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

Ayudantía 12 - Teoría de números

21 de junio de 2024

Martín Atria, Paula Grune, 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.
- **Teorema:**

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

- **Operacion módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \bmod n$.
- **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 $n \mid b$.

1. Representación de números

Demuestre que todo número $n \in \mathbb{N}$ se puede representar de la forma:

$$n = e_k \cdot 3^k + \cdots + e_1 \cdot 3^1 + e_0$$

donde $e_0, \ldots, e_k \in \{1, 0, -1\}$

2. Divisibilidad

1. Demuestre que si $\gcd(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.
2. Demuestre que si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.
3. En clases se demostró que todo número natural $n > 1$ se puede descomponer como:

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$$

   con $p_1, \ldots, p_k$ primos y $p_1 \leq p_2 \leq \cdots \leq p_k$. Demuestre usando el resultado en el punto anterior que esta descompocición es única.

3. Uno cortito

Sean $a, b \in \mathbb{Z}$ tales que $a, b > 0$. Demuestre que $a \mid (a + 1)^b - 1$.