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

Ayudantía 15 - Teoría de números

21 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:**
$$a \equiv_n b \Longleftrightarrow a \bmod n = b \bmod n$$
- **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**: si $\gcd(m_i, m_j) = 1$ para $i \neq j$, entonces el sistema
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$
tiene solución única en $\mathbb{Z}_m$ con $m = \prod_{i=1}^{n} m_i$.

1 Divisibilidad

Sea $k \in \mathbb{Z}$ tal que $k > 0$, y considere k números enteros consecutivos $x_1, \ldots, x_k$.
Demuestre que $k \left| \prod_{i=1}^{k} x_i \right.$.

2 MCD

- Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Demuestre que $\text{MCD}(a, b) = |b|$ si y sólo si $b \mid a$.
- Sean $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Demuestre que $\frac{a}{\text{MCD(a,b)}}, \quad \frac{b}{\text{MCD(a,b)}}$ son coprimos.

3 MOD

1. Determine si existe solución para cada una de las siguientes congruencias lineales. En caso que exista, encuentre su solución.
   (a) $8x \equiv 6 \pmod{19}$
   (b) $21x \equiv 12 \pmod{35}$
2. Demuestre que todos los elementos de $\mathbb{Z}_p \setminus \{0\}$ tienen inverso multiplicativo en módulo p, si y sólo si p es primo.