

Ejercicio 1.

- a. Como $\text{mcd}(19, 2) = 1$ y $\varphi(19) = 18 = (2)(3^2)$ basta con probar que $2^6 \not\equiv 1 \pmod{19}$ y $2^9 \not\equiv 1 \pmod{19}$. Calculamos: $2^6 = 64 \equiv 7 \pmod{19} \not\equiv 1 \pmod{19}$ y $2^9 = 2^6 2^3 \equiv 7(8) \pmod{19} \equiv 56 \pmod{19} \equiv 18 \pmod{19} \not\equiv 1 \pmod{19}$.
- b. (**Ejercicio 8bi del práctico 9.2**) Si m es el orden de g en $U(p^2) \Rightarrow g^m \equiv 1 \pmod{p^2} \Rightarrow p^2 \mid (g^m - 1) \Rightarrow p \mid (g^m - 1) \Rightarrow g^m \equiv 1 \pmod{p}$ y entonces el orden de g en $U(p)$ divide a m . Al ser g raíz primitiva módulo p , el orden de g en $U(p)$ es $p-1$ y por lo tanto $p-1 \mid m$.
- c. Por la parte anterior sabemos que si m es el orden del 2 en $U(19^2)$, $18 \mid m$. Pero además $m \mid \varphi(19^2) = 18(19)$ por lo que $m = 18$ o $m = 18(19)$. Calculamos $2^{18} \pmod{361}$ (usaremos que $361(3) = 1083$). $2^{10} = 1024 \equiv -59 \pmod{361} \Rightarrow 2^{12} \equiv (-59)(4) \equiv -236 \equiv 125 \Rightarrow 2^{15} \equiv 1000 \equiv (-83) \Rightarrow 2^{17} \equiv -332 \equiv 29$ y entonces $2^{18} \equiv 58 \pmod{361} \not\equiv 1 \pmod{361}$. Por lo tanto $m \neq 18$, y entonces $m = 18(19)$ por lo que 2 es raíz primitiva módulo 361.
- d. (**Ejercicio 10a del práctico 9.2**) Al ser p primo impar tenemos que $\text{mcd}(2, p^2) = 1$ y por lo tanto, utilizando el Teo Chino del Resto tenemos que

$$x^m \equiv 1 \pmod{2p^2} \Leftrightarrow \begin{cases} x^m \equiv 1 \pmod{2} \\ x^m \equiv 1 \pmod{p^2} \end{cases}.$$

Si x es impar, x^m es impar y por lo tanto $x^m \equiv 1 \pmod{2}$ y entonces $x^m \equiv 1 \pmod{2p^2} \Leftrightarrow x^m \equiv 1 \pmod{p^2}$.

- e. Tomando $x = 2 + 361 = 363$ y $p = 19$, tenemos que $2p^2 = 2(361) = 722$ y por la parte anterior tenemos que $(363)^m \equiv 1 \pmod{722} \Leftrightarrow (363)^m \equiv 1 \pmod{361} \Leftrightarrow 2^m \equiv 1 \pmod{361} \Leftrightarrow (18)(19) \mid m$ (lo último por la parte c). Así que el orden de 363 en $U(722)$ es $(18)(19) = \varphi(722)$ por lo que 363 es raíz primitiva módulo 722.

Ejercicio 2.

- a. $x^2 \in H \Rightarrow o(x^2) \mid 24 \Rightarrow o(x^2) \in \{1, 2, 3, 4, 6, 8, 12, 24\}$ y $2o(x^2) \in \{2, 4, 6, 8, 12, 16, 24, 48\}$ (respectivamente). Como $x \notin H$, $o(x) \nmid 24$ y en particular $o(x) \neq o(x^2) = \frac{o(x)}{\text{mcd}(o(x), 2)} \Rightarrow \text{mcd}(o(x), 2) \neq 1 \Rightarrow \text{mcd}(o(x), 2) = 2 \Rightarrow o(x) = 2o(x^2)$. Por lo tanto $2o(x^2) = o(x) \nmid 24$ así que las únicas posibilidades para $o(x) = 2o(x^2)$ son 16 y 48.
- b. (**Ejercicio 4 del práctico 9.2**) Como 241 es primo, el teorema de la raíz primitiva nos asegura que existe $g \in G$ tal que $G = \langle g \rangle = \{g^m : m \in \{1, 2, \dots, 240\}\}$. Como

$$o(g^m) = \frac{o(g)}{\text{mcd}(o(g), m)} = \frac{240}{\text{mcd}(240, m)}$$

tenemos que $o(g^m) \mid 24 \Leftrightarrow \frac{240}{\text{mcd}(240, m)} \mid 24 \Leftrightarrow 10 \mid \text{mcd}(240, m) \Leftrightarrow 10 \mid m$. Entonces $H = \{g^m : m \in \{1, 2, \dots, 240\} \text{ y } 10 \mid m\} = \{g^{10z} : z \in \{1, 2, \dots, 24\}\}$ y por lo tanto $\#H = 24$.

- c. Calculamos el orden de $\bar{2}$ en $U(241)$: $2^8 = 256 \equiv 15 \not\equiv 1$; $2^9 \equiv 30$, $2^{10} \equiv 60$, $2^{11} \equiv 120$, $2^{12} \equiv 240 \equiv -1 \not\equiv 1$ y $2^{24} \equiv 1$. Por lo tanto $o(2) \mid 24$ y $o(2) \nmid 8, 12$ por lo que $o(\bar{2}) = 24$. Ahora (por consecuencia de Lagrange) si $h \in \langle \bar{2} \rangle$, $o(h) \mid |\langle \bar{2} \rangle| = 24$ y entonces $h \in H$. Por lo tanto $\langle \bar{2} \rangle \subset H$ y como ambos conjuntos tienen 24 elementos $\langle \bar{2} \rangle = H$.

Para listar los elementos de H , observamos que como $2^{12} \equiv -1$, entonces $2^{12+k} \equiv -2^k \equiv 241 - 2^k \pmod{241}$. Así que los elementos de H son las clases de $\pm 2^k$ con $k = 0, 1, \dots, 11$; los listamos a continuación:

k	0	1	2	3	4	5	6	7	8	9	10	11
$2^k \equiv$	1	2	4	8	16	32	64	128	15	30	60	120
$2^{12+k} \equiv$	240	239	237	233	225	209	177	113	226	211	181	121

- d. Por la parte anterior tenemos que $11 \notin H$ y $11^2 = 121 = 2^{23} \in H$. Así que por la parte a), $o(11) \in \{16, 48\}$ y $o(11^2) = 2o(11) \in \{8, 24\}$ respectivamente.
 Pero como $11^2 = 2^{23}$ y $\text{mcd}(23, 24) = 1$, $o(11^2) = o(2^{23}) = o(2) = 24$ por lo que $o(11) = 48$.
- e. $o(10^5) = o(2^{20}) = \frac{24}{\text{mcd}(24, 20)} = \frac{24}{4} = 6$. Entonces $\frac{o(10)}{\text{mcd}(o(10), 5)} = 6$ y como $10 \notin H$, $o(10) \neq 6$ por lo que $o(10) = 30$.
- f. Por las partes anteriores tenemos que $o(10^6) = \frac{30}{6} = 5$ y $o(11) = 48$. Como $\text{mcd}(5, 48) = 1$ tenemos que $o(10^6(11)) = 5(48) = 240$ y por lo tanto $10^6(11)$ es raíz primitiva módulo 241.
 Otra posibilidad es que $o(10^2) = 15$ que es coprimo con $o(11^3) = 16$, así que $o((10)^2(11)^3) = 15(16) = 240$ por lo que $(10)^2(11)^3$ también es raíz primitiva módulo 241.
- g. Tenemos que $k \equiv g^{ab}$ (mód 241) por lo que en $U(241)$,

$$o(k) = o(g^{ab}) = \frac{o(g)}{\text{mcd}(o(g), ab)} = \frac{240}{\text{mcd}(240, 50(56))} = \frac{240}{80} = 3.$$

Como $3 \mid 24$ tenemos que $k \in H = \langle \bar{2} \rangle$. Así que $k \equiv 2^m$ (mód 241) con $m \in \{1, \dots, 24\}$ y como $3 = o(k) = o(2^m) = \frac{24}{\text{mcd}(24, m)}$ concluimos que $\text{mcd}(24, m) = 8$ y por lo tanto por lo que $m = 8$ o $m = 16$. Entonces $k \equiv 2^8 \equiv 15$ o $k \equiv 2^{16} \equiv 225$.

Ejercicio 3. Las 3 primeras partes de este ejercicio se encuentran en las notas del curso, en los enunciados y demostraciones de Teorema de Lagrange y del Teorema de Órdenes (Teoremas 3.8.1 y 3.9.8).

- a. (**pag. 56**) Si $k \in C$, tenemos que $g \in C \Leftrightarrow g \sim k \Leftrightarrow gk^{-1} \in H \Leftrightarrow \exists h \in H : gk^{-1} = h \Leftrightarrow \exists h \in H : g = hk$. Entonces $C = \{hk : h \in H\}$; es decir que multiplicando a k (a la izquierda) por todos los elementos de H obtenemos todos los elementos de C . Para ver que $\#C = |H|$ resta ver que si $h \neq h'$, los elementos que obtenemos en C (hk y $h'k$) son distintos. Esto se debe a la propiedad cancelativa en un grupo G ya que $hk = h'k \Leftrightarrow h = h'$ (cancelando k).
- b. (**pag. 60**) $g \sim k \Leftrightarrow gk^{-1} \in H = \ker(F) \xrightarrow{\text{def. } \ker(F)} F(gk^{-1}) = e_A$. Al ser F homomorfismo, tenemos que $F(gk^{-1}) = F(g)F(k^{-1}) = F(g)F(k)^{-1}$; así que $g \sim k \Leftrightarrow F(g)F(k)^{-1} = e_A \xLeftrightarrow[\times F(k)] F(g) = F(k)$.
- c. **Enunciado (Teorema 3.9.8, pag. 59):** Si $F : G \rightarrow A$ es un homomorfismo de grupos finitos, entonces $|G| = |\ker(F)||\text{Im}(F)|$.
Demostración (por ejemplo pág. 55 y pág. 60): Consideramos la relación de equivalencia de la letra para $H = \ker(F)$. El conjunto $\mathcal{C} = \{C_1, \dots, C_m\}$ de clases de equivalencia (distintas) es una partición de G (son disjuntas y su unión es G), así que

$$|G| = \sum_{i=1}^m \#C_i \stackrel{(a)}{=} \sum_{i=1}^m |H| = m|H| = m|\ker(F)|.$$

Resta ver que $m = |\text{Im}(F)|$ (donde m es la cantidad de clases de equivalencia):

Fijado i , por la parte b) tenemos que $\forall k, g \in C_i, F(k) = F(g)$. Llamamos entonces $a_i = F(g)$ siendo g cualquier elemento de C_i y como $G = C_1 \cup \dots \cup C_k$ tenemos que $\text{Im}(F) = F(C_1) \cup \dots \cup F(C_m) = \{a_1, \dots, a_m\}$. Ahora, si $i \neq j$, tomando $g \in C_i$ y $g \in C_j$ tenemos que $g \not\sim k \stackrel{(b)}{\Rightarrow} F(g) \neq F(k) \Rightarrow a_i \neq a_j$. Por lo que $m = \#\{a_1, \dots, a_m\} = |\text{Im}(F)|$.

- d. Por una consecuencia de Lagrange tenemos que si $a \in A$ entonces $a^{|A|} = e_A$. Si F es sobreyectiva $A = \text{Im}(F)$ y entonces $a^{|\text{Im}(F)|} = e_A$. Elevando ambos lados a $|\ker(F)|$ tenemos que $a^{|\text{Im}(F)||\ker(F)|} = e_A^{|\ker(F)|} = e_A$ y por el Teorema de Homomorfismos concluimos que $a^{|G|} = e_A$.