Examen de Matemática Discreta 2

IMERL/FIng/UdelaR

15 de diciembre de 2018

1. (a) i. Definir grupo, subgrupo normal y homomorfismo de grupos.
   ii. Enunciar el Primer Teorema de Isomorfismos.

   (b) Sean G un grupo e $\mathrm{Iso}(G,G)$ el grupo de los isomorfismos de G en G con la composición. Dado $a \in G$, se define $I_a : G \to G$ mediante $I_a(g) = aga^{-1}$.
   i. Demostrar que $I_a \in \mathrm{Iso}(G,G)$.
   ii. Probar que $I : G \to \mathrm{Iso}(G,G)$ definida mediante $I(a) = I_a$ es un morfismo de grupos y que su núcleo coincide con el centro de G; esto es:

   $$\mathrm{Ker(I)} = Z(G) = \{a \in G : \forall g \in G \quad ag = ga\}.$$

   Deducir que $\dfrac{G}{Z(G)} \cong \mathrm{Im}(I)$.

   (c) Sea $G := \mathrm{GL}_2(\mathbb{R})$, el grupo de las matrices reales invertibles de dimensión 2. Una matriz $A \in G$ de se dice *escalar* si es de la forma $\lambda\,\mathrm{Id}_{2\times 2} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ para algún número real λ.

   Sea $R := \{A \in G \mid A \text{ es escalar}\}$. Se considera el morfismo $I : G \to \mathrm{Iso}(G)$ definido en la parte anterior, esto es: $I_A(X) := A \cdot X \cdot A^{-1}$. Se pide:
   i. Probar que $\dfrac{G}{R} \cong \mathrm{Im}(I)$.
   ii. Deducir que $I_A = I_B$ si y sólo si $B = \lambda A$ para algún real λ no nulo.

2. (a) Definir la función $\varphi : \mathbb{N} \to \mathbb{N}$ de Euler.

   (b) Probar que $\phi(p^k) = p^k - p^{k-1}$ para p primo y $k \in \mathbb{N} \setminus \{0\}$.

   (c) i. Probar que 5 es una raíz primitiva de 27 y hallar una raíz primitiva de 54.
   ii. Hallar todos los morfismos $f : U(54) \to \mathbb{Z}_{36}$.

3. (a) Describir el criptosistema RSA, explicando:
   i. Cómo se define la clave pública (n, e).
   ii. Cómo se define la función de cifrado y la de descifrado.

   (b) i. Enunciar el teorema de Euler. Deducir el teorema de Fermat.
   ii. Probar que la función de descifrado es la inversa de la función de cifrado.

   (c) El alfabeto de los números en base exadecimal es `0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F`. Estos caracteres se corresponden con los números en base 10 según la tabla:

`0`	`1`	`2`	`3`	`4`	`5`	`6`	`7`	`8`	`9`	`A`	`B`	`C`	`D`	`E`	`F`
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

   Se considera la clave pública $(n, e) = (3977, 193)$. Se pide:
   i. Encriptar usando ECB el número hexadecimal `C414`. **Usar:** $14^2 \equiv_{3977} 196$ y $196^{16} \equiv_{3977} = 3650$.
   ii. Sabiendo que $\varphi(n) = 3840$, halle la función de descifrado correspondiente a la clave (n, e).

Solución

1. (a) i. Ver las notas de Pereira, Qureshi y Rama en el sitio EVA del curso: https://eva.fing.edu.uy/mod/resource/view.php?id=62664

   ii. Ver las notas de Solotar, Farinatti y Suárez-Álvarez en el sitio EVA del curso:https://eva.fing.edu.uy/mod/resource/view.php?id=76989

   i. La composicion de los morfismos es asociativa, el neutro u es el isomorfismo de grupos tal que $u(x) = x$ para todo $x \in G$ y el opuesto de un isomorfismo de grupos α es α^{-1}.

   - $\underline{I_a \text{ es homomorfismo de grupos}}$.
     Dados $g, h \in G$ $I_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = I_a(g)I_a(h)$.
   - $\underline{I_a \text{ es inyectiva}}$.
     Si $g \in KerI_a$ entonces $I_a(g) = aga^{-1} = e$ entonces $g = a^{-1}aga^{-1}a = a^{-1}ea = e$, por lo tanto $g = e$.
   - $\underline{I_a \text{ es sobreyectiva}}$.
     Dado $g \in G$ es claro que $I_a(a^{-1}ga) = a^{-1}aga^{-1}a = g$.

   ii. - $\underline{I \text{ es un homomorfismo de grupos}}$.
     Dados $a, b \in G$, Para todo $g \in G$ se tiene:

     $$I_{ab}(g) = abg(ab)^{-1} = abga^{-1}b^{-1} = aI_b(g)a^{-1} = I_a(I_b(g)),$$

     por lo tanto $I_{ab} = I_a \circ I_b$.
   - $\underline{KerI = Z(G)}$.

     $$KerI = \{a \in G : I_a = u\} = \{a \in G : aga^{-1} = I_a(g) = u(g) = g \; \forall g \in G\}$$

     $$= \{a \in G : ag = ga \; \forall g \in G\} = Z(G)$$

   - Dados $f \in Iso(G, G)$ e $I_a \in Int(G)$ tenemos que $f \circ I_a \circ f^{-1}(x) = f(I_a(f^{-1}(x))) = f(af^{-1}(x)a^{-1}) = f(a)f(f^{-1})(x)f(a^{-1}) = f(a)(x)f(a)^{-1} = I_{f(a)}(x)$. Por lo tanto $f \circ I_a \circ f^{-1} = I_{f(a)}$, lo que implica que $Int(G)$ es normal en $Iso(G, G)$.
   - El Primer Teorema de isomorfismo nos dice que

     $$\frac{G}{KerI} \cong ImI$$

     Como $ImI = Int(G)$ y $KerI = Z(G)$ por lo visto antes se obtiene la tesis.

   (b) i. Como $Z(\mathrm{GL}_2(\mathbb{R})) = R$ por la parte anterior $\frac{\mathrm{GL}_2(\mathbb{R})}{R} = ImI$.

   ii. $I_A = A_B \Leftrightarrow AXA^{-1} = BXB^{-1}$ para todo $X \in \mathrm{GL}_2(\mathbb{R}) \Leftrightarrow B^{-1}AX = XB^{-1}A$ para todo $X \in \mathrm{GL}_2(\mathbb{R}) \Leftrightarrow B^{-1}A \in Z(\mathrm{GL}_2(\mathbb{R})) = R \Leftrightarrow B^{-1}A = \lambda^{-1}Id_{2\times 2} \Leftrightarrow B = \lambda A$

2. (a) Ver las notas de Pereira, Qureshi y Rama en el sitio EVA del curso: https://eva.fing.edu.uy/mod/resource/view.php?id=62664

(b) $\varphi(p^k) = p^{k-1}(p-1)$. Ver las notas de Pereira, Qureshi y Rama en el sitio EVA del curso: https://eva.fing.edu.uy/mod/resource/view.php?id=62664

(c) $\varphi(27) = 18$. Como $5^9 \equiv 19$ mód 27 y $5^6 \equiv 26$ mód 27 entonces 5 es raíz primitiva módulo 27. Usando ahora que 5 es impar y que 27 es la potencia de un primo impar se deduce que 5 es raiz primitiva de 54.

(d) Como el orden de 5 en $U(54)$ es $\varphi(54) = 18$ y $U(54)$ es un grupo cíclico por tener raíz primitiva para definir un morfismo de grupos f solamente tenemos que ver como se define en 5. Para que la función f es un morfismo de grupos solamente hay que verificar $o(f(5)) \mid o(5) = 18$. Por lo tanto tenemos un morfismo de grupos por cada elemento par de $\mathbb{Z}_{36}$

3. (a) Ver las notas de Pereira, Qureshi y 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 y Rama en el sitio EVA del curso: https://eva.fing.edu.uy/mod/resource/view.php?id=62664

(c) i. Buscamos el exponente $k \in \mathbb{N}$ tal que $16^k < 3977 < 16^{k+1}$. Vemos que $k = 2$ es el exponente y por lo tanto, se ha de cortar el número `C414` en bloques de largo 2.
El bloque `C4` representa al número decimal 196 y el bloque `14` al decimal 20. La función de encriptado es $E(x) :\equiv_{3977} x^{193}$. Debemos calcular $E(20)$ y $E(196)$, lo que haremos mediante exponenciación rápida.
El exponente 193 en base 2 es 11000001, de modo que $E(20) \equiv_{3977} 20^{2^7} \times 20^{2^6} \times 20$, y $E(196) \equiv_{3977} 196^{2^7} \times 196^{2^6} \times 196$.

Para eso usamos la siguiente tabla:

i	2^i	196^{2^i}	20^{2^i}
0	1	196	20
1	2	2623	400
2	4	3896	920
3	8	2584	3276
4	16	3650	2230
5	32	3527	1650
6	64	3650	2232
7	128	3527	2620

Como $3650 \times 3527 \equiv_{3977} 1$, se tiene $E(196) \equiv_{3977} 196$ y por otro lado $E(20) \equiv_{3977} 1184$; de modo que el número encriptado es `0C44A0` (recordar que los bloques encriptados tienen un caracter más).

ii. La función de descifrado es $D(x) \equiv_{3977} x^d$ donde $d \equiv_{3840} (193)^{-1}$. Es claro que para que esto sea posible, 193 y 3840 deben ser coprimos. Calculamos $m := \gcd(3840, 193)$ por el algoritmo de

Euclides generalizado, el cual nos permite expresar a m como combinación lineal de 3840 y 193. Las divisiones sucesivas para hacer el cálculo son las siguientes:

3840	193
173	19

193	173
20	1

173	20
13	8

20	13
7	1

13	7
6	1

7	6
1	1

Estas divisiones generan el siguiente producto de matrices de transición:

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \quad \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix} \quad \begin{pmatrix} 2 & -17 \\ -3 & 26 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & -19 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -17 \\ -3 & 26 \end{pmatrix} \quad \begin{pmatrix} -17 & 19 \\ 26 & -29 \end{pmatrix} \quad \begin{pmatrix} 19 & -378 \\ -29 & 577 \end{pmatrix}$$

Esto en particular dice que:

$$\begin{pmatrix} 3840 \\ 193 \end{pmatrix}$$

$$\begin{pmatrix} 19 & -378 \\ -29 & 577 \end{pmatrix} \quad \begin{pmatrix} 6 \\ 1 \end{pmatrix}$$

De modo que $(-29) \times 3840 + 577 \times 193 = 1$ y entonces $577 \equiv_{3840} (193)^{-1}$. La función de descifrado es: $D(x) :\equiv_{3977} x^{577}$.