

EXAMEN DE MATEMÁTICA DISCRETA II

Ejercicio 1.

A. Si a y b son enteros y $d = \text{mcd}(a, b)$ entonces $\exists x, y \in \mathbb{Z}$ tales que $ax + by = d$.

B. Sea $d = \text{mcd}(a, b)$

(\Rightarrow) Si $\exists x, y \in \mathbb{Z}$ tales que $ax + by = c$, como $d|a$ y $d|b$ entonces $d|ax$ y $d|by$ y por lo tanto $d|ax + by$; entonces $d|c$.

(\Leftarrow) Como $d|c$, escribimos $c = kd$ con $k \in \mathbb{Z}$. Por Bezout tenemos que existen $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0 + by_0 = d$. Multiplicando por k tenemos $ax_0k + by_0k = dk$ y por lo tanto $a(x_0k) + b(y_0k) = c$; es decir $x = x_0k$ e $y = y_0k$ es solución entera de la ecuación.

C. Realizamos el algoritmo de Euclides extendido para $a = 35$ y $b = 15$ obteniendo $35(1) - 15(2) = 5$. Multiplicando la ecuación por 16 obtenemos: $35(16) - 15(32) = 80$ y todas las soluciones son de la forma $x = 16 + 3t$, $y = 32 + 7t$ para algún $t \in \mathbb{Z}$.

Ahora $x \geq 5 \Leftrightarrow 16 + 3t \geq 5 \Leftrightarrow 3t \geq -11 \Leftrightarrow t \geq -3$ (pues $t \in \mathbb{Z}$). También $y \leq 16 \Leftrightarrow 32 + 7t \leq 16 \Leftrightarrow 7t \leq -16 \Leftrightarrow t \leq -3$ (pues $t \in \mathbb{Z}$). Por lo tanto $t = -3$ y $x = 16 - 9 = 7$ e $y = 32 - 21 = 11$.

Ejercicio 2.

A. Claramente $*$: $K \times K \rightarrow K$.

- Asociativa: Sean $k = (g, h)$, $k' = (g', h')$ y $k'' = (g'', h'') \in K$; $(k * k') * k'' = ((g, h) * (g', h')) * (g'', h'') = (gg', hh') * (g'', h'') = ((gg')g'', (hh'h''))$ (y por asociativa en G y H) $= (g(g'g''), h(h'h'h'')) = (g, h) * (g'g'', h'h'') = k * (k' * k'')$.
- Neutro: Sea $e_K = (e_G, e_H)$, (donde e_G y e_H son los neutros de G y H respectivamente); entonces $e_K * (g, h) = (e_G, e_H) * (g, h) = (e_G g, e_H h) = (g, h) = (g e_G, h e_H) = (g, h) * (e_G, e_H) = (g, h) * e_K$, para todo $(g, h) \in K$. Entonces e_K es el neutro de K .
- Inversos: $k = (g, h) \in K$, por ser G y H grupos, $\exists g^{-1} \in G$, $h^{-1} \in H$. Sea $k^{-1} = (g^{-1}, h^{-1})$, entonces $k * k^{-1} = (g, h) * (g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H) = e_K = (e_G, e_H) = (g^{-1}g, h^{-1}h) = (g^{-1}, h^{-1}) * (g, h) = k^{-1} * k$.

B. Veamos primero que es Subgrupo:

- $e_K = (e_G, e_H) \in N$.
- Si $(g, e_H) \in N \Rightarrow (g, e_H)^{-1} = (g^{-1}, e_H) \in N$.
- Si $(g, e_H), (g', e_H) \in N$ entonces $(g, e_H)(g', e_H) = (gg', e_H e_H) = (gg', e_H) \in N$.

Veamos ahora que es normal: hay que ver que $kNk^{-1} \subset N$. Sea $n = (g, e_H) \in N$ y $k = (g', h) \in K$; entonces $knk^{-1} = (g', h)(g, e_H)((g')^{-1}, h^{-1}) = (g'gg'^{-1}, he_Hh^{-1}) = (g'gg'^{-1}, e_H) \in N$.

- C. Sea $\psi : G \rightarrow N$ dado por $\psi(g) = (g, e_N)$; entonces ψ es morfismo de grupos: $\psi(gg') = (gg', e_N) = (g, e_N)(g', e_N) = \psi(g)\psi(g')$ y claramente ψ es biyectiva (su inversa es $\psi^{-1} : N \rightarrow G$ dada por $\psi^{-1}(g, e_N) = g$ para todo $(g, e_N) \in N$). Entonces ψ es un isomorfismo.
- D. Sea $\varphi : K \rightarrow H$, dada por $\varphi(g, h) = h$. Tenemos que φ es morfismo de grupos: $\varphi((g, h)(g', h')) = \varphi(gg', hh') = hh' = \varphi(g, h)\varphi(g', h')$. Además $\text{Im}\varphi = H$ (pues para todo $h \in H$, $h = \varphi(g, h)$ para cualquier $g \in G$). Y $\ker \varphi = \{(g, h) \in K : \varphi(g, h) = e_H\} = \{(g, h) \in K : h = e_H\} = N$. Por el primer teorema de isomorfismos tenemos que $K/N \simeq H$.

Ejercicio 3.

- A. $x = a13 + b101$ con

$$\begin{aligned} a13 &\equiv 91 \pmod{101} \Leftrightarrow a \equiv 7 \pmod{101} \\ b101 &\equiv 10 \pmod{13} \Leftrightarrow b10 \equiv 10 \pmod{13} \Leftrightarrow b \equiv 1 \pmod{13}. \end{aligned}$$

Entonces $x \equiv 7(13) + 101 \pmod{101(13)} \equiv 91 + 101 \pmod{1313}$. Entonces $x = 192$.

- B. Como $\text{mcd}(\varphi(n), e) = 1$, existe $d \in \mathbb{Z}$ tal que $ed \equiv 1 \pmod{\varphi(n)}$. La función de descifrado es $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dada por $D(y) = y^d \pmod{n}$. Para mostrar que descifra hay que ver que para todo $x \in \mathbb{Z}_n$, $D(E(x)) = x$; es decir $(x^e)^d \equiv x \pmod{n}$ (ver teórico; por ejemplo en las notas de criptografía en la pág. del curso).

- C. Hay que calcular $E(10) = 10^{271} \pmod{1313}$. Usamos que $1313 = 13 \times 101$:

Si $E(10) \equiv 10^{271} \pmod{1313} \Rightarrow E(10) \equiv 10^{271} \pmod{101}$. Y como $\varphi(101) = 100$, por el teorema de Fermat tenemos que $10^{100} \equiv 1 \pmod{101}$ por lo tanto $10^{271} = 10^{71} \pmod{101}$. Ahora $10^2 = 100 \equiv (-1) \pmod{101}$ y por lo tanto $10^{71} = (10^2)^{35} 10 \equiv (-1)^{35} 10 \pmod{101} \equiv -10 \pmod{101} \equiv 91 \pmod{101}$. Es decir $E(10) \equiv 91 \pmod{101}$.

Por otro lado, como $\varphi(13) = 12$, tenemos que $E(10) \equiv 10^{271} \pmod{13} \equiv (10^{12})^{22} 10^7 \equiv 10^7 \pmod{13}$ (nuevamente por Fermat). Y $10^7 \equiv (-3)^7 \pmod{13} \equiv (-27)^2(-3) \pmod{13} \equiv (-1)^2(-3) \equiv -3 \pmod{13} \equiv 10 \pmod{13}$. Por lo tanto $E(10) \equiv 10 \pmod{13}$.

Por la parte A. concluimos que $E(10) = 192$.

Ejercicio 4.

- A. (i) Sea $d = \text{mcd}(m, n)$ y $m = dm'$. Entonces $g^m = (g^d)^{m'} \in \langle g^d \rangle$ y por lo tanto $\langle g^m \rangle \subset \langle g^d \rangle$.

Por Bezout tenemos que existe $x, y \in \mathbb{Z}$ tales que $d = mx + ny$. Entonces $g^d = g^{mx+ny} = g^{mx}g^{ny} = (g^m)^x(g^n)^y = (g^m)^xe = (g^m)^x \in \langle g^m \rangle$. Entonces $\langle g^d \rangle \subset \langle g^m \rangle$.

- (ii) Si $d|n$, llamamos $n' = n/d \in \mathbb{Z}$.

Entonces $(g^d)^{n'} = g^{dn'} = g^n = e$ y si $(g^d)^k = e \Rightarrow g^{dk} = e \Rightarrow n|dk \Rightarrow dn'|dk \Rightarrow n'|k$. Entonces si $n' > 0$ tenemos que $o(g^d) = n'$ y si $n' < 0$ tenemos que $o(g^d) = -n'$.

- (iii) Los subgrupos de un grupo cíclico son cíclicos; sean $m_1, m_2 \in \mathbb{N}$ tales que $H = \langle g^{m_1} \rangle$ y $K = \langle g^{m_2} \rangle$. Sean $d_1 = \text{mcd}(m_1, n)$ y $d_2 = \text{mcd}(m_2, n)$. Por la parte (i) tenemos que $H = \langle g^{d_1} \rangle$ y $K = \langle g^{d_2} \rangle$. Por la parte (ii) tenemos que $|H| = o(g^{d_1}) = n/d_1$ y $|K| = o(g^{d_2}) = n/d_2$. Y como $|H| = |K|$, tenemos que $n/d_1 = n/d_2$; es decir $d_1 = d_2$. Entonces $H = \langle g^{d_1} \rangle = \langle g^{d_2} \rangle = K$.

- B. (i)** ■ $k = 3$: $5^{2^{3-3}} = 5^{2^0} = 5^1 = 5 \equiv 1 + 2^2 \pmod{2^3}$.
 ■ Si la congruencia vale para k , tenemos que $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$. Entonces $5^{2^{k-3}} = 1 + 2^{k-1} + m2^k$ para algún $m \in \mathbb{Z}$. Entonces

$$\begin{aligned}
 \left(5^{2^{k-3}}\right)^2 &= \left(1 + 2^{k-1} + m2^k\right)^2 \Rightarrow \\
 5^{2^{k-3} \cdot 2} &= 1 + \left(2^{k-1}\right)^2 + \left(m2^k\right)^2 + 2\left(2^{k-1} + m2^k + 2^{k-1}m2^k\right) \Rightarrow \\
 5^{2^{k+1-3}} &= 1 + 2^{2(k-1)} + m^2 2^{2k} + 2^{k+1-1} + m2^{k+1} + 2^{k-1}m2^{k+1} \Rightarrow \\
 5^{2^{k+1-3}} &= 1 + 2^{k+1}2^{k-3} + 2^{k+1}m^2 2^{k-1} + 2^{k+1-1} + m2^{k+1} + 2^{k-1}m2^{k+1} \Rightarrow \\
 5^{2^{k+1-3}} &= 1 + 2^{k+1-1} + 2^{k+1} \left(\underbrace{2^{k-3} + m^2 2^{k-1} + m + 2^{k-1}m}_{\in \mathbb{Z} \text{ pues } k \geq 3} \right).
 \end{aligned}$$

Por lo tanto $5^{2^{k+1-3}} \equiv 1 + 2^{k+1-1} \pmod{2^{k+1}}$ y la congruencia vale para $k + 1$.

- (ii)** $(1 + 2^{k-1})^2 = 1 + 2^{2(k-1)} + 2 \cdot 2^{k-1} = 1 + 2^k 2^{k-2} + 2^k \equiv 1 \pmod{2^k}$ y $1 + 2^{k-1} \not\equiv 1 \pmod{2^k}$. Entonces $o(1 + 2^{k-1}) = 2$.

Usando la parte anterior tenemos que

$$\begin{aligned}
 5^{2^{k-3}} &\equiv 1 + 2^{k-1} \pmod{2^k} \Rightarrow \left(5^{2^{k-3}}\right)^2 \equiv (1 + 2^{k-1})^2 \pmod{2^k} \equiv 1 \pmod{2^k}. \text{ Entonces} \\
 5^{2^{k-2}} &\equiv 1 \pmod{2^k}. \text{ Por otro lado como } \varphi(2^k) = 2^{k-1} \text{ sabemos que } o(5) | 2^{k-1} \text{ y tenemos} \\
 \text{que } 5^{2^{k-3}} &\neq e \text{ y } 5^{2^{k-2}} = e, \text{ entonces } o(5) = 2^{k-2}.
 \end{aligned}$$

- C.** Sean los subgrupos de $U(2^k)$ dados por $H = \langle 1 + 2^{k-1} \rangle$ y $K = \langle -1 \rangle$. Entonces $|H| = o(1 + 2^{k-1}) = 2$ y $|K| = 2$. Además $K \neq H$ pues $1 + 2^{k-1} \not\equiv -1 \pmod{2^k}$. Si $U(2^k)$ fuera cíclico, no podría tener dos subgrupos distintos de orden 2 (por la parte A(iii)).