

SOLUCIÓN DEL EXAMEN DE MATEMÁTICA DISCRETA 2
22 DE JULIO DE 2008

Ejercicio 1.

- a) El elemento neutro de Q es la matriz identidad 2×2 la cual denotaremos como 1 (es un abuso de notación, el lector sabrá reconocer cuando nos referimos a la matriz identidad o al entero 1).

$$wz = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, zw = -wz, z^2 = w^2 = -1, z^3 = -z, w^3 = -w, z^4 = w^4 = 1.$$

Por otra parte, como los elementos w y z tienen orden 4 resulta que $w^{4q+r} = w^r$ y $z^{4q+r} = z^r$ para todo $q \in \mathbb{N}$ y $r = 0, 1, 2$ ó 3 .

- b) i) Se observa de la parte anterior que $wz \neq zw$.
- ii) Por definición de subgrupo generado tenemos que $Q = \langle w, z \rangle = \{w^{\alpha_1} z^{\beta_1} w^{\alpha_2} z^{\beta_2} \dots w^{\alpha_t} z^{\beta_t} : \alpha_1, \dots, \alpha_t, \beta_1, \dots, \beta_t \in \mathbb{Z}, t \in \mathbb{Z}^+\}$. Como $wz = -zw = z^3w$ resulta que $Q = \{z^\alpha w^\beta : \alpha, \beta \in \mathbb{Z}\}$. Finalmente como $z^2 = w^2 = -1$ resulta que $Q = \{1, -1, z, -z, w, -w, zw, -zw\}$ y es claro que todos los elementos de ese conjunto son distintos dos a dos por lo que $|Q| = 8$.
- iii) Sea $H < Q$, si $H = \{1\}$ ó Q se cumple trivialmente que $H \triangleleft Q$, así que supondremos de ahora en más que H es no trivial. Como $|Q| = 8$ por Lagrange tenemos que $|H| = 2$ ó 4 . Si $|H| = 4$ entonces $[Q : H] = 2$ por lo tanto $H \triangleleft Q$. Si $|H| = 2$ entonces $H = \{1, x\}$ donde $x \neq 1$ y $x^2 = 1$; como $(\pm w)^2 = (\pm z)^2 = (\pm zw)^2 = -1$ la única opción es que $x = -1$ y obtenemos el único subgrupo de orden 2, $H = \{1, -1\}$. En este caso como $g(-1)g^{-1} = -gg^{-1} = -1 \in H$ para todo $g \in Q$ resulta que H es un subgrupo normal de Q .
- iv) Una posibilidad para probar esta parte es haciendo la tabla de multiplicación del grupo Q y observando que los únicos elementos que conmutan con todos los elementos del grupo son el 1 y el -1 .
Otra manera es analizando cardinales, como $Z(Q) < Q \Rightarrow |Z(Q)| = 1, 2, 4$ ó 8 (Lagrange). Pero $|Z(Q)| \neq 1$ pues Q es un 2-grupo (corolario de la ecuación de clase), $|Z(Q)| \neq 8$ pues Q no es abeliano. Si $|Z(Q)| = 4 \Rightarrow |Q/Z(Q)| = 2 \Rightarrow Q/Z(Q)$ sería cíclico y Q sería abeliano, pero como no lo es, tenemos que $|Z(Q)| = 2$. En la parte anterior vimos que hay un único subgrupo de orden 2 que viene dado por $\{1, -1\}$ por lo tanto $Z(Q) = \{1, -1\}$.

- d) Tenemos que $Q/Z(Q) = Q/\{1, -1\} = \{\bar{1}, \bar{z}, \bar{w}, \bar{zw}\}$ donde $\bar{x} = \{x, -x\}$ es la clase de $x \in Q$ en el cociente. A continuación escribiremos la tablas del producto de los grupos $Q/Z(Q)$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$:

\cdot	$\bar{1}$	\bar{z}	\bar{w}	\bar{zw}	$+$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$\bar{1}$	$\bar{1}$	\bar{z}	\bar{w}	\bar{zw}	$(0, 0)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
\bar{z}	\bar{z}	$\bar{1}$	\bar{zw}	\bar{w}	$(0, 1)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
\bar{w}	\bar{w}	\bar{zw}	1	\bar{z}	$(1, 0)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
\bar{zw}	\bar{zw}	\bar{w}	\bar{z}	1	$(1, 1)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

Observamos que bajo la identificación $\bar{1} \mapsto (0, 0), \bar{z} \mapsto (0, 1), \bar{w} \mapsto (1, 0)$ y $\bar{zw} \mapsto (1, 1)$ la tabla de producto se preserva, por lo tanto, ambos grupos han de ser isomorfos (y la identificación anterior es el isomorfismo correspondiente, claro).

Ejercicio 2.

- a) Por propiedad del mcm, para cada $i = 1, 2, \dots, t$ existe $k_i \in \mathbb{Z}^+$ tal que $\delta(n) = k_i \phi(p_i^{\alpha_i})$. Como $\text{mcd}(a, n) = 1 \Rightarrow \text{mcd}(a, p_i^{\alpha_i}) = 1$ para cada $i = 1, 2, \dots, t$. Luego, por el Teorema de Euler-Fermat $a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Elevando a la k_i de ambos lados de la congruencia tenemos que $a^{\delta(n)} \equiv 1 \pmod{p_i^{\alpha_i}}$, con lo cual (por el Teorema del Resto Chino) tenemos que $a^{\delta(n)} \equiv 1 \pmod{n}$.
- b) Como $\text{mcd}(a, 30) = 1 \Rightarrow \text{mcd}(a, 120) = 1$ (pues 30 y 120 tienen los mismos primos en la descomposición factorial). Entonces $a^{\delta(120)} \equiv 1 \pmod{120}$, pero $\delta(120) = \text{mcm}\{\phi(8), \phi(3), \phi(5)\} = \text{mcm}\{4, 2, 4\} = 4$.
- c) i) $a_0 \equiv a_1 \equiv 0 \pmod{3}$ y si para algún $n \geq 0$ se tiene que $a_n \equiv a_{n+1} \equiv 0 \pmod{3}$ entonces $a_{n+2} = 7a_{n+1} + 40a_n \equiv 7 \cdot 0 + 40 \cdot 0 \equiv 0 \pmod{3}$. Luego $a_n \equiv 0 \pmod{3}$ para todo $n \geq 0$.
- ii) Para todo $n \geq 2$ se tiene que $a_n = 7a_{n-1} + 40a_{n-2} \equiv 7a_{n-1} \pmod{120}$ (como $a_{n-2} \equiv 3 \Rightarrow 40a_{n-2} \equiv 120 \pmod{120}$). Aplicando lo anterior reiteradas veces $a_{2008} \equiv 7a_{2007} \equiv 7^2 a_{2006} \equiv \dots \equiv 7^{2007} a_1 \equiv 7^{2007} \cdot 21 \equiv 7^{2008} \cdot 3 \pmod{120}$. Por la parte anterior $7^{2008} = (7^4)^{502} \equiv 1^{502} \equiv 1 \pmod{120}$, así que $a_{2008} \equiv 3 \pmod{120}$.

Ejercicio 3.

- a) Ver teórico.
- b) La clave $k = 17^{70} \pmod{73}$, por Fermat $17^{72} \equiv 1 \pmod{73}$, así que $17^2 k \equiv 1 \pmod{73}$. Resolviendo la ecuación diofántica correspondiente obtenemos $k = 24$.
- c) Hay que escribir 24 en base 13, nos queda $24 = 1 \cdot 13 + 11$ así que $a = 1, b = 11$ y $E(x) = x + 11 \pmod{13}$. $E(BIEN) = E(0, 4, 2, 5) = 11, 2, 0, 3 = TEBG$.
- d) $E(G) = B \Rightarrow E(3) = 3a + b = 0 \pmod{13}$ y $E(D) = U \Rightarrow E(1) = 3a + b = 12 \pmod{13}$.
Planteamos el sistema de congruencias:
$$\begin{cases} 3a + b \equiv 0 \pmod{13} \\ a + b \equiv 12 \pmod{13} \end{cases}$$

Resolvemos este sistema obteniendo $a \equiv 7 \pmod{13}$ y $b \equiv 5 \pmod{13}$, las únicas soluciones en el intervalo considerado son $a = 7$ y $b = 5$. Si $7x + 5 \equiv 8 \pmod{13} \Rightarrow x \equiv 6 \pmod{13}$ por lo tanto $D(Q) = O$, así que el mensaje descryptado es GOOD.