Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Tarea 7

19 de Noviembre de 2025

2º semestre 2025 - Profesores M. Arenas - A. Kozachinskiy - M. Romero

---

Requisitos

- La tarea es **individual**. Los casos de copia serán sancionados con la reprobación del curso con nota 1,1.
- Cada pregunta tiene una nota de 1 a 7 (hay 1 punto base). La nota final es el promedio de ambas preguntas.
- **Entrega**: Hasta las 23:59 del jueves 27 de noviembre a través del buzón habilitado en el sitio del curso (Canvas).
  - Esta tarea debe ser hecha completamente en LaTeX. Tareas hechas a mano o en otro procesador de texto **no serán corregidas**.
  - Debe usar el template LaTeX publicado en la página del curso.
  - Cada solución de cada problema debe comenzar en una nueva hoja. ***Hint:*** Utilice `\newpage`
  - Los archivos que debe entregar son el archivo `PDF` correspondiente a su solución y un `zip` conteniendo el archivo `.tex` que compila su tarea. Si su `.tex` hace referencia a otros archivos, debe incluirlos también.
- El no cumplimiento de alguna de las reglas se penalizará con un descuento de 0.5 en la nota final (acumulables).
- No se aceptarán tareas atrasadas (salvo que utilice algún cupón `#problemaexcepcional`).
- Si tiene alguna duda, el foro de Github (issues) es el lugar oficial para realizarla.

Pregunta 1

Sea $n \geq 2$ y $a, b \in \{0, \ldots, n-1\}$. Decimos que b es un a raíz cuadrada de a en módulo n si $(b \cdot b) \equiv_n a$. Por ejemplo, 2 y 5 son raíces cuadradas de 4 en módulo 7 puesto que $(2 \cdot 2) \equiv_7 4$ y $(5 \cdot 5) \equiv_7 4$.

Sean r y s dos números impares distintos tales que $r \geq 3$ y $s \geq 3$, y sea $n = r \cdot s$. Demuestre que existe $a \in \{0, \ldots, n-1\}$ tal que a tiene al menos cuatro raíces cuadradas en módulo n (note que estas raíces tienen que ser números entre 0 y $n-1$). Por ejemplo, si $r = 5$ y $s = 7$, tenemos que $n = 35$, y $a = 16$ es un testigo de que el teorema es cierto en este caso puesto que $(4 \cdot 4) \equiv_{35} 16$, $(11 \cdot 11) \equiv_{35} 16$, $(24 \cdot 24) \equiv_{35} 16$, y $(31 \cdot 31) \equiv_{35} 16$.

Solución. Basta mostrar que existen 4 distintos números $b_1, b_2, b_3, b_4 \in \{0, 1, \ldots, n\}$ tal que $b_1^2 \equiv_n b_2^2 \equiv_n b_3^2 \equiv_n b_4^2$. Sea, sin pérdida de generalidad, $r > s$. Definimos:

$$b_1 = \frac{r-s}{2}, \qquad b_2 = \frac{r+s}{2}, \qquad b_3 = n - \frac{r+s}{2}, \qquad b_4 = n - \frac{r-s}{2}.$$

Observe que ya que r, s son impares, la división por 2 en la definición de $b_1, \ldots, b_4$ nos da números enteros.

Al principio, mostramos que b_1, b_2, b_3, b_4 son distintos elementos de $\{0, 1, \ldots, n-1\}$. Más precisamente, mostramos que

$$0 < b_1 < b_2 < b_3 < b_4 < n.$$

Desigualdades $0 < b_1, b_4 < n$ salen del hecho que $r > s$. En su turno, desigualdades $b_1 < b_2, b_3 < b_4$ salen del hecho que $s > 0$. Al final, mostramos que $b_2 < b_3$, vale decir, que $\frac{r+s}{2} < n - \frac{r+s}{2}$. Basta ver que $r + s < n = rs$. En efecto, $r + s \leq 2\,\text{máx}\{r, s\} < \text{mín}\{r, s\} \cdot \text{máx}\{r, s\} = rs = n$, donde la segunda desigualdad sale del hecho que $\text{mín}\{r, s\} \geq 3$.

Ahora mostramos que $b_1^2 \equiv_n b_2^2 \equiv_n b_3^2 \equiv_n b_4^2$. Notamos que $b_1 = n - b_4, b_2 = n - b_3$, lo que nos da:

$$b_1^2 = (n - b_4)^2 \equiv_n (-b_4)^2 = b_4^2,$$
$$b_2^2 = (n - b_3)^2 \equiv_n (-b_3)^2 = b_3^2.$$

Entonces, nos falta mostrar $b_1^2 \equiv_n b_2^2$, es decir, que $n | b_2^2 - b_1^2$. En efecto, tenemos $b_2^2 - b_1^2 = (b_2 - b_1)(b_2 + b_1) = rs = n$. □

Commentario. Explicaremos cómo se puede llegar a esté solución. Es facil notar que si b es una raíz cuadrada de a, entonces $n - b \equiv_n -b$ es también. Entonces, es suficiente construir un número a que tiene dos raices cuadradas b_1, b_2 que no son "opuestos" modulo n. Ahora, si $b_1^2 \equiv_n b_2^2$, entonces $n = rs | b_2^2 - b_1^2 = (b_2 - b_1)(b_2 + b_1)$. Una manera de que el producto $(b_2 - b_1)(b_2 + b_1)$ sea divisble por rs es cuando $b_2 - b_1 = s, b_2 + b_1 = r$. Esa sistema tiene la única solución $b_1 = \frac{r-s}{2}, b_2 = \frac{r+s}{2}$. Vale decir que es cricial verificar que las condiciones $r \leq 3, s \leq 3$ nos garantizan b_1, b_2, b_3, b_4 que obtenemos en esa manera son distintos.

Pregunta 2

Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$ y $\text{MCD}(a, b) = \text{MCD}(a^2 - b^3, a^3 + b^2)$. Demuestre que $\text{MCD}(a, b) = 1$.

Solución. Sea $d = \text{MCD}(a, b)$. Por definición, existen $u, v \in \mathbb{Z}$ enteros tal que $a = du, b = dv$. Entonces,

$$a^2 - b^3 = d^2u^2 - d^3v^3 = d^2(u^2 - dv^3),$$
$$a^3 + b^2 = d^3u^3 + d^2v^2 = d^2(du^3 - v^2).$$

Es decir $d^2|a^2 - b^3, d^2|a^3 + b^2$. Por el otro lado, $\text{MCD}(a^2 - b^3, a^3 + b^2) = d$. Entonces, $d^2 \leq d$. Ya que $d \geq 1$ por definición, eso implica que $d = 1$.

□