Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas — 1' 2022

PAUTA TAREA 6

Pregunta 1

Pregunta 1.a

Demuestre que si a es un número impar, entonces $a^2 \equiv 1 \pmod 8$.

Solución: Existen varias formas de enfrentar este problema, procedemos a mostrar tres soluciones distintas.

1. **Solución 1:** División entera.

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

   $$a = 8 \cdot q + r \tag{1}$$

   con $0 \leq r < 8$. Es claro que podemos reescribir (1) como:

   $$a \equiv r \pmod 8.$$

   Elevando al cuadrado ambos lados de la congruencia obtenemos que $a^2 \equiv r^2 \pmod 8$, por lo que basta con demostrar que $r^2 \equiv 1 \pmod 8$. 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:

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

   Es fácil ver que:

   $$\begin{aligned} 1^2 &\equiv 1 \equiv 1 \pmod 8 & \qquad 3^2 &\equiv 9 \equiv 1 \pmod 8 \\ 5^2 &\equiv 25 \equiv 1 \pmod 8 & \qquad 7^2 &\equiv 49 \equiv 1 \pmod 8 \end{aligned}$$

   y así $a^2 \equiv r^2 \equiv 1 \pmod 8$. Vale la pena notar que una demostración equivalente sería hacer la división entera por 4 envés de por 8 en (1). $\square$

2. **Solución 2:** Método directo.

   Demostración. Sea $a \in \mathbb{Z}$ un número impar. Es decir, $a = 2k + 1$ para algún $k \in \mathbb{Z}$. Entonces,

   $$a \equiv 2k + 1 \pmod 8.$$

   Elevando al cuadrado ambos lados de la congruencia,

   $$\begin{aligned} a^2 &\equiv (2k+1)^2 \pmod 8 \\ &\equiv 4k^2 + 4k + 1 \pmod 8 \\ &\equiv 4\mathbf{k}(\mathbf{k}+\mathbf{1}) + 1 \pmod 8 \end{aligned}$$

Como tenemos k y $(k+1)$ como términos, es claro que uno de los dos debe ser par, sin pérdida de generalidad asuma que k es par, luego $k = 2q$ para algún $q \in \mathbb{Z}$ y entonces

$$\begin{aligned} a^2 &\equiv 4(2q)(2q+1) + 1 \pmod 8 \\ &\equiv 8 \cdot q(2q+1) + 1 \pmod 8 \\ &\equiv 1 \pmod 8 \end{aligned}$$

□

3. **Solución 3:** Inducción fuerte.

   Demostración. Considere el predicado

   $$P(n) := \text{si } n \text{ es impar entonces } n^2 \equiv 1 \pmod 8.$$

   Se procede mediante inducción fuerte.

   Caso base $(n = 1)$: $1^2 \equiv 1 \pmod 8$ trivialmente.

   Caso inductivo $(n > 1)$: Suponga que $P(k)$ se cumple para todo $k < n$. Si n es par se cumple $P(n)$ trivialmente. Sea n impar entonces. Es claro que $n-2$ también será impar, así que por HI:

   $$\begin{aligned} (n-2)^2 &\equiv 1 \pmod 8 \\ n^2 - 4n + 4 &\equiv 1 \pmod 8 \\ n^2 &\equiv 4n - 3 \pmod 8 \end{aligned}$$

   Como $n = 2k + 1$ para algún $k \in \mathbb{Z}$, reemplazando al lado derecho

   $$\begin{aligned} n^2 &\equiv 4(2k+1) - 3 \pmod 8 \\ &\equiv 8k + 1 \pmod 8 \\ &\equiv 1 \pmod 8 \end{aligned}$$

   Entonces, por el principio de inducción fuerte, $P(n)$ es cierto para todo $n \in \mathbb{N}$ (el enunciado no impone que $a \in \mathbb{Z}$, por lo que esto se considera como una solución válida). □

Dado lo anterior la atribución de puntajes es la siguiente:

1. **Solución 1:** División entera.

   (**2 Puntos**) Por aplicar la división por 8, llegando a la expresión (1).

   (**3 Puntos**) Por llegar a que a es congruente a r en módulo 8.

   (**4 Puntos**) Por obtener los posibles valores de r.

2. **Solución 2:** Método directo.

   (**2 Puntos**) Por llegar al valor de a^2 en función de k.

   (**3 Puntos**) Por notar de alguna manera que k o $(k+1)$ debe ser divisible por 2.

   (**4 Puntos**) Por una demostración correcta.

3. **Solución 3:** Inducción fuerte.

   (**2 Puntos**) Por solo enunciar el caso base y el caso inductivo.

   (**3 Puntos**) Por hacer el desarrollo del caso inductivo con errores.

   (**4 Puntos**) Por una demostración correcta.

Pregunta 1.b

Decimos que dos números $a, b \in \mathbb{Z} \setminus \{0\}$ son *primos relativos* si, y solo sí $\gcd(a, b) = 1$. Usando la identidad de Bézout, demuestre que si m es primo relativo con m_1, m_2, …, m_k, simultáneamente, entonces m es primo relativo con $m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

<u>Solución</u>:

Demostración. Dado que $\gcd(m, m_i) = 1$, aplicando la identidad de Bézout, tenemos que $\exists s_i, t_i \in \mathbb{Z}$ tal que

$$s_i \cdot m + t_i \cdot m_i = 1. \qquad \text{para } 1 \leq i \leq k \tag{2}$$

es claro que podemos reescribir (2) como $t_i m_i = 1 - s_i m$. Es decir, tenemos las siguientes k identidades:

$$\begin{aligned} t_1 \cdot m_1 &= 1 - s_1 \cdot m \\ t_2 \cdot m_2 &= 1 - s_2 \cdot m \\ &\vdots \\ t_k \cdot m_k &= 1 - s_k \cdot m \end{aligned}$$

Multiplicando todas estas identidades entre sí,

$$(t_1 \cdot t_2 \cdots t_k) \cdot (m_1 \cdot m_2 \cdots m_k) = (1 - s_1 \cdot m)(1 - s_2 \cdot m) \cdots (1 - s_k \cdot m). \tag{3}$$

Ahora, se podría desarrollar el lado derecho completamente, sin embargo es más útil notar lo siguiente: sólo se están multiplicando términos de la forma

$$(1 - s_i \cdot m)$$

lo que quiere decir que al distribuir vamos a obtener como primer término 1 y todo el resto de los términos van a ser factorizables por m. Es decir,

$$(1 - s_1 \cdot m)(1 - s_2 \cdot m) \cdots (1 - s_k \cdot m) = 1 - s' \cdot m. \qquad \text{para algún } s' \in \mathbb{Z}$$

Así, reemplazando en (3), se llega a que existen s' y $t' = t_1 \cdot t_2 \cdots t_k$ en $\mathbb{Z}$ tales que

$$s'm + t'(m_1 \cdot m_2 \cdots m_k) = 1 \tag{4}$$

es decir, $1 \in \langle m, m_1 \cdot m_2 \cdots m_k \rangle$. Como justamente

$$\gcd(m, m_1 m_2 \cdots m_k) = \min\{g \in \langle m, m_1 m_2 \cdots m_k \rangle \mid g > 0\},$$

al ser 1 el menor entero positivo, entonces $\gcd(m, m_1 m_2 \cdots m_k) = 1$ y m es primo relativo con $m_1 \cdot m_2 \cdots m_k$. □

<u>Solución alternativa</u>: Vale mencionar que una solución más elegante sería escribir las k identidades descritas en (2) como congruencias en módulo m:

$$\begin{aligned} \cancelto{0}{s_i \cdot m} + t_i \cdot m_i &\equiv 1 \pmod{m} \\ t_i \cdot m_i &\equiv 1 \pmod{m} \qquad \text{para } 1 \leq i \leq k. \end{aligned}$$

Luego multiplicando las k congruencias entre sí se obtiene

$$(t_1 \cdot t_2 \cdots t_k)(m_1 \cdot m_2 \cdots m_k) \equiv 1 \pmod{m}$$

que es equivalente a

$$(t_1 \cdot t_2 \cdots t_k)(m_1 \cdot m_2 \cdots m_k) = 1 + m \cdot s \qquad \text{para algún } s \in \mathbb{Z}.$$

Tomando $s' = -s$ se llega a (4) desde donde se puede completar la demostración de igual manera.

Dado lo anterior la atribución de puntajes es la siguiente:

(**2 Puntos**) Por una demostración correcta pero que no utiliza la identidad de Bézout. O bien, por expresar las k identidades de Bézout dadas por $\gcd(m, m_i)$ y que se debe encontrar un s' y un t' que cumplan con la identidad de Bezóut para que la afirmación sea correcta.

(**3 Puntos**) Por multiplicar las k identidades de Bézout y obtener el término $m_1 \cdot m_2 \cdots m_k$.

(**4 Puntos**) Por encontrar s' y t' que hacen verdadera la afirmación a demostrar.

Pregunta 2

Un homomorfismo desde $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ es una función $h : V_1 \to V_2$ tal que si $\{u, v\} \in E_1$, entonces $\{h(u), h(v)\} \in E_2$. Decimos que G_1 es homomorfo a G_2 si existe un homomorfismo desde G_1 a G_2.

Pregunta 2.a

Demuestre que, para todo $G = (V, E)$, una línea L_n con $n \geq 2$ es homomorfo a G si y solo si $E \neq \emptyset$.

Solución: Llamaremos $G = (V, E)$ y $L_n = (V', E')$ donde:

$$V' = \{0, ..., n-1\}$$

y

$$E' = \{\{i, i+1\}| \quad i = 0, 1, ..., n-2\} \quad n \geq 2$$

($\Rightarrow$) Sea $G = (V, E)$ grafo tal que L_n es homomorfo a G, es decir, existe:

$$h : \{0, ..., n-1\} \to V \quad \text{tal que}$$

$$\{i, j\} \in E' \to \{h(i), h(j)\} \in E \tag{1}$$

Por demostrar: $|E| \geq 1$

Dado que $n \geq 2$, L_n tiene al menos una arista, a saber:

$$\{0, 1\} \in E'$$

Luego, por 1 sabemos que

$$\{h(0), h(1)\} \in E$$

Y por lo tanto $|E| \geq 1$, lo que es precisamente lo que estábamos buscando demostrar.

Dado lo anterior la distribución de puntaje es la siguiente:

(**1 Punto**) Por hipótesis de existencia de h

(**1 Punto**) Por concluir usando 1

($\Leftarrow$) Sea G tal que $|E| \geq 1$
Como $|E| \geq 1$, existe al menos una arista $\{u, v\} \in E$
Luego, definimos $h : \{0, ..., n-1\} \to V$

$$h(i) = \begin{cases} u & \text{si} \quad i \mod 2 = 0 \\ v & \text{si} \quad i \mod 2 = 1 \end{cases}$$

Sea $\{i, j\} \in E'$ una arista cualquiera de L_n.
SPDG, $j = i + 1$ (por defición de L_n).
Luego,

$$\{h(i), h(j)\} = \{h(i), h(i+1)\}$$
$$\{h(i), h(j)\} = \{u, v\}$$

Como $\{u, v\} \in E$, se cumple que h es homomorfismo de L_n a G.
Por lo tanto, L_n es homomorfo a G.
Como hemos demostrado al doble implicancia en ambas direcciones, queda demostrada la expresión inicial.

Dado lo anterior la distribución de puntaje es la siguiente:

(**1 Punto**) Por definir h

(**1 Punto**) Por demostrar la proposición de las aristas

Pregunta 2.b

Demuestre que, para todo G, K_n es homomorfo a G si y solo si G contiene a K_n como subgrafo isomorfo.

<u>Solución:</u>

($\Rightarrow$) Sea $G = (V, E)$ tal que $K_n = (V_n, E_n)$ es homomorfo a él, es decir, existe $h : V_n \to V$ tal que:

$$\{u, v\} \in E_n \to \{h(u), h(v)\} \in E \tag{1}$$

Queremos demostrar que existe $G' \subseteq G$, $G' = (V', E')$ subgrafo de G tal que K_n es isomorfo a G'.

Definimos $G' = (V', E')$ donde:

- $V' = img(h)$
- $E' = \{e \in E \mid \ \mid e \cap img(h) \mid = 2\}$

En otras palabras, G' tiene como vértices a las posibles imágenes de h y mantiene las aristas entre estos vértices en G. Demostraremos que $f : K_n \to V'$ dada por:

$$f(u) = h(u)$$

es biyectiva y cumple con ser isomorfismo.

- Sobreyectiva: Como $V' = img(h)$, f es sobreyectiva.
- Inyectiva: Sean $u \neq v$. Demostraremos que $f(u) \neq h(v)$.

  Como $u \neq s$, $\{u, v\} \in E_n$ (K_n es clique). Luego, por (1), tenemos que $\{h(u), h(v)\} \in E$ y, por lo tanto, $f(u) = h(u) \neq h(v) = f(v)$.
- Dada $\{u, v\} \in E_n$, tenemos:
  $$\{f(u, f(v)\} = \{h(u), h(v)\} \in E'$$
  Como toda arista está en E_n:
  $$\{u, v\} \in E_n \Leftrightarrow \{f(u), f(v)\} \in E'$$
  Entonces, f es isomorfismo.

  (**1 Punto**) Por definir f

  (**1 Punto**) Por probar que es isomorfismo entre K_n y G'

($\Leftarrow$) Sea G tal que existe $G' = (V', E')$ subgrafo $G' \subseteq G$ tal que $K_n \cong G'$. Es decir, existe isomorfismo $f : V_n \to V'$ donde:

$$\{u, v\} \in E_n \leftrightarrow \{f(u), f(v)\} \tag{2}$$

Queremos demostrar que existe el homomorfismo h de K_n a G. Definimos $h : V_n \to V$ como:

$$h(u) = f(u)$$

Sea $\{u, v\} \in E_n$. Podemos decir que, por (2):

$$\{h(u), h(v)\} = \{f(u), f(v)\} \in E'$$

Como $E' \subseteq E$, $\{h(u), h(v)\} \in E$. Por lo tanto, h es homomorfismo de K_n a G.

Dado lo anterior la distribución de puntaje es la siguiente:

(**1 Punto**) Por definir h

(**1 Punto**) Por demostrar propiedad de aristas

Importante: Si se obtiene 1 punto según considerando la distribución de puntaje anterior, se asignan 0 puntos. Esto porque el mínimo puntaje a obtener en las tareas es 2 puntos.