Algoritmos en teoría de números

Parte V

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:

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

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 $a_1, \ldots, a_k$ 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

Recordatorio: 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: 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 $|G|$

Outline

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

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:

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

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 $a \in \{1, \ldots, n-1\}$, 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:

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

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?)** □

Una propiedad fundamental de S_n^+ y S_n^- para n primo

Proposición 2

Si $n \geq 3$ es primo: $|S_n^+| = |S_n^-| = \frac{n-1}{2}$

Para demostrar la proposición, primero vamos a demostrar un lema.

Sea $p(x)$ un polinomio:

$$p(x) = \sum_{i=0}^{k} a_i x^i,$$

donde $k \geq 1$, cada $a_j \in \{0, \ldots, n-1\}$ para $0 \leq j \leq k-1$, y $a_k \neq 0$.

Decimos que a es una **raíz de $p(x)$ en módulo n** si

$$p(a) \equiv 0 \pmod{n}$$

Número de raíces de un polinomio

Lema

$p(x)$ tiene a lo más k raíces en módulo n

Demostración

Decimos que dos polinomios $p_1(x)$ y $p_2(x)$ son **congruentes en módulo n** si para todo $a \in \{0, \ldots, n-1\}$:

$$p_1(a) \equiv p_2(a) \pmod{n}$$

Para esto usamos la notación $p_1(x) \equiv p_2(x) \pmod{n}$.

Sea a una raíz de $p(x)$ en módulo n. Vamos a demostrar que existe un polinomio $q(x)$ de grado $k-1$ tal que:

$$p(x) \equiv (x-a) \cdot q(x) \pmod{n}$$

Número de raíces de un polinomio

Demostración

Veamos que al demostrar esta propiedad se concluye que el lema es cierto.

Si c es una raíz de $p(x)$ en módulo n, entonces $p(c) \equiv 0 \pmod{n}$

- Como $p(x) \equiv (x - a) \cdot q(x) \pmod{n}$, concluimos que $(c - a) \cdot q(c) \equiv 0 \pmod{n}$

Dado que n es primo, si $d \cdot e \equiv 0 \pmod{n}$, entonces $d \equiv 0 \pmod{n}$ o $e \equiv 0 \pmod{n}$

- Tenemos entonces que $c \equiv a \pmod{n}$ o $q(c) \equiv 0 \pmod{n}$

Número de raíces de un polinomio

Demostración

Así, tenemos que c es la raíz a que ya habíamos identificado o es una raíz de $q(x)$ en módulo n

Concluimos que el número de raíces de $p(x)$ en módulo n es menor o igual a uno más el número de raíces de $q(x)$ en módulo n

- Como $q(x)$ tiene grado $k-1$, si continuamos usando este argumento (o usamos inducción) concluimos que el número de raíces de $p(x)$ es menor o igual a k

Número de raíces de un polinomio

Demostración

Nótese que el argumento anterior no funciona si n es compuesto.

- Dado que podemos tener d y e tales que $d \cdot e \equiv 0 \pmod{n}$, $d \not\equiv 0 \pmod{n}$ y $e \not\equiv 0 \pmod{n}$

De hecho, si n es compuesto no es necesariamente cierto que el número de raíces de un polinomio está acotado superiormente por su grado.

Ejemplo

Si $n = 35$, tenemos que $5 \cdot 7 \equiv 0 \pmod{3)5}$, pero $5 \not\equiv 0 \pmod{3)5}$ y $7 \not\equiv 0 \pmod{3)5}$

En este caso tenemos cuatro raíces para el polinomio $p(x) = x^2 - 1$

- Ya que $1^2 \equiv 1 \pmod{3)5}$, $6^2 \equiv 1 \pmod{3)5}$, $29^2 \equiv 1 \pmod{3)5}$ y $34^2 \equiv 1 \pmod{3)5}$

Número de raíces de un polinomio

Demostración

Volvemos entonces a la demostración de que existe un polinomio $q(x)$ de grado $k-1$ tal que:

$$p(x) \equiv (x-a)\cdot q(x) \pmod{n}$$

Definimos $q(x)$ como:

$$q(x) = \sum_{i=0}^{k-1} b_i x^i,$$

donde $b_i = a_{i+1} + a_{i+2}\cdot a + \cdots + \cdot a_k \cdot a^{k-1-i}$

Número de raíces de un polinomio

Demostración

Se tiene que:

$$\begin{aligned}
(x-a)\cdot q(x) &= \left(\sum_{i=0}^{k-1} b_i x^{i+1}\right) + \left(\sum_{i=0}^{k-1}(-a\cdot b_i)x^i\right) \\
&= \left(\sum_{i=1}^{k} b_{i-1} x^i\right) + \left(\sum_{i=0}^{k-1}(-a\cdot b_i)x^i\right) \\
&= b_{k-1}\cdot x^k + \left(\sum_{i=1}^{k-1}(b_{i-1} - a\cdot b_i)x^i\right) - a\cdot b_0
\end{aligned}$$

Así, dado que:

$$b_{k-1} = a_k$$

Número de raíces de un polinomio

Demostración

Y dado que para $i \in \{1, \ldots, k-1\}$:

$$\begin{aligned}
(b_{i-1} - a \cdot b_i) &= a_i + a_{i+1} \cdot a + \cdots + \cdot a_k \cdot a^{k-i} - \\
&\quad a \cdot (a_{i+1} + a_{i+2} \cdot a + \cdots + \cdot a_k \cdot a^{k-1-i}) \\
&= a_i + a_{i+1} \cdot a + \cdots + \cdot a_k \cdot a^{k-i} - \\
&\quad a_{i+1} \cdot a - a_{i+2} \cdot a^2 - \cdots - \cdot a_k \cdot a^{k-1} \\
&= a_i
\end{aligned}$$

Concluimos que:

$$(x-a) \cdot q(x) = \left(\sum_{i=1}^{k} a_i \cdot x^i \right) - a \cdot b_0$$

Número de raíces de un polinomio

Demostración

Pero:

$$\begin{aligned} -a \cdot b_0 &= -a \cdot (a_1 + a_2 \cdot a + \cdots + \cdot a_k \cdot a^{k-1}) \\ &= -a_1 \cdot a - a_2 \cdot a^2 - \ldots - a_k \cdot a^k \end{aligned}$$

De lo cual deducimos que:

$$a_0 \equiv -a \cdot b_0 \pmod{n},$$

ya que $a_k \cdot a^k + \cdots + a_1 \cdot a + a_0 \equiv 0 \pmod{n}$

Tenemos entonces que:

$$(x - a) \cdot q(x) \equiv p(x) \pmod{n}$$

Demostración de la proposición: continuación

Demostración

Sea $R = \{b^2 \mid 1 \leq b \leq \frac{n-1}{2}\}$

Por el Teorema de Fermat, tenemos que:

$$R \quad \subseteq \quad \{a \in \{1, \ldots, n-1\} \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}$$

Además, sabemos que si $1 \leq b < c \leq \frac{n-1}{2}$ y $b^2 \equiv c^2 \pmod{n}$:

$$(c-b) \cdot (c+b) \equiv 0 \pmod{n}$$

Así, dado que $2 \leq b + c \leq n - 1$, concluimos que $b \equiv c \pmod{n}$

- Dado que n es primo

Demostración de la proposición: continuación

Demostración

Pero $b \equiv c \pmod{n}$ no pueder ser cierto puesto que $1 \leq (c - b) \leq \frac{n-1}{2}$

- Por lo tanto: $|R| = \frac{n-1}{2}$

Además, sabemos que $p(x) = x^{\frac{n-1}{2}} - 1$ tienes a lo más $\frac{n-1}{2}$ raíces en módulo n.

- Por lo tanto: $|\{a \in \{1, \ldots, n-1\} \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}| \leq \frac{n-1}{2}$

Demostración de la proposición: continuación

Demostración

Concluimos que:

$$\frac{n-1}{2} \;=\; |R| \;\leq\; |\{a \in \{1,\ldots,n-1\} \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}| \;\leq\; \frac{n-1}{2}$$

Por lo tanto:

$$|S_n^+| \;=\; |\{a \in \{1,\ldots,n-1\} \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}| \;=\; \frac{n-1}{2}$$

Así, dado que $|S_n| = |\mathbb{Z}_n^*| = n-1$ y $|S_n^+| + |S_n^-| = |S_n|$, concluimos que:

$$|S_n^-| \quad = \quad \frac{n-1}{2}$$

□

Una propiedad fundamental de S_n para n compuesto

Teorema

Sea $n = n_1 \cdot n_2$, donde $n_1, n_2 \geq 3$ y $\gcd(n_1, n_2) = 1$. Si existe $a \in \mathbb{Z}_n^*$ tal que $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, entonces:

$$|S_n| \quad \leq \quad \frac{1}{2} \cdot |\mathbb{Z}_n^*|$$

Para demostrar el teorema necesitamos el Teorema Chino del resto