

SOLUCIÓN EXAMEN DE MATEMÁTICA DISCRETA 2

Ejercicio 1.

- A.** Sean $a, b \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$ entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$.
- B.** Por identidad de Bezout tenemos que existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$, luego $cax + cby = c$. Como $a|cax$ y $a|bcy$ entonces $a|cax + cby$, es decir $a|c$.
- C.** Sea $d = \text{mcd}(a, b)$ y escribimos $a = a'd$, $b = b'd$ sabiendo que $\text{mcd}(a', b') = 1$. Como $a|7b$ entonces $a'|7b'$, por parte **B.** tenemos que $a'|7$. Como $a' > b'$, $a' \neq 1$ y entonces $a' = 7$. Por otro lado tenemos que $\text{mcm}(a, b) = a'b'd = 245 = 7^2 \cdot 5$. Por la descomposición anterior puede pasar que $b' = 5$ y $d = 7$ o $b' = 1$ y $d = 35$. Los números buscados son $(a, b) = (49, 35)$ y $(a, b) = (245, 35)$.
- D.** Si denotamos por x a la cantidad de leños por atado y por y a la cantidad de leños que lleva cada uno, debemos resolver la siguiente ecuación

$$63x + 7 = 23y.$$

Para esto resolvemos $-63x + 23y = 1$, observemos que tenemos

$$63 = 23 \cdot 2 + 17 \quad 23 = 17 + 6 \quad 17 = 6 \cdot 2 + 5 \quad 6 = 5 + 1$$

Luego

$$\begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 63 \\ 23 \end{pmatrix} = \begin{pmatrix} 3 & -8 \\ -4 & 11 \end{pmatrix} \begin{pmatrix} 63 \\ 23 \end{pmatrix}$$

Luego $1 = (-63) \cdot 4 + 23 \cdot 11$ y $7 = (-63) \cdot 28 + 23 \cdot 77$, luego todas las soluciones son $x = 28 + 23k$ e $y = 63k + 77$. Como $0 \leq y \leq 50$ entonces $k = -1$ y la respuesta es que había $x = 28 - 23 = 5$ leños en cada atado.

Ejercicio 2.

- A.** $x \equiv 8 \pmod{31} \Leftrightarrow \exists k \in \mathbb{Z} : x = 8 + 31k$. Si además, $x \equiv 11 \pmod{17} \Rightarrow \exists k' \in \mathbb{Z} : 8 + 31k = 11 + 17k'$. Entonces, $31k - 17k' = 3$. Haciendo el algoritmo de Euclides extendido vemos que $31(-6) + 17(11) = 1$, así que $31(-18) + 17(33) = 3$ y $31(-18 + 17z) - 17(-33 + 31z) = 3$ para todo $z \in \mathbb{Z}$. Por lo tanto todas las soluciones de $31k - 17k' = 3$ son de la forma: $k = -18 + 17z$ y $k' = -33 + 31z$ con $z \in \mathbb{Z}$ y entonces las soluciones del sistema original son $x = 8 + 31k = 8 + 31(-18 + 17z) : z \in \mathbb{Z}$, por lo tanto $x \equiv 504 \pmod{527}$.
- B.** Escribimos $de = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$. Hay que probar que $D(E(x)) = x$ para todo $x \in \mathbb{Z}_n$. Es decir, hay que probar que para todo $a \in \mathbb{Z}$, $(a^e)^d \equiv a \pmod{n}$. Si $\text{mcd}(a, n) = 1$, por el teorema de Euler sabemos que $a^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow (a^{\varphi(n)})^k \equiv 1 \pmod{n} \Rightarrow (a^{\varphi(n)})^k a \equiv a \pmod{n} \Rightarrow a^{\varphi(n)k+1} \equiv a \pmod{n} \Rightarrow a^{ed} \equiv a \pmod{n}$. Si $\text{mcd}(a, n) \neq 1$, como $n = pq$ con p y q primos, alguno de los dos factores divide a a . Si ambos factores dividen a a , entonces n divide a a entonces $a \equiv 0 \pmod{n}$ y claramente $a^{de} = a \pmod{n}$. Si sólo uno de los factores, supongamos p , divide a a , entonces $a \equiv 0 \pmod{p}$ y por lo tanto $a^{de} \equiv a \pmod{p}$. Ahora bien, si q no divide a a , usando Fermat tenemos que $a^{q-1} \equiv 1 \pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} \equiv 1 \pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} a \equiv a \pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} a \equiv a \pmod{q} \Rightarrow a^{de} \equiv a \pmod{q}$. Entonces tenemos que $\begin{cases} a^{de} \equiv a \pmod{p} \\ a^{de} \equiv a \pmod{q} \end{cases}$ y como p y q son coprimos, concluimos que $a^{de} \equiv a \pmod{pq}$.

- C. (i) Tenemos que hallar d talque $de \equiv 1 \pmod{\varphi(n)}$; es decir, tenemos que resolver $107d \equiv 1 \pmod{16 \times 30}$, o sea, $107d \equiv 1 \pmod{480}$. Con el Algoritmo de Euclides extendido vemos que $480(35) + 107(-157) = 1$, y por lo tanto $d \equiv -157 \pmod{480} \equiv 323 \pmod{480}$.
- (ii) Tenemos que $x \equiv 250^{323} \pmod{31 \times 17}$, y como 31 y 17 son coprimos, tenemos que esto pasa si y sólo si, $\begin{cases} x \equiv 250^{323} \pmod{31} \\ x \equiv 250^{323} \pmod{17} \end{cases}$. Como $255 = 15 \times 17$ tenemos que $250 \equiv -5 \pmod{17}$ y como $248 = 8 \times 31$, $250 \equiv 2 \pmod{31}$. Así que la primer ecuación nos queda: $x \equiv 250^{323} \pmod{31} \Rightarrow 2^{323} \pmod{31} \Rightarrow (2^5 \pmod{31})^{64} \cdot 2^3 \pmod{31} \Rightarrow x \equiv 8 \pmod{31}$. La segunda ecuación nos queda: $x \equiv 250^{323} \pmod{17} \Rightarrow x \equiv (-5)^{323} \pmod{17} \Rightarrow (\text{por Fermat tenemos que } (-5)^{16} \equiv 1 \pmod{17}) \Rightarrow x \equiv (-5)^3 \pmod{17} \equiv 25(-5) \pmod{17} \equiv 8(-5) \pmod{17} \equiv -40 \pmod{17} \equiv 11 \pmod{17}$. Así que $\begin{cases} x \equiv 8 \pmod{31} \\ x \equiv 11 \pmod{17} \end{cases}$ y por la parte A. tenemos que $x \equiv 504 \pmod{527}$.

Ejercicio 3.

- A. Si G es un grupo finito y H es un subgrupo de G , entonces $|H|$ divide a $|G|$.
- B. Si $H = \langle g \rangle$, el subgrupo de G generado por g , tenemos que $|H| = o(g)$. Por el Teorema de Lagrange $|H|$ divide a $|G|$ y luego $o(g) \mid |G|$. Por lo tanto $|G| = o(g)k$ con $k \in \mathbb{Z}$ y

$$g^{|G|} = g^{o(g)k} = (g^{o(g)})^k = e^k = e.$$

- C. Por Teorema de Lagrange sabemos que $o(f(g))$ divide a $|G_2|$. Por definición de homomorfismo $f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1)$ entonces $f(e_1) = e_2$. Como $f(g)^{o(g)} = f(g^{o(g)}) = f(e_1) = e_2$ tenemos que $o(f(g))$ divide a $o(g)$ que divide a $|G_1|$. Por lo tanto $o(f(g))$ divide a $\text{mcd}(|G_1|, |G_2|)$.
- D. Si f es un homomorfismo, entonces $f(\bar{0}) = \bar{1}$. Si $f(\bar{1}) = \bar{1}$ entonces f es trivial y es homomorfismo. Si f no es trivial, entonces $f(\bar{1}) \in \{\bar{3}, \bar{5}, \bar{7}\} \subset U(8)$. Así que en cualquiera de estos casos, $f(\bar{1}) \neq \bar{1}$ y $f(\bar{1})^2 = \bar{1}$ (es decir, $f(\bar{1})$ es un elemento de orden 2). Con cualquier elección de $f(\bar{1}) \in \{\bar{3}, \bar{5}, \bar{7}\}$, la función obtenida es homomorfismo; veamos esto:

$$f(\bar{0} + \bar{1}) = f(\bar{1}) = \bar{1}f(\bar{1}) = f(\bar{0})f(\bar{1}), \quad y$$

y

$$f(\bar{1} + \bar{1}) = f(\bar{0}) = \bar{1} = (f(\bar{1}))^2 = f(\bar{1})f(\bar{1}).$$

Así que todos los homomorfismos son f_1, f_2, f_3, f_4 donde

$$f_i(\bar{0}) = \bar{1}, \quad \forall i \in \{1, 2, 3, 4\} \quad y \quad f_1(\bar{1}) = \bar{1}, \quad f_2(\bar{1}) = \bar{3}, \quad f_3(\bar{1}) = \bar{5}, \quad f_4(\bar{1}) = \bar{7}.$$

- E. Al ser $\text{im}(f)$ un subgrupo de \mathbb{Z}_p tenemos que $|\text{im}(f)|$ divide a $|\mathbb{Z}_p| = p$. Al ser p primo $|\text{im}(f)|$ es 1 o p . Pero como f es no trivial entonces $|\text{im}(f)| \neq 1$ y por lo tanto $|\text{im}(f)| = p$. Por otro lado (por el teo de órdenes para homomorfismos) tenemos que $51 = |\mathbb{Z}_{51}| = |\ker(f)| |\text{im}(f)| = |\ker(f)| \cdot p$. De aquí (como p es primo, $p \neq 1$) vemos que o $p = 3$ y $|\ker(f)| = 17$ o $p = 17$ y $|\ker(f)| = 3$. De $f(\bar{17}) = 0$, tenemos que $\bar{17} \in \ker(f)$ y como $o(\bar{17}) = 3$ entonces (por Lagrange) que 3 divide a $|\ker(f)|$. Así que $|\ker(f)| = 3$ y $p = 17$.