

Examen parcial de Matemática Discreta 2

IMERL/FIng/UdelaR

28 de junio de 2018

1. (a) Definir subgrupo, subgrupo normal y grupo cociente.
(b) Sea G un grupo, $H \triangleleft G$ y $\pi_H : G \rightarrow G/H$ la proyección al cociente. Sea $\varphi : G \rightarrow G'$ un morfismo de grupos tal que $H \subset \text{Ker}(\varphi)$.
 - i. Probar que existe un único morfismo $\hat{\varphi} : G/H \rightarrow G'$ tal que $\varphi = \hat{\varphi} \circ \pi_H$; es decir, tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi_H \downarrow & \nearrow \hat{\varphi} & \\ G/H & & \end{array}$$

- Probar que $\text{Im}(\hat{\varphi}) = \text{Im}(\varphi)$ y que $\text{Ker}(\hat{\varphi}) = \pi_H(\text{Ker}(\varphi))$.
- ii. Concluir que $G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$.
 - (c) Se consideran los grupos $G = (\mathbb{R}, +, 0)$ y $G' = (\mathbb{C}^*, \cdot, 1)$. Se define $\varphi : G \rightarrow G'$ como $\varphi(x) := e^{2\pi xi} = \cos(2\pi x) + i \sin(2\pi x)$.
 - i. Probar que φ es un morfismo de G en G' .
 - ii. Hallar el núcleo y la imagen de φ . Justificar.
 - iii. Sean los grupos $H := (\mathbb{Z}, +, 0)$ y $K = (\{z \in \mathbb{C} \mid |z| = 1\}, \cdot, 1)$. Probar que G/H es isomorfo a K .
2. (a) Describir el criptosistema RSA, explicando:
 - i. Cómo se define la clave pública (n, e) .
 - ii. Cuál es la función de cifrado y cuál la de descifrado.
 - (b) Explicar el método de Fermat para atacar al criptosistema RSA con clave (n, e) , cumpliendo las siguientes etapas:
 - i. Definir el algoritmo de factorización de n . Justificar que el algoritmo termina.
 - ii. Probar que el resultado del algoritmo descompone a n en factores primos.
 - iii. Explicar cómo se usa la factorización hallada para calcular la función de descifrado.
 - (c) Aplicando el método de Fermat, hallar la función de descifrado para la clave pública $(1073287, 385)$.

3. (a)
 - i. Definir raíz primitiva para un módulo n . Enunciar (en función de los factores primos de n) una condición necesaria y suficiente para que existan raíces primitivas módulo n (teorema de la raíz primitiva).
 - ii. Supongamos que conocemos g , una raíz primitiva módulo p con p primo impar. Describir un algoritmo que permita hallar a partir de g una raíz primitiva módulo p^k .
- (b) Probar que si $n \in \mathbb{N}$ es un impar y existe una raíz primitiva módulo n , entonces también existe una raíz primitiva módulo $2 \times n$.
- (c)
 - i. Decir para cuáles de los siguientes naturales n existen raíces primitivas módulo n , justificando la respuesta:
 - $n = 41$.
 - $n = 115856201 = 41^5$.
 - $n = 2 \times 115856201$.
 - $n = 256$.
 - ii. Cuando sea posible, para cada uno de los naturales n de la parte 3.(c)i., hallar una raíz primitiva módulo n . Justificar.

SOLUCIÓN:

1. (a) Ver las notas de Solotar, Farinatti & Suárez-Álvarez en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=76989>
- (b) Ver las notas de Solotar, Farinatti & Suárez-Álvarez en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=76989>
- (c) φ es un morfismo, ya que $\varphi(x+y) = e^{2\pi(x+y)i} = e^{2\pi xi} \times e^{2\pi yi} = \varphi(x) \times \varphi(y)$. El núcleo de φ son los reales x tales que $\cos(2\pi x) + i \sin(2\pi x) = 1$, es decir, los reales x tales que
$$\begin{cases} \cos(2\pi x) = 1 \\ \sin(2\pi x) = 0 \end{cases}$$
 Estas dos ecuaciones se satisfacen a la vez cuando $2\pi x$ es múltiplo entero de 2π , es decir, cuando $x \in \mathbb{Z}$. Concluimos que $\text{Ker}(\varphi) = \mathbb{Z}$. Por otra parte:

$$|e^{2\pi xi}| = |\cos(2\pi x) + i \sin(2\pi x)| = \sqrt{\cos^2(2\pi x) + \sin^2(2\pi x)} = 1$$

Entonces, $\text{Im}(\varphi) \subseteq \{z \in \mathbb{C} \mid |z| = 1\}$. Recíprocamente, todo complejo z de módulo 1 es de la forma $z = \cos(\alpha) + i \sin(\alpha)$ para algún $\alpha \in [-\pi, \pi)$. Se tiene que $\cos(\alpha) + i \sin(\alpha) = e^{\alpha i} = e^{2\pi(\frac{\alpha}{2\pi})i} = \varphi(\frac{\alpha}{2\pi})$. Concluimos entonces que $\text{Im}(\varphi) = \{z \in \mathbb{C} \mid |z| = 1\}$.

Entonces, $\text{Ker}(\varphi) = H$ y $\text{Im}(\varphi) = K$. Aplicando la parte 1.(b), concluimos que $G/H \cong K$.

2. (a) Ver las notas de Pereira, Qureshi & Rama en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=62664>
- (b) Ver las notas de Pereira, Qureshi & Rama en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=62664>
- (c) Aplicamos Fermat, buscando el primer cuadrado perfecto de la forma $t^2 = n + s^2$. Tenemos:
 - $1073287 + 1 = 1073288$ no es un cuadrado perfecto.
 - $1073287 + 2^2 = 1073291$ no es un cuadrado perfecto.
 - $1073287 + 3^2 = 1073296 = 1036^2$.

Sean $t = 1036$ y $s = 3$. Tenemos entonces que $n = (t-s)(t+s) = 1033 \times 1039$.

Entonces $\varphi(n) = 1032 \times 1038 = 1071216$. Buscamos el inverso d de $e = 385$ módulo 1071216 mediante el algoritmo de Euclides extendido, obteniendo $d = 80689$:

Las sucesivas divisiones enteras son:

$$\begin{array}{r|l} 1071216 & 385 \\ \hline 146 & 2782 \end{array} \quad \begin{array}{r|l} 385 & 146 \\ \hline 93 & 2 \end{array} \quad \begin{array}{r|l} 146 & 93 \\ \hline 53 & 1 \end{array} \quad \begin{array}{r|l} 93 & 53 \\ \hline 40 & 1 \end{array}$$

$$\begin{array}{r|l} 53 & 40 \\ \hline 13 & 1 \end{array} \quad \begin{array}{r|l} 40 & 13 \\ \hline 1 & 3 \end{array}$$

Esto da como resultado las siguiente matrices de transición:

$$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \\ -1 & 2 \\ 4 & -7 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \\ 2 & -3 \\ -7 & 11 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -3 \\ -7 & 11 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \\ -3 & 8 \\ 11 & -29 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2782 \\ 8 & -22259 \\ -29 & 80689 \end{pmatrix}$$

Entonces tenemos:

$$\begin{pmatrix} 8 & -22259 \\ -29 & 80689 \end{pmatrix} \begin{pmatrix} 1071216 \\ 385 \\ 13 \\ 1 \end{pmatrix}$$

En particular, tenemos $(-29) \times 1071216 + 80689 \times 385 = 1$, de lo que se concluye que $80689 \equiv_{1071216} 385^{-1}$.

La función de cifrado es entonces $E(x) \equiv_{1071216} x^{385}$ y la de descifrado es $D(y) \equiv_{1071216} y^{80689}$.

3. (a) Ver las notas de Pereira, Qureshi & Rama en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=62664>. También está en los apuntes sobre el teorema de la raíz primitiva, en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=77461>
- (b) Ver los apuntes sobre el teorema de la raíz primitiva, en el sitio EVA del curso: <https://eva.fing.edu.uy/mod/resource/view.php?id=77461>
- (c) Primero observamos que $\varphi(41) = 40 = 2^3 \times 5$. Una raíz primitiva módulo 41 es un entero g tal que $1 \leq g \leq 40$, $g^{\frac{40}{2}} = g^{20} \not\equiv_{41} 1$ y $g^{\frac{40}{5}} = g^8 \not\equiv_{41} 1$. El menor entero positivo que cumple esto es 6, de modo que es raíz primitiva módulo 41.
Como $6^{40} \equiv_{41^2} 124 \not\equiv_{41^2} 1$ (exponenciación rápida), entonces 6 es raíz primitiva módulo 41^5 .
Como 6 es par, entonces $6 + 41^5$ es raíz primitiva módulo 2×41^5 . Por otra parte, $256 = 2^8$, que según el teorema de la raíz primitiva, no admite raíz primitiva.