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

Examen

8 de julio de 2024
Profesores: Nicolás Alvarado - Pedro Bahamondes - Sebastián Bugedo

Instrucciones

- La duración del examen es de 2:30 horas.
- Durante la evaluación **no puede** hacer uso de sus apuntes o slides del curso.
- Rellene sus datos en cada hoja de respuesta que utilice.
- Cada pregunta debe responderse en hojas separadas.
- Entregue al menos una hoja por pregunta.
    - Si entrega la pregunta **completamente en blanco**, tiene nota mínima 1.5 en vez de 1.0 en la pregunta entregada. **Esto solo aplica a preguntas completas**.
- Escriba sus respuestas con lápiz pasta. Por el uso de lápiz mina usted pierde el derecho a recorreción.
- Una vez terminado el examen, tendrá 10 minutos para escanear sus respuestas. Se habilitará un buzón para cada sección en el módulo de tareas donde podrá subir uno o más archivos en formatos de imagen o pdf con sus respuestas. En caso de que deje alguna pregunta en blanco, también es necesario entregarla en el buzón. Debe preocuparse de que la copia digital sea legible. Se recomienda el uso de algún software de escaneo como CamScanner o la app de Google Drive.

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 φ y ψ fórmulas en $\mathcal{L}(P)$. Si ψ es una tautología, entonces $\varphi \to \psi$ 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 cuociente $\mathcal{L}(P)/\equiv$ tiene exactamente 2^{2^n} elementos.

Solución

1. F.

   Dado que A es enumerable, podemos enumerar sus elementos como una lista infinita $A = \{a_0, a_1, a_2, ...\}$. 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 $A \times A$:

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

   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 σ una valuación. Si $\sigma(\varphi) = 0$, entonces $\sigma(\varphi \to \psi) = 1$, mientras que si $\sigma(\varphi) = 1$, entonces $\sigma(\varphi \to \psi) = \sigma(\psi) = 1$ pues ψ es una tautología. Dado que σ es arbitraria, concluimos que $\sigma(\varphi \to \psi) = 1$ siempre, es decir, que $\varphi \to \psi$ 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 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 $b^p \equiv_p b \equiv_p a^p \equiv a$. 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

- $\varnothing \in \mathcal{T}$.
- $X \in \mathcal{T}$.
- 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 $A_1, \ldots, A_n \in \mathcal{T}$, 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 $\mathcal{T} = \{\varnothing, X\}$, por ejemplo $X = \{0\}$ y $\mathcal{T} = \{\varnothing, X\}$. Demostremos que satisface la definición:

- $\varnothing \in \mathcal{T}$: Trivialmente por la definición de $\mathcal{T}$.
- $X \in \mathcal{T}$: Trivialmente por la definición de 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:
  - $\varnothing$: En este caso, la unión es vacía y ya vimos que pertenece a $\mathcal{T}$
  - $\{\varnothing\}$: En este caso, la unión también es vacía e igualmente vimos que $\varnothing$ pertenece a $\mathcal{T}$.
  - $\{X\}$: En este caso, la unión es exactamente X, que ya vimos que pertenece a $\mathcal{T}$.
  - $\{\varnothing, X\}$: En este caso, la unión también es exactamente X, que ya vimos que pertenece a $\mathcal{T}$.

- Si $A_1, ..., A_n \in \mathcal{T}$, entonces $\bigcap_{i=1}^{n} A_i \in \mathcal{T}$: Los únicos subconjuntos de $\mathcal{T}$ son:
  - $\varnothing$: En este caso, la intersección es vacía y ya vimos que pertenece a $\mathcal{T}$
  - $\{\varnothing\}$: En este caso, la intersección también es vacía e igualmente vimos que $\varnothing$ pertenece a $\mathcal{T}$.
  - $\{X\}$: En este caso, la intersección es exactamente X, que ya vimos que pertenece a $\mathcal{T}$.
  - $\{\varnothing, X\}$: En este caso, la intersección es exactamente $\varnothing$, 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 $A \subsetneq X$, $\mathcal{T} = \{\varnothing, A, X\}$; los intervalos abiertos en $\mathcal{R}$, donde $\mathcal{X} = \mathbb{R}$ y $\mathcal{T} = \{I_{a,b} \mid a \in \mathbb{R}, b \in \mathbb{R} \text{ y } a \leq b\}$ donde $I_{a,b} = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

(b) Debemos mostrar 4 cosas nuevamente:

- $\varnothing \in S$

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

  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 $\{G_i | G_i \subseteq X \text{ e } i \geq 1\} \subseteq \mathcal{T}$, notamos que $G := \bigcup_{i \geq 1} G_i \in \mathcal{T}$.

  Nuevamente, por definición de S, lo anterior nor 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 $A_1, ..., A_n \in \mathcal{T}$, entonces $\bigcap_{i=1}^{n} A_i \in \mathcal{T}$

  Sean $A_1, ..., A_n \in \mathcal{T}$. Luego, por definición de S, para cada $i \in \{1, ..., n\}$, existe $G_i \in \mathcal{T}$ tal que $A_i = G_i \cap Y$. Como $\mathcal{T}$ es topología y $G_1, ..., G_n \in \mathcal{T}$, 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 φ 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 φ y por ℓ_{ij} al j-ésimo literal de C_i.

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

```
DNF-SAT(C_1 ∨ C_2 ∨ ··· ∨ C_m, k):
1   for i ∈ {1, ..., m} do
2       sat ← TRUE
3       for j ∈ {1, ..., k − 1} do
4           for t ∈ {j + 1, ..., k} do
5               if ℓ_mj y ℓ_mt son complementarios then
6                   sat ← FALSE
7       if sat then
8           return TRUE
9   return FALSE
```

Definimos la función $T(n)$ como el número de ejecuciones de la línea 5 de `DNF-SAT` cuando se llama para φ 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 cuociente 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.

Solución

(a) Sean G_1 y G_2 grafos tales que G_1 es subgrafo isomorfo de G_2 y G_2 es subgrafo isomorgo de G_1. Por simplicidad, en lo que sigue, si G es un grafo denotaremos por $V(G)$ a su conjunto de vértices y por $E(G)$ a su conjunto de aristas.

Dado que G_1 es subgrafo isomorfo de G_2, existe H_1 subgrafo de G_2 tal que $G_1 \cong H_1$. Como H_1 es subgrafo de G_2, tenemos que $V(H_1) \subseteq V(G_2)$ y $E(H_1) \subseteq E(G_2)$. En particular, esto implica que

$$|V(H_1)| \leq |V(G_2)| \tag{1}$$

y

$$|E(H_1)| \leq |E(G_2)| \tag{2}$$

Igualmente, como $G_1 \cong H_1$, tenemos que existe una función $f : V(G_1) \to V(H_1)$ biyectiva y tal que $(e_1, e_2) \in E(G_1)$ si y solo si $(f(e_1), f(e_2)) \in E(H_1)$.

Notemos entonces que dado que f es biyectiva, se tiene que

$$|V(G_1)| = |V(H_1)| \tag{3}$$

Por lo demás, la propiedad de isomorfismo nos permite definir la biyección $h : E(G_1) \to E(H_1)$ definida por $h((e_1, e_2)) = (f(e_1), f(e_2))$, por lo que también se tiene que

$$|E(G_1)| = |E(H_1)| \tag{4}$$

Juntando (1) y (3), obtenemos:

$$|V(G_1)| \leq |V(G_2)| \tag{5}$$

Por otra parte, juntando (2) y (4), obtenemos:

$$|E(G_1)| \leq |E(G_2)| \tag{6}$$

Por el mimso razonamiento, dado que G_2 también es subgrafo de G_1, tenemos que

$$|V(G_2)| \leq |V(G_1)| \tag{7}$$
$$|E(G_2) \leq |E(G_1)| \tag{8}$$

Luego, considerando lo anterior planteado:

$$(5) \text{ y } (7) \Rightarrow |V(G_1)| = |V(G_2)| \tag{9}$$
$$(6) \text{ y } (8) \Rightarrow |E(G_1)| = |E(G_2)| \tag{10}$$

Juntando ahora (3) y (9) obtenemos que $|V(H_1)| = |V(G_2)|$. Como además $V(H_1) \subseteq V(G_2)$, esto nos permite concluir que $V(H_1) = V(G_2)$.

Del mismo modo, juntando (4) y (10), obtenemos que $|E(H_1)| = |E(G_2)|$. Como también $E(H_1) \subseteq E(G_2)$, esto nos permite concluir que $V(H_1) = V(G_2)$.

Juntando ambas igualdades, obtenemos que $H_1 = G_2$, por lo que f, el isomorfismo entre G_1 y H_1, es de hecho un isomorfismo entre G_1 y G_2, por lo que $G_1 \cong G_2$. $\square$

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

Refleja: Para cualquier grafo G, G es trivialmente subgrafo de sí mismo. La función identidad es trivialmente un isomorfismo, por lo que también todo grafo es subgrafo isomorfo 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 $G_1 \cong H_1$.
- H_2 es subgrafo de G_3 y $G_2 \cong H_2$.

Dado que $G_1 \cong H_1$, sea $f : V(G_1) \to V(H_1)$ (donde $V(H_1) \subseteq V(G_2)$) el isomorfismo de G_1 a H_1, y dado que $G_2 \cong H_2$, sea $g : V(G_2) \to V(H_2)$ (donde $V(H_2) \subseteq V(G_3)$) el isomorfismo de G_2 a H_2.

Sea el grafo $H_3 = (V, E)$ definido por

$$\begin{aligned} V &= \{(g \circ f)(v) \mid v \in V(G_1)\} && (\subseteq V(G_3)) \\ E &= \{((g \circ f)(e_1), (g \circ f)(e_2)) \mid (e_1, e_2) \in E(G_1)\} && (\subseteq E(G_3)) \end{aligned}$$

es por construcción un subgrafo de G_3 isomorfo a G_1, con isomorfismo $g \circ f$, por lo que $[G_1]_{\cong} \preceq [G_3]_{\cong}$. Concluimos que la relación $\preceq$ es transitiva.

Finalmente, puesto que la relación $\preceq$ es refleja, antisimétrica y transitiva, concluimos que $(A, \preceq)$ es un orden parcial.

Pauta (6ptos)

(a)
- 1 punto por mostrar la desigualdad en cardinalidades inducida por ser subgrafo isomorfo.
- 1 puntos por juntar las desigualdades para concluir que el subgrafo es de hecho el mismo grafo.

- 0.5 por concluir a partir de lo anterior que el isomorfismo al subgrafo es de hecho un isomorfismo al grafo.
- 0.5 por concluir de lo anterior que los grafos son isomorfos.

(b)
- 1 punto por cada propiedad.

Puntajes parciales y soluciones correctas alternativas a criterio del corrector.

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.

Solución

(a) (I) $x \equiv 15 \pmod{19}$

(II) No tiene solución ya que $\texttt{MCD}(21, 35) = 7$ y $7 \nmid 12$.

(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.

Pauta (6 pts.)

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