

Algoritmos en teoría de números

Parte III

Segundo semestre 2022

IIC2283

Prof. Nicolás Van Sint Jan

Recordatorio: segunda versión del test de primalidad

Una observación importante: si n es compuesto, entonces puede existir $a \in \mathbb{Z}_n^*$ tal que $a^{n-1} \not\equiv 1 \pmod{n}$

■ Por ejemplo: $3^{15} \bmod 16 = 11$

En lugar de considerar \mathbb{Z}_n^* en el test de primalidad, consideramos:

$$J_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod{n}\}$$

Si demostramos que para cada número compuesto n se tiene que $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$, entonces tenemos un test de primalidad.

■ Puesto que para p primo: $|J_p| = |\mathbb{Z}_p^*| = p - 1$

Recordatorio: segunda versión del test de primalidad

Recuerde que en nuestros algoritmos consideramos $n \geq 2$

TestPrimalidad3(n, k)

sea a_1, \dots, a_k una secuencia de números elegidos de
manera uniforme e independiente desde $\{1, \dots, n-1\}$

for $i := 1$ **to** k **do**

if $\text{MCD}(a_i, n) > 1$ **then return** COMPUESTO

else

if $\text{EXP}(a_i, n-1, n) \neq 1$

then return COMPUESTO

return PRIMO

Recordatorio: Teoría de grupos

Definición

Un conjunto G y una función (total) $\circ : G \times G \rightarrow G$ forman un **grupo** si:

1. (**Asociatividad**) Para cada $a, b, c \in G$:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

2. (**Elemento neutro**) Existe $e \in G$ tal que para cada $a \in G$:

$$a \circ e = e \circ a = a$$

3. (**Inverso**) Para cada $a \in G$, existe $b \in G$:

$$a \circ b = b \circ a = e$$

Propiedades básicas

- **Neutro es único:** Si e_1 y e_2 satisfacen 2, entonces $e_1 = e_2$
- **Inverso de cada elemento a es único:** Si $a \circ b = b \circ a = e$ y $a \circ c = c \circ a = e$, entonces $b = c$

Outline

Teorema de Lagrange (cont.)

Test de primalidad: tercera versión

Teoría de grupos: algunos ejemplos

Ejercicios

Muestre que los siguientes son grupos:

1. $(\mathbb{Z}_n, +)$, donde $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ y $+$ es la suma en módulo n
2. (\mathbb{Z}_n^*, \cdot) , donde \cdot es la multiplicación en módulo n
3. (J_n, \cdot) , donde \cdot es la multiplicación en módulo n

Teoría de grupos: subgrupos

Definición

(H, \circ) es un subgrupo de un grupo (G, \circ) , para $\emptyset \subsetneq H \subseteq G$, si (H, \circ) es un grupo.

Ejercicio

Demuestre que (J_n, \cdot) es un subgrupo de (\mathbb{Z}_n^*, \cdot)

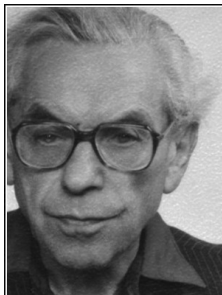
Propiedades básicas

- Si e_1 es el neutro en (G, \circ) y e_2 es el neutro de (H, \circ) , entonces $e_1 = e_2$
- Para cada $a \in H$, si b es el inverso de a en (G, \circ) y c es el inverso de a en (H, \circ) , entonces $c = b$

Teoría de grupos: una propiedad fundamental

Teorema de Lagrange

Si (G, \circ) es un grupo finito y (H, \circ) es un subgrupo de (G, \circ) , entonces $|H|$ divide a $|G|$



Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.

— Paul Erdős —

AZ QUOTES

Teorema de Lagrange: demostración

Demostración

Suponga que e es el elemento neutro de (G, \circ) y a^{-1} es el inverso de a en (G, \circ)

Sea \sim una relación binaria sobre G definida como:

$$a \sim b \text{ si y sólo si } b \circ a^{-1} \in H$$

Lema

\sim es una relación de equivalencia.

Teorema de Lagrange: demostración del primer lema

Lema

Sea \sim una relación binaria sobre G definida como:

$$a \sim b \text{ si y sólo si } b \circ a^{-1} \in H$$

\sim es una relación de equivalencia.

Demostración

(Refleja) $a \sim a$ ya que $a \circ a^{-1} = e$ y $e \in H$.

(Simétrica) Suponga que $a \sim b$. Demostramos que $b \sim a$.

Dado que $a \sim b$: $b \circ a^{-1} \in H$, tenemos que demostrar que $a \circ b^{-1} \in H$.
pause Tenemos que:

$$\begin{aligned}(b \circ a^{-1}) \circ (a \circ b^{-1}) &= (b \circ (a^{-1} \circ a)) \circ b^{-1} \\ &= (b \circ e) \circ b^{-1} \\ &= b \circ b^{-1} \\ &= e\end{aligned}$$

Teorema de Lagrange: demostración del primer lema

Lema

Sea \sim una relación binaria sobre G definida como:

$$a \sim b \text{ si y sólo si } b \circ a^{-1} \in H$$

\sim es una relación de equivalencia.

Demostración

De la misma forma concluimos que $(a \circ b^{-1}) \circ (b \circ a^{-1}) = e$. Por lo tanto,

$$(b \circ a^{-1})^{-1} = a \circ b^{-1}.$$

Concluimos que $a \circ b^{-1}$ está en H , ya que (H, \circ) es un subgrupo de (G, \circ) .

Teorema de Lagrange: demostración del primer lema

Lema

Sea \sim una relación binaria sobre G definida como:

$$a \sim b \text{ si y sólo si } b \circ a^{-1} \in H$$

\sim es una relación de equivalencia.

Demostración

(**Transitiva**) Suponga que $a \sim b$ y $b \sim c$. Tenemos que demostrar que $a \sim c$.

Por hipótesis: $b \circ a^{-1} \in H$ y $c \circ b^{-1} \in H$. Tenemos que demostrar que $c \circ a^{-1} \in H$.

Pero $(c \circ b^{-1}) \circ (b \circ a^{-1}) = c \circ a^{-1}$ y \circ es cerrada en H .

Por lo tanto: $c \circ a^{-1} \in H$



Teorema de Lagrange: demostración

Demostración

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim

Lema

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Del lema se concluye el teorema (!). Puesto que las clases de equivalencia de \sim particionan G .

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

1. Se tiene que:

$$\begin{aligned} a \in [e]_{\sim} &\Leftrightarrow e \sim a \\ &\Leftrightarrow a \circ e^{-1} \in H \\ &\Leftrightarrow a \circ e \in H \\ &\Leftrightarrow a \in H \end{aligned}$$

2. Sean $a, b \in G$, y defina la función f de la siguiente forma:

$$f(x) = x \circ (a^{-1} \circ b)$$

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

Se tiene que:

$$\begin{aligned}x \in [a]_{\sim} &\Rightarrow a \sim x \\&\Rightarrow x \circ a^{-1} \in H \\&\Rightarrow (x \circ a^{-1}) \circ e \in H \\&\Rightarrow (x \circ a^{-1}) \circ (b \circ b^{-1}) \in H \\&\Rightarrow (x \circ (a^{-1} \circ b)) \circ b^{-1} \in H \\&\Rightarrow f(x) \circ b^{-1} \in H \\&\Rightarrow b \sim f(x) \\&\Rightarrow f(x) \in [b]_{\sim}\end{aligned}$$

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

Por lo tanto: $f : [a]_{\sim} \rightarrow [b]_{\sim}$.

Vamos a demostrar que f es una **biyección**, de lo cual concluimos que $|[a]_{\sim}| = |[b]_{\sim}|$.

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

f es 1-1:

$$\begin{aligned} f(x) = f(y) &\Rightarrow x \circ (a^{-1} \circ b) = y \circ (a^{-1} \circ b) \\ &\Rightarrow (x \circ (a^{-1} \circ b)) \circ (b^{-1} \circ a) = \\ &\quad (y \circ (a^{-1} \circ b)) \circ (b^{-1} \circ a) \\ &\Rightarrow x \circ (a^{-1} \circ (b \circ b^{-1}) \circ a) = \\ &\quad y \circ (a^{-1} \circ (b \circ b^{-1}) \circ a) \\ &\Rightarrow x \circ ((a^{-1} \circ e) \circ a) = y \circ ((a^{-1} \circ e) \circ a) \\ &\Rightarrow x \circ (a^{-1} \circ a) = y \circ (a^{-1} \circ a) \\ &\Rightarrow x \circ e = y \circ e \\ &\Rightarrow x = y \end{aligned}$$

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

f es sobre:

$$\begin{aligned} y \in [b]_{\sim} &\Rightarrow b \sim y \\ &\Rightarrow y \circ b^{-1} \in H \\ &\Rightarrow (y \circ b^{-1}) \circ (a \circ a^{-1}) \in H \\ &\Rightarrow ((y \circ b^{-1}) \circ a) \circ a^{-1} \in H \\ &\Rightarrow a \sim ((y \circ b^{-1}) \circ a) \\ &\Rightarrow ((y \circ b^{-1}) \circ a) \in [a]_{\sim} \end{aligned}$$

Teorema de Lagrange: demostración del segundo lema

Lema

Sea $[a]_{\sim}$ la clase de equivalencia de $a \in G$ bajo la relación \sim . Luego:

1. $[e]_{\sim} = H$
2. Para cada $a, b \in G$: $|[a]_{\sim}| = |[b]_{\sim}|$

Demostración

Sea $x = ((y \circ b^{-1}) \circ a)$. Tenemos que:

$$\begin{aligned} f(x) &= x \circ (a^{-1} \circ b) \\ &= ((y \circ b^{-1}) \circ a) \circ (a^{-1} \circ b) \\ &= y \circ (b^{-1} \circ (a \circ a^{-1}) \circ b) \\ &= y \circ ((b^{-1} \circ e) \circ b) \\ &= y \circ (b^{-1} \circ b) \\ &= y \circ e \\ &= y \end{aligned}$$



Test de primalidad: segunda versión (continuación)

Dejamos pendiente la siguiente pregunta:

¿Qué enfoque podríamos usar para demostrar que $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$?

R: Usamos el Teorema de Lagrange.

Dado que (J_n, \cdot) es un subgrupo de (\mathbb{Z}_n^*, \cdot) :

Si existe $a \in (\mathbb{Z}_n^* \setminus J_n)$, entonces $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$

¿Tenemos entonces nuestro test de primalidad?

Test de primalidad: segunda versión (continuación)

Definición

Un número n es de Carmichael si $n \geq 2$, n es compuesto y $|J_n| = |\mathbb{Z}_n^*|$

Ejemplo

561, 1105 y 1729 son números de Carmichael.

Teorema (Alford-Granville-Pomerance)

Existe un número infinito de números de Carmichael.

Conclusión: Este test de primalidad no va a funcionar.

Outline

Teorema de Lagrange (cont.)

Test de primalidad: tercera versión

Test de primalidad: tercera versión

No todo está perdido.

En lugar de utilizar J_n , vamos a usar las herramientas que desarrollamos sobre el siguiente conjunto (n impar):

$$S_n = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n} \text{ ó } a^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}$$

Spoiler: Ahora sí va a funcionar.

Test de primalidad: un intento exitoso

Vamos a diseñar un test de primalidad considerando los conjuntos:

$$S_n^+ = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}$$

$$S_n^- = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}$$

Así, podemos definir S_n a partir de estos conjuntos:

$$S_n = S_n^+ \cup S_n^-$$

Para hacer esto necesitamos estudiar algunas propiedades de los conjuntos S_n^+ , S_n^- y S_n .

- Consideramos primero el caso en que n es primo, y luego el caso en que n es compuesto

Una propiedad fundamental de S_n para n primo

Proposición 1

Si $n \geq 3$ es primo, entonces $S_n = \mathbb{Z}_n^*$.

Demostración

Si $a \in \{1, \dots, n-1\}$, tenemos que $a^{n-1} \equiv 1 \pmod{n}$

Por lo tanto $\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \pmod{n}$, de lo cual se deduce que:

$$\left(a^{\frac{n-1}{2}} + 1\right) \cdot \left(a^{\frac{n-1}{2}} - 1\right) \equiv 0 \pmod{n}$$

Así, dado que n es primo se concluye que $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ ó $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ (**¿Por qué?**)

