



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN
IC2283 - DISEÑO Y ANÁLISIS DE ALGORITMOS

Ayudantía 8 - Repaso Aritmética Modular

30 de octubre de 2020

Profesor Marcelo Arenas

Bernardo Barías y Ricardo Rodríguez

Pregunta 1

Demuestre que

- a) $a \equiv b \pmod{n}$ si y solo si $(a \pmod{n}) = (b \pmod{n})$
- b) $a \equiv (a \pmod{n}) \pmod{n}$

Pregunta 2

Demuestre que si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces

- a) $a + c \equiv b + d \pmod{n}$
- b) $a \cdot c \equiv b \cdot d \pmod{n}$

Pregunta 3

Demuestre que

- a) $a^k \equiv (a \pmod{n})^k \pmod{n}$
- b) n es divisible por 3 si y solo si sus dígitos son divisibles por 3.

Pregunta 4 - Inverso modular

Sea $a, n \in \mathbb{Z}$. Muestre que si $\text{MCD}(a, n) = 1$, entonces existe un $b \in \mathbb{Z}$ tal que $a \cdot b \equiv 1 \pmod{n}$.