PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
1er semestre - 2022
Lothar Droppelmann

Ayudantía 7

Repaso aritmética modular

Definición: Inverso modular

b es inverso de a en módulo n si $a \cdot b \equiv 1 \mod n$

Identidad de Bézout

Para cada $a, b \in \mathbb{N}$ tales que $a \neq 0$ y $b \neq 0$ existen $s, t \in \mathbb{Z}$ tal que:

$$\text{MCD}(a, b) = s \cdot a + t \cdot b$$

Teorema de la existencia del inverso modular

$a \in N$ tiene inverso en módulo n si y sólo si:

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

Pequeño teorema de Fermat

Sea p un número primo. Si $a \in \{0, ..., p-1\}$, entonces $a^p \equiv a \mod p$.

Preguntas

1. Demuestre la identidad de Bézout
2. Demuestre el teorema de la existencia del inverso modular
3. Demuestre el pequeño teorema de Fermat