

Examen parcial de Matemática Discreta 2

IMERL/FIng/UdelaR

28 de noviembre de 2019

1. Sea G un grupo finito y g un elemento de G .
 - (a) Definir $o(g)$ (orden del elemento g en G).
 - (b) Dado $k \in \mathbb{Z}$, probar que $o(g^k) = \frac{o(g)}{\text{mcd}(o(g), k)}$.
 - (c)
 - i. Probar que 2 es raíz primitiva módulo 13.
 - ii. Hallar todas las raíces primitivas módulo 13.
2.
 - (a) Definir morfismo de grupos.
 - (b) Sean G y K dos grupos finitos y $f : G \rightarrow K$ un morfismo de grupos. Probar que

$$|G| = |\text{Ker } f| |\text{Im } f|$$

- (c) Probar que no hay morfismos no triviales entre S_3 y \mathbb{Z}_{11}
3.
 - (a) Describir el criptosistema RSA, explicando:
 - Cómo se define la clave pública (n, e) .
 - Cuál es la función de cifrado E y cuál es la de descifrado D .
 - (b) Probar que $D(E(x)) \equiv x \pmod{n}$.
 - (c) Si $(n, e) = (1313, 271)$ calcular $E(10)$. (Observar que $1313 = 13 \times 101$)

Solución

1.
 - (a) Ver notas, Definición 3.7.6. página 52.
 - (b) Ver notas, Proposición 3.7.8. página 53.
 - (c)
 - i. Como $\phi(13) = 12$ debemos probar que $2^4 \not\equiv 1 \pmod{13}$ y que $2^6 \not\equiv 1 \pmod{13}$.
 - $2^4 = 16 \equiv 3 \not\equiv 1 \pmod{13}$
 - $2^6 = 2^4 \times 2^2 \equiv 3 \times 4 \equiv 12 \not\equiv 1 \pmod{13}$.
 - ii. Usando la parte b del ejercicio tenemos que 2^k es raíz primitiva si y solo si $\text{mcd}(k, 12) = 1$. Por lo tanto los valores de k que nos dan las raíces primitivas son $\{1, 5, 7, 11\}$. Se deduce que las raíces primitivas son $\{2(\equiv 2^1), 6(\equiv 2^5), 11(\equiv 2^7), 7(\equiv 2^{11})\}$.

2. (a) Ver notas, Definición 3.9.1. página 55.
 - (b) Ver notas, Teorema 3.9.8. página 58
 - (c) Supongamos que $f : S_3 \rightarrow \mathbb{Z}_{11}$ es un morfismo de grupos. Como Imf es un subgrupo de K , por el Teorema de Lagrange $|Imf|/|\mathbb{Z}_{11}| = 11$. Por otro lado, por la parte anterior $|Imf|/|S_3| = 6$. Como 6 y 11 son coprimos $|Imf| = 1$, lo que implica que f es el morfismo trivial.
3. (a) Ver notas, página 70.
 - (b) Ver notas, Proposición 5.3.1. página 71.
 - (c) Como $E(x) = x^{271} \pmod{1313}$, tenemos que calcular $10^{271} \pmod{1313}$. Sabemos que $1313 = 13 \times 101$, por lo tanto

$$x \equiv 10^{271} \pmod{1313} \Leftrightarrow \begin{cases} x \equiv 10^{271} \pmod{13}. \\ x \equiv 10^{271} \pmod{101}. \end{cases}$$

Usando el Teorema de Euler-Fermat el sistema anterior nos queda equivalente al siguiente

$$\begin{cases} x \equiv 10^{271} \pmod{13}. \\ x \equiv 10^{271} \pmod{101}. \end{cases} \Leftrightarrow \begin{cases} x \equiv 10^7 \pmod{13}. \\ x \equiv 10^{71} \pmod{101}. \end{cases}$$

Como $10^7 \equiv 10 \pmod{13}$ y $10^2 \equiv -1 \pmod{100}$ tenemos que

$$x \equiv 10^{271} \pmod{1313} \Leftrightarrow \begin{cases} x \equiv 10 \pmod{13}. \\ x \equiv 91 \pmod{101}. \end{cases}$$

Como $101^{-1} \equiv 4 \pmod{13}$ y $13^{-1} \equiv 70 \pmod{101}$, resulta que $x \equiv 10 \times 101 \times 4 + 91 \times 13 \times 70 \equiv 192 \pmod{1313}$ es solución del sistema. Por lo tanto $10^{271} \equiv 192 \pmod{1313}$.