Apuntes Discretas

Oskar Denis Siodmok

15 de noviembre 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.

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

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

Definición 2.2.

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

Teorema 2.2.

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

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)**.**

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

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

Además:

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

Teorema 3.2.

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

Parte II
Combinatoria

4. Conteo de conjuntos

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

1. $|A \cup B| = |A| + |B| + |A \cap B|$.
2. $B \subseteq A \implies |B| \le |A|,\ |A \setminus B| = |A| - |B|$.
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.

$$PC_n = (n-1)!$$

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 $n_i > 1 \,\forall\, i$.

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

7. Combinaciones

Definición 7.1. Las combinaciones son variaciones donde el orden no importa.

Definición 7.2. $C_{m,n}$: Combinación de m elementos tomados de n en n $(m \geq n)$.

$$C_{m,n} = \binom{m}{n} = \frac{m!}{n!(m-n)!}$$

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

Definición 7.3. $CR_{m,n}$: Combinación con repetición de m elementos tomados de n en n $(m \geq n)$.

$$CR_{m,n} = \binom{m+n-1}{n}$$

Parte III

Teoría de grafos

8. Grafos, digrafos y multigrafos

Definición 8.1. Un grafo simple se denota como un par $G = (E, V)$ donde E se refiere a las aristas y V a los vértices. Las aristas se definen como:

$$E \subseteq \{\{u, v\} : u, v \in V,\ u \neq v\}$$

Definición 8.2. Un multigrafo o grafo no dirigido $G = (V, E)$ tiene $E = \{e_i\}_{i \in I}$, que denota una familia, no un conjunto. Además, $e_i = \{u_i, v_i\}$, $(u_i, v_i) \in V \times V \, \forall i \in I$.

Definición 8.3. Un digrafo $G = (V, E)$ tiene $E \subseteq \{(a, b) \in V \times V : a \neq b\}$, o sea, las aristas son ordenadas y los pares indican la dirección de estas.

Definición 8.4. Un multigrafo o grafo dirigido $G = (V, E)$ tiene $E = \{e_i\}_{i \in I}$ donde $e_i \in V \times V$.

Definición 8.5. u adyacente a $v \iff \{u, v\} \in E$, donde $G = (V, E)$. Entonces, $e = \{u, v\}$ conecta u y v quiere decir que e incidente con u y v y que u y v son los extremos de la arista e.

Definición 8.6. $gr(u)$ donde $u \in V$ se refiere al número de aristas a las que pertenece u. $gr(u) = 0 \longrightarrow u$ es un vértice aislado.

Teorema 8.1. Para $G = (V, E)$ no dirigido:

$$\sum_{v \in V} gr(v) = 2|E|$$

Definición 8.7. En un $G = (V, E)$ dirigido, para $(u, v) \in E$: u es el vértice inicial de (u, v) y v el final. Sabiendo esto, se define el grado de entrada $gr^+(u)$ como el número de aristas con vértice final u. $gr^-(u)$ será el grado de salida y se referirá al número de aristas con u como vértice inicial.

Teorema 8.2. Para $G = (V, E)$ dirigido:

$$|E| = \sum_{v \in V} gr^+(v) = \sum_{v \in V} gr^-(v)$$

9. Isomorfismo de grafos

Definición 9.1. Para $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ simples, (G_1, G_2) isomorfos $\iff \exists\, f : V_1 \to V_2$ biyectiva / $\forall\, u, v \in V_1 : \{u, v\} \in E_1 \iff \{f(u), f(v)\} \in E_2$. En ese caso, se dice que f es un isomorfismo de (G_1, G_2). Esta definición se puede extender a multigrafos y multidigrafos.

Observación 9.1.

1. Para (G_1, G_2) isomorfos, se cumple $|V_1| = |V_2|$ y $|E_1| = |E_2|$.
2. Para f isomorfismo de (G_1, G_2), se cumple $gr(u) = gr(f(u)) \, \forall\, u \in V_1$.

10. Árboles

Definición 10.1. Un camino entre v_0 y v_k de $G = (V, E)$ no dirigido es una secuencia de vértices $C = (v_0, v_1, \ldots, v_k)$ no necesariamente distintos. Se cumple que $e_i = \{v_{i-1}, v_i\} \in E \, \forall\, i \in \{1, 2, \ldots, k\}$. C es un ciclo $\iff v_0 = v_k \wedge v_i \neq v_j \, \forall\, i, j \in \{1, 2, \ldots, k-1\}$.

Definición 10.2. $G = (V, E)$ conexo $\iff \exists\, C \, \forall\, (v, u) \in V \times V,\ v \neq u$.

Definición 10.3. $G = (V, E)$ es un arbol $\iff$ G es conexo, sin ciclos y no dirigido. G no tiene cilclos $\implies$ G es un grafo simple.

Teorema 10.1. $G = (V, E)$ es un arbol $\iff$

1. G es conexo $\wedge |V| = |E| + 1$.
2. G no tiene ciclos $\wedge |V| = |E| + 1$.
3. $\exists! \, C \, \forall \, (v, u) \in V \times V$.
4. G es conexto y al suprimir cualquier arista G pasa a ser no conexto $\implies$ G es un grafo conexo minimal.

Definición 10.4. $G' = (V', E')$ es subgrafo de $G = (V, E) \iff V' \subseteq V \ \wedge \ E' \subseteq E$.

Definición 10.5. $G' = (V', E')$ es un árbol generador de $G = (V, E) \iff G'$ subgrafo $G \ \wedge \ V' = V$.

Teorema 10.2. $G = (V, E)$ simple es conexo $\iff \exists$ abrol generador de G.