

Ejercicio 1.

- a. Definir la función φ de Euler.
Ver notas teóricas.

- b. Enunciar y demostrar el Teorema de Euler.
Ver notas teóricas.

- c. i) Probar que 127 es primo.

Solución: Como $127 < 13^2$ alcanza con probar que 127 no es divisible por los primos 2, 3, 5, 7 y 11. Veamos eso: $127 = 63 \cdot 2 + 1$, $127 = 42 \cdot 3 + 1$, $127 = 25 \cdot 5 + 2$, $127 = 18 \cdot 7 + 1$ y $127 = 11 \cdot 11 + 6$.

- ii) Hallar $0 \leq x < 127$ tal que $x \equiv 3^{502} \pmod{127}$.

Solución: Como $\text{mcd}(3, 127) = 1$ podemos aplicar el Teorema de Euler. Como 127 es primo sabemos que $\varphi(127) = 126$ y $502 = 126 \cdot 3 + 124 \equiv -2 \pmod{126}$. Por lo tanto $3^{502} \equiv 3^{-2} \pmod{127} \equiv 9^{-1} \pmod{127}$. Utilizando el Algoritmo extendido de Euclides vemos que $1 = 9 \cdot (-14) + 127 \cdot 1$ de donde deducimos que

$$3^{502} \equiv 9^{-1} \pmod{127} \equiv -14 \pmod{127} \equiv 113 \pmod{127}.$$

- d. Hallar $0 \leq x < 363$ tal que $x \equiv 12^{332} \pmod{363}$.

Solución: En este caso no podemos aplicar el Teorema de Euler ya que $\text{mcd}(12, 363) = 3$. Pero podemos aplicar el teorema chino del resto de la siguiente manera:

$$x \equiv 12^{332} \pmod{363} \Leftrightarrow \begin{cases} x \equiv 12^{332} \pmod{3} \\ x \equiv 12^{332} \pmod{11^2} \end{cases}$$

Claramente $12^{332} \equiv 0 \pmod{3}$, por lo que falta reducir la otra congruencia. Sabemos que $\varphi(11^2) = 11 \cdot 10 = 110$ y $\text{mcd}(12, 11^2) = 1$, aplicando el Teorema de Euler vemos que $12^{332} \equiv 12 \equiv 12^2 \pmod{11^2} \equiv 144 \pmod{11^2} \equiv 23 \pmod{11^2}$. Tenemos que resolver entonces:

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 23 \pmod{11^2} \end{cases},$$

que tiene solución $23 + 11^2$. Por lo tanto $x = 23 + 11^2 = 144$.

Ejercicio 2.

a. Sea G un grupo abeliano y $x, y \in G$ tales que $o(x) = ab$, con $a, b \in \mathbb{Z}^+$.

i) Probar que $o(x^a) = b$.

Solución: Alcanza con probar que $(x^a)^b = e$ y que si $(x^a)^c = e$ entonces $b|c$.

Veamos la primer afirmación: $(x^a)^b = x^{ab} = e$ ya que $o(x) = ab$. Si $(x^a)^c = e$ entonces $x^{ac} = e$ y $ab|ac$ de donde concluimos que $b|c$.

ii) Probar que si x e y tienen órdenes coprimos entonces $o(xy) = o(x)o(y)$. **Solución:**
Ver notas teóricas: Lema 4.1.7

b. Sea G el grupo de invertibles módulo 157, $G = U(157)$.

i) Sabiendo que en G , $o(16) = 13$ y que $2^{12} \equiv 14 \pmod{157}$, hallar el orden de 2 en G .

Solución: $o(2^4) = 13 \Rightarrow \frac{o(2)}{\text{mcd}(o(2), 4)} = 13 \Rightarrow o(2) = 13 \text{ mcd}(o(2), 4)$. Y como $\text{mcd}(o(2), 4) \in \{1, 2, 4\}$ tenemos que $o(2) \in \{13, 26, 52\}$. Por letra $2^{12} \equiv 14 \pmod{157} \Rightarrow 2^{13} \equiv 28 \pmod{157} \Rightarrow o(2) \neq 13$. También $2^{26} = (2^{13})^2 \equiv (28)^2 \pmod{157} \equiv 156 \pmod{157} \Rightarrow o(2) \neq 26$ y por lo tanto $o(2) = 52$.

ii) Sabiendo que $2^{46} \equiv 27 \pmod{157}$ hallar el orden de 3 en G .

Solución $o(3^3) = o(27) = o(2^{46}) = \frac{o(2)}{\text{mcd}(o(2), 46)} = \frac{52}{\text{mcd}(52, 46)} = 26$, y como

$o(3^3) = \frac{o(3)}{\text{mcd}(o(3), 3)}$ tenemos que $o(3) = 26 \text{ mcd}(o(3), 3)$

Si $\text{mcd}(o(3), 3) = 1$ tendríamos que $o(3) = 26$; calculamos entonces 3^{26} :

$3^{26} = 3^{24}3^2 = (3^3)^8 9 \equiv (2^{46})^8 9 \equiv 2^{368} 9 \equiv (2^{52})^7 2^{49} \equiv (1)^7 16(9) \equiv 144 \pmod{157} \neq 1$ por lo que $o(3) \neq 26$ y entonces $o(3) = 78$.

iii) Hallar una raíz primitiva módulo 157.

Solución: Por la parte a(ii), al ser G abeliano, podemos buscar x e y con $\text{mcd}(o(x), o(y)) = 1$ y $o(x)o(y) = 156 = \varphi(157)$. En ese caso tomando $g = xy$ tendríamos (por a(ii)) que $o(g) = o(x)o(y) = 156$, y entonces g sería raíz primitiva módulo 157

Como $o(2) = 52 = 13 \times 4$ y $o(3) = 78 = 2 \times 39$, por la parte a(i) tenemos que $o(2^{13}) = 4$ y $o(3^2) = 39$ y como $\text{mcd}(4, 39) = 1$ y $4 \times 39 = 156$ tomamos $x = 2^{13} \equiv 28$ e $y = 3^2 = 9$. Entonces $g = xy = 28 \times 9 \equiv 95 \pmod{157}$ es r.p. módulo 157

iv) ¿Cuántos homomorfismos $f : U(314) \rightarrow \mathbb{Z}_{15}$ hay?

Solución: Como $314 = 2(157)$ y 157 es primo, sabemos que existe g raíz primitiva módulo 314; es decir $U(314) = \langle g \rangle$ (y $o(g) = 156$.)

Por lo tanto, los homomorfismo $F : U(314) \rightarrow \mathbb{Z}_{15}$ quedan determinados por $F(g) = k$ tal que $o(k) | o(g)$ (y luego $F(g^n) = F(g)^n (= nk)$).

Es decir, que hay tantos homomorfismos como posibles $k \in \mathbb{Z}_{15}$ con $o(k) | 156$. Como (por Lagrange) $o(k) | |\mathbb{Z}_{15}| = 15$ buscamos los $k \in \mathbb{Z}_{15}$ tales que $o(k) | \text{mcd}(156, 15) = 3$. Los únicos k son $k = \bar{0}$ (de orden 1) y $k = \bar{5}$ o $k = \bar{10}$ (ambos de orden 3).

Entonces hay 3 homomorfismos.

Ejercicio 3.

- a. Hallar todos los a, b enteros positivos tales que $a + b = 87$ y $\text{mcd}(a, b) + \text{mcm}(a, b) = 633$.

Solución: Sea $d = \text{mcd}(a, b)$, como $d|a$ y $d|b$ entonces $d|87 = 3 \cdot 29$. Por otro lado, como $d|\text{mcm}(a, b)$ entonces $d|633$ y $d|\text{mcd}(87, 633) = 3$. Concluimos que $d \in \{1, 3\}$. También sabemos que $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = |ab|$ y como buscamos a y b positivos tenemos que

$$ab + d^2 = d633.$$

Si $d = 1$: tenemos $ab = 632 = 2^3 \cdot 79$ y $a + b = 87$. Como $d = 1$ entonces a y b son coprimos y vemos que las únicas opciones en este caso son $(a, b) = (8, 79)$ y $(a, b) = (79, 8)$.

Si $d = 3$: tenemos $ab + 9 = 3 \cdot 633$ y $ab = 3(633 - 3) = 3^2(211 - 1) = 2 \cdot 3^3 \cdot 5 \cdot 7$. Viendo las opciones posibles deducimos que las soluciones que nos sirven son $(a, b) = (45, 42)$, $(a, b) = (42, 45)$.

- b. Enunciar y demostrar el Lema de Euclides.

Ver notas teóricas.

- c. Hallar todos los a, b enteros tales que $ab + 3a = \frac{4b^2}{\text{mcd}(a, b)} + 9b$.

Solución: Definimos $d = \text{mcd}(a, b)$ y escribimos $a = d \cdot a^*$, $b = d \cdot b^*$, donde sabemos que $\text{mcd}(a^*, b^*) = 1$. Por lo tanto $d^2 a^* b^* + 3da^* = 4d(b^*)^2 + 9db^*$, eliminando una d obtenemos

$$da^* b^* + 3a^* = 4(b^*)^2 + 9b^*.$$

Claramente b^* divide a el lado derecho de esa ecuación, por lo tanto $b^*|da^* b^* + 3a^*$ y $b^*|3a^*$. Como a^* y b^* son coprimos entonces por el Lema de Euclides deducimos que $b^*|3$, por lo que $b^* \in \{1, 3\}$.

Si $b^* = 1$: entonces $a^*(d + 3) = 13$ por lo que $a^* = 1$ o $a^* = 13$, ya que 13 es primo.

Si $a^* = 1$ entonces $d = 10$, de donde obtenemos la solución $(a, b) = (10, 10)$. Si $a^* = 13$ entonces $d + 3 = 1$, que no puede pasar.

Si $b^* = 3$ entonces $a^*(d + 1) = 21$. Como antes $a^* = 1$, $a^* = 3$, $a^* = 7$ o $a^* = 21$. Si $a^* = 1$ entonces $d = 20$ y obtenemos la solución $(a, b) = (20, 60)$. No puede pasar $a^* = 3$ ya que tiene que ser coprimo con b^* . Si $a^* = 7$ entonces $d = 2$ y obtenemos la solución $(a, b) = (14, 6)$. No puede pasar $a^* = 21$ ya que tiene que ser coprimo con b^* .

Las soluciones entonces son

$$(10, 10), (20, 60), (14, 6).$$