Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería
Instituto de Matemática y Estadística

EXAMEN - 31 JULIO 2024 - DURACIÓN: 3 HORAS.

Número de examen	Cédula	Nombre y Apellido

Las respuestas deben estar correctamente argumentadas. Se debe incluir el razonamiento utilizado para obtener cada resultado.

1. (a) Definir la función φ de Euler y enunciar el Teorema de Euler.
   (b) Probar que $\varphi(mn) = \varphi(m)\varphi(n)$ si m y n son coprimos.
   (c) Calcular los dos últimos dígitos de 7^{42}.

2. (a) Describir el método RSA, incluyendo su función de cifrado y descifrado.
   (b) Supongamos que nuestra clave pública es (n, e), con $n = 11 \times 83$, y $e = 267$. Hallar el valor de los parámetros de nuestra función de descifrado.
   (c) Sea $n = p \times q$, con p y q primos distintos desconocidos.
      i. Explicar cómo hallar p y q de forma eficiente, conociendo el valor de n y $\varphi(n)$.
      ii. Factorizar $n = 2059$, sabiendo que $\varphi(n) = 1960$. Puede ser útil saber que $\sqrt{1764} = 42$.

3. Sean G un grupo y H un subgrupo de G.
   (a) Definir subgrupo normal.
   (b) Probar que si H es un subgrupo normal en G, entonces las clases laterales a izquierda forman un grupo.
   (c) Enunciar el Primer Teorema de Isomorfismo.
   (d) Sea $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Probar que $S^1 \cong \mathbb{R}/\mathbb{Z}$.

Solución

Problema 1

(a) Ver Definición 2.6.1. de las notas del curso.

(b) Ver Teorema 2.6.3. de las notas del curso.

(c) Tenemos que calcular $7^{42} \pmod{100}$. Para esto podemos aplicar el Teorema de Euler, debido a que 7 es coprimo con 100.

- Calculamos primero $\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = (4-2)(25-5) = 40$.
- Entonces, por el Teorema de Euler: $7^{40} \equiv 1 \pmod{100}$.
- Por lo tanto: $7^{42} = 7^{40}7^2 \equiv 7^2 \pmod{100} = 49 \pmod{100}$.

Problema 2

(a) *Describir el método RSA, incluyendo su función de cifrado y descifrado.*

Supongamos que Ana y Bob desean intercambiar un mensaje mediante RSA. Ana publica su clave pública, formada por un par de enteros (n, e). La clave privada de Ana son dos primos p y q distintos, tales que: $n = p \times q$. Esta clave no es compartida.

Supongamos que Bob desea enviar un mensaje a Ana, cifrado mediante RSA. Bob debe cifrar el mensaje $x \in \mathbb{Z}$ con la clave de Ana, mediante la función de cifrado: $E(x) \equiv x^e \pmod{n}$.

Cuando Ana recibe el mensaje cifrado $y = E(x)$, lo descifra mediante su función de descifrado: $D(y) \equiv y^d \pmod{n}$; donde d es tal que: $de \equiv 1 \pmod{\varphi(n)}$. Para que exista d, es necesario que e y $\varphi(n)$ sean coprimos.

La seguridad del método radica en que calcular $\varphi(n)$ es tan difícil como factorizar n en primos.

(b) *Supongamos que nuestra clave pública es (n, e), con $n = 11 \times 83$, y $e = 267$. Hallar el valor de los parámetros de nuestra función de descifrado.*

La función de descifrado es $D(y) \equiv y^d \pmod{n}$. Los parámetros son $n = 913$, y el exponente d, tal que: $d \times 267 \equiv 1 \pmod{\varphi(913)}$. Sabemos que $913 = 11 \times 83$, con 11 y 83 primos. Por lo tanto $\varphi(913) = \varphi(11)\varphi(83) = 10 \times 82 = 820$. Entonces buscamos d tal que:

$$d \times 267 \equiv 1 \pmod{820} \Leftrightarrow 267 \times d - 820 \times m = 1, \quad d, m \in \mathbb{Z}.$$

Para hallar una solución de esta ecuación diofántica, vamos a usar el algoritmo de Euclides extendido. Las divisiones necesarias son:

$$820 = 3 \times 267 + 19, \quad 267 = 14 \times 19 + 1.$$

Esto nos dice que: $mcd(820, 267) = mcd(267, 19) = mcd(19, 1) = 1$; por lo que la ecuación tiene solución. Despejando el resto de la segunda división: $19 = 820 - 3 \times 267$, y reemplazando en la primera división, se obtiene:

$$1 = 267 - 14 \times 19 = 267 - 14 \times (820 - 3 \times 267) = 43 \times 267 - 14 \times 820.$$

Por lo tanto: $d \equiv 43 \pmod{820}$.

(c) *Sea $n = p \times q$, con p y q primos distintos desconocidos.*

i. *Explicar cómo hallar p y q de forma eficiente, conociendo el valor de n y $\varphi(n)$.*
Como p y q son primos, sabemos que: $\varphi(n) = \varphi(p) \times \varphi(q) = (p-1)(q-1)$. Por otro lado, sabemos que $n = p \times q$. Esto da un sistema de dos ecuaciones con incógnitas p y q:

$$\begin{cases} (p-1) \times (q-1) = \varphi(n) \\ p \times q = n \end{cases}.$$

De la segunda ecuación: $p = \frac{n}{q}$. Reemplazando en la primera ecuación:

$$\left(\frac{n}{q} - 1\right) \times (q-1) = \varphi(n) \Leftrightarrow nq - q^2 - n + q = q\varphi(n) \Leftrightarrow q^2 + (\varphi(n) - n - 1)q + n = 0.$$

Esta es una ecuación cuadrática en q, que se puede resolver usando Bhaskara.

ii. *Factorizar $n = 2059$, sabiendo que $\varphi(n) = 1960$. Puede ser útil saber que $\sqrt{1764} = 42$.*
La ecuación cuadrática en q es: $q^2 - 100q + 2059 = 0$. Usando Bhaskara:

$$q = \frac{100 \pm \sqrt{100^2 - 4 \times 2059}}{2} = \frac{100 \pm \sqrt{10000 - 8236}}{2} = \frac{100 \pm \sqrt{1764}}{2} = \frac{100 \pm 42}{2}.$$

Las soluciones son: $q_1 = 29$ y $q_2 = 71$. Ambos valores son primos. Los respectivos valores de $p = \frac{n}{q}$, son: $p_1 = \frac{2059}{29} = 71$ y $p_2 = \frac{2059}{71} = 29$.

Problema 3

(a) Ver notas de teórico sobre subgrupos normales y grupo cociente.

(b) Ver notas de teórico.

(c) Ver notas de teórico.

(d) Sea $f : \mathbb{R} \to \mathbb{C}^*$, tal que: $f(x) = e^{2\pi i x} = \cos(2\pi i x) + i \sin(2\pi i x)$. Entonces:

- f es un homomorfismo de grupos, pues:

$$f(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y} = f(x)f(y), \ \forall \ x, y \in \mathbb{R}.$$

- Veamos que $\ker(f) = \mathbb{Z}$. En efecto:

$$f(x) = 1 \Leftrightarrow \cos(2\pi x) + i\sin(2\pi x) = 1 + i0 \Leftrightarrow \cos(2\pi ix) = 1,\ \sin(2\pi ix) = 0 \Leftrightarrow x \in \mathbb{Z}.$$

- Veamos que $Im(f) = S^1$. Para esto vamos a probar la doble inclusión de conjuntos.
  i. Sea $y \in Im(f)$. Es decir: $y = f(x)$, para algún $x \in \mathbb{R}$. Se cumple:

$$|y| = |f(x)| = \cos(2\pi x)^2 + \sin(2\pi x)^2 = 1.$$

  Esto prueba que $y \in S^1$. Por lo tanto: $Im(f) \subseteq S^1$.
  ii. Por otro lado, dado $z \in \mathbb{C}^*$, lo podemos expresar en polares como: $z = re^{i\theta}$. Si asumimos que $z \in S^1$, entonces $r = 1$ y $z = e^{i\theta} = e^{2\pi i\frac{\theta}{2\pi}}$. Esto prueba que $z = f\left(\frac{\theta}{2\pi}\right)$; por lo que $z \in Im(f)$. Por lo tanto: $S^1 \subseteq Im(f)$.
- Usando el Primer Teorema de Isomorfismo, con la función f definida anteriormente, se obtiene el isomorfismo buscado:

$$Im(f) = S^1 \cong \mathbb{R}/ker(f) = \mathbb{R}/\mathbb{Z}.$$