PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CURSO: MATEMÁTICAS DISCRETAS
AYUDANTES: FRANCISCA CAPRILE, CATALINA ORTEGA, MATÍAS FERNÁNDEZ E IGNACIO VERGARA

Ayudantía 13

17 de noviembre de 2023

2º semestre 2023 - Profesores G. Diéguez - S. Bugedo - N. Alvarado- B. Barías

---

Resumen

Árboles

- **Árbol:** Un grafo $T = (V, E)$ es un árbol si para cada par de vértices $x, y \in V$ existe un único camino entre ellos. También existen defínciones equivalentes tales como:
  - Un grafo $T = (V, E)$ es un árbol si y solo si es conexo y acíclico.
  - Un grafo $T = (V, E)$ es un árbol si y solo si es conexo y todas sus aristas son de corte.
  - Un grafo $T = (V, E)$ con n vértices es un árbol si y solo si es conexo y tiene exactamente $n - 1$ aristas.

  A partir de esto,
  - Llamaremos a uno de los vértices $r \in V$ como la raíz del árbol y a los vértices de grado menor o igual a 1 hojas.
- **Bosque:** Un grafo $T = (V, E)$ es un bosque si para cada par de vértices $x, y \in V$ si existe un camino entre ellos, este es único.
- **Teorema:** Todo árbol es un grafo bipartito.
- **Teorema:** Si T es un árbol y v es una hoja de él, entonces el grafo $T - v$ es un árbol.
- Sea $T = (V, E)$ un árbol con raíz r y x un vértice cualquiera. Luego,
  - La profundidad de x es el largo del camino que lo une con r (r tiene profundidad 0).
  - La altura o profundidad del árbol es el máximo de las profundidades de sus vértices.
  - Los ancestros de x corresponden a los vértices que aparecen en el camino entre él y r (x es ancestro de sí mismo).
  - El padre de x es su ancestro (propio) con mayor profundidad. Se dice que x es hijo de su padre.
  - Dos vértices x e y con el mismo padre son hermanos.
- **Arbol Binario:** Un árbol con raíz se dice binario si todo vértice tiene grado a lo más 3 o equivalentemente si todo vértice tiene a lo más dos hijos.

Teoría de números

- **Relación divide a:** La relación divide a denotada por $|$ sobre $\mathbb{Z}$ sin 0 es tal que $a|b$ si y solo si $\exists k \in \mathbb{Z}$ tal que $b = ka$.
- **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 $n|(b-a)$. Esta relación es de equivalencia.
- **Teorema:**
$$a \equiv_n b \iff a \mod n = b \mod n$$
- **Operación módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \mod n$.
- **Máximo común divisor:** Dados a y b diremos que su máximo común divisor denotado como $MCD(a,b)$ es el máximo natural n tal que $n|a$ y $n|b$.
- **Teorema:** Si $a, b \in \mathbb{Z}$, entonces existen $s, t \in \mathbb{Z}$ tales que
$$MCD(a,b) = s \cdot a + t \cdot b$$
.
- b es inverso de a en módulo n si $a \cdot b \equiv_n 1$

Ejercicio 1 | Teoría de números

Demuestre que si a es un número impar, entonces $a^2 \equiv 1 (\text{mod} 8)$.

Solución

Sea $a \in \mathbb{Z}$ un número impar. Luego sabemos que existe un único par $q, r \in \mathbb{Z}$ tal que

$$a = 8q + r \text{ con } 0 \leq r < 8 \ (1)$$

.

Es claro que podemos reescribir (1) como:

$$a \equiv r (\text{mod} 8)$$

Elevando al cuadrado ambos lados de la congruencia obtenemos que $a^2 \equiv r^2 (\text{mod} 8)$, por lo que basta con demostrar que $r^2 \equiv 1 (\text{mod} 8)$.

Volviendo a (1), como a es impar, realmente existen solo las siguientes posibilidades: a = 8q + 1, a = 8q + 3, a = 8q + 5, a = 8q + 7. Es decir:

$$r \in \{1, 3, 5, 7\}$$

Luego, notemos que:

- Si r = 1: $1^2 \equiv 1 \equiv 1 (\text{mod} 8)$
- Si r = 3: $3^2 \equiv 9 \equiv 1 (\text{mod} 8)$
- Si r = 5: $5^2 \equiv 25 \equiv 1 (\text{mod} 8)$
- Si r = 7: $7^2 \equiv 49 \equiv 1 (\text{mod} 8)$

y así $a^2 \equiv r^2 \equiv 1 (\text{mod} 8)$.

Ejercicio 2 | Teoría de números

Considere el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Demuestre que el sistema tiene solución si y solo si $\mathrm{MCD}(m_1, m_2) \mid (a_1 - a_2)$.

Solución:

($\Rightarrow$) Sea $d = \mathrm{MCD}(m_1, m_2)$. Si el sistema tiene solución, entonces existe $x \in \mathbb{Z}$ tal que

$$x = a_1 + m_1 k_1 = a_2 + m_2 k_2$$

para algunos $k_1, k_2 \in \mathbb{Z}$. De lo anterior, tenemos que

$$a_1 - a_2 = m_2 k_2 - m_1 k_1.$$

Finalmente, como d divide a m_1 y a m_2 (por ser el máximo común divisor entre ambos), obtenemos que $\mathrm{MCD}(m_1, m_2) \mid (a_1 - a_2)$.

($\Leftarrow$) Suponemos $d \mid (a_1 - a_2)$, en otras palabras, existe $k \in \mathbb{Z}$ tal que $a_1 - a_2 = dk$. Utilizando el algoritmo extendido de Euclides, sabemos que existen enteros s y t tales que $d = sm_1 + tm_2$. Si juntamos lo anterior, obtenemos

$$a_1 - a_2 = dk = (sm_1 + tm_2)k.$$

Luego podemos obtener $a_1 + (sk)m_1 = a_2 + (tk)m_2$, lo que significa que existe un entero z tal que $z \equiv a_1 \pmod{m_1}$ y $z \equiv a_2 \pmod{m_2}$.

Ejercicio 3 | Árboles

1. (Existencia de hojas) Sea T un árbol con al menos dos vértices. Demuestre que T tiene al menos dos *hojas*.
2. (Árbol generador) Todo grafo conexo G tiene un árbol T que usa todos sus vértices.

Solución

1. Sea $\delta = d_1 \leq d_2 \leq \ldots \leq d_v = \Delta$ la secuencia de todos los grados de los vértices de T y note que $\delta \geq 1$ porque T es conexo no-trivial. Entonces

   $$v - 1 = e = \frac{1}{2} \sum_{j=1}^{v} d_j.$$

   Por contradicción, asumamos que $d_2 \geq 2$, entonces

   $$v - 1 \geq \frac{1}{2}(1 + 2(v-1)) = \frac{1}{2} + v - 1;$$

   contradicción.

2. Sea G un grafo conexa. Si G no tiene ciclos entonces G es un árbol y ya acabamos. Si G tiene tiene un ciclo $(v_0, v_1, v_2, \ldots, v_k = v_0)$, quitémosle a G la arista $\{v_0, v_{k-1}\}$.

   El subgrafo que queda sigue siendo conexo, la demotración es la siguiente:

   Sean h_1, h_2 vértices de G. Como G era conexa, había al menos un recorrido que unía h_1, h_2. Si el recorrido no usaba la arista $\{v_0, v_{k-1}\}$ entonces es un recorrido en el subgrafo. Si el recorrido si la usaba, entonces cada vez que aparezca la pareja (v_0, v_{k-1}) en el recorrido, la cambiamos por $(v_0, v_2, v_3, \ldots, v_{k-1})$

y si aparece la pareja (v_{k-1}, v_0) la cambiamos por $(v_{k-1}, v_{k-2}, \dots, v_0)$. Con esto ya no usamos la arista $\{v_0, v_{k-1}\}$, por lo que el nuevo recorrido sí es un recorrido en el subgrafo. Con esto el subgrafo es conexo. Además $(v_0, v_2, \dots, v_k = v_0)$ no es un ciclo de el subgrafo. Podemos repetir el argumento hasta que ya no nos queden ciclos, con lo que obtenemos el árbol que buscábamos.