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

Segundo parcial - 27 de junio de 2019. Duración: 3:30 horas

N° de parcial	Apellido y Nombre	Cédula

Ejercicio 1.

a. Probar que 98 es raíz primitiva módulo 101.

b. ¿Existen elementos de orden 25 en U(101)? En caso afirmativo encontrar alguno y decir cúantos hay. Justificar las afirmaciones que se den.

c. Alicia y Beatriz quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello acuerdan públicamente el uso del primo $p = 101$ y el número $g = 98$ como raíz primitiva. Alicia le envía el número 11 a Beatriz. Beatriz elige en secreto $m = 31$ y le envía el número 83 a Alicia.
¿Cuál es la clave común k acordada?

Solución:

a. Primero vemos que $\varphi(101) = 100 = 2^2 5^2$ por lo que tenemos que probar:

$$\begin{cases} 98^{\frac{100}{2}} \not\equiv 1 \pmod{101} \equiv 98^{50} \pmod{101} \\ 98^{\frac{100}{5}} \not\equiv 1 \pmod{101} \equiv 98^{20} \pmod{101} \end{cases}$$

Observamos que $98 \equiv -3 \pmod{101}$, y utilizamos el método de exponenciación rápida para -3.

k	$(-3)^{2^k} \pmod{101}$
0	-3
1	9
2	$81 \equiv -20 \pmod{101}$
3	$400 \equiv -4 \pmod{101}$
4	16
5	$256 \equiv 54 \pmod{101}$.

Entonces $98^{20} = 98^{2^4} \cdot 98^{2^2} \equiv 16 \cdot -20 \pmod{101} \equiv -320 \pmod{101} \equiv -17 \pmod{101} \not\equiv 1 \pmod{101}$. Y $98^{50} = 98^{2^5} \cdot 98^{2^4} \cdot 98^{2^1} \equiv 54 \cdot 16 \pmod{101} \equiv 7776 \pmod{101} \equiv 100 \pmod{101} \not\equiv 1 \pmod{101}$. Concluimos que 98 es una raíz primitiva módulo p.

b. Como 98 es raíz primitiva módulo 101 sabemos que tiene orden 100, podemos utilizar la fórmula $\mathrm{o}(g^k) = \frac{\mathrm{o}(g)}{\mathrm{mcd}(\mathrm{o}(g),k)}$ para $g = \overline{98}$ en U(101) y vemos que $25 = \mathrm{o}(98^k) = \frac{100}{\mathrm{mcd}(100,k)}$, por lo que $\mathrm{mcd}(100, k) = 4$. Tomando $k = 4$ vemos que $\overline{98}^4 = \overline{81}$ tiene orden 25. Para ver cúantos hay vemos que los posibles k módulo 100 son $\{1 \leq k \leq 100 : \mathrm{mcd}(k, 100) = 4\} = \{1 \leq k \leq 100 : k = 4k',\ \mathrm{mcd}(k', 25) = 1\} = \{4, 8, 12, 16, 24, 28, 32, 36, 44, 48, 52, 56, 62, 66, 74, 78, 82, 86, 92, 96\}$ por lo que hay 20 elementos de orden 25.

c. Tenemos que calcular $11^{31} \pmod{101}$. Utilizamos exponenciación rápida para 11

k	$11^{2^k} \pmod{101}$
0	11
1	$121 \equiv 20 \pmod{101}$
2	$400 \equiv -4 \pmod{101}$
3	16
4	$256 \equiv 54 \pmod{101}$.

Y, $11^{31} = 11^{16} 11^8 11^4 11^2 11^1 \equiv 11 \cdot 20 \cdot -4 \cdot 16 \cdot 54 \pmod{101} \equiv 18 \cdot -4 \cdot 16 \cdot 54 \pmod{101} \equiv 29 \cdot 16 \cdot 54 \pmod{101} \equiv 60 \cdot 54 \pmod{101} \equiv 8 \pmod{101}$.

Ejercicio 2. Sean G un grupo y dos elementos g, $h \in G$ de orden finito.

a. Probar que si $g^n = e$ entonces $\mathrm{o}(g) \mid n$.

b. Probar que $|\langle g \rangle| = \mathrm{o}(g)$.

c. Probar que si $gh = hg$ y $\mathrm{mcd}(\mathrm{o}(g), \mathrm{o}(h)) = 1$, entonces $\mathrm{o}(gh) = \mathrm{o}(g)\mathrm{o}(h)$.

Si utilizan alguna propiedad de ordenes deben probarla.
Solución: Ver notas teóricas.

Ejercicio 3. Sean $(G, \cdot)$ y $(K, \times)$ dos grupos y $f : G \to K$ un homomorfismo.

a. Si e_G y e_K son los neutros de G y K respectivamente, probar que $f(e_G) = e_K$.

b. Probar que $\mathrm{Im}(f)$ es un subgrupo de K.

c. Probar que si G y K son finitos y $\mathrm{mcd}(|G|, |K|) = 1$, entonces f es el homomorfismo trivial.

Solución:

a. Primero vemos que $f(e_G) = f(e_G \cdot e_G) = f(e_G) \times f(e_G)$, y utilizando la propiedad cancelativa de K tiene que pasar que $f(e_G) = e_K$.

b. Por definición tenemos que $\mathrm{Im}(f) = \{f(g) : g \in G\} \subset K$. Veamos que cumple las tres propiedades de subgrupo.

- Por la parte anterior $e_K = f(e_G) \in \mathrm{Im}(f)$.
- Si $f(g), f(g') \in \mathrm{Im}(f)$ entonces, como f es homomorfismo tenemos que $f(g) \times f(g') = f(g \cdot g') \in \mathrm{Im}(f)$
- Falta ver que si $f(g) \in \mathrm{Im}(f)$ entonces $f(g)^{-1} \in \mathrm{Im}(f)$. Esto se prueba viendo que $f(g) \times f(g^{-1}) = f(g \cdot g') = f(e_G) = e_K$, y por lo tanto $f(g)^{-1} = f(g^{-1}) \in \mathrm{Im}(f)$.

c. Si $g \in G$, tenemos que $\mathrm{o}(f(g)) \mid \mathrm{o}(g) \mid |G|$ y por otro lado tenemos que $\mathrm{o}(f(g)) \mid |\mathrm{Im}(f)| \mid |K|$. Por lo tanto, $\mathrm{o}(f(g)) \mid \mathrm{mcd}(|G|, |K|) = 1$, y concluimos que $o(f(g)) = 1$, por lo tanto $f(g) = e_K$ para todo $g \in G$.

Ejercicio 4. Para los siguientes grupos G, K, determinar si existen homomorfismos $f : G \to K$ no triviales. En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

a. Para un primo impar p, $G = \mathbb{Z}_p$ el grupo de enteros módulo p y $K = S_{p-1}$ el grupo de permutaciones de $p - 1$ elementos.

b. $G = \mathbb{Z}_{100}$ el grupo de enteros módulo 100, y $K = \mathrm{U}(101)$ el grupo de invertibles módulo 101.

c. $G = U(12)$ el grupo de invertibles módulo 12 y $\mathbb{Z}_4$ el grupo de enteros módulo 4.

Solución:

a. Vemos $|G| = p$ y $|K| = (p - 1)!$, que son coprimos. Por lo tanto el único homomorfismo es el trivial.

b. Sabemos G es cíclico de orden 100 con generador $\overline{1}$. Por el teorema de la raíz primitiva sabemos que $\mathrm{U}(101)$ es cíclico. Sea $g \in \mathrm{U}(101)$ un generador. Por lo visto en las notas teóricas, el morfismo $f(n \cdot \overline{1}) = f(\overline{n}) = g^n$ está bien definido y es un morfismo. Es más, f es un isomorfismo.

c. Veamos como es G, $\mathrm{U}(12) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Los elementos $\overline{5}, \overline{7}, \overline{11}$ tienen orden 2 y $\overline{5} \cdot \overline{7} = \overline{11}$, sabemos que $\mathrm{o}(f(g)) \mid \mathrm{o}(g)$ para $g \in G$ y K tiene un solo elemento de orden 2 que es $\overline{2}$, puedo definir el morfismo $f(\overline{1}) = \overline{0}, f(\overline{5}) = \overline{2}, f(\overline{7}) = \overline{0}, f(\overline{11}) = \overline{2}$.