

Solución - Examen de Matemática Discreta II

Ejercicio 1

- (a) Ver el Teorema 1.7.1 de las Notas del Curso.
- (b) Ver el Corolario 1.7.2 de las Notas del Curso. Ver notas del curso.

Ejercicio 2

- (a) Ver el Teorema 2.5.1 de las Notas del Curso.
- (b) Para hallar $x \equiv 53^{901} \pmod{100}$, observemos que $100 = 2^2 \times 5^2 = 4 \times 25$, y por el Teorema Chino del resto tenemos que x es el único elemento de \mathbb{Z}_{100} que satisface el sistema de congruencias:

$$\begin{cases} x \equiv 53^{901} \pmod{25}, \\ x \equiv 53^{901} \pmod{4}. \end{cases}$$

Notemos que $53 \equiv 3 \pmod{25}$, y 3 es coprimo con 25, de donde, por Euler $3^{\varphi(25)} \equiv 1 \pmod{25}$. Como $\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$, resulta que $3^{901} = 3^{45 \times 20 + 1} \equiv 3^1 \equiv 3 \pmod{25}$. Por otra parte $53 = 4 \times 13 + 1 \equiv 1 \pmod{4}$. El sistema de congruencias anterior es entonces equivalente al siguiente:

$$\begin{cases} x \equiv 3 \pmod{25}, \\ x \equiv 1 \pmod{4}. \end{cases}$$

De donde $x = 3 + 25t \equiv 1 \pmod{4} \Rightarrow t \equiv 2 \pmod{4} \Rightarrow t = 2 + 4s \Rightarrow x = 3 + 25(2 + 4s) = 53 + 100s$. De donde $x \equiv 53$.

Ejercicio 3

Sea $(G, *)$ un grupo finito de orden n . Consideremos el conjunto formado por todas las funciones biyectivas $\text{Sim}(G) = \{\varphi : G \rightarrow G, \varphi \text{ biyectiva}\}$.

- (a) La función identidad $\text{id} : G \rightarrow G$ es el neutro bajo la composición de funciones biyectivas. Notemos que la composición de biyectivas es biyectiva, por lo que la cerradura es inmediata, y el inversa de una función biyectiva es biyectiva.
- (b) Sea $f : G \rightarrow \text{Sim}(G)$ tal que $f(g)(x) = g * x$. Por la propiedad cancelativa, se deduce que $f(g)$ es inyectiva, y como $f(g) : G \rightarrow G$, y G es finito, también es sobreyectiva, y por lo tanto biyectiva. Veamos que f es homomorfismo de grupos. Sean $g_1, g_2 \in G$. Entonces:

$$f(g_1 * g_2)(x) = g_1 * (g_2 * x) = f(g_1)(g_2 * x) = f(g_1)(f(g_2)(x)) = (f(g_1) \circ f(g_2))(x),$$

y las igualdades valen para todo $x \in G$. Luego, las funciones $f(g_1 * g_2)$ y $f(g_1) \circ f(g_2)$ son idénticas, y f es un morfismo de grupos. Veamos por último que el núcleo es solamente la identidad. En efecto, si $f(g) = \text{id}$ entonces $f(g)(x) = x$ para todo $x \in G$ entonces $g * x = x = e * x$ para todo x , y cancelando tenemos que $g = e$, el neutro de G . Luego $\text{Ker}(f) = \{e\}$. Concluimos entonces que f define un morfismo inyectivo, como queríamos demostrar.

- (c) Claramente G es isomorfo a $\text{Im}(f)$, pues el homomorfismo f de antes considerada como función de G a $\text{Im}(G)$ es sobreyectivo, y como ya era inyectiva, es una biyección y por lo tanto un isomorfismo entre G en el subgrupo $\text{Im}(G)$ de $\text{Sim}(G)$.

Ejercicio 4

- (a) Las letras F y Q tienen mayor frecuencia en el cifrado $GQDQPFJF$. A partir de la pista, una letra se corresponde con la A y la otra con la E . Tenemos dos posibilidades, y solo una nos brinda un texto con significado en castellano.

Probemos con el cifrado que asigna $A \rightarrow Q$ y $E \rightarrow F$. Traduciendo a números con la tabla dada, nuestro cifrado debe cumplir que $0 \rightarrow 17$ y $4 \rightarrow 5$. Con esta información, ya podemos despejar nuestras incógnitas a y b de la función de encriptación $E(x) = ax + b \pmod{28}$, que cumplen el sistema de congruencias:

$$\begin{cases} E(0) = b \equiv 17 \pmod{28}, \\ E(4) = 4a + b \equiv 5 \pmod{28}. \end{cases}$$

De la primera sabemos que $b = 17$, y reemplazando en la segunda tenemos que $4a \equiv -12 \pmod{28} \Rightarrow a \equiv -3 \pmod{7} \Rightarrow a \equiv 4 \pmod{7}$, lo cual contradice la condición impuesta.

Probemos con el cifrado que asigna $A \rightarrow F$ y $E \rightarrow Q$. Traduciendo a números con la tabla dada, nuestro cifrado debe cumplir que $0 \rightarrow 5$ y $4 \rightarrow 17$. Con esta información, ya podemos despejar nuestras incógnitas a y b de la función de encriptación $E(x) = ax + b \pmod{28}$, que cumplen el sistema de congruencias:

$$\begin{cases} E(0) = b \equiv 5 \pmod{28}, \\ E(4) = 4a + b \equiv 17 \pmod{28}. \end{cases}$$

De la primera sabemos que $b = 5$, y reemplazando en la segunda tenemos que $4a \equiv 12 \pmod{28} \Rightarrow a \equiv 3 \pmod{7}$, que tiene soluciones $a \in \{3, 10, 17, 24\}$. Las soluciones 10 y 24 se pueden descartar porque a debe ser coprimo con 28 para que exista la función de descifrado D . Probemos si tiene sentido en nuestro idioma encriptar usando $a = 3$. En este caso, $E(x) = 3x + 5$, y como $3^{-1} \equiv 19 \pmod{28}$, tenemos que $D(x) = 19(y - 5) \pmod{28}$. Si aplicamos $D(x)$ al texto brindado, tenemos:

SERENATA

Hemos descubierto el elemento de seducción del músico que sabe de criptografía.

- (b) $E(x) = 3x + 5 \pmod{28}$.
(c) $D(x) = 19(y - 5) \pmod{28}$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	\tilde{N}	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27