Apuntes Discretas

Oskar Denis Siodmok

5 de noviembre de 2020

Parte I
Aritmética modular

1. Conceptos básicos

Definición 1.1.

$$a \equiv b \ (\text{mód } n) \iff a - b = \dot{n} \ \wedge \ a \bmod n = b \bmod n, \ n > 1$$

Teorema 1.1.

$$\forall a \in \mathbb{Z} \, \exists \, b \in \{0, 1, \ldots, n-1\} \subseteq \mathbb{Z} \ / \ a \equiv b \ (\text{mód } n), \ n \in \mathbb{N} \setminus \{1\}$$

Definición 1.2.

$$[a]_n = \{b \in \mathbb{Z} : a \equiv b \ (\text{mód } n)\}$$

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

$$a \equiv b \ (\text{mód } n) \iff [a]_n = [b]_n$$

Definición 1.3.

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

Observación 1.2.

$$[a]_n \longrightarrow a \equiv a + n \equiv a + 2n \equiv \ldots \ (\text{mód } n) \implies$$

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

Por ejemplo:

$$x \equiv 17 \ (\text{mód } 11) \iff x \equiv 17 - 11 \ (\text{mód } 11) \iff x \equiv 17 \bmod 11 \ (\text{mód } 11) \iff x \equiv 6 \ (\text{mód } 11)$$

Siendo ésta última ecuación la solución para x.

Observación 1.3.

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

Demostración:

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

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

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.

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

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

Definición 2.2.

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

Teorema 2.2.

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

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

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

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

3. Sistemas de congruencias

Teorema 3.1 (Teorema chino del resto)**.**

$$\begin{matrix} \forall\, n_1, n_2, \dots, n_k \in \mathbb{Z}^+ \setminus \{1\} \\ \forall\, a_1, a_2, \dots, a_k \in \mathbb{Z} \end{matrix} :$$

$$\exists\, x / \left\{ \begin{array}{l} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \qquad \vdots \\ x \equiv a_k \pmod{n_k} \end{array} \right\} \Longleftarrow \mathrm{mcd}(n_i, n_j) = 1,\ \forall\, i, j \in \{1, \dots, k\} \subseteq \mathbb{N},\ i \neq j$$

Además:

$$x, x' \text{ son soluciones} \implies x \equiv x' \pmod{\prod_{i=1}^{k} n_i}$$

Teorema 3.2.

$$\begin{matrix} \forall\, n_1, n_2 \in \mathbb{Z}^+ \setminus \{1\} \\ \forall\, a_1, a_2 \in \mathbb{Z} \end{matrix} : \exists x / \left\{ \begin{array}{l} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{array} \right\} \iff a_1 \equiv a_2 \pmod{\mathrm{mcd}(n_1, n_2)}$$

Parte II
Combinatoria

4. Conteo de conjuntos

Observación 4.1. $|A| < \infty > |B|$:

1. $|A \cup B| = |A| + |B| + |A \cap B|$.
2. $B \subseteq A \implies |B| \leq |A|,\ |A \setminus B| = |A| - |B|$.
3. $|A \times B| = |A||B|$.
4. Principio de Palomar: $|A| > |B| \implies \nexists\, f : B \to A \,/\, f$ es inyectiva.

Observación 4.2. Las observaciones 4.1.2 y 4.2.4 se pueden generalizar a:

1. $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ (imposible de generalizar).
2. $|\prod_{i=1}^{|A|} A_i| = \prod_{i=1}^{|A|} |A_i|$

5. Variaciones

Definición 5.1. $V_{m,n}$: Variación odrinaria sin repetición de m elementos tomados de n en n ($m \geq n$).

$$V_{m,n} = \frac{m!}{(m-n)!} = \prod_{i=0}^{n+1}(m-i)$$

:

- No entran todos los elementos.
- Importa el orden.
- No se repiten los elementos.

Definición 5.2. $VR_{m,n}$: Variación ordinaria con repetición de m elementos tomados de n en n.

$$VR_{m,n} = m^n$$

- Pueden entrar todos los elementos si $m \leq n$.
- Importa el orden.
- Se repiten los elementos.

6. Permutaciones

Definición 6.1. Las permutaciones son un caso particular de variaciones donde $m = n$.

Definición 6.2. P_n: Permutación de n elementos.

$$P_n = n!$$

- Entran todos los elementos.
- Importa el orden.
- No se repiten los elementos.

Definición 6.3. PC_n: Permutación circular. Los elementos se repetirán de forma cílcica, por lo cual, por ejemplo, la ordenación 1234 sería equivalente a 3412.

$$P_n = n!$$

Definición 6.4. $PR_n^{n_1,n_2,\ldots,n_s}$: Permutaciones con repeticiones de n elementos, donde hay s elementos que se repiten con $n_i > 1 \, \forall \, i$.

$$PR_n^{n_1,n_2,\ldots,n_s} = \frac{n!}{\prod_{i=1}^{s} n_i!}$$