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

EXAMEN - 7 DE FEBRERO DE 2019. DURACIÓN: 210 MINUTOS

**Ejercicio 1.**

**a**. Sean $(G, *, e)$ un grupo y sea $g \in G$. Definir orden de $g$ en $G$ (que se anota $o(g)$ o bien $|g|$), sea finito o infinito.
**Solución**:
Ver la Definición 3.7.6 de las Notas de Teórico. Para facilitar al lector incluimos la definición aquí.

Sea $(G, *, e)$ un grupo y $g \in G$. Definimos el **orden** del elemento $g$ (y lo escribiremos $o(g)$) de la siguiente manera:

- si $g^n \neq e$ para todo $n \in \mathbb{Z}^+$, decimos que $o(g) = \infty$;
- en caso contrario, definimos $o(g) = \min\{n \in \mathbb{Z}^+ : g^n = e\}$.

**b**. Dados un grupo finito $(G, *)$, y elementos $x, y \in G$, tales que $xy = yx$, con $o(x) = a$, $o(y) = b$, m=mcm$(a, b)$ y d=mcd$(a, b)$, entonces, probar que $o(xy)|m$, y que $\frac{m}{d}|o(xy)$.
**Solución**:
Recordar que $a \times b = m \times d$, según Proposición 1.2.15 de las Notas de Teórico. Luego, si $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$, entonces $m = a' \times b = a \times b'$, recordando que $\text{mcd}(a', b') = 1$.
Por lo tanto $(xy)^m = x^m \times y^m = x^{a \times b'} \times y^{a' \times b} = (x^a)^{b'} \times (y^b)^{a'} = e \times e = e$, donde la primer igualdad se basa en que $x$ e $y$ conmutan. Por lo tanto $(xy)^m = e$, con lo cual $o(xy)$ divide a $m$, obteniendo así lo primero que se pedía.

Ahora probaremos que $\frac{m}{d}$ divide al orden de $xy$:
Sea $s = o(xy)$, entonces $x^s \times y^s = (xy)^s = e$, donde la primer igualdad se basa en que $x$ e $y$ conmutan. Luego $e = (xy)^{sb} = x^{sb} \times (y^b)^s = x^{sb}$, pues $b = o(y)$, con lo cual $x^{sb} = e$. Entonces $o(x) = a|sb$, o sea $d \times a'|s \times d \times b'$, por lo tanto $a'|b's$. Como recordamos antes $\text{mcd}(a', b') = 1$, con lo cual, por Lema 1.2.10 de las Notas de Teórico, $a'|s$. En resumen, hasta aquí hemos probado que $a'$ divide a $s = o(xy)$, pero haciendo un razonamiento simétrico (elevando $xy$ al exponente $s \times a$) obtendremos que $b'$ divide a $o(xy)$. Concluimos que $a'|o(xy)$, $b'|o(xy)$ y $\text{mcd}(a', b') = 1$, con lo cual $a' \times b' \mid o(xy)$. Pero $a' \times b' = \frac{m}{d}$, con lo cual hemos probado lo solicitado: $\frac{m}{d}| \, o(xy)$.

**c**. Considerar el grupo U(19) (también se usa la notación $\text{U}(19) = \mathbb{Z}_{19}^*$) y calcular el orden de 4, 18 y $4 \times 18$, usando la parte anterior.
**Solución**:
Es fácil calcular $4^i$ en U(19), para $i = 1, 2, ...$:
$4^0 = 1$, $4^1 = 4$, $4^2 = 16 = -3$, $4^3 = -12 = 7$, $4^4 = 9$, $4^5 = -2$, $4^6 = -8$, $4^7 = 6$, $4^8 = 5$, $4^9 = 1$ , con lo cual $o(4) = 9$ en U(19) (recordar que $|\text{U}(19)| = \varphi(19) = 18$).
Por otro lado $18 = -1$ en U(19), con lo cual $o(18) = 2$. Luego $\text{mcd}(9, 2) = 1$, y recordando que U(19) es conmutativo, entonces, usando la parte anterior, $o(15) = o(4 \times 18) = \frac{mcm(9,2)}{mcd(9,2)} = 18$. O sea, 15 es raíz primitiva en U(19).

**Ejercicio 2.**

**a**. Definir cuándo dos enteros, $x, y \in \mathbb{Z}$ son congruentes módulo $n \in \mathbb{N}^*$.
Enunciar el Teorema de Euler y el Teorema de Fermat.
**Solución**:
Ver la Definición 2.2.1 de las Notas de Teórico, y los enunciados del Teorema 2.6.5 (Euler) y del Corolario 2.6.6 (Fermat). Adjuntamos aquí, para facilitar la lectura, la definición y ambos enunciados:

Fijado $n \in \mathbb{Z}$, y dados $x, y \in \mathbb{Z}$, decimos que $x$ **es congruente con** $y$ **módulo** $n$ y escribimos

$$x \equiv y \pmod{n}$$

si $n \mid x - y$.
En caso contrario escribiremos

$$x \not\equiv y \pmod{n}.$$

[Teorema de Euler] Sean $n, a \in \mathbb{Z}$ tales que $\text{mcd}(a, n) = 1$, entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

[Teorema de Fermat] Si $p$ es primo y $a \in \mathbb{Z}$ es tal que $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

**b**. Sean $p, a, b$ naturales tales que $p$ es primo, $b \equiv 0$ mód$(p-1)$ y $p$ no divide a $a$. Encontrar (en función de $p$) el menor natural $x$ que satisface las siguientes condiciones:

$$\begin{gathered} a^b x^3 + 8x \equiv 5x^2 + 4 \text{ mód}(p); \\ x \not\equiv 1 \text{ mód}(p); \\ x > p. \end{gathered}$$

(Sug.: Factorizar el polinomio: $g(x) = x^3 - 5x^2 + 8x - 4$).
**Solución**:
Factorizamos primero, como sugiere la letra, al polinomio $g(x)$. Es fácil ver que 1 es raíz de $g(x)$ (la suma de los coeficientes es cero). Luego $g(x) = (x-1)(x-2)^2$.
Por otro lado, como $b \equiv 0$ mód$(p-1)$, existe $t \in \mathbb{Z}$, tal que $b = (p-1) \times t$.

Luego $a^b = (a^{p-1})^t \equiv 1 \pmod{p}$, por Fermat.
Entonces $a^b x^3 + 8x \equiv 5x^2 + 4$ mód$(p) \Leftrightarrow a^b x^3 - 5x^2 + 8x - 4 \equiv 0$ mód$(p) \Leftrightarrow x^3 - 5x^2 + 8x - 4 \equiv 0$ mód$(p) \Leftrightarrow (x-1)(x-2)^2 \equiv 0$ mód$(p)$ por lo probado antes. Esto último es equivalente a que $p \mid (x-1)(x-2)^2$, con $x \in \mathbb{N}$. Como $p$ es primo, es equivalente a que $p \mid x-1$ o $p \mid x-2$. Pero $p$ no puede dividir a $x-1$ pues, por hipótesis, $x \not\equiv 1$ mód$(p)$. Luego la única posibilidad es que $p \mid x-2$, con $x \in \mathbb{N}$, y esto es equivalente a que $x = h \times p + 2$, con $h$ entero no negativo. Como se pide $x > p$, tenemos que $h$ tiene que ser positivo. O sea $x = h \times p + 2$, con $h \geq 1$. El menor natural en esas condiciones es $x = p + 2$.

**c**. Sea $x$ el natural hallado en la parte anterior. Calcular $(x-p)^{10325}$ mód(35).
**Solución**:
Como $x = p + 2$, entonces $(x-p)^{10325}$ mód(35) $= (2)^{10325}$ mód(35). Ahora $\varphi(35) = \varphi(5)\varphi(7) = 4 \times 6 = 24$, y por otro lado $10325 = 430 \times 24 + 5$, con lo cual $(2)^{10325}$ mód(35) $= ((2)^{24})^{430} \times 2^5$ mód(35) $= (2)^5$ mód(35), por el Teorema de Euler. O sea $(2)^{10325} \equiv 32$ mód(35).

**Ejercicio 3.**

**a**. i) Definir raíz primitiva.

ii) Probar que 2 y 22 son raíces primitivas en U(53) (también se usa la notación U(53) $= \mathbb{Z}_{53}^*$).

**Solución**:
La definición aparece en las Notas de Teórico, Definición 4.1.1:
Dado un $n \in \mathbb{Z}^+$, un entero $g \in \{1, \cdots, n\}$ es **raíz primitiva módulo** $n$, si $\langle \overline{g} \rangle = U(n)$.

Para probar que 2 es raíz primitiva en U(53), simplemente calculamos las potencias en base 2.

| **n** | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^n$ | 1 | 2 | 4 | 8 | 16 | 32 | 11 | 22 | 44 | 35 | 17 | 34 | 15 | 30 | 7 | 14 | 28 | 3 | 6 | 12 | 24 | 48 | 43 | 33 | 13 | 26 | $-1$ |

Vemos que $2^i \not\equiv 1$ mód(53), para $i = 4; 26$. Pero $\varphi(53) = 52 = 4 \times 13$. Luego, usando la Proposición 4.1.4 (parte 4) de las Notas de Teórico, concluimos que 2 e raíz primitiva.

A su vez $22 \equiv 2^7$ mód(53) según lo visto en la tabla anterior. Como 2 es raíz primitiva en U(53) y $\text{mcd}(7, 52) = 1$, siendo 52= |U(53)|, tenemos que $2^7 \equiv 22$ mód(53) es también un generador del grupo y por lo tanto raíz primitiva.

**b**. Andrea y Basilio acuerdan comunicarse estableciendo una clave privada mediante el método de Diffie-Hellman. Deciden usar el módulo primo $p = 53$ y como base $g = 22$. Andrea elige el entero $m = 5$, enviándole a Basilio $g^m$ mód(53), mientras que Basilio envía a Andrea $20 \equiv g^n$ mód(53).

i) ¿Cuál es la clave privada que acuerdan Andrea y Basilio?
**Solución**:
Tenemos que calcular $20^5$ mód(53), pues 20 es el valor enviado por Basilio a Andrea (es decir $20 \equiv g^n$ mód(53)) y $m = 5$.
Así $20^5 = 4^5 \times 5^5$ mód(53) $\equiv 100 \times 100 \times 80 \times 4 \equiv 47 \times 47 \times 27 \times 4 \equiv (-6) \times (-6) \times 27 \times 2 \times 2 \equiv 36 \times 1 \times 2 \equiv 72 \equiv 19$ mód(53). O sea la clave acordada es $k = 19$.

ii) ¿Es la clave acordada una raíz primitiva en U(53)? Jusitfique su respuesta.
**Solución**:
Sí, es una raíz primitiva, porque $g = 22$ es raíz primitiva y la clave acordada es $k = (22^7)^5$ y $35 = 7 \times 5$ es coprimo con $52 = 4 \times 13 = |\text{U}(53)|$.

**c**. Andrea le envía a Basilio el siguiente mensaje:

LA GATA GATINA

Y Basilio le responde con un mensaje encriptado utilizando la clave hallada en b. i), y usando el método de cifrado César, con el alfabeto

| 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 |

EGRDMYWRDSMCCS

¿Cuál fue la respuesta de Basilio?
**Solución**:
Recordar el Método César, Sección 5.1.1 de las Notas de Teórico.
Lleva este nombre en honor a Julio César, que lo usaba para comunicarse con sus generales. Como primer paso el método enumera las letras del alfabeto, por ejemplo la letra A tiene asignado el 0, la letra B el 1, ..., la letra Z el 26 y a el espacio le asignamos el número 27. La enumeración se puede ver en la tabla. Luego definimos la clave $k$ como un número entre 0 y 27. Para cifrar un mensaje lo que hacemos es sumarle a cada letra, la clave $k$ y reducir módulo 28. Para descifrar el mensaje debemos restar $k$ a cada letra y reducir módulo 28.

La respuesta de Basilio fue:

NO MUGE MAÚLLA