

Soluciones

Ejercicio 1

1) Ver el teórico

2) Como r es un elemento del grupo $U(n)$, entonces por un resultado del teórico que dice que en cualquier grupo $g^i = g^j$ sii $i \equiv j \pmod{o(g)}$. Pero como r es raíz primitiva, $o(r) = \varphi(n)$.

3) Demostrar que 2 es una raíz primitiva módulo 11. Como $\varphi(11) = 10 = 2 \cdot 5$ basta ver que $2^2 \not\equiv 1 \pmod{11}$ y que $2^5 \not\equiv 1 \pmod{11}$, Efectivamente $2^2 \equiv 4 \not\equiv 1 \pmod{11}$ y $2^5 \equiv 32 \equiv -1 \not\equiv 1 \pmod{11}$.

4) Haciendo $y = 2x$ tenemos que

$$x^5 \equiv -1 \pmod{11} \iff y^5 2^5 \equiv -1 \pmod{11} \iff y^5 \equiv 1 \pmod{11}$$

Que tiene 5 soluciones por la parte 1.

5) Como 2 es raíz primitiva, entonces existirá i tal que $y = 2^i$, de modo que $2^{5i} \equiv 2^0 \pmod{11}$ lo cual, por la parte 2) sucede sii $5i \equiv 0 \pmod{10} \iff i \equiv 0 \pmod{2} \iff i = 2h$ con $h = 0, 1, 2, 3, 4$, de donde las soluciones son $x = 2 \cdot 2^{2h}$ con $h = 0, 1, 2, 3, 4$, o sea $x = 2, 8, 32 \equiv 10, 7, 6$ respectivamente.

Ejercicio 2

Partes (a), (b) y (d) ver teórico.

Parte (c): Deben conmutar, en S_3 tomamos $x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ y $y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, entonces $o(x) = 2$ y $o(y) = 3$, pero $o(xy) \neq 6$, pues los elementos de S_3 solo tienen ordenes 1, 2 y 3. Que sean coprimos también debe ser cumplido, como ejemplo, si $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $x = (1, 0)$ y $y = (0, 1)$, entonces $xy = yx$, $o(x) = o(y) = 2$ pero $o(xy) = 2$.

Ejercicio 3

(a) $x = 91 + 101k \equiv 10 \pmod{13} \Rightarrow 91 + 101k \equiv 10 \pmod{13} \Rightarrow 10k \equiv 10 \pmod{13} \Rightarrow k \equiv 1 \pmod{13} \Rightarrow x = 91 + 101(1 + 13h) \Rightarrow x = 192 + 1313h$, de donde $x = 192$

(b) Ver teórico.

(c) Para calcular $E(10) \equiv 10^{271} \pmod{1313}$ hacemos $E(10) \equiv \pmod{101}$ y $E(10) \equiv \pmod{13}$. Para ello hacemos $10^{271} \equiv 10^{71} \pmod{101}$ pues $\varphi(101) = 100$. Además $10^{71} = 100^{35} \times 10 \equiv (-1)^{35} \times 10 \equiv -10 \equiv 91 \pmod{101}$. Por otro lado $E(10) \equiv 10^7 \pmod{13}$ pues $271 \equiv 7 \pmod{\varphi(13)}$. Haciendo exponenciación rápida tenemos $10^2 = 100 \equiv 9 \pmod{13}$ y $9^2 = 81 \equiv 3 \pmod{13}$, luego $10 = 10 \cdot 9 \cdot 3 \equiv -3 \cdot 9 \cdot 3 = -9^2 \equiv -3 \equiv 10 \pmod{13}$. Por lo que $x = 192$.