanza probar que  $5^{51} \not\equiv 1 \pmod{103}$ , que  $5^{34} \not\equiv 1 \pmod{103}$ , y que  $5^6 \not\equiv 1 \pmod{103}$ .

En efecto calculamos  $5^2 \equiv 25$ ,  $5^4 \equiv 7$ ,  $5^8 \equiv 49$ ,  $5^{16} \equiv 32$ ,  $5^{32} \equiv -6$ . Ahora tenemos que  $5^6 \equiv 5^4 \cdot 5^2 \equiv 7 \cdot 25 \equiv 72 \not\equiv 1$ , que  $5^{34} \equiv 5^{32} \cdot 5^2 \equiv -6 \cdot 25 \equiv 56 \not\equiv 1$ , y que  $5^{51} \equiv 5^{34} \cdot 5^{16} \cdot 5 \equiv 56 \cdot 32 \cdot 5 \equiv -1 \not\equiv 1$

iii) Llamemos  $n$  al orden de  $g$  módulo  $103^2$ . Como  $g^n \equiv 1 \pmod{103^2}$  también  $g^n \equiv 1 \pmod{103}$  y por la parte anterior tenemos que  $102 \mid n$ .

Por otra parte sabemos que  $n \mid \varphi(103^2) = 102 \cdot 103$ . Como 103 es primo las únicas posibilidades son  $n = 102$  o  $n = 102 \cdot 103$ .

Como  $g^{102} \not\equiv 1 \pmod{103^2}$ , concluimos que  $n = 102 \cdot 103$  y por lo tanto  $g$  es raíz primitiva módulo  $103^2$ .

- iv) Por Lema 4.1.12 enunciado en teórico, si  $g$  es raíz primitiva módulo  $p^2$ , donde  $p$  es un primo impar, entonces es raíz primitiva módulo  $p^k$  para todo  $k$ .

Si se quiere hacer explícitamente: llamando  $n_k$  al orden de  $g$  módulo  $p^k$ , procediendo como en la parte anterior se ve que  $n_k = (p-1)p^i$  con  $i \in \{0, \dots, k-1\}$ .

Para finalizar, usando que  $g^{p-1} \equiv 1752 \equiv 1 + 17p \pmod{p^2}$  se puede probar por inducción en  $k \geq 2$  que  $g^{(p-1)p^{k-2}} \equiv 1 + 17p^{k-1} \not\equiv 1 \pmod{p^k}$ . Concluimos que  $n_k \nmid (p-1)p^{k-2}$  y la única opción posible es  $n_k = (p-1)p^{k-1}$ .

- b. i) Ana y Beto eligen un primo grande  $p$  y un elemento  $g \in U(p)$  con orden grande (por ejemplo, una raíz primitiva).  
 Ana elige un entero secreto  $A$  y calcula  $a \equiv g^A \pmod{p}$ , enviándolo a Beto.  
 Beto elige un entero secreto  $B$  y calcula  $b \equiv g^B \pmod{p}$ , enviándolo a Ana.  
 Son públicos  $p, g, a, b$ , y secretos  $A$  (conocido por Ana) y  $B$  (conocido por Beto).  
 Ana calcula  $k \equiv b^A \pmod{p}$  y Beto calcula  $k' \equiv a^B \pmod{p}$ .  
 ii) En efecto  $k \equiv b^A \equiv (g^B)^A \equiv g^{BA} \equiv g^{AB} \equiv (g^A)^B \equiv a^B \equiv k'$ .

#### Ejercicio 4.

- a. Describir todos los elementos de  $(U(15), \times)$  indicando su orden y cuál es su inverso.  
 b. Describir todos los homomorfismos de  $(\mathbb{Z}_4, +)$  en  $(U(15), \times)$ .  
 Indicar cuáles son inyectivos.  
 c. i) Encontrar un homomorfismo inyectivo  $f : (\mathbb{Z}_2, +) \rightarrow (U(15), \times)$  y un homomorfismo inyectivo  $g : (\mathbb{Z}_4, +) \rightarrow (U(15), \times)$  tales que  $\text{Im}(f) \cap \text{Im}(g) = \{1\}$ .  
 ii) Probar que la función  $h : (\mathbb{Z}_2 \times \mathbb{Z}_4, +) \rightarrow (U(15), \times)$  dada por

$$h(a, b) = f(a)g(b)$$

es un homomorfismo.

- iii) ¿Es el homomorfismo  $h$  un isomorfismo?

#### Solución.

- a.  $U(15) = \{x = 1, \dots, 15 : \text{mcd}(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ . Elevando al cuadrado encontramos que  $4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$  y  $\{4, 11, 14\}$  son todos elementos de orden 2. Además  $2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4 \pmod{15}$ , entonces  $2^4 \equiv 7^4 \equiv 8^4 \equiv 13^4 \equiv 1 \pmod{15}$  y  $\{2, 7, 8, 13\}$  son todos elementos de orden 4 (no pueden tener orden 3 por el Teorema de Lagrange). Finalmente 1 tiene orden 1.

- b. Como  $\mathbb{Z}_4$  es cíclico generado por 1 de orden 4, cualquier homomorfismo es de la forma  $g(n) = x^n$  para algún  $x \in U(15)$  con  $o(x) \mid 4$ . Esto último vale para cualquier  $x \in U(15)$ , entonces hay 8 homomorfismos  $g : \mathbb{Z}_4 \rightarrow U(15)$ , uno para cada posible  $x$ .

La imagen de  $g(n) = x^n$  es el subgrupo  $\langle x \rangle$  de  $U(15)$ . Para que  $g$  sea inyectivo, su imagen debe tener orden 4, es decir  $o(x) = 4$ . Entonces los homomorfismos inyectivos son los cuatro dados por  $g(n) = x^n$  donde  $x = 2, 7, 8, 13$ .

- c. i) Por ejemplo  $f(n) = 11^n$  y  $g(n) = 2^n$ , ya que  $\text{Im}(f) = \{1, 11\}$  y  $\text{Im}(g) = \{1, 2, 4, 8\}$ .  
 ii) Sean  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$  y  $(a', b') \in \mathbb{Z}_2 \times \mathbb{Z}_4$ . Entonces  $h(a + a', b + b') = 11^{a+a'} \cdot 2^{b+b'} = 11^a \cdot 11^{a'} \cdot 2^b \cdot 2^{b'} = (11^a \cdot 2^b) \cdot (11^{a'} \cdot 2^{b'}) = h(a, b) \cdot h(a', b')$ .  
 iii) En efecto  $\text{Im}(h)$  contiene a  $\text{Im}(f)$  y a  $\text{Im}(g)$  entonces  $|\text{Im}(h)| \geq 5$  pero por el Teorema de Lagrange debe dividir a  $|U(15)| = 8$ . Entonces  $h$  es sobreyectiva, y como  $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8 = |U(15)|$  se concluye que  $h$  es un isomorfismo.

Nota: también pueden calcularse explícitamente los 8 valores de  $h$  y verificar de manera directa que el núcleo es trivial.