

Solución del examen de Matemática Discreta 2

Ejercicio 1.**A. (17pts)**

$$\begin{cases} 2x + 3 \equiv 8 \pmod{21} \\ 3x + 2 \equiv 3 \pmod{11} \end{cases} \Rightarrow \begin{cases} 2x \equiv 5 \pmod{21} \\ 3x \equiv 1 \pmod{11} \end{cases} \Rightarrow \begin{cases} 2x \equiv 5 \pmod{21} \equiv -16 \pmod{21} \\ x \equiv 4 \pmod{11} \end{cases} \Rightarrow \begin{cases} x \equiv -8 \pmod{21} \\ x \equiv 4 \pmod{11} \end{cases}$$

Por el Teorema Chino del resto se tiene que $x = 21A + 11B + k(21)(11)$ con $k \in \mathbb{Z}$ y

$$\begin{cases} 21A \equiv 4 \pmod{11} \\ 11B \equiv -8 \pmod{21} \end{cases} \Rightarrow \begin{cases} -A \equiv 4 \pmod{11} \\ 22B \equiv -16 \pmod{21} \end{cases} \Rightarrow \begin{cases} A \equiv -4 \pmod{11} \\ B \equiv -16 \pmod{21} \equiv 5 \pmod{21}. \end{cases}$$

Entonces $x = 21(-4) + 11(5) + k(231) = -29 + k(231)$ y por lo tanto el menor $x > 0$ es $x = -29 + 231 = 202$.

- B. (13pts)** Sea $d = \text{mcd}(a, b)$ y escribimos $a = a'd$ y $b = b'd$ (por lo tanto a' y b' son coprimos). Entonces $a'b'd = \text{mcm}(a, b) = x \text{mcd}(a, b) = 202d$ y por lo tanto $a'b' = 202 = 2 \times 101$. Entonces las posibilidades para el par (a', b') son $(1, 202)$, $(2, 101)$, $(101, 2)$ y $(202, 1)$. Por otro lado $a + b = d(a' + b') = 618$ así que $a' + b'$ divide a 618 y por lo tanto las únicas posibilidades para (a', b') son $(2, 101)$ y $(101, 2)$; en ambos casos $a' + b' = 103$ y por lo tanto $d = 618/103 = 6$ y entonces $(a, b) = (12, 606)$ o $(a, b) = (606, 12)$.

Ejercicio 2.

- A. (i) (4pts)** En S_3 $(13)(12) = (123)$ y $(12)(13) = (132)$, así que $(13)(12) \neq (12)(13)$ y por lo tanto S_3 no es conmutativo.
- (ii) (3pts)** El mismo ejemplo funciona para S_n si $n > 3$.
- B. (i) (10pts)** Si $\psi : \mathbb{Z}_7 \rightarrow S_6$ es un homomorfismo entonces $\ker \psi < \mathbb{Z}_7$ y por lo tanto $|\ker \psi|$ divide a $|\mathbb{Z}_7| = 7$. Entonces $|\ker \psi| = 1$ o 7 . Si $|\ker \psi| = 7$ entonces $\ker \psi = \mathbb{Z}_7$ y por lo tanto ψ es el homomorfismo nulo. Si $|\ker \psi| = 1$, por el Primer Teo. de Isomorfismo se tiene que $|\text{Im} \psi| = |\mathbb{Z}_7| = 7$ pero $\text{Im} \psi$ es un subgrupo de S_6 y por lo tanto su orden debe dividir a $|S_6| = 6!$; pero 7 no divide $n!$ así que $|\ker \psi| \neq 1$. Resulta entonces que el único ψ posible es el nulo.
- (ii) (10pts)** Si existe un homomorfismo $\phi : \mathbb{Z}_n \rightarrow S_n$, sea $\phi(\bar{1}) = \sigma \in S_n$. Como ϕ es homomorfismo se tiene que $\phi(\bar{k}) = \sigma^k$ y $e = \phi(\bar{0}) = \phi(\bar{n}) = \sigma^n$. Por lo tanto $o(\sigma)$ debe dividir a n . Pero si $o(\sigma) = k < n$ tendríamos que $\phi(\bar{k}) = \sigma^k = e$ y por lo tanto ϕ no sería inyectivo. Así que $o(\sigma)$ tiene que ser n . Tomando $\sigma = (1\ 2 \cdots n)$ queda que $\phi : \mathbb{Z}_n \rightarrow S_n$ dado por $\phi(\bar{k}) = \sigma^k$ es un homomorfismo inyectivo.
- C. (8pts)** Si existe un isomorfismo $\mu : \mathbb{Z}_n \rightarrow S_m$, al ser \mathbb{Z}_n un grupo conmutativo, S_m también es conmutativo. Por la parte A. tenemos que $m = 1$ o 2 . En ambos casos se tiene que cumplir que $n = |\mathbb{Z}_n| = |S_m| = m!$. Si $m = 1$ entonces $n = 1$, y si $m = 2$ entonces $n = 2$.

Ejercicio 3.

- A.(10pts)** Si $o(g) < \infty$ sea $n = o(g)$; entonces si $i = kn + j$ entonces $g^i = (g^n)^k g^j = g^j$ y por lo tanto $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$. Para ver que el cardinal de este conjunto es n , basta ver que si $0 \leq i < j < n$ entonces $g^i \neq g^j$. Si $g^i = g^j$, multiplicando a ambos lados por $(g^i)^{-1}$ tenemos que $e = g^{j-i}$; por lo tanto $n|(j-i)$ lo cual es absurdo pues $0 < j-i < n$. Y si $o(g)$ es infinito, por el mismo argumento, todas las potencias de g son distintas, y por lo tanto $\langle g \rangle = \infty$.
- B.(5pts)** Por el Teo. de Lagrange tenemos que $|\langle g \rangle|$ divide a $|G|$ y por la parte anterior tenemos que $|\langle g \rangle| = o(g)$. Por lo tanto $o(g)$ divide a $|G|$.
- C.(10pts)** Como $118 = 2 \times 59$ tenemos que $\varphi(118) = 58 = 2 \times 29$. Como $11 \in U(118)$ y $|U(118)| = \varphi(118) = 58$, las posibilidades para $o(11)$ son los divisores de 58. Es decir que $o(11) = 1, 2, 29$ o 58. Para probar que 11 es raíz primitiva módulo 118 basta con probar que $o(11) = 58$. Claramente $o(11) \neq 1$. Ahora $11^2 = 121 \equiv 3 \pmod{118}$, así que $o(11) \neq 2$. Ahora $11^4 \equiv 3^2 \pmod{118} \equiv 9 \pmod{118}$, $11^8 \equiv 81 \pmod{118}$, $11^{10} = 11^8 11^2 \equiv 81 \times 3 \pmod{118} \equiv 243 \pmod{118} \equiv 7 \pmod{118}$, $11^{20} \equiv 49 \pmod{118}$ y $11^{30} \equiv 253 \pmod{118} \equiv 107 \pmod{118}$. Entonces $o(11) \neq 29$ porque si fuera 29 tendríamos que $11^{30} = 11^{29} 11 \equiv 11 \pmod{118}$.
- D.(10pts)** Si x no es coprimo con 118 no cumple que $x^4 \equiv 33 \pmod{118}$ pues x^4 no es coprimo con 118 y 33 sí lo es.

Si x es coprimo con 118, como 11 es raíz primitiva módulo 118, tenemos que $x \equiv 11^a \pmod{118}$ para algún $a \in \mathbb{Z}$. Así que existe $x \in \mathbb{Z}$ tal $x^4 \equiv 33 \pmod{118}$ si y sólo si existe $a \in \mathbb{Z}$ tal que $(11^a)^4 \equiv 33 \pmod{118}$. Por otro lado $33 = 3 \times 11 \equiv 11^2 \times 11 \pmod{118} \equiv 11^3 \pmod{118}$. Así que hay que investigar si existe $a \in \mathbb{Z}$ tal que $11^{4a} \equiv 11^3 \pmod{118}$. Tenemos que $11^{4a} \equiv 11^3 \pmod{118} \Leftrightarrow 11^{4a-3} \equiv 1 \pmod{118} \Leftrightarrow o(11)|(4a-3) \Leftrightarrow 58|(4a-3) \Leftrightarrow 4a-3 = 58k$ para algun $k \in \mathbb{Z}$; es decir si y sólo si la ecuación $4a - 58k = 3$ tiene solución entera. Pero $\text{mcd}(4, 58) = 2$ y 2 no divide a 3, por lo tanto la ecuación no tiene solución.