

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

SOLUCIÓN DEL SEGUNDO PARCIAL (CUARTA PRUEBA)
29 DE NOVIEMBRE DE 2018
DURACIÓN: 3 HORAS

Ejercicio 1. (14 puntos)

- a. Probar que, dado un entero $n \geq 2$ y $g \in U(n)$ si para todo $d \neq \varphi(n)$ tal que $d| \varphi(n)$, se tiene que $g^d \not\equiv 1 \pmod{n}$ entonces g es una raíz primitiva módulo n .

Solución: El elemento g es raíz primitiva en $U(n)$, por definición, si $g^{\varphi(n)} \equiv 1 \pmod{n}$ y $g^t \not\equiv 1 \pmod{n}$ para todo $t < \varphi(n)$. Asumamos que $o(g) = \alpha$, entonces, sabemos que α divide a todo natural s tal que $g^s \equiv 1 \pmod{n}$ (Proposición 3.7.8, ítem 4, página 54 de las notas de Teórico). En particular α debiera dividir a $\varphi(n)$. Pero, usando la hipótesis del ejercicio, la única chance para que esto suceda es que $\alpha = \varphi(n)$, lo que queríamos demostrar.

- b. Probar que $g = 2$ es raíz primitiva en $U(67)$.

Solución: Sabemos por Fermat o Euler que $2^{66} \equiv 1 \pmod{67}$, pues $\varphi(67) = 66$.

Consideremos el grupo generado por 2:

$\langle 2 \rangle = \{2, 4, 8, 16, 32, -3, -6, -12, -24, 19, 38, 9, 18, 36, 5, 10, 20, 40, 13, 26, 52, 37, 7, 14, 28, 56, 45, 23, 46, 25, 50, 33, 66 = -1, \dots\}$.

Vemos que:

- $2^2 = 4 \pmod{67}$;
- $2^3 = 8 \pmod{67}$;
- $2^6 = 64 \equiv -3 \pmod{67}$;
- $2^{11} = 38 \pmod{67}$;
- $2^{22} = 37 \pmod{67}$;
- $2^{33} = 66 \equiv -1 \pmod{67}$.

Luego, por la parte anterior podemos deducir que 2 es raíz primitiva de $U(67)$.

Observación: utilizamos en esta solución el cálculo hecho previamente y el resultado de la parte anterior. Sin embargo puede reducirse el análisis, usando los resultados dados en clase (teórico y/o práctico), considerando solamente los exponentes 2^6 , 2^{22} y 2^{33} .

- c. Describir el método de Diffie-Hellman.

Solución: Supongamos que Ana y Bernardo quieren ponerse de acuerdo en una clave común que sea secreto (o sea que solo ellos conozcan la clave). Pero ellos se encuentran lejos uno del otro y la única forma de comunicarse entre ellos es a través de un canal. El problema es que el canal está interceptado por espías que pueden acceder a la conversación de Ana y Bernardo. Diffie-Hellman nos da un posible método para resolver el problema:

- i) Ana y Bernardo se ponen de acuerdo en un primo p y raíz primitiva g con $1 < g < p$.
- ii) Ana elige un número al azar n .
- iii) Bernardo elige un número al azar m .
- iv) Ana calcula $g^n \pmod{p}$ y se lo manda por el canal.
- v) Bernardo calcula $g^m \pmod{p}$ y se lo manda por el canal.
- vi) La clave común es $c \equiv g^{nm} \pmod{p} \equiv (g^n)^m \pmod{p} \equiv (g^m)^n \pmod{p}$, que tanto Ana como Bernardo pueden calcular.

El espía que accede a la conversación puede conocer p, g, g^n y g^m . Si el espía con esos datos fuese capaz de calcular g^{nm} entonces hemos fallado en el intento de acordar la clave común. La propuesta del método se basa en la dificultad en acceder a n y m conociendo esos datos (o sea la dificultad del cálculo del Logaritmo Discreto).

- d. ■ Calcular $34^{29} \pmod{67}$ por exponenciación rápida.

Solución:

Observemos inicialmente que $1 = 68 = 2 \times 34 \pmod{67}$. O sea $2^{-1} = 34 \pmod{67}$.

Para calcular $34^{29} \pmod{67}$ por exponenciación rápida, vemos, para comenzar, que $29 = 16 + 8 + 4 + 1$.

Así, $34^1 = 34$; y $34^2 = 34 \times 34 = 34 \times (2 \times 17) = (34 \times 2) \times 17 = 1 \times 17 = 17 \pmod{67}$.

Ahora $34^4 = 17 \times 17 \pmod{67} = 100 + 70 + 70 + 49 = 33 + 3 + 3 + 49 = 21 \pmod{67}$.

Un paso más $34^8 = 21 \times 21 \pmod{67} = 21 \times 3 \times 7 = (-4) \times 7 = -28 = 39 \pmod{67}$.

Finalmente $34^{16} = 39 \times 39 \pmod{67} = 39 \times 3 \times 13 = 50 \times 13 \pmod{67} = (-17) \times 13 = -(100 + 70 + 30 + 21) = -(33 + 3 + 51) \pmod{67} = 20 \pmod{67} = 47 \pmod{67}$.

Luego queremos calcular $34^{29} = 34^{16} \times 34^8 \times 34^4 \times 34^1 = 47 \times 39 \times 21 \times 34 \pmod{67}$, por lo calculado antes.

Mas $47 \times 39 \times 21 \times 34 \pmod{67} = (-20) \times (-28) \times 21 \times 34 \pmod{67} = 20 \times 28 \times 21 \times 34 \pmod{67} = 10 \times 28 \times 21 \pmod{67}$ porque $2^{-1} = 34 \pmod{67}$.

Ahora $10 \times 28 \times 21 \pmod{67} = (10 \times 7) \times (4 \times 21) \pmod{67} = 3 \times 17 \pmod{67} = 51 \pmod{67}$.

Entonces $34^{29} = 51 \pmod{67}$.

- Calcular la clave en común que generan Ana y Bernardo, si toman $p = 67$ (como primo), $g = 2$ (como raíz primitiva), y $m = 29$, $n = 65$ (como parámetros de exponenciación).

Solución: La clave común, hechas las partes anteriores, se calcula directamente. Queremos calcular $(2^{65})^{29} \pmod{67}$. Pero $2^{66} = 1 \pmod{67}$, entonces $2^{65} = 2^{-1} \pmod{67} = 34 \pmod{67}$.

Concluimos que $(2^{65})^{29} \pmod{67} = 34^{29} \pmod{67} = 51 \pmod{67}$, por lo visto en la parte anterior.

Ejercicio 2. (13 puntos)

En $U(41)$,

- a. Probar que $o(3) = 8$ y hallar los elementos de $H = \langle 3 \rangle$.

Solución: El cardinal de $U(41)$ es 40 pues $\varphi(41) = 40$, ya que 41 es primo. El subgrupo generado por 3 es: $H = \langle 3 \rangle = \{3, 9, 27, 40 = -1, 38, 32, 14, 1\}$. En particular $o(3) = 8$.

(Recordar para lo que sigue que si $y \notin H$ entonces $o(y) \nmid 8$.)

- b. Elegir un $y \notin H$. Verificar que $y^8 \neq 1 \pmod{41}$ y hallar $o(y)$.

Solución: Podemos tomar $y = 2$, tenemos:

$$\langle 2 \rangle = \{2, 4, 8, 16, 32, 23, 5, 10, 20, -1, -2, -4, -8, -16, -32, -23, -5, -10, -20, 1\}.$$

Así $o(y) = o(2) = 20$, en particular $2^8 \neq 1 \pmod{41}$.

- c. Hallar $g = 3^r y^s$ una raíz primitiva módulo 41.

Solución: Como $o(2) = 20$, entonces $o(4) = 10$ y $o(16) = 5$. Luego tenemos los elementos 3 y 16, con $o(3) = 8$ y $o(16) = 5$, y $\text{mcd}(5, 8) = 1$. Luego, si consideramos $2^4 \cdot 3 = 7 \pmod{41}$, o sea $o(7) = 40$ raíz primitiva de $U(41)$.

Ejercicio 3. (18 puntos) Sean $f : G_1 \rightarrow G_2$ y $g : G_2 \rightarrow G_3$ morfismos de grupos.

- a. ■ Probar que $g \circ f$ es morfismo de grupos.

Solución: Asumamos las notaciones $(G_1, *_1)$, $(G_2, *_2)$, $(G_3, *_3)$ para cada uno de los grupos. Para probar que $g \circ f$ es morfismo de grupos, tenemos que probar que para todo $x, y \in G_1$, $g \circ f(x *_1 y) = g \circ f(x) *_3 g \circ f(y)$. Pero $g \circ f(x *_1 y) = g(f(x *_1 y)) = g(f(x) *_2 f(y))$ pues f es morfismo de grupos. Luego $g(f(x) *_2 f(y)) = g(f(x)) *_3 g(f(y)) = g \circ f(x) *_3 g \circ f(y)$ pues g es morfismo de grupos.

- ¿Qué relación tienen $\text{Im}(g \circ f)$ e $\text{Im}(g)$? Justificar.

Solución: Vale que $\text{Im}(g \circ f) \subseteq \text{Im}(g)$, pues $\text{Im}(f) = f(G_1) \subseteq G_2$, luego $\text{Im}(g \circ f) = g(f(G_1)) \subseteq g(G_2) = \text{Im}(g)$. Como la imagen de un morfismo es un subgrupo del codominio, entonces $\text{Im}(g \circ f) < \text{Im}(g)$, o sea $\text{Im}(g \circ f)$ es un subgrupo de $\text{Im}(g)$.

Supongamos que $|G_1| = m$, $|G_2| = n$ y $|G_3| = r$, con $m, n, r \in \mathbb{N}$.

- b. ■ Probar que $|\text{Im}(f)|$ divide a $\text{mcd}(m, n)$.

Solución: Como $\text{Im}(f)$ es un subgrupo de G_2 entonces, por Lagrange, $|\text{Im}(f)|$ divide a $|G_2| = n$. Por otro lado, el Teorema de órdenes (3.9.8), nos dice que $|\text{Ker}(f)| \times |\text{Im}(f)| = |G_1|$. En particular $|\text{Im}(f)|$ divide a $|G_1| = m$. Luego $|\text{Im}(f)|$ divide a m y n , por lo que $|\text{Im}(f)|$ divide al $\text{mcd}(m, n)$ (Corolario 1.2.9).

- Probar que $|\text{Im}(g \circ f)|$ divide a $\text{mcd}(m, n, r)$.

Solución: Por lo visto antes $|\text{Im}(g \circ f)|$ divide al orden del dominio y del codominio. O sea $|\text{Im}(g \circ f)|$ divide a m y r . Por otro lado $\text{Im}(g \circ f) = \text{Im}(g|_{\text{Im}(f)})$, es decir el conjunto imagen de la composición coincide con la imagen del morfismo g restringiendo el dominio a la $\text{Im}(f)$. En particular, usando nuevamente el Teorema de órdenes, $|\text{Im}(g|_{\text{Im}(f)})|$ divide a $|\text{Im}(f)|$ que a su vez, al ser un subgrupo de G_2 divide a $|G_2| = n$. Luego $|\text{Im}(g \circ f)|$ divide a m , n , y r . Por lo tanto $|\text{Im}(g \circ f)|$ divide a $\text{mcd}(m, n, r)$.

- c. Resolver (encontrar todas las soluciones) en $U(29)$ de la ecuación $x^2 - 1 = 0$. ¿Qué orden tienen las soluciones halladas?

Solución: $x^2 - 1 = 0 \pmod{29} \Leftrightarrow x^2 = 1 \pmod{29} \Leftrightarrow (x - 1)(x + 1)$ es múltiplo de 29. Pero 29 es primo, por lo que 29 divide a $x - 1$ o 29 divide a $x + 1$, con $x \in 0, \dots, 28$. Entonces $x = 1$ o $x = 28 = -1 \pmod{29}$. Entonces las soluciones son $x = 1$; y $x = 28 = -1 \pmod{29}$.

- d. Sean $G_1 = D_7$, el grupo dihedral de orden 14, $G_2 = S_5$ el grupo de permutaciones de 5 elementos, $G_3 = \mathbb{Z}_{15}$, y $G_4 = U(29)$.

- Hallar todos los morfismos de dominio G_1 y codominio G_3 que factorizan por G_2 .

Solución: Observemos que $|G_1| = |D_7| = 14$ y $|G_3| = |\mathbb{Z}_{15}| = 15$. Como $\text{mcd}(14, 15) = 1$, entonces el único morfismo posible es $f : D_7 \rightarrow \mathbb{Z}_{15}$ tal que $f(x) = 0$, para todo $x \in D_7$. Lo anterior se argumenta en el hecho que la única posibilidad es $|\text{Im}(f)| = 1$, si f es morfismo con dominio D_7 y codominio \mathbb{Z}_{15} , y el neutro del grupo codominio ha de estar siempre en la $\text{Im}(f)$ para todo morfismo f , pues $\text{Im}(f)$ es un subgrupo.

Evidentemente el morfismo trivial $f : D_7 \rightarrow \mathbb{Z}_{15}$ tal que $f(x) = 0$, para todo $x \in D_7$, factoriza por S_5 :

$$D_7 \rightarrow S_5 \rightarrow \mathbb{Z}_{15}$$

tal que:

$$x \rightsquigarrow id_{S_5}; \quad y \rightsquigarrow 0,$$

para todo $x \in D_7$ y para todo $y \in S_5$, siendo id_{S_5} la permutación identidad de S_5 .

- Hallar todos los morfismos de dominio G_1 y codominio G_4 que factorizan por G_2 .

Solución: Observemos que $G_1 = D_7$ y $G_4 = U(29)$ con $|D_7| = 14$ y $|U(29)| = \varphi(29) = 28$, pues 29 es primo. A su vez buscamos morfismos que factorizan por $G_2 = S_5$, con

$|S_5| = 5! = 120$. Por la parte b. de este ejercicio, todo morfismo f con dominio D_7 y codominio $U(29)$ que factorice por S_5 verifica que $|Im(f)|$ divide a $\text{mcd}(14, 120, 28) = 2$. Luego $|Im(f)| = 1$ o $|Im(f)| = 2$. En el primer caso, f es el morfismo trivial $f : D_7 \rightarrow \mathbb{Z}_{15}$ tal que $f(x) = 0$, para todo $x \in D_7$, que factoriza por S_5 como vimos arriba.

Nos queda analizar el caso $|Im(f)| = 2$, que ha de factorizar por S_5 , o sea $f = h \circ g$, con $g : D_7 \rightarrow S_5$, y $h : S_5 \rightarrow U(29)$. Como $\text{mcd}(14, 120) = 2$, haciendo el mismo tipo de análisis que arriba, $|Im(g)| = 1$ o $|Im(g)| = 2$.

En el primer caso, g es el morfismo trivial, o sea, $g : D_7 \rightarrow S_5$ tal que $g(x) = id$, para todo $x \in D_7$. En ese caso, como todo morfismo de grupos tiene que llevar el neutro en el neutro, $f = h \circ g$ es necesariamente el morfismo trivial.

Por último consideremos el caso $|Im(g)| = 2$, verificando si es posible y cuándo es posible. Tenemos que $D_7 = \{id_{D_7}, r, r^2, r^3, r^4, r^5, r^6, s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}$, siendo r la rotación de ángulo $\frac{2\pi}{7}$, y s es una de las simetrías. Sabemos que D_7 tiene un subgrupo $\langle r \rangle = \{id_{D_7}, r, r^2, r^3, r^4, r^5, r^6\}$ donde todos los elementos tienen orden 7, excepto la identidad. Luego $g(r) = id_{S_5}$ forzosamente. Si $g(s) = id_{S_5}$, entonces g queda definido como el morfismo trivial. Por ende queda solo el caso en que $g(s)$ no es la identidad. Como $o(s) = 2$ y estamos considerando el caso en que $g(s)$ no es la identidad, entonces $o(g(s))$ solo puede ser 2, es decir $g(s) = (jk)$ una trasposición de dos elementos diferentes, j, k . Así g queda definida como: $g : D_7 \rightarrow S_5$ tal que $g(r^i) = id_{S_5}$, para todo $i = 0, \dots, 6$, y $g(s) = (ij)$ con lo cual $g(sr^i) = (jk)$ para todo $i = 0, 1, \dots, 6$.

Como vimos en la parte c. de este Ejercicio solo hay dos elementos de orden 2 en $U(29)$, y si no queremos que el morfismo h sea trivial (implicaría que $f = h \circ g$ sea trivial), no podemos tomar $h((jk)) = 1$.

Luego consideramos $h : S_5 \rightarrow U(29)$ tal que $h(\sigma) = 1$ para todo σ permutación de orden par y $h((jk)) = 28$. Luego $h(\nu)$, con ν de orden impar, la definimos así: $h(\nu \circ (jk)) = 1$, pues $\nu \circ (jk)$ es par, luego como queremos que sea morfismo, $1 = h(\nu \circ (jk)) = h(\nu) \cdot h((jk)) = 1 \cdot 28 = 28$.

Luego f queda definida como la composición de ambas: $f : D_7 \rightarrow U(29)$ tal que $f(r^i) = 1$, para todo $i = 0, \dots, 6$, y $f(sr^i) = 28$ para todo $i = 0, \dots, 6$.

Aunque hemos construido los mapas h, g y f para que sean morfismos, dejamos como tarea del lector revisar que esas definiciones determinan morfismos de grupos. Es el único morfismo posible no trivial. Hemos encontrado todos los morfismos que pedía el ejercicio.