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 $(31 \cdot 31) \equiv_{35} 16$.

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 $\text{MCD}(a, b) = 1$.