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

Ayudantía 13 - Teoría de números

28 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:**

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

- **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 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 Congruencia módulo

Demuestre que si a es un número impar, entonces $a^2 \equiv 1 \pmod 8$.

3 Números primos

1. Sea p un número impar. Demuestre que para cada $a \in \mathbb{Z}_p$, 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, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

2. Demuestre que si $p > 3$ es un número primo, entonces $p^2 \equiv 1 \pmod{24}$.

4 Perros 🐕 y gatos 🐈

1. Sean $a, b, c \in \mathbb{Z}$. Demuestre que la ecuación $ax + by = c$ tiene al menos una solución si y solo si $gcd(a, b)|c$.

2. Un grupo de perros y gatos gastaron \$100 en una tienda de juguetes para mascotas. Sabiendo que cada perro gastó \$8, y que cada gato gastó \$5, ¿puedes encontrar cuantos perros y cuantos gatos hay en el grupo?