# Apuntes Discretas

Oskar Denis Siodmok

28 de octubre de 2020

# Parte I
# Aritmética modular

## 1. Conceptos básicos

**Definición 1.1.**
$$a \equiv b \pmod{n} \iff a - b = \dot{n} \wedge a \bmod n = b \bmod n,\ n > 1$$

**Teorema 1.1.**
$$\forall a \in \mathbb{Z}\ \exists\, b \in \{0, 1, \ldots, n-1\} \subseteq \mathbb{Z} \,/\, a \equiv b \pmod{n},\ n \in \mathbb{N} \setminus \{1\}$$

**Definición 1.2.**
$$[a]_n = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$$

**Observación 1.1.** Se cumple, debido a la propiedad transitiva:

$$a \equiv b \pmod{n} \iff [a]_n = [b]_n$$

**Definición 1.3.**
$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

**Observación 1.2.**
$$[a]_n \longrightarrow a \equiv a + n \equiv a + 2n \equiv \ldots \pmod{n} \implies$$

Se puede aplicar la propiedad transitiva para transformar congruencias en otras equivalentes más sencillas

Por ejemplo:

$$x \equiv 17 \pmod{11} \iff x \equiv 17 - 11 \pmod{11} \iff x \equiv 17 \bmod 11 \pmod{11} \iff x \equiv 6 \pmod{11}$$

Siendo ésta última ecuación la solución para $x$.

**Observación 1.3.**

$$a + c \equiv b + d \pmod{n} \Longleftarrow \left\{ \begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \right\} \Longrightarrow ac \equiv bd \pmod{n}$$

Demostración:

$$\left. \begin{array}{c} a - b = kn \\ c - d = ln \end{array} \right\} a + c - b - d = kn + ln = n(k + l) \implies a + c \equiv b + d \pmod{n}$$

$$\left. \begin{array}{c} a - b = kn;\ ac - bc = kn \\ c - d = ln;\ cb - db = ln \end{array} \right\} ac + cb - bc - db = kn + ln = n(k + l) = ac - db \implies ac \equiv bd \pmod{n}$$

**Definición 1.4.** Debido a estas observaciones, se define la suma y producto de clases módulo n como:

$$[a]_n + [b]_n = [a + b]_n$$
$$[a]_n [b]_n = [ab]_n$$

## 2. Congruencias lineales

**Definición 2.1.** Se define una congruencia lineal como:

$$ax + b \equiv c \pmod{n};\ a, b, c \in \mathbb{Z}$$

**Teorema 2.1.**

$$\operatorname{mcd}(a, n) = 1 \iff \exists\, b \,/\, ab \equiv 1 \pmod{n}$$

Se dice que $\exists\, [a]_n^{-1}$ para el producto en $\mathbb{Z}_n$

**Definición 2.2.**

$$\begin{aligned} \phi : \mathbb{Z}^+ &\longrightarrow \mathbb{Z}^+ \\ n &\longmapsto \phi(n) = \#\{m \in \mathbb{N} : \operatorname{mcd}(m, n) = 1,\ m \leq n\} \\ &\qquad\quad\ = \#\{m \in \mathbb{N} : m \text{ coprimo con } n,\ m \leq n\} \end{aligned}$$

**Teorema 2.2.**

$$\begin{aligned} &\phi(p) = p - 1 \iff p \in \text{primos} \\ &\phi(p^\alpha) = p^\alpha - p^{\alpha-1}\ \forall\, \alpha \in \mathbb{N} \iff p \in \text{primos} \\ &\phi(mn) = \phi(m)\phi(n)\ \forall\, m, n \in \mathbb{Z}^+ \iff \operatorname{mcd}(m, n) = 1 \\ &n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},\ n \in \mathbb{Z}^+ \implies \phi(n) = \textstyle\prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \end{aligned}$$

Donde $p_i^{\alpha_i}$ hace referencia a la descomposición en primos de $n \in \mathbb{Z}^+$

**Teorema 2.3** (Euler-Fermat)**.**

$$\operatorname{mcd}(a, n) = 1,\ a, n \in \mathbb{Z},\ n > 1 \longrightarrow a^{\phi(n)} \equiv 1 \pmod{n} \longrightarrow [a]_n^{-1} = [a^{\phi(n)-1}]_n$$

## 3. Sistemas de congruencias