Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

Ayudantía 8 - Aritmética Modular

5 de noviembre de 2021

Profesor Marcelo Arenas

Bernardo Barías

Pregunta 1

Demuestre que

a) $a \equiv b \mod n$ si y solo si $(a \mod n) = (b \mod n)$

b) $a \equiv (a \mod n) \mod n$

Pregunta 2

Demuestre que si $a \equiv b \mod n$ y $c \equiv d \mod n$, entonces

a) $a + c \equiv b + d \mod n$

b) $a \cdot c \equiv b \cdot d \mod n$

Pregunta 3

Demuestre que

a) $a^k \equiv (a \mod n)^k \mod n$

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 $a \cdot b \equiv 1 \mod n$.

Pregunta 5 - Pequeño teorema de Fermat

Sea p un número primo y $a \in \mathbb{Z}$ tal que p no divide a. Luego

$$a^p \equiv a \pmod{p}$$

Demuestre el teorema y concluya que

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