Examen final de Matemática Discreta 2. Curso 2018
IMERL/FIng/UdelaR
10 de julio de 2018

Ejercicio 1.

a. i) Dados dos enteros m y n tales que $(m, n) \neq (0, 0)$, definir el *máximo común divisor de m y n*.

ii) Enunciar el teorema de Bézout.

b. Sean a, b, c enteros, con a y b no nulos a la vez. Se considera la ecuación diofántica

$$ax + by = c \tag{1}$$

Se pide:

i) Probar que la ecuación (1) tiene solución si y sólo si $\gcd(a, b) \mid c$.

ii) Probar que si (x_0, y_0) es solución de la ecuación (1), entonces el conjunto de soluciones de la ecuación (1) es

$$\mathrm{Sol}(ax + by{=}c) = \{(x_0 + b^*k, y_0 - a^*k) \mid k \in \mathbb{Z}\} \tag{2}$$

donde $a^* = \dfrac{a}{\gcd(a, b)}$ y $b^* = \dfrac{b}{\gcd(a, b)}$.

c. Un cliente compra burlete en una ferretería. Lleva la medida que precisa expresada como x metros con y centímetros. El ferretero intercambia los metros con los centímetros, despachando y metros con x centímetros. Al llegar a la casa, el cliente usa 68 centímetros de burlete y descubre que le queda el doble de lo que él pensaba que había comprado. ¿Cuál es la menor cantidad de burlete (en metros y centímetros) que pudo haber pedido dicho cliente? Justificar cuidadosamente todas las etapas de la resolución.

Ejercicio 2.

a. i) Definir grupo y homomorfismo de grupos.

ii) Enunciar el Primer Teorema de Isomorfismos.

b. Sea $f : G \to G'$ un morfismo de grupos. Probar que $\mathrm{Ker}(f) \lhd G$.

c. Se considera $\mathrm{GL}_n := \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid A \text{ es invertible}\}$ (el grupo multiplicativo de las matrices reales de $n \times n$). Se pide:

i) Probar que $\det : \mathrm{GL}_n \to \mathbb{R}^*$ es un morfismo de grupos.

ii) Sea $N := \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid \det(A) = 1\}$. Probar que $N \lhd \mathrm{GL}_n$, que $\dfrac{\mathrm{GL}_n}{N} \cong \mathbb{R}^*$ y que $A \sim_N B$ si y sólo si $\det A = \det B$.

Ejercicio 3.

a. Describir el método de Diffie-Hellman de intercambio de clave.

b. Sea $n \in \mathbb{N}^*$. Sea $g \in \mathbb{Z}_n^*$.

i) Probar que g es raíz primitiva módulo n si y sólo si para todo $d \mid \varphi(n)$, $d \neq 1$, se tiene que $g^{\frac{\varphi(n)}{d}} \not\equiv_n 1$.

ii) Probar que g es raíz primitiva módulo n si y sólo si para todo p primo, si $p \mid \varphi(n)$, entonces $g^{\frac{\varphi(n)}{p}} \not\equiv_n 1$.

c. Sea $p = 10037$ (primo). Se pide:

i) Probar que 2 es raíz primitiva módulo p. (**Sug.:** pueden usar sin demostrar que $2^{256} \equiv_p 8637$ y que $2^{2509} \equiv_p 6766$).

ii) Dos interlocutores A y B acuerdan una clave común c mediante el método de Diffie-Hellman. Para eso usarán el primo p y la raíz primitiva g de la parte anterior. Asumimos el lugar del interlocutor B, el cual recibe de A el entero 5314 y elige el entero 32. ¿Qué entero enviamos a A para determinar la clave c?

iii) Fijamos la codificación del alfabeto que aparece en la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

A y B usarán la clave c para comunicarse mediante el método de cifrado de Vigenère. Sea $c = \Sigma_{i=0}^{k} \alpha_i 28^i$ el desarrollo de c en base 28. La palabra clave para el cifrado Vigenère será la que corresponde en la tabla con la secuencia $\alpha_k, \ldots, \alpha_0$ de las cifras del desarrollo. Hallar la palabra clave.

iv) Descifrar el mensaje `SFAEOZGCMFZNYS`.

Solución:

Ejercicio 1.

a. i) Ver teórico

ii) Ver teórico

b. i) Ver teórico

ii) Ver teórico

c. $C := 100y + x$ expresa en centímetros la longitud de burlete que pidió el cliente. $F := 100x + y$ expresa en centímetros la longitud de burlete que le despachó el ferretero. Como al usar el cliente 68 centímetros le queda el doble de C, tenemos la ecuación $F - 68 = 2C$, que se expresa en función de x, y mediante:

$$-199x + 98y = 68 \tag{3}$$

Sólo resta resolver la ecuación diofántica (3) y buscar la que corresponde a la menor longitud para C.

Observamos que 199 es primo y concluimos que $\gcd(199, 98) = 1$ (199 no es un factor primo de 98). Entonces aplicando (b)i., la ecuación (3) tiene solución. Mediante el algoritmo de Euclides generalizado hallamos $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha \times 199 + \beta \times 98 = 1$. Esto nos dice que $x_0 = -\alpha \times 68$ e $y_0 = \beta \times 68$ constituyen una solución particular (x_0, y_0) de la ecuación (3).

Las sucesivas divisiones que se hacen para calcular $\gcd(199, 98)$ son:

199	98
3	2

98	3
2	32

3	2
1	1

Estas dan lugar al siguiente producto de matrices de transición:

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -32 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 1 & -32 \\ -1 & 33 \end{pmatrix} \begin{pmatrix} -32 & 65 \\ 33 & -67 \end{pmatrix}$$

Concluimos entonces que

$$\begin{pmatrix} -32 & 65 \\ 33 & -67 \end{pmatrix} \begin{pmatrix} 199 \\ 98 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

y entonces $\alpha = -33$, $\beta = -67$ y $(x_0, y_0) = (-2244, -4556)$ es una solución particular de (3). Aplicando la fórmula de (b)ii., obtenemos:

$$\mathrm{Sol}(-11x + 98y = 68) = \{(-2244 + 98k, -4556 + 199k) \mid k \in \mathbb{Z}\}. \tag{4}$$

Claramente $k = 23$ genera la menor solución (x_k, y_k) con x_k, y_k positivos, que es $(x_k, y_k) = (10, 21)$. Concluimos que la longitud de burlete que solicitó el cliente fué de 10 metros con 21 centímetros.

Ejercicio 2.

a. i) Un grupo es una terna $(G, *, e)$ que satisfacen:

- $* : G \times G \to G$ ($*$ es una operación binaria en G).
- $\forall x, y, z \in G \quad x * (y * z) = (x * y) * z$ (prop. asociativa).

- $e \in G$ cumple que $\forall x \in G \quad x * e = e * x = x$ (e es neutro para $*$).
- $\forall x \in G \quad \exists y \in G \quad x * y = y * x = e$ (existencia de inversos resp. de $*$).

Es fácil probar que el inverso de x es único. Es usual denotarlo como x^{-1}.

Dados $(G, *, e)$ y $(G', \bullet, e')$ dos grupos, un morfismo de G en G' es una función $f : G \to G'$ que satisface $\forall x, y \in G \quad f(x * y) = f(x) \bullet f(y)$.

Cuando no da lugar a confusiones es común referirse a un grupo $(G, *, e)$ simplemememente como el grupo G. Es habitual además adoptar la notación multiplicativa para la operación $*$, escribiendo xy en lugar de $x * y$.

ii) Primer teorema de isomorfismos:

Sean G, G' grupos y sea $f : G \to G'$ un morfismo de grupos. Entonces $\dfrac{G}{\mathrm{Ker}(f)} \cong \mathrm{Im}(f)$.

b. Lo probamos por definición de normalidad: Sea $x \in G$. Para todo $y \in \mathrm{Ker}(f)$, $f(xyx^{-1}) = f(x)f(y)(f(x^{-1})) = f(x)(f(x))^{-1} = e$. Entonces $xyx^{-1} \in \mathrm{Ker}(f)$. Conluimos entonces que $\forall x \in G \quad x\,\mathrm{Ker}(f)x^{-1} \subseteq \mathrm{Ker}(f)$, lo que permite concluir que $\mathrm{Ker}(f) \lhd G$.

c. i) Es evidente, ya que $\det(AB) = \det A \det B$.

ii) Como 1 es el neutro de $\mathbb{R}^*$, entonces $N = \mathrm{Ker}(\det)$, de donde, por la parte (b), se concluye que $N \lhd \mathrm{GL}_n$. Es claro que la imagen de det es todo $\mathbb{R}^*$ ya que toda matriz invertible tiene determinante no nulo y todo real α no nulo es el determinante de $\alpha Id_{n\times n}$.

Aplicando el primer teorema de isomorfismo, concluimos que $\dfrac{\mathrm{GL}_n}{N} \cong \mathbb{R}^*$.

Por definición $A \sim_N B$ si y sólo si $AB^{-1} \in N$, es decir, si y sólo si $1 = \det A \det B^{-1} = \det(A)(\det B)^{-1}$, lo que equivale a decir que $\det(A) = \det(B)$.

Ejercicio 3.

a. Ver teórico

b. i) Ver teórico

ii) Ver teórico

c. i) Empezamos por factorizar $\varphi(10037) = 10036$: Lo dividimos entre 2 todo lo que sea posible, obteniendo: $10036 = 2^2 \times 2509$. Por criterios de divisibilidad es evidente que 2509 no es divisible entre $2, 3$ y 5. Dividiendo observamos que no es divisible entre 7 ni entre 11. Entre 13 obtenemos: $2509 = 13 \times 193$. Como la raíz cuadrada de 193 es menor que 14 y ya vimos que los primos menores que 13 no dividen a 2509, el único primo que podría dividir a 193 es 13. Como $13 \nmid 193$, concluimos que 193 es primo. En definitiva, $10036 = 2^2 \times 13 \times 193$.

Probaremos que 2 es ra iz primitiva módulo 10037. Aplicando el criterio de la parte (b)ii. basta con probar que si $m \in \{\frac{10036}{193} = 52, \frac{10036}{13} = 772, \frac{10036}{2} = 5018\}$ entonces $2^m \not\equiv_p 1$. Como $5018 = 2509 \times 2$, utilizando el dato proporcionado tenemos que $2^{5018} = (2^{2509})^2 \equiv_p (6766)^2 \equiv_p 10036 \not\equiv_p 1$. Para los otros exponentes utilizaremos el método de exponenciación rápida. Los números 52 y 772 expresados en base 2 son 110100 y 1100000100 respectivamente; es decir, $52 = 2^5 + 2^4 + 2^2$ y $772 = 2^9 + 2^8 + 2^4$ y por lo tanto $2^{52} = 2^{2^5}2^{2^4}2^{2^1}$ y

$2^{772} = 2^{2^9}2^{2^8}2^{2^4}$. en la siguiente tabla cada fila se obtiene reduciendo módulo 10037 el cuadrado de la fila anterior (como $256 = 2^8$, utilizamos el dato brindado para saltearnos las filas $i = 6, 7$ ya que no las necesitamos).

i	$2^{(2^i)}$ mód 10037
0	2
1	4
2	16
3	256
4	5314
5	4515
⋮	⋮
8	8637 (dato)
9	2785

Entonces:

- $2^{52} = 4515 \times 5314 \times 16 = 8258$ módulo 10037 y
- $2^{772} = 2785 \times 8637 \times 16 = 5992$ módulo 10037.

Concluimos que 2 es R.P. módulo 10037.

ii) $2^{32} = 2^{2^5} = 4515$ (está en la tabla).

iii) La clave es $c = 5314^{(2^5)}$. En la tabla tenemos que $5314 = 2^{2^4}$, de modo que $c = \left(2^{2^4}\right)^{2^5} = 2^{2^2 2^5} = 2^{2^9} = 2785$ (que está en la tabla). Tenemos $c = 3 \times 28^2 + 15 \times 28 + 13$, de modo que su expresión en base 28 es: $(3, 15, 13)$, que corresponde a la palabra clave `DON`.

iv) Para cifrar un mensaje con el sistema Vigenère, primero se transforma el mensaje original a una secuencia de números entre 0 y 27 (utilizando la tabla brindada) y luego a esta secuencia se le suma módulo 28 la secuencia (numérica) correspondiente a repetir la palabra clave, esto es: `DONDONDONDON...` que corresponde a la secuencia $(3, 15, 13, 3, 15, 13, 3, 15, 13, \cdots)$. El resultado traducido a texto es el mensaje codificado, que se envía al interlocutor. Por lo tanto, para descifrar un mensaje hay que realizar el proceso inverso. Es decir, al texto recibido debemos convertitlo en una secuencia numérica, a la cual le restamos módulo 28 la secuencia de la clave. Al resultado lo convertimos a texto y obtenemos el mensaje original.

texto recibido	S	F	A	E	O	Z	G	C	M	F	Z	N	Y	S
conv. a $\mathbb{N}$	19	5	0	4	15	26	6	2	12	5	26	13	25	19
clave	3	15	13	3	15	13	3	15	13	3	15	13	3	15
resta mod 28	16	18	15	1	0	13	3	15	27	2	11	0	22	4
conv. a texto	P	R	0	B	A	N	D	O	_	C	L	A	V	E