Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2, semipresencial

Segundo parcial - 30 de noviembre de 2017. Duración: 4 horas

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

Ejercicio 1.

a. Probar que 2 es raíz primitiva módulo 19.

b. Sea p es primo y g una raíz primitiva módulo p. Si m es el orden de g en $U(p^2)$, probar que $p-1 \mid m$.

c. Hallar una raíz primitiva módulo $19^2 = 361$.

d. Probar que si x es un entero impar y p es un primo impar, entonces que $x^m \equiv 1 \pmod{2p^2} \Leftrightarrow x^m \equiv 1 \pmod{p^2}$.

e. Hallar una raíz primitiva módulo 722.

Ejercicio 2. Sea $G = U(241)$ y $H = \{h \in G, \text{ tal que } o(h) \mid 24\}$.

a. Probar que si $x \notin H$ y $x^2 \in H$ entonces $o(x) \in \{16, 48\}$.

b. Probar que $\#H = 24$ (*sugerencia:* 241 *es primo*).

c. Probar que $H = \langle \overline{2} \rangle$ y listar los elementos de H.

d. Probar, utilizando lo anterior, que $o(\overline{11}) = 48$.

e. Sabiendo que $10^5 \equiv 2^{20} \pmod{241}$, hallar $o(\overline{10})$.

f. Hallar (justificando) una raíz primitiva módulo 241 (puede quedar expresada como producto de potencias).

g. Para utilizar el método Diffie Hellman de intercambio de 5 clave, Ana y Bruno eligen g una raìz primitiva módulo 241. Si Ana elige el exponente $a = 50$ y Bob elige el exponente $b = 56$, probar que la clave fijada es $k = 15$ o $k = 225$.

Ejercicio 3. Sea G un grupo y $H < G$. Consideramos en G la relación de equivalencia $g \sim k \Leftrightarrow gk^{-1} \in H$ (NO es necesario verificar que es relación de equivalencia).

a. Probar que si C es una clase de equivalencia, entonces $\#C = |H|$.

b. Probar que si $F : G \to A$ es un homomorfismo de grupos y $H = \ker(F)$ entonces para $g, k \in G$ se tiene que $g \sim k \Leftrightarrow F(g) = F(k)$.

c. Enunciar y demostrar el Teorema de órdenes para homomorfismos de grupos.

d. Probar que si $F : G \to A$ es un homomorfismo sobreyectivo entre grupos finitos, entonces $a^{|G|} = e_A$ para todo $a \in A$.

Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2

Segundo parcial - 29 de junio de 2017. Duración: 3 horas

El parcial es *sin* material y *sin* calculadora.

Ejercicio 1. Sea $g \in G$ tal que $o(g) = n$

a. Probar que para todo $m \in \mathbb{Z}$ se cumple $g^m = e \iff n \mid m$.

b. Probar que $g^a = g^b \iff a \equiv b \pmod{n}$.

c. Probar que $|\langle g \rangle| = n$.

d. Usar el Teorema de Lagrange para probar que si G es finito, entonces $n \mid |G|$.

Solución.

a. ($\Rightarrow$) Si $g^m = e$, dividiendo m entre n tenemos que $m = nq + r$ con $0 \leq r < n$. Por lo tanto $e = g^m = g^{nq+r} = (g^n)^q\, g^r = e^q\, g^r = g^r$. En otras palabras $g^r = e$, pero n es el menor entero positivo que cumple $g^n = e$, y como $0 \leq r < n$ debe ser $r = 0$. Luego, $m = nq$ y $n \mid m$.

($\Leftarrow$) Si $m = nq$, entonces $g^m = g^n q = (g^n)^q = e^q = e$.

b. $g^a = g^b \Leftrightarrow g^{a-b} = e \overset{(\mathbf{a})}{\iff} n \mid a - b \Leftrightarrow a \equiv b \pmod{n}$.

c. Por la parte anterior $\langle g \rangle = \{g^k \ : \ k \in \mathbb{Z}\} = \{g^0, g^1, \ldots, g^{n-1}\}$, donde los elementos $g^0, g^1, \ldots, g^{n-1}$ son todos distintos. Concluimos que $|\langle g \rangle| = n$.

d. Como $\langle g \rangle$ es un subgrupo de G, el Teorema de Lagrange implica que $n = |\langle g \rangle| \mid |G|$.

Ejercicio 2.

a. Probar que 11 es una raiz primitiva módulo 71.

b. Aldo y Beatriz eligen $p = 71$ y $g = 11$ para intercambiar claves utilizando el método de Diffie y Hellman. Beatriz elige $m = 7$ y Aldo le envía el número $g^n \equiv 61 \pmod{71}$. ¿Cuál es la clave que acuerdan?

Solución.

a. Como 71 es primo $\varphi(71) = 70 = 2{\cdot}5{\cdot}7$. Entonces alcanza probar que $11^{10} \not\equiv 1 \pmod{71}$, que $11^{14} \not\equiv 1 \pmod{71}$, y que $11^{35} \not\equiv 1 \pmod{71}$. En efecto calculamos $11^2 \equiv 50$, $11^4 \equiv 50^2 \equiv 15$, $11^8 \equiv 15^2 \equiv 12$, $11^{16} \equiv 12^2 \equiv 2$, $11^{32} \equiv 2^2 \equiv 4$. Ahora $11^{10} \equiv 11^8 \cdot 11^2 \equiv 32 \not\equiv 1$, $11^{14} \equiv 11^{10} \cdot 11^4 \equiv 54 \not\equiv 1$, y $11^{35} \equiv 11^{32} \cdot 11^2 \cdot 11 \equiv 70 \not\equiv 1$.

b. La clave que acuerdan es $g^{nm} = (g^n)^m \equiv 61^7 \pmod{71}$. Calculamos $61^2 \equiv 29$, $61^4 \equiv 29^2 \equiv 60$, y tenemos $61^7 \equiv 61 \cdot 61^2 \cdot 61^4 \equiv 60 \cdot 10 \cdot 29 \equiv 66 \pmod{71}$.

Ejercicio 3. Alicia y Beto quieren comunicarse con el método ElGamal. A tales efectos eligen un primo p y una raíz primitiva g módulo p. Alicia elige un entero a como su clave privada y calcula $h \equiv g^a \pmod{p}$ como su clave pública. Beto quiere enviar un mensaje $m \in \mathbb{Z}_p$ a Alicia.

a. Describir el algoritmo de cifrado E que debe usar Beto.

b. Describir la función de descifrado D que debe usar Alicia.

c. Demostrar que $D(E(m)) = m$ para todo $m \in \mathbb{Z}_p$.

Solución.

a. Beto elige un entero b secreto (utilizable una única vez) y calcula $r \equiv g^b \pmod{p}$ y $c \equiv h^b \cdot m \pmod{p}$, obteniendo $E(m) = (r, c)$.

b. Ana calcula $D(r, c) = c \cdot r^{-a} \pmod{p}$

c. $D(E(m)) \equiv D(g^b, h^b \cdot m) \equiv (h^b \cdot m) \cdot (g^b)^{-a} \equiv (g^a)^b \cdot m \cdot g^{-ab} \equiv m \cdot (g^{ab} \cdot g^{-ab}) \equiv m \pmod{p}$

Ejercicio 4. Consideramos el grupo dihedral D_3.

a. Describir todos los elementos de D_3 indicando su orden.

b. Sean $u, v \in D_3$ dos elementos distintos de orden 2. Probar que uv tiene orden 3.

c. Consideramos la función $f : D_3 \to D_3$ dada por $f(x) = x^2$. ¿Es f un homomorfismo?

d. Describir todos los homomorfismos $h : \mathbb{Z}_6 \to D_3$.

Solución.

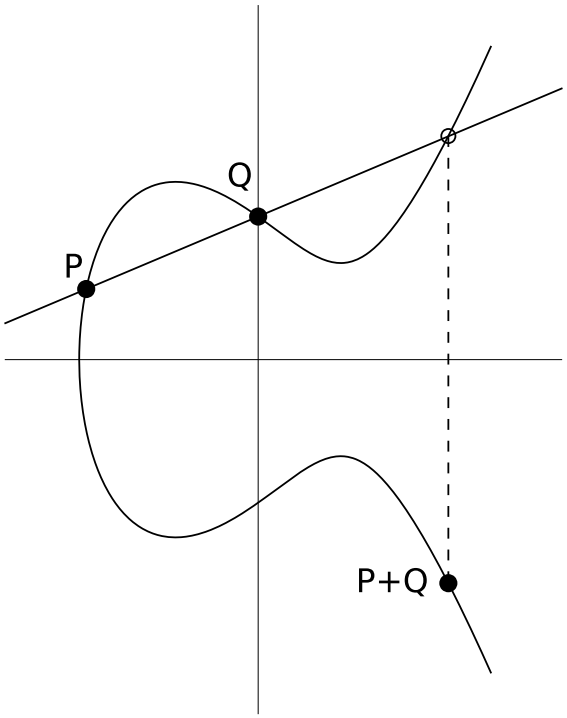
a. $D_3 = \{e, r, r^2, s, sr, sr^2\}$ donde r y r^2 son rotaciones y tienen orden 3, mientras que s, sr y sr^2 son simetrías axiales y tienen orden 2.

b. Como u y v tienen orden 2 son simetrías axiales. Entonces uv es un movimiento directo, debiendo ser 1, r, o r^2. Pero $u \neq v$ implica que $uv \neq e$. Entonces uv es una rotación, luego tiene orden 3.

c. No es un homomorfismo, por ejemplo si u y v son como en la parte anterior $f(u) = e$ y $f(v) = e$, pero $f(uv) = (uv)^2 \neq e$.

d. Como $\mathbb{Z}_6$ es cíclico generado por $\overline{1}$ de orden 6, cualquier homomorfismo es de la forma $h(\overline{n}) = g^n$ para algún $g \in D_3$ con $o(g) \mid 6$. Pero esto último vale para cualquier $g \in D_3$, entonces hay 6 homomorfismos $h : \mathbb{Z}_6 \to D_3$, uno para cada posible g.

Bonus. Determinar geométricamente el punto $\mathsf{P} + \mathsf{Q}$ en la siguiente curva elíptica:



Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2, semipresencial

Solución cuarta prueba (segundo parcial) - 1 de diciembre de 2016.

Ejercicio 1. (15 puntos) *(Ejercicio 1 del segundo parcial del curso semipresencial de 2015)*

a. Probar que 2 es raíz primitiva módulo 53.

b. Hallar todos los $x \in \mathbb{Z}$ tales que $x^{19} \equiv 32 (\text{mód } 53)$.

c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo $p = 53$ y la raíz primitiva $g = 2$. Archibaldo selecciona el número $m = 28$ y le remite el número 49 a Baldomero. Éste selecciona el número $n = 5$. ¿Cuál es la clave común k que acordaron Archibaldo y Baldomero?

Solución Ejercicio 1:

a. Observemos primero que $52 = 2^2 \cdot 13$. Por lo tanto, si queremos probar que 2 es raíz primitva módulo 53, debemos probar que $2^{\frac{52}{p}} \not\equiv 1 (\text{mód } 53)$, para todo p primo, con $p|52$. O sea debemos calcular 2^4 y 2^{26}.

n	$2^n \pmod{53}$
0	$1 \pmod{53}$
1	$2 \pmod{53}$
2	$4 \pmod{53}$
3	$8 \pmod{53}$
4	**16 mód53**
5	$32 \pmod{53}$
6	$11 \pmod{53}$
7	$22 \pmod{53}$
8	$44 \pmod{53}$
9	$35 \pmod{53}$
10	$17 \pmod{53}$
11	$34 \pmod{53}$
12	$15 \pmod{53}$
13	$30 \pmod{53}$
14	$7 \pmod{53}$
15	$14 \pmod{53}$
$\vdots$	$\vdots$

Luego $2^{26} = 2^{13} \times 2^{13} \equiv 900 \pmod{53} \equiv -1 \pmod{53}$.
Entonces 2 es raíz primitiva módulo 53.

b. Como $32 = 2^5$ la ecuación a resolver se transforma en: $x^{19} \equiv 2^5 (\text{mód } 53)$. Por otro lado, como 2 es raíz primitva módulo 53, entonces para todo $x \in \mathbb{Z}$ existe $0 \leq t(x) \leq 52$ tal que $x = 2^{t(x)}$. Luego la ecuación a resolver se transforma en: $2^{t(x)^{19}} \equiv 2^5 (\text{mód } 53)$. Nuevamente como 2 es raíz primitiva, la ecuación anterior es equivalente a: $19 \cdot t(x) \equiv 5 \pmod{52}$. Esto último a su vez es equivalente a $t(x) \equiv 3 \pmod{52}$. Luego $x = 2^3 \pmod{53}$, o sea $x = 8 + 53 \cdot z$, con $z \in \mathbb{Z}$.

c. Archibaldo toma $m = 28$ y le envía $2^{28} \equiv 49 \pmod{53}$ a Baldomero. Éste toma $m = 5$ y le envía $49^5 \pmod{53}$ a Archibaldo. O sea, $49^5 \equiv (-4)^5 \pmod{53} = -2^{10} \pmod{53} \equiv -17 \pmod{53} \equiv 36 \pmod{53}$. O sea que la clave común acrodada es $k = 36$.

Ejercicio 2. (20 puntos)

a. Calcular el número de raíces primitivas en $U(29)$.

b. Encontrar todas las raíces primitivas de $U(29)$.
(Sugerencia: Calcular $2^n \pmod{29}$, para todo $0 \leq n \leq 14$, para faciitar los cálculos posteriores.)

c. Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior: $r_1 \leq r_2 \leq r_3 \leq r_4 \leq r_5 \leq .....$ Luego escribir la secuencia: $r_1 r_5 0 r_9 r_3 r_1 r_7$. Finalmente traducir usando la numeración de los símbolos:

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

d. Utilizando el método de Vigenère **decodificar** el siguiente texto, usando la palabra clave hallada en el ítem anterior:

$$OZ\_LPTSOKMS\_BUCBRSNCG$$

Solución Ejercicio 2:

a. El número de raíces primitvas en $U(n)$ (si hay) es $\varphi(\varphi(n))$, siendo φ la función de Euler. En este caso $\varphi(29) = 28$, pues 29 es primo. Luego $\varphi(28) = \varphi(4 \times 7) = \varphi(4) \cdot \varphi(7) = 2 \cdot 6 = 12$. Entonces el número de raíces primitvas en $U(29)$ es 12.

b. Para encontrar todas las raíces primitivas calculamos los valores sugeridos en la letra del ejercicio, en la siguiente tabla:

n	$2^n \pmod{29}$
0	1 (mód 29)
1	2 (mód 29)
2	4 (mód 29)
3	**8 mód29**
4	16 (mód 29)
5	**3 mód29**
6	6 (mód 29)
7	12 (mód 29)
8	24 (mód 29)
9	**19 mód29**
10	9 (mód 29)
11	**18 mód29**
12	7 (mód 29)
13	**14 mód29**
14	-1 (mód 29)
$\vdots$	$\vdots$

Luego se concluyen varias cosas de la tabla anterior:

- Por un lado $2^{14} \not\equiv 1 \pmod{29}$ y también se verifica: $2^4 \not\equiv 1 \pmod{29}$. Entonces $o(2) = 28$, concluyendo que 2 es raíz primitiva en $U(29)$.
- Como 2 es raíz primitiva, entonces $2^s \pmod{29}$ es raíz primitiva para todo $s \in \mathbb{N}$ tal que $\text{mcd}(s, 28) = 1$. Entonces las que están marcadas en "negrita" en la tabla son también raíces primitivas. Así que tenemos hasta ahora las siguientes raíces primitivas: 2, 3, 8, 14, 18 y 19.

- Por último puede observarse que $-2, -3, -8, -14, -18$ y -19 son raíces primitivas de $U(29)$. O sea, $27, 26, 21, 15, 11$ y 10 son raíces primitivas de $U(29)$. Sugerimos tres caminos para probar la última afirmación.
  - Completar la tabla anterior hasta $n = 28$.
  - Probar teóricamente que si a es raíz primitva en $U(29)$ entonces $(-a)$ también.
  - Hacer las cuentas a mano en cada caso.

c. Por lo tanto las raíces primitivas, ordenadas en forma creciente son:

$$2 \leq 3 \leq 8 \leq 10 \leq 11 \leq 14 \leq 15 \leq 18 \leq 19 \leq 21 \leq 26 \leq 27.$$

La palabra clave es: CLASICO (sería CLÁSICO).

d. Por último decodificando el mensaje oculto

$$OZ\_LPTSOKMS\_BUCBRSNCG$$

utilizando Vigenère, obtenemos el mensaje:

$$NO\_TIREN\_MAS\_GARRAFAS$$

Ejercicio 3. (10 puntos) Describir el "Método de Fermat"de ataque al RSA, y demostrar la validez del algoritmo planteado.

Solución Ejercicio 3
Ver los apuntes de Teórico, Capítulo 5, ítem 5.3.4, Método de Fermat de ataque al RSA.

Segundo parcial - 29 de junio de 2016.

Primera parte: Múltiple Opción

Ejercicio 1. Austria y Bielorusia quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello toman el primo $p = 499$ y $g = 7$ raíz primitiva módulo p. Austria elije el número $m = 394$ y le envía el número 489 a Bielorusia. Bielorusia elije el número $n = 18$. ¿Cuál es la clave k común que acordaron Austria y Bielorusia?
Indicar cuál de las opciones es correcta:

A. $k = 331$. **B**. $k = 77$. **C**. $k = 80$. **D**. $k = 64$.

Solución:
Tenemos que calcular $489^{18} \pmod{499} \equiv (-10)^{18} \pmod{499} \equiv ((-10)^3)^6 \pmod{499} \equiv (-1000)^6 \pmod{499} \equiv (-2)^6 \pmod{499} \equiv 64 \pmod{499}$.

Ejercicio 2. Sean $n = 209$ y $e = 7$. Para los datos anteriores sea función de descifrado $D : \mathbb{Z}_n \to \mathbb{Z}_n$ definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

A. $D(y) = y^{103} \pmod{n}$. **C**. $D(y) = y^{119} \pmod{n}$.

B. $D(y) = y^{30} \pmod{n}$. **D**. $D(y) = y^{163} \pmod{n}$.

Solución:
La función de descifrado es $D(y) = y^d \pmod{n}$ donde d es tal que $d \equiv e^{-1} \pmod{\varphi(n)}$. La factorización de n es $209 = 11 \cdot 19$, por lo que $\varphi(11 \cdot 19) = 10 \cdot 18 = 180$. Utilizando el algoritmo extendido de Euclides obtenemos $d \equiv 103 \pmod{180}$.

Segunda parte: Desarrollo

Ejercicio 3.

a. Sea $(G, *)$ un grupo finito y H un subgrupo de G. Definimos la siguiente relación en G:

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

b. Sean G, K grupos finitos y $f : G \to K$ un homomorfismo de grupos. Probar que $\mathrm{Ker}(f)$ es un subgrupo de G.

c. Probar el teorema de órdenes para grupos:

Sean G y K dos grupos finitos y $f : G \to K$ un homomorfismo de grupos. Entonces

$$|G| = |\mathrm{Ker}(f)||\mathrm{Im}(f)|.$$

Solución: Ver la segunda demostración del Teorema de Ordenes de las notas, Teorema 3.9.8.

Ejercicio 4.

a. Sean G un grupo finito, $g \in G$ y $n \in \mathbb{N}$, probar que $\mathrm{o}\left(g^n\right) = \frac{\mathrm{o}(g)}{\mathrm{mcd}(\mathrm{o}(g),n)}$.
Solución: Ver Proposición 3.7.8 parte 7 de las notas.

b. Probar que 2 es raíz primitiva módulo 101 y hallar un elemento de $U(101)$ con orden 10.
Solución: Para ver que 2 es r.p. módulo 101, alcanza con ver $2^{50} \not\equiv 1 \pmod{101}$ y $2^{20} \not\equiv 1 \pmod{101}$, ya que $\varphi(101) = 100 = 2^2 5$ y $100/2 = 50$, $100/5 = 20$. Entonces $2^{20} = (2^{10})^2 \equiv (1024)^2 \pmod{101} \equiv 14^2 \pmod{101} \equiv 196 \pmod{101} \equiv 95 \pmod{101} \not\equiv 1 \pmod{101}$. También $2^{50} = (2^{20})^2 \cdot 2^{10} \equiv (95)^2 \cdot 14 \pmod{101} \equiv (-6)^2 \cdot 14 \pmod{101} \equiv 36 \cdot 14 \pmod{101} \equiv 504 \pmod{101} \equiv -1 \pmod{101}$. Con es probamos que 2 es r.p. módulo 101.
Para hallar un elemento de orden 10 utilizamos la parte anterior y el hecho que que el orden de 2 es 100. Utilizamos $n = 10$ y obtenemos

$$\mathrm{o}\left(2^{10}\right) = \frac{\mathrm{o}(2)}{\mathrm{mcd}(\mathrm{o}(2), 10)} = \frac{100}{\mathrm{mcd}(100, 10)} = \frac{100}{10} = 10.$$

Por lo tanto $\mathrm{o}(14) = 10$.

Ejercicio 5. Sean los grupos $G = \mathbb{Z}_{100}$ y $K = U(101)$.

a. Probar que los grupos G y K son isomorfos.
Solución: Dado que $\bar{1}$ es generador de G y tiene orden 100 que es el orden de 2 en K, el morfismo $f : G \to K$ dado por $f(\bar{n}) = 2^n \pmod{101}$ es un morfismo bien definido. Es fácil ver que es inyectivo ya que $f(n) = 1$ si y solo si $2^n \equiv 1 \pmod{101}$, o sea si $n \equiv 0 \pmod{100}$. Como G y K tienen igual orden entonces es biyectivo y por lo tanto es un isomorfismo.

b. Describir todos los isomorfismos entre G y K.
Solución: En la parte anterior podemos cambiar f por f_k donde $f_k(n) = 2^{kn} \pmod{101}$ y k otro elemento de orden 100 de $\mathbb{Z}_{100}$. El nuevo f_k es isomorfismo de igual manera que antes. Por el ejercicio anterior vemos que los k que cumplen que son generadores de $\mathbb{Z}_{100}$ son los que cumplen $\mathrm{mcd}(k, 100) = 1$. Y por lo tanto obtuvimos todos los isomorfismos entre G y K.

Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2, semipresencial

Primer parcial - 3 de diciembre de 2015. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre

Ejercicio 1.

a. Probar que 2 es raíz primitiva módulo 53.

b. Hallar todos los $x \in \mathbb{Z}$ tales que $x^{19} \equiv 32 \pmod{53}$.

c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo 53 y la raíz primitiva $g = 2$. Archibaldo selecciona el número $m = 28$ y le remite el número 49 a Baldomero. Baldomero selecciona el número $n = 5$. ¿Cuál es la clave k común que acordaron Archibaldo y Baldomero?

Ejercicio 2.

a. Sea $(G, *)$ un grupo finito y H un subgrupo de G. Definimos la siguiente relación en G:

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

b. Sean G, K grupos finitos y $f : G \to K$ un homomorfismo de grupos. Probar que $\mathrm{Ker}(f)$ es un subgrupo de G.

c. Probar el teorema de órdenes para grupos:

Sean G y K dos grupos finitos y $f : G \to K$ un homomorfismo de grupos. Entonces

$$|G| = |\mathrm{Ker}(f)||\mathrm{Im}(f)|.$$

Ejercicio 3.

a. Sea $f : G \to K$ un homomorfismo de grupos y $g \in G$ un elemento de orden $o(g)$ finito. Probar que $o(f(g)) \mid o(g)$.

b. Para los pares de grupos G y K, determinar si existen homomorfismos no triviales $f : G \to K$. Si existen encontrarlos todos, de lo contrario justificar por qué no existen.

i) $G = \mathbb{Z}_6$ el grupo de enteros módulo 6 y $K = S_3$ el grupo de permutaciones de 3 elementos.

ii) $G = S_6$ el grupo de permutaciones de 6 elementos y $K = \mathbb{Z}_7$ el grupo de enteros módulo 7.

c. Sean $G = D_{12}$ el grupo dihedral y $K = S_3 \times U(8)$ el producto cartesiano de los grupos S_3 (permutaciones de 3 elementos) y $U(8)$ ¿Son isomorfos estos grupos? De serlo, dar un isomorfismo entre ellos, de lo contrario justificar por qué no lo son.

Segundo parcial - 4 de julio de 2014. Duración: 3 horas y media

N° de parcial	Cédula	Apellido y nombre	Salón

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

Ejercicio 1.

a. Sea $n \in \mathbb{Z}^+$, y g un entero coprimo con n. Probar que si a es el orden de $\overline{g}$ en $U\left(n^2\right)$ y b es el orden de $\overline{g}$ en $U(n)$, entonces $b \mid a$.

b. Sea $p = 19$.

i) Probar que 10 es raíz primitiva módulo p.

ii) ¿Es 10 raíz primitiva módulo p^2? Pueden utilizar los siguientes datos: $10^5 \equiv 3 \pmod{p^2}$ y $3p^2 = 1083$.

iii) Para cada $k \in \mathbb{Z}^+$ hallar una raíz primitiva módulo $2p^k$.

Ejercicio 2.

a. Si $f : G \to K$ es un homomorfismo de grupos probar que $o(f(g)) \mid o(g)$ para todo $g \in G$.

b. En cada parte, hallar todos los homomorfismos $f : G \to K$ justificando debidamente.

i) $G = S_4$ con la composición como operación y $K = \mathbb{Z}_{35}$ con la suma de clases como operación.

ii) $G = \mathbb{Z}_{15}$ y $K = \mathbb{Z}_6$, ambos grupos con la suma de clases como operación.

Ejercicio 3. Sea G un grupo y $g \in G$ de orden finito. Probar que:

a. Si $k \in \mathbb{Z}^+$, entonces $o(g^k) = \dfrac{o(g)}{\text{mcd}(o(g), k)}$.

b. Si $H = \langle\, g \,\rangle$, entonces existen $\varphi(o(g))$ elementos en H que generan H.

Ejercicio 4.

a. Ana y Bruno quieren acordar una clave común usando el protocolo Diffie-Hellman. Para ello eligen el primo $p = 1009$ y la raíz primitiva $g = 11$. Ana elige el número $m = 260$ le envía a Bruno el número 1005. Bruno elige el entero $n = 8$. ¿Cuál es la clave k común que acordaron Ana y Bruno?.

b. Ahora Ana quiere comunicarse con Bruno través de un sistema Vigenere donde la palabra clave consiste de 3 letras de la siguiente manera: se toma la clave k común acordada en la parte anterior y se la escribe en base 28:

$$k = L_2 28^2 + L_1 28 + L_0.$$

Luego la clave común resulta de sustituir en $L_2L_1L_0$ por sus respectivas letras (por ejemplo si $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$ entonces la clave común será `YAC`).

i) Calcular la clave k como $L_2L_1L_0$.

ii) Usando la clave anterior descifrar el siguiente mensaje: `WUFAGHFCWÑKZBXHEÑ␣DXMUG`.

Ejercicio 5. Enunciar y demostrar el Teorema de Lagrange para grupos.

Solución segundo parcial

Ejercicio 1 (18 pts).

a) Probar que 2 es raíz primitiva módulo 101.

b) Alicia y Bernardo eligen $p = 101$, $g = 27$ para intercambiar claves en Diffie-Hellman.

i. Bernardo elige $m = 3$ y Alicia le envía el número $g^n = 22 \mod(101)$. ¿Cuál es la clave K que acuerdan?

ii. ¿Qué número (n) eligió Alicia?

c) Se utiliza el método César afín para encriptar siendo la función de encriptado $E : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$, donde $E(x) = cx + e$, con $K = e28 + c$ escrito en base 28.

i. Hallar la función de desencriptar $D : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$ explícitamente.

ii. Desencriptar *GBZWFÑRJGDSFUB*.

Solución Ejercicio 1

a. Alcanza con ver, por el Ejercicio 1, parte C, del Práctico 8, que $2^{100/p} \not\equiv 1 \pmod{101}$ para todo primo p que divide a 100. En efecto

$$2^{100/5} = 2^{20} = (2^{10})^2 \equiv 14^2 \equiv 95 \pmod{101}$$
$$2^{100/2} = 2^{50} = (2^{10})^5 \equiv 14^5 = (14^2)^2 \cdot 14 \equiv (-6)^2 \cdot 14 \equiv 100 \pmod{101}.$$

Luego 2 es una raíz primitiva módulo 101.

b.i. La clave que acuerdan al utilizar Diffie-Hellman es $g^{nm} = (g^n)^m = 22^3 = 43 \pmod{101}$.

b.ii. Como $g = 27 = 2^7 \pmod{101}$ entonces $g^2 = 2^{14} = 27 \cdot 27 = 22 \pmod{101}$. Luego como $g^n = 22 \pmod{101}$, entonces

$$2^{7n} \equiv 2^{14} \pmod{101}.$$

Luego, usando que 2 es raíz primitiva módulo 101 por la parte anterior y usando el Ejercicio 6 del Práctico 8 (Logartimo Discreto), de este parcial, se tiene que $7n \equiv 14 \pmod{100}$. O sea que $n = 2$ es solución.

c. $K = 43 = 28 \cdot 1 + 15$. Por lo que $e = 1$ y $c = 15$.

c.i. Sabemos que $D(x) = c'(x - e) \pmod{28}$ donde c' es el inverso de c módulo 28. Luego como $c = 15$, se puede probar que $c' = 15$ (pues

$15 \cdot 15 = 225 = 1 \pmod{28}$). Y como $e = 1$, entonces $D(x) = 15(x-1) \pmod{28}$.

c.ii. La desencriptación de *GBZWFÑRJGDSFUB* es *SALVÉ DISCRETA*.

Ejercicio 2 (15 pts).

a) Sea H es un subgrupo no nulo de $\mathbb{Z}$.

i. Probar que si $a \in H$ entonces $na \in H$ para todo entero n.

ii. Sea $x = \text{mín}\{a > 0 : a \in H\}$. Probar que $H = x\mathbb{Z} = \{xn : n \in \mathbb{Z}\}$.

b) Sean $x, y \in \mathbb{Z}$. Probar que $x\mathbb{Z} \cap y\mathbb{Z} = mcm(x, y)\mathbb{Z}$.

c) Concluir, usando las partes anteriores, que si H y H' son dos subgrupos no nulos de $\mathbb{Z}$ entonces $H \cap H' \neq 0$.

d) Dados $x, y \in \mathbb{Z}$ probar que el grupo generado por x e y es $\langle x,\ y\rangle = \text{mcd}(x, y)\mathbb{Z}$.

Solución Ejercicio 2

a.i. Como H es un subgrupo de $\mathbb{Z}$ y $a \in H$, entonces $< a >\subset H$. Pero $< a >= \{na \ / \ n \in \mathbb{Z}\} = \{\underbrace{a + a + \cdots + a}_{n-veces} \ / \ n \in \mathbb{Z}^+\} \cup \{0\} \cup \{\underbrace{(-a) + (-a) + \cdots + (-a)}_{(-n)-veces} \ / \ n \in \mathbb{Z}^-\}$, y por tanto $na \in H$ para todo entero n.

a.ii. Sea $a \in H$. Como $x > 0$, se puede hacer la división entera de a por x y obtener

$$a = qx + r \text{ con } q, r \text{ enteros, y } 0 \leq r < x.$$

La parte anterior aplicada a $x \in H$ implica $qx \in H$. Como a también está en H, entonces

$$r = a - qx \in H.$$

Y dado que x es el mínimo elemento positivo de H, r debe ser necesariamente 0. O sea que $a = qx$. Luego $H = \{nx : n \in \mathbb{Z}\}$.

b. La igualdad de conjuntos se sigue de las siguientes equivalencias inmediatas

$$z \in x\mathbb{Z} \cap y\mathbb{Z} \Longleftrightarrow x, y | z \Longleftrightarrow mcm(x, y) | z \Longleftrightarrow z \in mcm(x, y)\mathbb{Z}.$$

c. Usando 2)a) se puede afirmar que como H es no nulo entonces existe $x > 0$ tal que $H =< x >$. Lo mismo se puede decir para H', es decir al ser no nulo hay un $y > 0$ tal que $H' =< y >$. Y ahora usando 2)b) se tiene que $H \cap H' = mcm(x, y)\mathbb{Z} \neq 0$.

d. La igualdad de conjuntos se sigue de las siguientes equivalencias inmediatas

$$z \in < x, y > \iff z = ax+by \text{ con } a, b \in \mathbb{Z} \iff mcd(x, y)|z \iff z \in mcd(x, y)\mathbb{Z}.$$

Ejercicio 3 (15 pts).

a) Sea r una raíz primitiva módulo p, con p primo. Probar que $r^a \equiv r^b \mod(p)$ si y solamente si $a \equiv b \mod(p-1)$.

b) Probar que 2 es raíz primitiva módulo 37.

c) Calcular $\log_2 17$.

d) Resolver $13^{5z} \equiv 17 \mod(37)$.

Solución Ejercicio 3
a.($\Longrightarrow$) Sean

$$a = q_1(p-1) + s_1 \text{ con } q_1, s_1 \text{ enteros, y } 0 \leq s_1 < p-1$$
$$b = q_2(p-1) + s_2 \text{ con } q_2, s_2 \text{ enteros, y } 0 \leq s_2 < p-1$$

las respectivas divisones enteras de a y b entre $p-1$. Luego

$$r^a = r^{q_1(p-1)+s_1} = (r^{p-1})^{q_1} \cdot r^{s_1} \equiv r^{s_1} \pmod{p}$$
$$r^b = r^{q_2(p-1)+s_2} = (r^{p-1})^{q_2} \cdot r^{s_2} \equiv r^{s_2} \pmod{p}$$

y como $r^a \equiv r^b \pmod{p}$, entonces $r^{s_1} \equiv r^{s_2} \pmod{p}$. Luego $r^{s_1-s_2} \equiv 1 \pmod{p}$, y por lo tanto $o(r)|s_1 - s_2$. Como r es una raíz primitva, entonces $o(r) = p-1$. Y como $0 \leq s_1, s_2 < p-1$ entonces $s_1 = s_2$.

($\Longleftarrow$) Si $a \equiv b \pmod{p-1}$ entonces a y b dejan el mismo resto al dividirse por $p-1$. Luego razonando como en el directo se obtiene $r^a \equiv r^b \pmod{p}$.

b. Al igual que en el Ejercicio 1, para ver que 2 es raíz primitiva módulo 37, como $\phi(37) = 36 = 2^2 \cdot 3^2$, alcanza con ver que $2^{36/2}$ y $2^{36/3}$ no son congruentes con 1 módulo 37. Pero

$$2^{36/2} = 2^{18} = (2^5)^3 \cdot 2^3 \equiv (-5)^3 \cdot 8 \equiv 36 \pmod{37}$$
$$2^{36/3} = 2^{12} = (2^5)^2 \cdot 2^2 \equiv (-5)^2 \cdot 4 \equiv 26 \pmod{37}$$

y por tanto 2 es raíz primitiva módulo 37.

c. Como $2^7 = 128 \equiv 17 \pmod{37}$ entonces $\log_2 17 = 7$.

d. Como $2^{11} = 2048 \equiv 13 \pmod{37}$ entonces

$$(2^{11})^{5z} \equiv 2^7 \pmod{37}.$$

Luego, usando que 2 es raíz primitiva módulo 37 y 3)a), se tiene que $55z \equiv 7 \pmod{36}$. Luego $z = 25$.

Ejercicio 4 (12 pts).

a) Enunciar el test de primalidad de Lucas.

b) Demostrarlo.

Solución Ejercicio 4
Fue dado en ambos Teóricos. Ver en el Texto *The Mathematics of Ciphers - Number Theory and RSA Cryptography*, S. C. Coutinho, pág. 151.

Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2012**
Instituto de Matemática y Estadística 4 de Julio de 2012.

SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA 2

Nombre	C.I.	No. de prueba .....

Duración: 4 horas. **Sin** material y **sin** calculadora.

Es necesario mostrar la resolución de los ejercicios y el procedimiento para llegar a la respuesta. Presentar únicamente la respuesta final carece de valor.

Ejercicio 1. (18 puntos) Sea $H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a = \pm 1, b \in \mathbb{Z} \right\}$.

A. Probar que H es un subgrupo *abeliano* de $GL_2(\mathbb{R})$ (las matrices 2×2 invertibles con entradas reales). Aclaración: no es necesario probar que $GL_2(\mathbb{R})$ es un grupo.

B. Hallar el orden de $g = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in H$, discutiendo según a y b.

C. Sean $(G_1, \cdot)$ y $(G_2, *)$ dos grupos con neutros e_1 y e_2 respectivamente. Probar que un homomorfismo $\varphi : G_1 \to G_2$ es inyectivo si y sólo si $\ker(\varphi) = \{e_1\}$.

D. Sea $\varphi : H \to Z_2 \times \mathbb{Z}$ tal que

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = \begin{cases} (\overline{0},\ b) & \text{si } a = 1 \\ (\overline{1}, -b) & \text{si } a = -1 \end{cases}.$$

Probar que φ es un homomorfismo. (La operación en $Z_2 \times \mathbb{Z}$ es coordenada a coordenada). ¿Es φ un isomorfismo?

Ejercicio 2. (10 puntos)

A. Enunciar el Teorema de órdenes para homomorfismos de grupos.

B. Sea G un grupo con 35 elementos. Dar todos los homomorfismos posibles $\varphi : \mathbb{Z}_{33} \to G$.

C. Sea G un grupo tal que $|G| = 34$. Probar que si un homomorfismo $\varphi : G \to \mathbb{Z}_{17}$ no es trivial, entonces su núcleo ($\ker \varphi$) tiene dos elementos.

Ejercicio 3. (15 puntos) Sea $(G, *)$ un grupo y $x, y \in G$ tales que $x * y = y * x$.
Para cada una de las siguientes afirmaciones, decidir si es verdadera o falsa y justificar la respuesta. En caso de ser verdadera dar una prueba, y en caso de ser falsa dar un contraejemplo (decidir si la afirmación es verdadera o falsa sin ninguna justificación carece de valor).

A. Si $o(x)$ y $o(y)$ son finitos, entonces $o(x * y)$ es finito.

B. Si $o(x)$ y $o(y)$ son finitos, entonces $o(x * y) = \text{mcm}(o(x), o(y))$.

C. Si $\text{mcd}(o(x), o(y)) = 1$ entonces $o(x * y) = o(x)o(y)$.

Ejercicio 4. (17 puntos)

A. Probar que en $U(71)$ el orden de $\overline{2}$ es 35.

B. Hallar una raíz primitiva módulo 71.

C. Alicia y Bruno utilizan el método de Diffie-Helmann de intercambio de clave, utilizando el primo $p = 71$ y una raíz primitiva módulo 71. Alicia elige $m = 5$ y Bruno elige $n = 10$. Si Alicia le manda a Bruno $x = 3$, ¿cuál es la clave común?

D. ¿Es posible que con los datos de la parte C. Alicia y Bruno hayan elegido la raíz primitiva obtenida en la parte B?

SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA 2

Nombre	C.I.	No. de prueba .....

Duración: 3:30 horas. Sin material y sin calculadora.
Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

Ejercicio 1.

A. Enuncie (y NO demuestre) el Teorema de Lagrange.

B. Probar que si G es un grupo finito y $g \in G$ entonces $o(g) \mid |G|$.

(*Obs. No se puede utilizar que* $g^{|G|} = e$ *ya que esto es consecuencia de lo que se pide probar; a menos que lo prueben de forma independiente*).

C. Probar que 2 es raíz primitiva módulo 29 y hallar $s \in \{0, 1, \cdots, 27\}$ tal que $9 \equiv 2^s \,(\text{mód } 29)$.

D. Hallar todos los $x \in \mathbb{Z}$ que verifican $x^{18} \equiv 9 \,(\text{mód } 29)$.

Ejercicio 2

A. Enuncie (y NO demuestre) el Primer Teorema de Isomorfismo.

B. Probar que $\dfrac{(\mathbb{R}^*, \cdot)}{\{1, -1\}} \simeq (\mathbb{R}, +)$.

($(\mathbb{R}^*, \cdot)$ *es el grupo* $\mathbb{R} - \{0\} = \mathbb{R} \setminus \{0\}$ *con el producto usual y* $(\mathbb{R}, +)$ *son los reales con la suma usual.*)

C. Sean p y q primos distintos.

i) Probar que si $\overline{z} \in \mathbb{Z}_{p^2}$ es tal que $o(\overline{z}) = p$ entonces $z \equiv kp \,(\text{mód } p^2)$ para algún $k \in \mathbb{Z}$.

(*Recordar que la estructura de grupo de* $\mathbb{Z}_{p^2}$ *es con la suma de clases, y no con el producto*).

ii) Probar que $H = \langle \overline{p} \rangle$ es el único subgrupo de $\mathbb{Z}_{p^2}$ de orden p.

iii) Si $\psi : \mathbb{Z}_{p^2} \to \mathbb{Z}_{pq}$ es un homomorfismo no trivial, hallar $\ker(\psi)$.

Ejercicio 3

A. Sea $\psi : G_1 \to G_2$ un homomorfismo, probar que $o(\psi(g)) \mid o(g)$ para todo $g \in G_1$.

B. Sea S_n el grupo de permutaciones de n elementos. Probar que si $\psi : S_n \to G$ es un homomorfismo que verifica $\psi(\tau) = e_G$ para toda **trasposición** $\tau \in S_n$, entonces ψ es el homomorfismo trivial (es decir, $\psi(\sigma) = e_G$, $\forall \sigma \in S_n$).

C. Probar que si G es un grupo de orden impar entonces no existen homomorfismos $\psi : S_n \to G$ no triviales. (*Sugerencia: utilizar las partes anteriores*).

D. Hallar todos los homomorfismos no triviales $\psi : S_3 \to \mathbb{Z}_4$.

Jueves 24 de Junio de 2010.

SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA II

Nombre	C.I.	No. de prueba .....

Duración: 4 horas.

Ejercicio 1.

A. Sea $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \text{ y } ad - bc = 1 \right\}$. Probar que G con la multiplicación de matrices es un grupo.

B. Fijamos $n \in \mathbb{N}$ y $K = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} : \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n \text{ y } ad - bc \equiv 1 \mod n \right\}$ con la multiplicación de matrices. Sea $\varphi : G \to K$ el homomorfismo dado por $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$.

Hallar $\ker \varphi$, el núcleo de φ. (NOTA: no es necesario probar que K es un grupo ni que φ es un homomorfismo)

C. Enuncie el Primer Teorema de isomorfismos para grupos.

Ejercicio 2. Sea G un grupo finito y H un subgrupo de G.

A. Definimos en G la siguiente relación: si $x, y \in G$, $x \sim y \Leftrightarrow xy^{-1} \in H$. Probar que $\sim$ es una relación de equivalencia en G.

B. Enunciar y probar el Teorema de Lagrange para grupos finitos.

C. Sea K otro grupo finito y $\varphi : G \to K$ un homomorfismo. Probar que si $g \in G$ es tal que $\text{mcd}(o(g), |K|) = 1$, entonces $g \in \ker(\varphi)$.

Ejercicio 3.

A. Sea G un grupo y $g, h \in G$ tales que $gh = hg$ y $\text{mcd}(o(g), o(h)) = 1$.

Probar que $o(gh) = o(g)o(h)$.

B. Sea $G = U(31)$. Calcular $o(5)$ y $o(29)$ y concluir que 21 es raíz primitiva módulo 31.

C. Con Fulano fijamos el primo $p = 31$ y $g = 21$ para el intercambio de clave con el método de Diffie-Hellman. Nosotros elegimos $m = 14$ y Fulano nos envía $x = 7$. Calcular la clave común k.

Ejercicio 4. En este ejercicio se puede utilizar que si $\sigma \in S_n$ entonces $\sigma(a_1, \cdots, a_k)\sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_k))$ (fue probado en el práctico 6). Sea $n \geq 5$ y $a, b, c, d, e \in \{1, 2, 3, \cdots, n\}$ cinco números distintos.

A. (i) Hallar σ_1 y σ_2 en S_n tales que: σ_1 y σ_2 son 3-ciclos, $\sigma_1(a) = b$, $\sigma_2(d) = a$ y $\sigma_2\sigma_1 = (a\,b)(c\,d)$.

(ii) Probar que si N es un subgrupo de A_n que contiene a todos los 3-ciclos, entonces $N = A_n$.

B. Sea N tal que $N \subset A_5$, $N \triangleleft S_5$ y $\sigma = (a\,b\,c) \in N$. Probar que $N = A_5$.

C. (i) Hallar $\tau \in S_n$ tal que $(a\,b\,c\,d\,e)\tau = (a\,d\,b)$.

(ii) Hallar $\gamma \in S_n$ tal que $(a\,b)(c\,d)\gamma = (a\,b\,e)$.

D. Probar que si $\{e\} \neq N \subset A_5$ y $N \triangleleft S_5$, entonces $N = A_5$. (*Sugerencia: Probar que necesariamente N contiene un 3-ciclo*).