



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE  
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN  
IIC1253 - MATEMÁTICAS DISCRETAS

## Examen

10 de julio de 2024

**Preguntas e incisos en blanco** se evalúan con nota 1.5 proporcional.

### Pregunta 1 - Verdadero/Falso

Para cada uno de los siguientes enunciados, indique si el enunciado es verdadero (V) o falso (F). Justifique su respuesta.

1. Si  $A$  es un conjunto enumerable, entonces  $A \times A$  es un conjunto no enumerable.
2. Si  $G = (V, E)$  es un grafo no dirigido, entonces  $E = E^{-1}$ .
3. Sea  $P$  un conjunto de proposiciones y sean  $\varphi$  y  $\psi$  fórmulas en  $\mathcal{L}(P)$ . Si  $\psi$  es una tautología, entonces  $\varphi \rightarrow \psi$  es una tautología.
4. Para todo conjunto  $A$ , existe una única relación que es a la vez una relación de orden parcial y una relación de equivalencia.
5. Si  $p$  es primo, entonces la relación  $\sim$ , definida sobre  $\mathbb{N}$  por  $a \sim b$  si y solo si  $a^p \equiv_p b$ , es de equivalencia.
6. Dado un conjunto  $P$  de  $n$  variables proposicionales, el conjunto cociente  $\mathcal{L}(P)/\equiv$  tiene exactamente  $2^{2^n}$  elementos.

### Solución

1. F.

Dado que  $A$  es enumerable, podemos enumerar sus elementos como una lista infinita  $A = \{a_0, a_1, a_2, \dots\}$ . Luego, se puede hacer una tabla infinita como en la demostración de que  $\mathbb{Z}$  es enumerable, poniendo los elementos de  $A$  en cada eje de una tabla y luego recorrerla por las diagonales.

...	...	...	...	...
$a_2$	$(a_0, a_2)$	$(a_1, a_2)$	$(a_2, a_2)$	...
$a_1$	$(a_0, a_1)$	$(a_1, a_1)$	$(a_2, a_1)$	...
$a_0$	$(a_0, a_0)$	$(a_1, a_0)$	$(a_2, a_0)$	...
	$a_0$	$a_1$	$a_2$	...

De esta manera, podemos construir una lista infinita con los elementos de  $A \times A$ :

$$A \times A = \{(a_0, a_0), (a_1, a_0), (a_0, a_1), (a_2, a_0), (a_1, a_1), (a_0, a_2), \dots\}$$

Con lo que concluimos que  $A \times A$  es enumerable.

2. V.

Si  $G = (V, E)$  es un grafo no dirigido, entonces la relación binaria  $E$  sobre  $V$  es simétrica. Si  $(a, b) \in E$ , entonces por simetría  $(b, a) \in E$ , y por definición de relación inversa,  $(a, b) \in E^{-1}$ . Como  $(a, b)$  es arbitrario en  $E$ , se cumple para todos los elementos de  $E$ , luego  $E \subseteq E^{-1}$ . La demostración de que  $E^{-1} \subseteq E$  es idéntica, pues  $E = (E^{-1})^{-1}$ . Luego,  $E = E^{-1}$ .

3. V.

Sea  $\sigma$  una valuación. Si  $\sigma(\varphi) = 0$ , entonces  $\sigma(\varphi \rightarrow \psi) = 1$ , mientras que si  $\sigma(\varphi) = 1$ , entonces  $\sigma(\varphi \rightarrow \psi) = \sigma(\psi) = 1$  pues  $\psi$  es una tautología. Dado que  $\sigma$  es arbitraria, concluimos que  $\sigma(\varphi \rightarrow \psi) = 1$  siempre, es decir, que  $\varphi \rightarrow \psi$  es una tautología.

4. V.

Si una relación es orden parcial y relación de equivalencia, entonces es refleja, transitiva, y además simétrica y antisimétrica a la vez. Esto último solo es posible para la relación identidad. Para ver esto, sean  $a, b \in A$  tales que  $aRb$ . Por simetría  $bRa$  y por antisimetría, como  $aRb$  y  $bRa$ , tenemos que  $a = b$ . Luego solo los elementos iguales se relacionan entre sí, es decir, la relación debe ser la identidad, que es a la vez refleja y transitiva.

5. V.

- **Refleja.** Es inmediato del teorema de Fermat.
- **Simétrica.** Sean  $a, b \in \mathbb{N}$  tales que  $a \sim b$ . Por definición, tenemos que  $a^p \equiv_p b$ . Por teorema de Fermat, tenemos que  $a^p \equiv_p a$  y  $b^p \equiv_p b$ . Luego por simetría y transitividad de la equivalencia modular, tenemos que  $b^p \equiv_p b \equiv_p a^p \equiv_p a$ . Como  $a, b$  eran arbitrarios, concluimos que la relación es simétrica.
- **Transitiva.** Sean  $a, b, c \in \mathbb{N}$  tales que  $a \sim b$  y  $b \sim c$ . Luego  $a^p \equiv_p b$  y  $b^p \equiv_p c$ . Por teorema de Fermat, tenemos además que  $b \equiv_p b^p$ , luego por transitividad de la equivalencia módulo, concluimos que  $a^p \equiv_p c$ . Como  $a, b, c$  eran arbitrarios, concluimos que la relación es transitiva.

Luego,  $\sim$  es una relación refleja, simétrica y transitiva, por lo que es de equivalencia.

6. V.

Cada clase en  $\mathcal{L}(P)$  corresponde a una clase de fórmulas de  $n$  variables proposicionales equivalentes entre sí, y por lo tanto, que comparten la misma tabla de verdad. La cantidad de clases corresponde entonces con la cantidad de tablas de verdad distintas para  $n$  variables proposicionales, lo que corresponde a  $2^{2^n}$ .

### Pauta (6 pts.)

1 pto por cada respuesta correcta y correctamente justificada. Puntajes parciales si la respuesta es correcta y la demostración tiene detalles menores, a criterio del corrector.

### Pregunta 2 - Conjuntos

Sea  $X$  un conjunto no vacío. Decimos que  $\mathcal{T} \subseteq \mathcal{P}(X)$  es una topología sobre  $X$  si cumple

- $\emptyset \in \mathcal{T}$ .
  - $X \in \mathcal{T}$ .
  - Si  $\{A_i \mid A_i \subseteq X \text{ e } i \geq 1\} \subseteq \mathcal{T}$ , entonces  $\bigcup_{i \geq 1} A_i \in \mathcal{T}$ .
  - Si  $A_1, \dots, A_n \in \mathcal{T}$ , entonces  $\bigcap_{i=1}^n A_i \in \mathcal{T}$ .
- (a) (2 ptos.) Dé un ejemplo de conjunto  $X$  y una topología  $\mathcal{T}$  sobre  $X$ . Demuestre que efectivamente satisface la definición.
- (b) (4 ptos.) Sea  $Y \subseteq X$  y  $\mathcal{T}$  una topología sobre  $X$ . Sea  $S$  el conjunto definido por

$$S := \{H \subseteq Y \mid H = G \cap Y, \text{ para algún } G \in \mathcal{T}\}.$$

Demuestre que  $S$  es una topología sobre  $Y$ .

### Solución

- (a) Podemos considerar  $X$  arbitrario no vacío y la topología  $\mathcal{T} = \{\emptyset, X\}$ , por ejemplo  $X = \{0\}$  y  $\mathcal{T} = \{\emptyset, X\}$ . Demostremos que satisface la definición:
- $\emptyset \in \mathcal{T}$ : Trivialmente por la definición de  $\mathcal{T}$ .
  - $X \in \mathcal{T}$ : Trivialmente por la definición de  $\mathcal{T}$ .
  - Si  $\{A_i \mid A_i \subseteq X \text{ e } i \geq 1\} \subseteq \mathcal{T}$ , entonces  $\bigcup_{i \geq 1} A_i \in \mathcal{T}$ : Los únicos subconjuntos de  $\mathcal{T}$  son:
    - $\emptyset$ : En este caso, la unión es vacía y ya vimos que pertenece a  $\mathcal{T}$ .
    - $\{\emptyset\}$ : En este caso, la unión también es vacía e igualmente vimos que  $\emptyset$  pertenece a  $\mathcal{T}$ .
    - $\{X\}$ : En este caso, la unión es exactamente  $X$ , que ya vimos que pertenece a  $\mathcal{T}$ .
    - $\{\emptyset, X\}$ : En este caso, la unión también es exactamente  $X$ , que ya vimos que pertenece a  $\mathcal{T}$ .
  - Si  $A_1, \dots, A_n \in \mathcal{T}$ , entonces  $\bigcap_{i=1}^n A_i \in \mathcal{T}$ : Los únicos subconjuntos de  $\mathcal{T}$  son:
    - $\emptyset$ : En este caso, la intersección es vacía y ya vimos que pertenece a  $\mathcal{T}$ .
    - $\{\emptyset\}$ : En este caso, la intersección también es vacía e igualmente vimos que  $\emptyset$  pertenece a  $\mathcal{T}$ .

- $\{X\}$ : En este caso, la intersección es exactamente  $X$ , que ya vimos que pertenece a  $\mathcal{T}$ .
- $\{\emptyset, X\}$ : En este caso, la intersección es exactamente  $\emptyset$ , que ya vimos que pertenece a  $\mathcal{T}$ .

**Observación:** A esta topología se le llama la topología trivial. Otras topologías más interesantes que pueden ser esperadas para este ejercicio incluyen la topología discreta, donde para  $X$  arbitrario no vacío, definimos  $\mathcal{T} = \mathcal{P}(X)$ ; la topología dada por  $X$  arbitrario no vacío, y para cualquier  $A \subsetneq X$ ,  $\mathcal{T} = \{\emptyset, A, X\}$ ; los intervalos abiertos en  $\mathcal{R}$ , donde  $\mathcal{X} = \mathbb{R}$  y  $\mathcal{T} = \{I_{a,b} \mid a \in \mathbb{R}, b \in \mathbb{R} \text{ y } a < b\}$  donde  $I_{a,b} = \{x \in \mathbb{R} \mid a < x < b\}$ .

(b) Debemos mostrar 4 cosas nuevamente:

- $\emptyset \in S$

Como  $\mathcal{T}$  es una topología, sabemos que  $\emptyset \in \mathcal{T}$ , y como  $\emptyset \cap Y = \emptyset$ , por definición de  $S$ , obtenemos que  $H = \emptyset \cap Y = \emptyset \in S$ .

- $Y \in S$

Como  $\mathcal{T}$  es una topología, sabemos que  $X \in \mathcal{T}$ , y como  $Y \subseteq X$ , tenemos que  $X \cap Y = Y$ . Luego, por definición de  $S$ , obtenemos que  $H = Y = X \cap Y \in S$ .

- Si  $\{A_i \mid A_i \subseteq Y \text{ e } i \geq 1\} \subseteq S$ , entonces  $\bigcup_{i \geq 1} A_i \in S$

Sea  $\{A_i \mid A_i \subseteq Y \text{ e } i \geq 1\} \subseteq S$ . Luego, por definición de  $S$ , para cada  $i \geq 1$  existe  $G_i \in \mathcal{T}$  que cumple que  $A_i = G_i \cap Y$ . Como  $\mathcal{T}$  es una topología y  $\{G_i \mid G_i \subseteq X \text{ e } i \geq 1\} \subseteq \mathcal{T}$ , notamos que  $G := \bigcup_{i \geq 1} G_i \in \mathcal{T}$ .

Nuevamente, por definición de  $S$ , lo anterior nos permite concluir que  $G \cap Y \in S$ . Notemos entonces que

$$\bigcup_{i \geq 1} A_i = \bigcup_{i \geq 1} (G_i \cap Y) = \left( \bigcup_{i \geq 1} G_i \right) \cap Y = G \cap Y$$

Por lo tanto,  $\bigcup_{i \geq 1} A_i \in S$ , que es lo queríamos demostrar.

- Si  $A_1, \dots, A_n \in \mathcal{T}$ , entonces  $\bigcap_{i=1}^n A_i \in \mathcal{T}$

Sean  $A_1, \dots, A_n \in \mathcal{T}$ . Luego, por definición de  $S$ , para cada  $i \in \{1, \dots, n\}$ , existe  $G_i \in \mathcal{T}$  tal que  $A_i = G_i \cap Y$ . Como  $\mathcal{T}$  es topología y  $G_1, \dots, G_n \in \mathcal{T}$ , notamos que  $G := \bigcap_{i=1}^n G_i \in \mathcal{T}$ .

Nuevamente, por definición de  $S$ , lo anterior nos permite concluir que  $G \cap Y \in S$ . Notemos entonces que

$$\bigcap_{i=1}^n A_i = \bigcap_{i=1}^n (G_i \cap Y) = \left( \bigcap_{i=1}^n G_i \right) \cap Y = G \cap Y$$

Por lo tanto,  $\bigcap_{i=1}^n A_i \in S$ , que es lo que queríamos demostrar.

### Pauta (6 pts.)

- El ejemplo debe ser válido o son 0 puntos. Luego, 1 pt. por demostrar cada propiedad correctamente.
- 1 pt. por cada propiedad correctamente demostrada.

Puntajes parciales a criterio del corrector cuando las demostraciones tienen detalles menores.

### Pregunta 3 - Algoritmos

Una fórmula proposicional  $\varphi$  está en  $k$ -DNF si está en DNF y cada conjunción tiene exactamente  $k$  literales. Por ejemplo, la fórmula  $(p \wedge \neg q \wedge \neg q) \vee (\neg p \wedge q \wedge p)$  está en 3-DNF. Denotamos por  $C_i$  a la  $i$ -ésima cláusula de  $\varphi$  y por  $\ell_{ij}$  al  $j$ -ésimo literal de  $C_i$ .

Considere el siguiente algoritmo para determinar si una fórmula en  $k$ -DNF es satisfactible.

[H] Fn: Letlet DNFSATAlgoDNF-SAT Inputinput Outputoutput

$(C_1 \vee C_2 \vee \dots \vee C_m, k) \ i \in \{1, \dots, m\} \ sat \leftarrow \text{TRUE} \ j \in \{1, \dots, k-1\} \ t \in \{j+1, \dots, k\} \ \ell_{mj} \text{ y } \ell_{mt}$   
son complementarios  $sat \leftarrow \text{FALSE} \quad sat \text{ TRUE}$

FALSE

Definimos la función  $T(n)$  como el número de ejecuciones de la línea 5 de DNF-SAT cuando se llama para  $\varphi$  con  $n$  literales en total (contando repetidos). Determine justificadamente una expresión en notación  $\mathcal{O}$  para  $T(n)$ .

### Solución

En primer lugar, obtendremos una expresión para la función  $T$  en términos de  $m$  y  $k$  (dado que  $n = mk$ ). Para esto, es posible realizar un análisis de mejor o peor caso. Mostraremos ambas opciones a continuación. Para ambas se considera un input con  $mk$  literales individuales.

- (a) El peor caso del algoritmo ocurre cuando la fórmula no es satisfactible. Esto significa que el algoritmo ejecuta todas las iteraciones de los bloques for en el código, obteniendo el máximo número de ejecuciones de la línea 5. La siguiente expresión permite calcular de forma explícita

dicho número:

$$\begin{aligned}
T(m, k) &= \sum_{i=1}^m \sum_{j=1}^{k-1} \sum_{t=j+1}^k 1 \\
&= \sum_{i=1}^m \sum_{j=1}^{k-1} (k - j) \\
&= \sum_{i=1}^m \left( \sum_{j=1}^{k-1} k - \sum_{j=1}^{k-1} j \right) \\
&= \sum_{i=1}^m \left( k(k-1) - \frac{(k-1)k}{2} \right) \\
&= \sum_{i=1}^m \frac{(k-1)k}{2} \\
&= m \frac{(k-1)k}{2} \\
&= \frac{mk^2}{2} - \frac{mk}{2}
\end{aligned}$$

Con esto, concluimos que en el peor caso,  $T(m, k) \in \mathcal{O}(mk^2)$ .

- (b) El mejor caso del algoritmo ocurre cuando la primera conjunción revisada por el algoritmo, i.e.  $C_1$ , no tiene literales complementarios. En tal caso, el for exterior (variable  $i$ ) solo toma valor  $i = 1$ , mientras que los for interiores completan una iteración completa. Es decir, y recurriendo a cálculos realizados en el peor caso, se obtiene

$$\begin{aligned}
T(m, k) &= \sum_{i=1}^1 \sum_{j=1}^{k-1} \sum_{t=j+1}^k 1 \\
&= \sum_{i=1}^1 \frac{(k-1)k}{2} \\
&= \frac{(k-1)k}{2} \\
&= \frac{k^2}{2} - \frac{k}{2}
\end{aligned}$$

Con esto, concluimos que en el mejor caso,  $T(m, k) \in \mathcal{O}(k^2)$ .

### Pauta (6 pts.)

- 1 punto por indicar qué tipo de ejecución se considerará (máximo número de iteraciones o un caso más favorable).

- 3 puntos por deducir una expresión para la función  $T$ .
- 2 puntos por deducir una expresión asintótica para  $T$ .

Puntajes parciales y soluciones alternativas a criterio del corrector.

#### Pregunta 4 - Grafos y relaciones de orden

Dado un grafo  $G = (V, E)$ , decimos que un grafo  $G' = (V', E')$  es subgrafo isomorfo de  $G$  si y solo si se cumple que existe un grafo  $H = (V_H, E_H)$  tal que:

- $H$  es subgrafo de  $G$ , es decir,  $V_H \subseteq V$ ,  $E_H \subseteq E$  y  $E_H \subseteq V_H \times V_H$ .
  - $H$  es isomorfo a  $G'$
- (a) (3 ptos.) Demuestre que si  $G_1$  es subgrafo isomorfo de  $G_2$  y  $G_2$  es subgrafo isomorfo de  $G_1$ , entonces  $G_1 \cong G_2$ .
- (b) (3 ptos.) Sea  $\mathcal{G}$  el conjunto de todos los grafos y sea  $A = \mathcal{G}/\cong$ . En otras palabras,  $A$  es el conjunto cociente del conjunto de grafos bajo la relación de isomorfismo. Definimos entonces la relación  $\preceq \subseteq A^2$  como

$$[G_1]_{\cong} \preceq [G_2]_{\cong} \text{ si y solo si } G_1 \text{ es subgrafo isomorfo de } G_2$$

Demuestre que  $(A, \preceq)$  es un orden parcial.

#### Parte (a)

Dado que  $G_1$  es subgrafo isomorfo de  $G_2$ , existe  $H_1$  subgrafo de  $G_2$  talque  $G_1 \cong H_1$ .

$H_1$  subgrafo de  $G_2 \Rightarrow V(H_1) \subseteq V(G_2)$  y  $E(H_1) \subseteq E(G_2)$

Por lo que se cumple  $|V(H_1)| \leq |V(G_2)|$  (1) y  $|E(H_1)| \leq |E(G_2)|$  (2)

$$G_1 \cong H_1 \Rightarrow \exists f: V(G_1) \rightarrow V(H_1) \text{ biyectiva, tal que } (e_1, e_2) \in E(G_1) \Rightarrow (f(e_1), f(e_2)) \in E(H_1)$$

$$G_1 \cong H_1 \Rightarrow |V(G_1)| = |V(H_1)| \text{ por biyectividad (3)}$$

$$(1) \text{ y } (3) \Rightarrow |V(G_1)| \leq |V(G_2)| \text{ (5)}$$

$$G_1 \cong H_1 \Rightarrow |V(G_1)| = |V(H_1)| \text{ por biyectividad (4)}$$

Luego, se cumple que  $|E(G_1)| = |E(H_1)|$  (4) ya que  $h : (e_1, e_2) \rightarrow (f(e_1), f(e_2))$  biyección por propiedad de isomorfismo.

$$(2) \text{ y } (4) \Rightarrow |E(G_1)| \leq |E(G_2)|, (6)$$

Por el mismo razonamiento, dado que  $G_2$  es subgrafo de  $G_1$ ,

$$|V(G_2)| \leq |V(G_1)| \text{ (7)}$$

$$|E(G_2)| \leq |E(G_1)| \quad (8)$$

Luego, considerando lo anterior planteado:

$$(5) \text{ y } (7) \Rightarrow |V(G_1)| = |V(G_2)| \quad (9)$$

$$(6) \text{ y } (8) \Rightarrow |E(G_1)| = |E(G_2)| \quad (10)$$

$$(3) \text{ y } (9) \Rightarrow |V(G_2)| = |V(H_1)| \text{ Dado que } V(H_1) \subseteq V(G_2) \rightarrow V(H_1) = V(G_2)$$

$$(4) \text{ y } (10) \Rightarrow |E(G_2)| = |E(H_1)|$$

Dado que  $E(H_1) \subseteq E(G_2)$ , tenemos que  $E(H_1) = E(G_2)$

Entonces considerando  $H_1 = G_2$  y que existe isomorfismo entre  $G_1$  y  $G_2 \rightarrow G_1 \cong G_2 \square$

### Parte (b)

Para demostrar que  $(A, \preceq)$  es un orden parcial, debemos probar que la relación  $\preceq$  es reflexiva, antisimétrica y transitiva.

**Reflexividad:** Para cualquier grafo  $G$ ,  $G$  es subgrafo de sí mismo. Por lo tanto,  $[G]_{\cong} \preceq [G]_{\cong}$ .

**Antisimetría:** Supongamos que  $[G_1]_{\cong} \preceq [G_2]_{\cong}$  y  $[G_2]_{\cong} \preceq [G_1]_{\cong}$ . Esto significa que  $G_1$  es subgrafo isomorfo de  $G_2$  y  $G_2$  es subgrafo isomorfo de  $G_1$ . Por la parte (a) de este problema, sabemos que esto implica que  $G_1 \cong G_2$ . Por lo tanto,  $[G_1]_{\cong} = [G_2]_{\cong}$ .

**Transitividad:** Supongamos que  $[G_1]_{\cong} \preceq [G_2]_{\cong}$  y  $[G_2]_{\cong} \preceq [G_3]_{\cong}$ . Esto significa que  $G_1$  es subgrafo isomorfo de  $G_2$  y  $G_2$  es subgrafo isomorfo de  $G_3$ . Existen grafos  $H_1$  y  $H_2$  tales que:

- $H_1$  es subgrafo de  $G_2$  y  $H_1 \cong G_1$ .
- $H_2$  es subgrafo de  $G_3$  y  $H_2 \cong G_2$ .

Dado que  $H_1 \cong G_1$  y  $H_2 \cong G_2$ , y considerando que  $H_1$  es subgrafo de  $H_2$ , podemos concluir que  $G_1$  es subgrafo isomorfo de  $G_3$ . Por lo tanto,  $[G_1]_{\cong} \preceq [G_3]_{\cong}$ .

Puesto que la relación  $\preceq$  es reflexiva, antisimétrica y transitiva,  $(A, \preceq)$  es un orden parcial.

### Puntaje:

- (a)
  - 1 punto por usar propiedades de biyecciones.
  - 1.5 por componer biyecciones.
  - 0.5 por concluir.
- (b)
  - 1 punto por cada propiedad.

### Pregunta 5 - Teoría de números

- (a) (3 ptos.) Determine si existe solución para cada una de las siguientes congruencias lineales. En caso que exista, encuentre su solución.

(I)  $8x \equiv 6 \pmod{19}$

(II)  $21x \equiv 12 \pmod{35}$

- (b) (3 ptos.) Demuestre que todos los elementos de  $\mathbb{Z}_p \setminus \{0\}$  tienen inverso multiplicativo en módulo  $p$ , si y solo si,  $p$  es primo.



### Parte (a)

1.  $x \equiv 15 \pmod{19}$
2. No tiene solución ya que  $(21, 35) = 7$ .

### Parte (b)

Supongamos que  $p$  es un número primo. Consideremos un elemento  $a \in \mathbb{Z}_p \setminus \{0\}$ . Como  $p$  es primo, el máximo común divisor de  $a$  y  $p$  es 1, es decir,  $\gcd(a, p) = 1$ .

El teorema de Bézout nos dice que existen enteros  $x$  y  $y$  tales que:

$$ax + py = 1$$

Tomando esta congruencia módulo  $p$ , obtenemos:

$$ax \equiv 1 \pmod{p}$$

Por lo tanto,  $x$  es el inverso multiplicativo de  $a$  en  $\mathbb{Z}_p$ . Esto demuestra que cada elemento  $a \in \mathbb{Z}_p \setminus \{0\}$  tiene un inverso multiplicativo cuando  $p$  es primo.

Supongamos que todos los elementos de  $\mathbb{Z}_p \setminus \{0\}$  tienen inverso multiplicativo en módulo  $p$ . Supongamos, por contradicción, que  $p$  no es primo. Entonces,  $p$  se puede factorizar como  $p = ab$  con  $1 < a, b < p$ . Consideremos el elemento  $a \in \mathbb{Z}_p \setminus \{0\}$ . Si  $a$  tiene un inverso multiplicativo, entonces existe un  $x \in \mathbb{Z}_p$  tal que:

$$ax \equiv 1 \pmod{p}$$

Esto implica que hay un entero  $k$  tal que:

$$ax = 1 + kp$$

Puesto que  $p = ab$ , podemos escribir:

$$ax = 1 + kab$$

Como  $a$  divide  $p$  (ya que  $p = ab$ ), la ecuación anterior implica que  $a$  divide 1, lo cual es una contradicción porque  $a > 1$ .

Por lo tanto, nuestra suposición de que  $p$  no es primo debe ser falsa. Así,  $p$  debe ser primo.

### Puntaje:

- 1.5 por cada congruencia en (a).
- 1.5 por cada dirección en (b).