Algortimos en teoría de números

Parte III

Segundo semestre 2022

IIC2283

Prof. Nicolás Van Sint Jan

Recordatorio: Un primer ingrediente

Pequeño Teorema de Fermat

Sea p un número primo. Si $a \in \{0, \ldots, p-1\}$, entonces

$$a^p \equiv a \pmod{p}$$

Corolario

Sea p un número primo. Si $a \in \{1, \ldots, p-1\}$, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

Recordatorio: Primera versión de un test de primalidad

El test de primalidad que vamos a estudiar está basado en estas propiedades ($n \geq 2$):

1. Si n es primo y $a \in \{1, \ldots, n-1\}$, entonces

$$a^{n-1} \equiv 1 \pmod{n}$$

2. Si n es compuesto, entonces **existe** $a \in \{1, \ldots, n-1\}$ tal que

$$a^{n-1} \not\equiv 1 \pmod{n}$$

Recordatorio: Test de primalidad: primera versión

Para $n \geq 2$, defina el conjunto $\mathbb{Z}_n^*$ como:

$$\mathbb{Z}_n^* \quad = \quad \{a \in \{1, \ldots, n-1\} \mid \text{gcd}(a, n) = 1\}$$

Es decir, $\mathbb{Z}_n^*$ es el conjunto de todos los primos relativos de n que son menores que él.

Suponga que n es compuesto. Luego si $a \in \{1, \ldots, n-1\} - \mathbb{Z}_n^*$, entonces $a^{n-1} \not\equiv 1 \bmod n$.

Test de primalidad entonces depende de qué tan grande es $\mathbb{Z}_n^*$.

Supongamos que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$.

Recordatorio: primera versión

TestPrimalidad1(n)

sea a un número elegido de manera uniforme desde $\{1, \ldots, n-1\}$

if **EXP**($a, n-1, n$) $\neq 1$

then return COMPUESTO

else

return PRIMO

Recordatorio: Versión mejorada

TestPrimalidad2(n, k)

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

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

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

then return COMPUESTO

return PRIMO

Recordatorio: La función ϕ de Euler

Considere la **función de Euler** $\phi : \mathbb{N} \to \mathbb{N}$ definida como

$$\phi(n) = \begin{cases} 0 & n = 1 \\ |\mathbb{Z}_n^*| & n > 1 \end{cases}$$

Teorema

$$\phi(n) \quad \in \quad \Omega\left(\frac{n}{\log_2(\log_2(n))}\right)$$

Conclusión

Para cada número n, el conjunto $\mathbb{Z}_n^*$ tiene un número de elementos cercano a n

- No es cierto que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$
- No podemos basar nuestro test en los elementos del conjunto $(\{1, \ldots, n-1\} - \mathbb{Z}_n^*)$

Outline

Test de primalidad: segunda versión

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

- Por ejemplo: $3^{15} \bmod 16 = 11$

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

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

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: $|J_p| = |\mathbb{Z}_p^*| = p - 1$

Test de primalidad: segunda versión

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

TestPrimalidad3(n, k)
    sea $a_1, \ldots, a_k$ una secuencia de números elegidos de
        manera uniforme e independiente desde $\{1, \ldots, n-1\}$
    for $i := 1$ **to** k **do**
        if MCD$(a_i, n) > 1$ **then return** COMPUESTO
        else
            if EXP$(a_i, n-1, n) \neq 1$
                then return COMPUESTO
    return PRIMO

Algunas consideraciones sobre **TestPrimalidad3**

Ejercicio

1. Demuestre que **TestPrimalidad3** funcionan en tiempo polinomial.

2. Suponiendo que para cada número compuesto n se tiene que $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$, demuestre que la probabilidad de error de **TestPrimalidad3** es menor o igual a $\left(\frac{1}{2}\right)^k$

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

Teoría de grupos

Definición

Un conjunto G y una función (total) $\circ : G \times G \to G$ 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 $b = c$

Teoría de grupos: algunos ejemplos

Ejercicios

Muestre que los siguientes son grupos:

1. $(\mathbb{Z}_n, +)$, donde $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ 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 $(\mathbb{Z}_n^*, \cdot)$

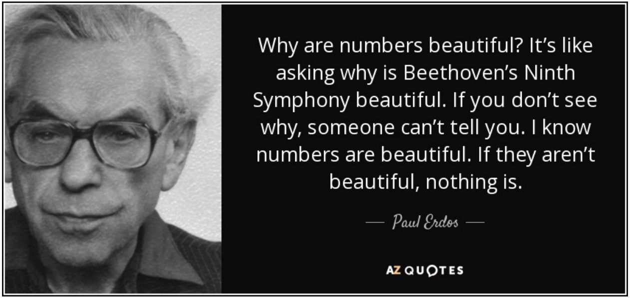
Propiedades básicas

- 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 $|G|$



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: $c \circ a^{-1} \in H$ $\square$

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:

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

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:

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

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:

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

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:

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

$\square$

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 $a \in (\mathbb{Z}_n^* \smallsetminus J_n)$, 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.

Outline

Un problema fundamental: verificación de primalidad

Vamos a ver un algoritmo aleatorizado para **verificar si un número es primo**.

- Este algoritmo es **mucho más eficiente** que los algoritmos sin componentes aleatorias para este problema

El ingrediente fundamental para el algoritmo es el uso de **aritmética modular**.

Un primer ingrediente

Pequeño Teorema de Fermat

Sea p un número primo. Si $a \in \{0, \ldots, p-1\}$, entonces

$$a^p \equiv a \pmod{p}$$

Un primer ingrediente

Corolario

Sea p un número primo. Si $a \in \{1, \ldots, p-1\}$, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

Demostración

Por teorema anterior sabemos que

$$a^p \equiv a \pmod{p}$$

Por lo tanto, existe $\alpha \in \mathbb{Z}$ tal que

$$a^p - a \quad = \quad \alpha \cdot p$$

Un primer ingrediente

Demostración

Dado que $a \mid (a^p - a)$, se tiene que $a \mid (\alpha \cdot p)$

Por lo tanto, dado que $a \in \{1, \ldots, p-1\}$ y p es un número primo, se concluye que $a \mid \alpha$.
Entonces $(a^{p-1} - 1) = \frac{\alpha}{a} \cdot p$, donde $\frac{\alpha}{a}$ es un número entero.

- Concluimos que $a^{p-1} \equiv 1 \bmod p$ $\square$

Test de primalidad: primera versión

El test de primalidad que vamos a estudiar está basado en estas propiedades ($n \geq 2$):

1. Si n es primo y $a \in \{1, \ldots, n-1\}$, entonces
$$a^{n-1} \equiv 1 \pmod{n}$$
2. Si n es compuesto, entonces **existe** $a \in \{1, \ldots, n-1\}$ tal que
$$a^{n-1} \not\equiv 1 \pmod{n}$$

Demostración

Suponga que n es compuesto. Sea $a \in \{1, \ldots, n-1\}$ tal que $\gcd(a, n) > 1$.

Luego a no tiene inverso en módulo n.

Concluimos que
$$a^{n-1} \not\equiv 1 \pmod{a}$$
dado que a^{n-2} no puede ser inverso de a en módulo n $\square$

Test de primalidad: primera versión

Para $n \geq 2$, defina el conjunto $\mathbb{Z}_n^*$ como:

$$\mathbb{Z}_n^* \quad = \quad \{a \in \{1, \ldots, n-1\} \mid \gcd(a, n) = 1\}$$

Es decir, $\mathbb{Z}_n^*$ es el conjunto de todos los primos relativos de n que son menores que él.

Suponga que n es compuesto. Luego si $a \in \{1, \ldots, n-1\} - \mathbb{Z}_n^*$, entonces $a^{n-1} \not\equiv 1 \bmod n$.

Test de primalidad entonces depende de qué tan grande es $\mathbb{Z}_n^*$.

Supongamos que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$.

Test de primalidad: primera versión

TestPrimalidad1(n)

sea a un número elegido de manera uniforme desde $\{1, \ldots, n-1\}$

if EXP($a, n-1, n$) $\neq 1$

then return COMPUESTO

else

return PRIMO

Algunas propiedades de **TestPrimalidad1**

Ejercicios

Recuerde que estamos suponiendo que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$

1. Demuestre que la probabilidad de error de **TestPrimalidad1** es menor o igual a $\frac{1}{2}$

2. Demuestre que **TestPrimalidad1** funcionan en tiempo polinomial.
   - Recuerde que el tiempo es medido en función del tamaño de la entrada, que en este caso es $\lfloor \log_2(n) \rfloor + 1$ si suponemos que la entrada está dada como una palabra sobre el alfabeto $\{0, 1\}$

3. De un algoritmo que reciba como parámetros a dos números enteros $n \geq 2$ y $k \geq 1$, y determina si n es un número primo con probabilidad de error menor o igual a $\left(\frac{1}{2}\right)^k$

Una solución al tercer ejercicio

TestPrimalidad2(n, k)

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

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

if **EXP**$(a_i, n-1, n) \neq 1$

then return COMPUESTO

return PRIMO

¿Pero la probabilidad de error de **TestPrimalidad2** está bien acotada?

Supusimos que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$

¿Es esta suposición correcta?

Considere la **función de Euler** $\phi : \mathbb{N} \to \mathbb{N}$ definida como

$$\phi(n) = \begin{cases} 0 & n = 1 \\ |\mathbb{Z}_n^*| & n > 1 \end{cases}$$

Hay acotar el valor de esta función

Una cota inferior para la función ϕ de Euler

Teorema

$$\phi(n) \quad \in \quad \Omega\left(\frac{n}{\log_2(\log_2(n))}\right)$$

Conclusión

Para cada número n, el conjunto $\mathbb{Z}_n^*$ tiene un número de elementos cercano a n

- No es cierto que $|\mathbb{Z}_n^*| \leq \left\lfloor \frac{n}{2} \right\rfloor$ para cada número compuesto $n \geq 2$
- No podemos basar nuestro test en los elementos del conjunto $(\{1, \ldots, n-1\} - \mathbb{Z}_n^*)$