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

Tarea 6

9 de noviembre de 2022

2º semestre 2022 - Profesores F. Suárez - S. Bugedo - N. Alvarado

---

Requisitos

- La tarea es individual. Los casos de copia serán sancionados con la reprobación del curso con nota 1,1.
- **Entrega**: Hasta las 23:59:59 del 29 de noviembre a través del buzón habilitado en el sitio del curso (Canvas).
    - Esta tarea debe ser hecha completamente en LaTeX. Tareas hechas a mano o en otro procesador de texto **no serán corregidas**.
    - Debe usar el template LaTeX publicado en la página del curso.
    - Cada solución de cada problema debe comenzar en una nueva hoja. ***Hint:*** Utilice `\newpage`
    - Los archivos que debe entregar son el archivo `PDF` correspondiente a su solución con nombre `numalumno.pdf`, junto con un `zip` con nombre `numalumno.zip`, conteniendo el archivo `numalumno.tex` que compila su tarea. Si su código hace referencia a otros archivos, debe incluirlos también.
- El no cumplimiento de alguna de las reglas se penalizará con un descuento de 0.5 en la nota final (acumulables).
- No se aceptarán tareas atrasadas.
- Si tiene alguna duda, el foro de Canvas es el lugar oficial para realizarla.

Problemas

Problema 1

a) Sea $G = (V, E)$ un bosque, demuestre que siempre existe una función $f : V \to \{0, 1\}$ tal que se cumple que

$$(u, v) \in E \text{ entonces } f(u) \neq f(v)$$

b) Sea G un grafo simple. Un árbol generador de G es un subgrafo de G tal que es un árbol que contiene a todos los vértices de G. De un ejemplo de un grafo simple G con 7 vértices y de un árbol generador asociado a G.

Problema 2

a) Para $n > 1$ y $a^n - 1$ primo, muestre que $a = 2$ y n es primo.

b) Demuestre que si m es un entero positivo mayor que 1 y $ac \equiv bc \mod m$, entonces $a \equiv b \mod \frac{m}{\gcd(m,c)}$

Soluciones

Problema 1

a) Sea $G = (V, E)$ un bosque, demuestre que siempre existe una función $f : V \to \{0, 1\}$ tal que se cumple que
$$(u, v) \in E \text{ entonces } f(u) \neq f(v)$$

b) Sea G un grafo simple. Un árbol generador de G es un subgrafo de G tal que es un árbol que contiene a todos los vértices de G. De un ejemplo de un grafo simple G con 7 vértices y de un árbol generador asociado a G.

Solución. a) Sea G un bosque. Notemos que el resultado es equivalente a probar que G es bipartito (la función f puede interpretarse como la asignación a una u otra partición). Demostraremos el resultado por inducción sobre el número de aristas de G.

- Para $|E| = 0$, el bosque consiste en nodos desconectados. En este caso, basta con tomar $f : V \to \{0, 1\}$ tal que $f(v) = 0$ para cada $v \in V$. Dado que no hay ninguna arista, f cumple la propiedad pedida, pues no hay vecinos que compartan la asignación.
- Suponemos que un bosque con $|E| = n$ cumple que existe f adecuada.
- Consideremos un bosque G tal que $|E| = n + 1$. Sea $e \in E$ una arista cualquiera y sea $G - e$ el grafo resultante de extraer únicamente la arista e de G. Como G es un bosque, está formado por una colección de árboles. Al sacar una arista, no es posible que aparezcan ciclos en $G - e$, de forma que $G - e$ es un bosque con a lo menos tantos árboles como G. Además, $|E(G - e)| = n$.

  Luego, por hipótesis inductiva, $G - e$ tiene una función $f : V \to \{0, 1\}$ adecuada. Es decir, para cada $(u, v) \in E - \{e\}$, se tiene que $f(u) \neq f(v)$. Luego, probaremos que f permite construir una función adecuada para G:

  - Si $f(u) \neq f(v)$, es decir, f asigna distintas categorías a los nodos de la arista eliminada, f satisface también las propiedades para G.
  - Si $f(u) = f(v)$, es decir, f asigna una misma categoría a los nodos de la arista eliminada, hay que invertir la asignación de categoría para los nodos del mismo árbol de alguno de los vértices de la arista eliminada.

    Denotaremos por $\overline{f(w)}$ al valor opuesto de $f(w)$. En tal caso, definimos la función $g : V \to \{0, 1\}$ según

$$g(w) = \begin{cases} \overline{f(w)} & \text{si } w \text{ está en la misma componente conexa que } v \\ f(w) & \text{si no} \end{cases}$$

Para las aristas (u_1, u_2) que conectan vértices en componentes conexas diferentes de v, g cumple $g(u_1) \neq g(u_2)$ por las propiedades de f. Para aristas (v_1, v_2) entre vértices de la componente conexa de v, $g(v_1) \neq g(v_2)$ pues se invierten ambos valores que ya eran diferentes. Finalmente, para la arista (u, v), dado que se invierte el valor de $f(v)$, $g(u) \neq g(v)$, lo que prueba lo pedido.

b) Consideremos el grafo simple G mostrado en la siguiente figura:

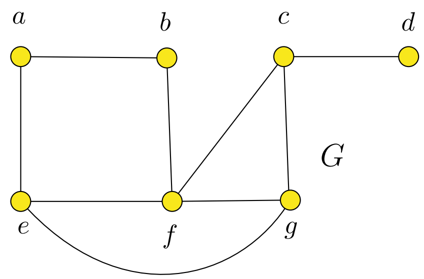

Figura 1: Grafo simple G de 7 vértices.

Notemos que G es conexo, pero no es un árbol. Si quitamos la aristas (a, e), (e, f) y (c, g) obtenemos un árbol generador asociado a G, pues sigue conteniendo a todos los vértices de G y es un árbol.

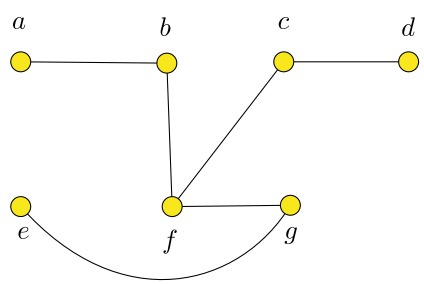

Figura 2: Un árbol generador asociado al grafo G.

$\square$

- P1a)
  - 0,5 puntos por notar la equivalencia con probar que G es bipartito.
  - 0,5 puntos por el caso base.
  - 2 puntos por mostrar la tésis inductiva.

- P1b)
  - 1 puntos por un ejemplo de grafo simple G de 7 vértices.
  - 2 puntos por un árbol generador asociado a G.

Problema 2

a) Para $n > 1$ y $a^n - 1$ primo, muestre que $a = 2$ y n es primo.

b) Demuestre que si m es un entero positivo mayor que 1 y $ac \equiv bc \mod m$, entonces $a \equiv b \mod \frac{m}{\gcd(m,c)}$

Solución. a) Sea $n > 1$. Luego notemos que

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1),$$

lo que implica que $(a-1)|(a^n - 1)$. De lo anterior y como $a^n - 1$ es un número primo tenemos dos casos. O $a - 1 = 1$ o $a - 1 = a^n - 1$. Como $n > 1$ es imposible que $a - 1 = a^n - 1$ entonces se tiene que $a - 1 = 1$ y así $a = 2$.

Por otra parte, supongamos que $n = x \cdot y$, donde $1 < x, y < n$. Luego,

$$a^{xy} - 1 = (a^x - 1)(a^{x(y-1)} + a^{x(y-2)} + \cdots + a^x + 1),$$

lo que significa que $2^n - 1$ es un número compuesto y por lo tanto obtenemos una contradicción. De esta forma n es un número primo.

b) Sea $m > 1$ y $ac \equiv bc \mod m$. Entonces tenemos que $m|c(a-b)$, lo que significa que existe algún entero k tal que $mk = c(a-b)$. Ahora, para algunos $x, y \in \mathbb{Z}$ coprimos tenemos que $c = x\gcd(m,c)$ y que $m = y\gcd(m,c)$. Por lo tanto,

$$\begin{aligned} c(a-b) &= mk \\ x(a-b)\gcd(m,c) &= ky\gcd(m,c) \\ x(a-b) &= ky. \end{aligned}$$

De la última igualdad podemos asegurar que $x|ky$ y por lo tanto $x|k$ (ya que x e y son coprimos) y luego $k/x \in \mathbb{Z}$.

Finalmente $a - b$ es un múltiplo de y lo que implica que $a \equiv b \mod y$, pero $y = m/\gcd(m,c)$ y de esta forma

$$a \equiv b \mod \frac{m}{\gcd(m,c)}.$$

□

- P2a)
  - 1 punto por concluir los casos $a - 1 = 1$ y $a - 1 = a^n - 1$ y justificar que $a = 2$.
  - 2 puntos justificar que n es primo.
- P2b)
  - 1,5 puntos por encontrar $x, y \in \mathbb{Z}$ coprimos y asegurar que $x | k$.
  - 1,5 puntos por llegar a la conclusión correcta argumentando la multiplicidad de $a - b$ respecto a y.