

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

EXAMEN - 15 DE JULIO DE 2022.

Soluciones.

**Ejercicio 1.**

- a. Enunciar la identidad de Bezout.

*Solución.* En las notas de teórico es el Teorema 1.2.8.

- b. Enunciar y demostrar el Lema de Euclides.

*Solución.* En las notas de teórico es el Lema 1.2.10.

- c. Sean  $a, b, c \in \mathbb{Z}$  y  $n \in \mathbb{Z}^+$ .

Probar que si  $ca \equiv cb \pmod{n}$  y  $\text{mcd}(c, n) = 1$  entonces  $a \equiv b \pmod{n}$ .

*Solución.* En las notas de teórico es la Proposición 2.2.4 parte 1.

- d. Encontrar todos los  $x \in \mathbb{Z}$  tales que

$$\begin{cases} 3x \equiv 18 \pmod{55} \\ 2x \equiv 17 \pmod{75} \end{cases}.$$

*Solución.* Por la parte (c), como  $\text{mcd}(3, 55) = 1$ , tenemos que

$$3x \equiv 18 \pmod{55} \iff x \equiv 6 \pmod{55}.$$

Del mismo modo, como  $\text{mcd}(2, 75) = 1$ ,

$$2x \equiv 17 \pmod{75} \iff x \equiv 46 \pmod{75}.$$

El sistema planteado es entonces equivalente a

$$\begin{cases} x \equiv 6 \pmod{55} \\ x \equiv 46 \pmod{75} \end{cases}.$$

Usando  $55 = 5 \cdot 11$  y  $75 = 25 \cdot 3$  tenemos

$$x \equiv 6 \pmod{55} \iff \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{11} \end{cases}$$

Observar que  $x \equiv 46 \pmod{75} \implies x \equiv 1 \pmod{5}$ , de modo que podemos eliminar la congruencia módulo 5 y concluimos que el sistema es equivalente a

$$\begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 46 \pmod{75} \end{cases}.$$

Ahora como  $\text{mcd}(11, 75) = 1$  el Teorema Chino del resto asegura que este sistema tiene solución única módulo  $11 \cdot 75 = 825$ , que debe cumplir  $x = 46 + 75k \equiv 6 \pmod{11}$ . Reduciendo módulo 11 obtenemos  $40 \equiv 2k \pmod{11}$  y de nuevo la parte (c) implica  $k \equiv 20 \equiv 9 \pmod{11}$ . Entonces  $x \equiv 46 + 75 \cdot 9 \pmod{825}$ , lo que es lo mismo  $x \equiv 721 \pmod{825}$ .

**Ejercicio 2.** Sea  $(G, \cdot)$  un grupo finito.

- a. Dado  $g \in G$  probar que existe  $n > 0$  tal  $g^n = e_G$ .

*Solución.* Como  $G$  es finito, el conjunto  $\{g^i : i \in \mathbb{Z}\}$  también es finito. Entonces debe haber dos potencias de  $g$  iguales, digamos  $g^m = g^k$  con  $m \neq k$ . Supongamos sin pérdida de generalidad que  $m > k$ . Entonces  $g^{m-k} = e_G$  por la propiedad cancelativa y concluimos que  $n = m - k > 0$  satisface  $g^n = e_G$ .

En las notas de teórico la Proposición 3.7.8 parte (6) es el contrareciproco de lo pedido.

- b. Definir el orden de  $g \in G$ , y ver que es finito.

*Solución.* En las notas de teórico es la Definición 3.7.6. Es finito por la parte (a).

Explícitamente

$$o(g) := \min\{n \in \mathbb{Z}^+ : g^n = e\};$$

el mínimo existe por el principio del buen orden, ya que la parte (a) asegura que el conjunto es no vacío.

- c. Definir el subgrupo generado por un elemento  $g \in G$  y probar que es un subgrupo.

*Solución.* En las notas de teórico la definición está justo después de la Proposición 3.7.4, y la demostración de que es un subgrupo sigue inmediatamente de dicha Proposición.

Explícitamente  $\langle g \rangle := \{g^i : i \in \mathbb{Z}\}$ . Para probar que  $\langle g \rangle$  es un subgrupo:

- $e_G = g^0$  de modo que  $e_G \in \langle g \rangle$ .
- Si  $h \in \langle g \rangle$  entonces  $h = g^i$  con  $i \in \mathbb{Z}$  y su inverso es  $h^{-1} = g^{-i} \in \langle g \rangle$ .
- Si  $h_1, h_2 \in \langle g \rangle$  entonces  $h_1 = g^{i_1}, h_2 = g^{i_2}$  con  $i_1, i_2 \in \mathbb{Z}$  y  $h_1 \cdot h_2 = g^{i_1+i_2} \in \langle g \rangle$ .

- d. Probar que  $|\langle g \rangle| = o(g)$ . Puede usar sin demostración el siguiente

**Lema.** Sea  $n = o(g)$ . Entonces  $g^m = g^k$  si y sólo si  $m \equiv k \pmod{n}$ .

*Solución.* En las notas de teórico es la Proposición 3.7.9. El Lema sugerido es la parte (6) de la Proposición 3.7.8.

Explícitamente, por el Lema tenemos que

$$\langle g \rangle = \{g^i : i \in \mathbb{Z}\} = \{g^0, g^1, \dots, g^{n-1}\}$$

tiene  $n$  elementos.

### Ejercicio 3.

- a. Probar que 2 es raíz primitiva módulo 121.

*Solución.* Hay que probar que  $o(2) = \varphi(121) = 110$ . Para esto utilizamos el criterio de la Proposición 4.1.4 (ítem 4). Como los divisores primos de 110 son 2, 5 y 11, alcanza ver que  $2^{55} \not\equiv 1 \pmod{121}$ , que  $2^{22} \not\equiv 1 \pmod{121}$  y que  $2^{10} \not\equiv 1 \pmod{121}$ .

Calculamos módulo 121:

$$\begin{aligned} 2^{10} &\equiv 1024 \equiv 56, \\ 2^{11} &\equiv 2 \cdot 56 \equiv 112 \equiv -9, \\ 2^{22} &\equiv (-9)^2 \equiv 81 \equiv -40, \\ 2^{44} &\equiv (-40)^2 \equiv 1600 \equiv 27, \\ 2^{55} &\equiv -9 \cdot 27 \equiv -243 \equiv -1. \end{aligned}$$

- b. i) ¿Cuántos homomorfismos  $f : U(121) \rightarrow U(11)$  hay?  
ii) ¿Cuántos homomorfismos  $f : U(121) \rightarrow U(13)$  hay?

*Solución.* Como  $U(121)$  es un grupo cíclico de orden 110, podemos usar la la Observación 3.9.10 que nos da una biyección entre los homomorfismos  $f : U(121) \rightarrow K$  y el conjunto  $\{k \in K : o(k) \mid 110\}$ . Aplicamos esto en cada caso:

- i) Cuando  $K = U(11)$ , si  $g$  es una raíz primitiva módulo 11 tenemos  $K = \{g^1, \dots, g^{10}\}$  de ordenes 10, 5, 10, 5, 2, 5, 10, 5, 10, 1 respectivamente (Proposición 3.7.8 parte 7). Todos los elementos tienen orden divisor de 110, por lo tanto hay 10 homomorfismos.
- ii) Cuando  $K = U(13)$ , si  $g$  es una raíz primitiva módulo 13 tenemos  $K = \{g^1, \dots, g^{12}\}$  de ordenes 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12, 1 respectivamente (Proposición 3.7.8 parte 7). Hay dos elementos de orden divisor de 110 ( $g^6$  de orden 2 y  $g^{12} = 1$  de orden 1). Por lo tanto hay 2 homomorfismos.