

SOLUCION del EXAMEN DE MATEMÁTICA DISCRETA 2

Ejercicio 1.

- A. Hay que probar que $10^n \equiv 10 \pmod{30}$. Por el Teo chino del resto, como $\text{mcd}(3, 10) = 1$, esto es equivalente a probar que

$$\begin{cases} 10^n \equiv 10 \pmod{10} \\ 10^n \equiv 10 \pmod{3}. \end{cases}$$

La primer ecuación vale dado que ambos lados son congruentes con 0 módulo 10. La segunda ecuación vale dado que ambos lados son congruentes con 1 módulo 3.

- B. Como 31 es primo y 31 no divide a 10, tenemos por Fermat que $10^{30} \equiv 1 \pmod{31}$. Por la parte A. tenemos que existe k entero tal que $10^n = 30k + 10$ así que $10^{10^n} = 10^{30k+10} = (10^{30})^k 10^{10} \equiv 10^{10} \pmod{31}$. Y como $10^2 = 100 \equiv 7 \pmod{31} \Rightarrow 10^4 = 49 \equiv 18 \pmod{31} \Rightarrow 10^8 = 18^2 = 324 \equiv 14 \pmod{31} \Rightarrow 10^{10} = 10^2 10^8 \equiv 7 \times 14 \pmod{31} \equiv 98 \pmod{31} \equiv 5 \pmod{31}$. Así que el resto de dividir 10^{10^n} entre 31 es 5.
- C. Por la parte B tenemos que $10^{10000} = 10^{10^4} \equiv 5 \pmod{31}$. Así que $10^{9999} 10 \equiv 5 \pmod{31}$. Si c es el inverso de 10 módulo 31, tenemos que $10^{9999} \equiv 5c \pmod{31}$. Como $1 = 31 - 3(10)$ así que $10(-3) \equiv 1 \pmod{31}$. Por lo tanto $10^{9999} \equiv 5(-3) \pmod{31} \equiv -15 \pmod{31} \equiv 16 \pmod{31}$. Así que el resto de dividir 10^{9999} entre 31 es 16.

Ejercicio 2.

- A. a) Sea r el resto de dividir a entre m ; entonces $a = km + r$ con $0 \leq r < m$. Entonces $g^a = g^{km+r} = (g^m)^k g^r = e^k g^r = e g^r = g^r$ (la tercer igualdad pues m es el orden de g). Si $m|a$ entonces $r = 0$ y por lo tanto $g^a = g^0 = e$. Si $g^a = e$, entonces $g^r = e$, pero por definición de orden, m es el menor entero mayor que cero tal que $g^m = e$; y como $0 \leq r < m$ necesariamente $r = 0$ así que $m|a$.
- b) Tenemos que $g^a = g^b \Leftrightarrow g^a (g^b)^{-1} = g^b (g^b)^{-1} \Leftrightarrow g^a (g^b)^{-1} = e \Leftrightarrow g^{a-b} = e$. Y por la parte a) esto vale si y sólo si $m|(a-b)$; es decir, si y sólo si $a \equiv b \pmod{m}$.
- B. Como x es coprimo con n y g es raíz primitiva módulo n , tenemos que existe c entero tal que $x = g^c \pmod{n}$. Así que $x^a \equiv g^b \pmod{n} \Leftrightarrow (g^c)^a \equiv g^b \pmod{n} \Leftrightarrow g^{ca} \equiv g^b \pmod{n}$. Como g es raíz primitiva módulo n , el orden de g en $U(n)$ es $\varphi(n)$; así que por la parte Ab) tenemos que $g^{ca} \equiv g^b \pmod{n} \Leftrightarrow ac \equiv b \pmod{\varphi(n)}$.
- C. Como $\varphi(242) = \varphi(2 \times 11^2) = \varphi(2)\varphi(11^2) = 1(11^2 - 11) = 110$ y $\text{mcd}(7, 242) = 1$, por Euler tenemos que $7^{110} \equiv 1 \pmod{242}$; así que por la parte Aa) tenemos que si m es el orden de 7 en $U(242)$ entonces $m|110$, es decir que m divide a $2 \times 5 \times 11$. Para probar que $m = 110$, basta con probar que m no divide ni a 10, ni a 22 ni a 55. Como $7^{10} \equiv 23 \pmod{242}$, en particular $7^{10} \not\equiv 1 \pmod{242}$ así que m no divide a 10. Además $7^{11} = 7^{10} \times 7 \equiv 23 \times 7 \pmod{242} \equiv 161 \pmod{242}$. Si m dividiera a 22, tendríamos que $7^{22} \equiv 1 \pmod{242}$ y por lo tanto tendríamos que $7^{55} = (7^{22})^2 7^{11} \equiv 7^{11} \pmod{242} \equiv 161 \pmod{242}$. Pero por dato tenemos que $7^{55} \equiv 241 \pmod{242}$ así que m no divide a 22. A su vez, como $7^{55} \equiv 241 \pmod{242} \not\equiv 1 \pmod{242}$ tenemos que m no divide a 55.
- D. Si $x^3 \equiv 23 \pmod{242}$, como $\text{mcd}(23, 242) = 1$ entonces $\text{mcd}(x^3, 242) = 1$ y entonces $\text{mcd}(x, 242) = 1$. Y como 7 es raíz primitiva, tenemos que $x \equiv 7^c \pmod{242}$ para algún entero c . Por la parte B. (como $23 \equiv 7^{10} \pmod{242}$) tenemos que $x^3 \equiv 7^{10} \pmod{242} \Leftrightarrow 3c \equiv 10 \pmod{110}$. Como $3 \times 37 \equiv 1 \pmod{110}$ tenemos que $c \equiv 10 \times 37$

(mód 110) $\equiv 40$ (mód 110). Por lo tanto $x^3 \equiv 23$ (mód 242) $\Leftrightarrow x \equiv 7^{40}$ (mód 242). Por otro lado, como 7 es raíz primitiva módulo 41, el orden de 7 en $U(41)$ es 40, así que $7^{20} \equiv -1$ (mód 41) $\equiv 40$ (mód 41). De forma análoga al anterior, tenemos que $x \equiv 7^d$ (mód 41) con d tal que $11d \equiv 20$ (mód 40); como $11(11) \equiv 1$ (mód 40) tenemos que $d \equiv 20(11)$ (mód 40) $\equiv 220$ (mód 40) $\equiv 20$ (mód 40). Así que $x^{11} \equiv 40$ (mód 41) $\Leftrightarrow x \equiv 7^{20}$ (mód 41) $\equiv 40$ (mód 41). Tenemos entonces que el sistema original es equivalente al sistema

$$\begin{cases} x \equiv 7^{20} \pmod{242} \\ x \equiv 40 \pmod{41}. \end{cases}$$

Y este sistema tiene solución pues $\text{mcd}(41, 242) = 1$.

Ejercicio 3.

- A. ■ Sea $x \in G$; $x \sim x \Leftrightarrow x^{-1}x \in H \Leftrightarrow e \in H$ y esto es cierto por ser H un subgrupo de G .
- Si $x \sim y$ entonces $x^{-1}y \in H$. Como H es un subgrupo, tenemos que $(x^{-1}y)^{-1} \in H$; así que $y^{-1}x \in H$ y por lo tanto $y \sim x$.
- Si $x \sim y$ e $y \sim z$ entonces $x^{-1}y \in H$ y $y^{-1}z \in H$; por ser H subgrupo tenemos que $(x^{-1}y)(y^{-1}z) \in H$; entonces $x^{-1}z \in H$ y por lo tanto $x \sim z$.

La clase de equivalencia de g es el conjunto $\{x \in G : g \sim x\} = \{x \in G : g^{-1}x \in H\} = \{x \in G : \exists h \in H : g^{-1}x = h\} = \{x \in G : \exists h \in H : x = gh\} = gH$.

- B. a) Tenemos que hallar $(ab)h$ para todo $h \in H$. Observar que para todo a, b como en la letra se tiene que $H = \{Id, (ab)(cd), (ac)(bd), (ad)(bc)\}$.
- $(ab)Id = (ab)$.
 - $(ab)(ab)(cd) = (ab)^2(cd) = Id(cd) = (cd)$.
 - $(ab)(ac)(bd) = \tau$. Tenemos que $\tau(a) = (ab)(ac)(bd)(a) = (ab)(ac)(a) = (ab)(c) = c$; $\tau(c) = (ab)(ac)(bd)(c) = (ab)(ac)(c) = (ab)(a) = b$; $\tau(b) = (ab)(ac)(bd)(b) = (ab)(ac)(d) = d$ y $\tau(d) = (ab)(ac)(bd)(d) = (ab)(ac)(b) = (ab)(b) = a$. Así que $\tau = (acbd)$.
 - $(ab)(ad)(bc) = \tau$. Tenemos que $\tau(a) = (ab)(ad)(bc)(a) = (ab)(ad)(a) = (ab)(d) = d$; $\tau(d) = (ab)(ad)(bc)(d) = (ab)(ad)(d) = (ab)(a) = b$; $\tau(b) = (ab)(ad)(bc)(b) = (ab)(ad)(c) = c$ y $\tau(c) = (ab)(ad)(bc)(c) = (ab)(ad)(b) = (ab)(b) = a$. Así que $\tau = (adbc) = (cadb)$.
- b) Tenemos que $IdH = H$. Por la parte anterior tenemos que
- $(12)H = \{(12), (34)(1324), (3142)\}$;
 $(13)H = \{(13), (24)(1234), (2143)\}$ y
 $(14)H = \{(14), (23)(1243), (2134)\}$. Por otro lado
- $(123)H = \{(123)Id, (123)(12)(34), (123)(13)(24), (123)(14)(23)\} = \{(123), (134), (243), (142)\}$. Hasta aquí tenemos 5 clases, cada una con 4 elementos, así que resta una clase que contiene a los elementos que no están en ninguna de las clases anteriores:
- $(132)H = \{(132), (143), (234), (124)\}$.
- c) Dado que sabemos que H es un subgrupo, para probar que $H \trianglelefteq S_4$ resta probar que $\sigma\tau\sigma^{-1} \in H$ para todo τ en H y σ en S_4 . Si $\tau = Id$ entonces $\sigma\tau\sigma^{-1} = \sigma\sigma^{-1} = Id \in H$. Si $\tau = (ab)(cd)$ con $\{a, b, c, d\} = \{1, 2, 3, 4\}$ entonces $\sigma\tau\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d)) \in H$.
- d) El orden en S_4/H de IdH es 1. El orden de $(ab)H$ es 2 y el orden de $(123)H$ y de $(132)H$ es 3. Por lo tanto no hay en S_4/H elementos de orden 6. Si hubiera un isomorfismo $f : \mathbb{Z}_6 \rightarrow S_4/H$, como en \mathbb{Z}_6 el orden de $\bar{1}$ es 6, el orden de $f(\bar{1})$ en S_4/H sería 6. Así que no existe tal isomorfismo.