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

Ayudantía 16 - Teoría de números

28 de noviembre de 2025

Manuel Villablanca, Elías Ayaach, Caetano Borges

Resumen

- **Relación divide a:** La relación divide a, denotada por $|$ sobre $\mathbb{Z}\backslash 0$, es tal que $a \mid b$ si y solo si $\exists k \in \mathbb{Z}$ tal que $b = k \cdot a$.
- **Identidad de Bézout:** Esta identidd enuncia que si $a, b \in \mathbb{Z}$ son distintos de 0 y $\gcd(a, b) = d$, entonces existen $x, y \in \mathbb{Z}$ tales que:

$$a \cdot x + b \cdot y = d$$

- **Relación módulo n:** La relación módulo n, denotada por $\equiv_n$ sobre $\mathbb{Z}$, es tal que $a \equiv_n b$ si y solo si $n \mid (b - a)$. Esta relación es de equivalencia.
- **Operacion módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \bmod n$.
- **Teorema:**

$$a \equiv_n b \iff a \bmod n = b \bmod n$$

- **Máximo común divisor:** Dados a y b diremos que su máximo común divisor denotado como $\gcd(a, b)$ es el máximo natural n tal que $n \mid a$ y $n \mid b$.
- **Teorema Chino del Resto**: el sistema de ecuaciones

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución única en $\mathbb{Z}_m$ con $m = \prod_{i=1}^{n} m_i$.

1 Pequeño Teorema de Fermat

Demuestre el Pequeño Teorema de Fermat:

Sea p un número primo. Si $a \in \mathbb{Z}_p = \{0, \ldots, p-1\}$, entonces $a^p \bmod p = a$

2 Teorema Fundamental de la Aritmética

1. Demuestre que si p es un número primo y $p \mid (a \cdot b)$, entonces $p \mid a$ o $p \mid b$.
2. Demuestre el Teorema Fundamental de la Aritmética: cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

3 Números primos

Sea p un número primo > 2. Demuestre que para cada $a \in \mathbb{Z}_p, a \neq 0$, se tiene que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Nota: $\mathbb{Z}_p$ denota al conjunto de las clases de equivalencia de enteros módulo p. Por ejemplo, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

4 Un último esfuerzo

1. Para $m > 1$ demuestre que si $a \equiv b \pmod{m}$, entonces $\gcd(a, m) = \gcd(b, m)$.
2. Para $m > 1$ demuestre que si $ac \equiv bc \pmod{m}$, entonces $a \equiv b \pmod{\frac{m}{\gcd(m,c)}}$.