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

# Ayudantía 14 - Teoría de números

29 de noviembre de 2024

Martín Atria, José Thomas Caraball, 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 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 Números primos

1. 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, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

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

# 3 Función $\varphi$ de Euler

La función $\varphi(n)$ de Euler es una función aritmética[1] que indica la cantidad de enteros positivos menores a $n$ que son coprimos a $n$, esto es,

$$\varphi(n) = |\{m \in \mathbb{Z} \mid 0 < m < n \wedge \gcd(n, m) = 1\}|$$

1. Una función aritmética $f$ es multiplicativa si cuando $n$ y $m$ son coprimos entonces $f(nm) = f(n)f(m)$, esto es, $\gcd(n, m) = 1 \Rightarrow f(nm) = f(n)f(m)$. Demuestre que $\varphi$ es multiplicativa.

2. Demuestre que $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

[1] Una función aritmética es una función cuyo dominio son los enteros positivos y su rango es cualquier subconjunto de los números complejos.