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

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

Teorema (Fermat)

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

Un primer ingrediente

Teorema (Fermat)

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

Demostración: Por inducción en a

Para $a = 0$ y $a = 1$ se cumple trivialmente. Suponga que $a^p \equiv a \bmod p$ y $2 \leq (a+1) < p$

Sabemos que:

$$(a+1)^p \quad = \quad \sum_{k=0}^{p} \binom{p}{k} a^k$$

Un primer ingrediente

Por lo tanto:

$$(a+1)^p - (a+1) \quad = \quad (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Lema

Si $k \in \{1, \ldots, p-1\}$, entonces $p | \binom{p}{k}$

Demostración: Sabemos que:

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{k!}$$

Como $k \in \{1, \ldots, p-1\}$ y p es un número primo:

$\frac{(p-1) \cdot \ldots \cdot (p-k+1)}{k!}$ es un número entero

Un primer ingrediente

Por lo tanto: $\binom{p}{k} = p \cdot \alpha$, donde α es un número entero

- Concluimos que $p \mid \binom{p}{k}$ $\square$

Del lema concluimos que $p \left| \sum_{k=1}^{p-1} \binom{p}{k} a^k \right.$

Un primer ingrediente

Por lo tanto: $\binom{p}{k} = p \cdot \alpha$, donde α es un número entero

- Concluimos que $p \Big| \binom{p}{k}$ $\square$

Del lema concluimos que $p \left| \displaystyle\sum_{k=1}^{p-1} \binom{p}{k} a^k \right.$

Por lo tanto, dado que $p \big| (a^p - a)$ por hipótesis de inducción, tenemos que: $p \big| ((a+1)^p - (a+1))$

- Concluimos que $(a+1)^p \equiv (a+1) \bmod p$ $\square$

Un primer ingrediente

Corolario (Fermat)

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

Un primer ingrediente

Corolario (Fermat)

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

Demostración: Por teorema anterior sabemos que

$$a^p \equiv a \bmod p$$

Por lo tanto: existe un número entero α tal que

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

Un primer ingrediente

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

Por lo tanto, dado que $a \in \{1, \ldots, p-1\}$ y p es un número primo, se concluye que $a | \alpha$

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

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

Demostración de 2. Sea $a \in \{1, \ldots, n-1\}$ tal que $\text{MCD}(a, n) > 1$

- a no tiene inverso en módulo n

Concluimos que $a^{n-1} \not\equiv 1 \bmod a$

- Dado que a^{n-2} no puede ser inverso de a en módulo n $\square$

Test de primalidad: primera versión

Para $n \geq 2$, sea:

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

Sabemos que para n compuesto: Si $a \in (\{1, \ldots, n-1\} \smallsetminus \mathbb{Z}_n^*)$, entonces $a^{n-1} \not\equiv 1 \bmod n$

Test de primalidad depende de cuan grande es $\mathbb{Z}_n^*$

Test de primalidad: primera versión

Para $n \geq 2$, sea:

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

Sabemos que para n compuesto: Si $a \in (\{1, \ldots, n-1\} \smallsetminus \mathbb{Z}_n^*)$, entonces $a^{n-1} \not\equiv 1 \bmod n$

Test de primalidad depende de cuan grande es $\mathbb{Z}_n^*$

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

Test de primalidad: primera versión

En nuestros algoritmos consideramos $n \geq 2$

Test de primalidad: primera versión

En nuestros algoritmos consideramos $n \geq 2$

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

- ¿Es esta suposición correcta?

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

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

- ¿Es esta suposición correcta?

Función de Euler: $\phi(1) = 0$ y $\phi(n) = |\mathbb{Z}_n^*|$ para $n \geq 2$

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

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

- ¿Es esta suposición correcta?

Función de Euler: $\phi(1) = 0$ y $\phi(n) = |\mathbb{Z}_n^*|$ para $n \geq 2$

- Necesitamos acotar el valor de esta función

Una cota inferior para la función ϕ de Euler

Teorema

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

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

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:

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

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 $n \geq 2$

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 $\left(\frac{1}{2}\right)^k$

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?

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 también juega un papel fundamental en el desarrollo del test de primalidad

Teoría de grupos

Definición

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

1. *Para cada $a, b, c \in G$:* $(a \circ b) \circ c = a \circ (b \circ c)$
2. *Existe $e \in G$ tal que para cada $a \in G$:* $a \circ e = e \circ a = a$
3. *Para cada $a \in G$, existe $b \in G$:* $a \circ b = b \circ a = e$

Teoría de grupos

Definición

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

1. *Para cada $a, b, c \in G$:* $(a \circ b) \circ c = a \circ (b \circ c)$
2. *Existe $e \in G$ tal que para cada $a \in G$:* $a \circ e = e \circ a = a$
3. *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

Definition

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

Teoría de grupos: subgrupos

Definition

$(H, \circ)$ 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 $(\mathbb{Z}_n^*, \cdot)$

Teoría de grupos: subgrupos

Definition

$(H, \circ)$ 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

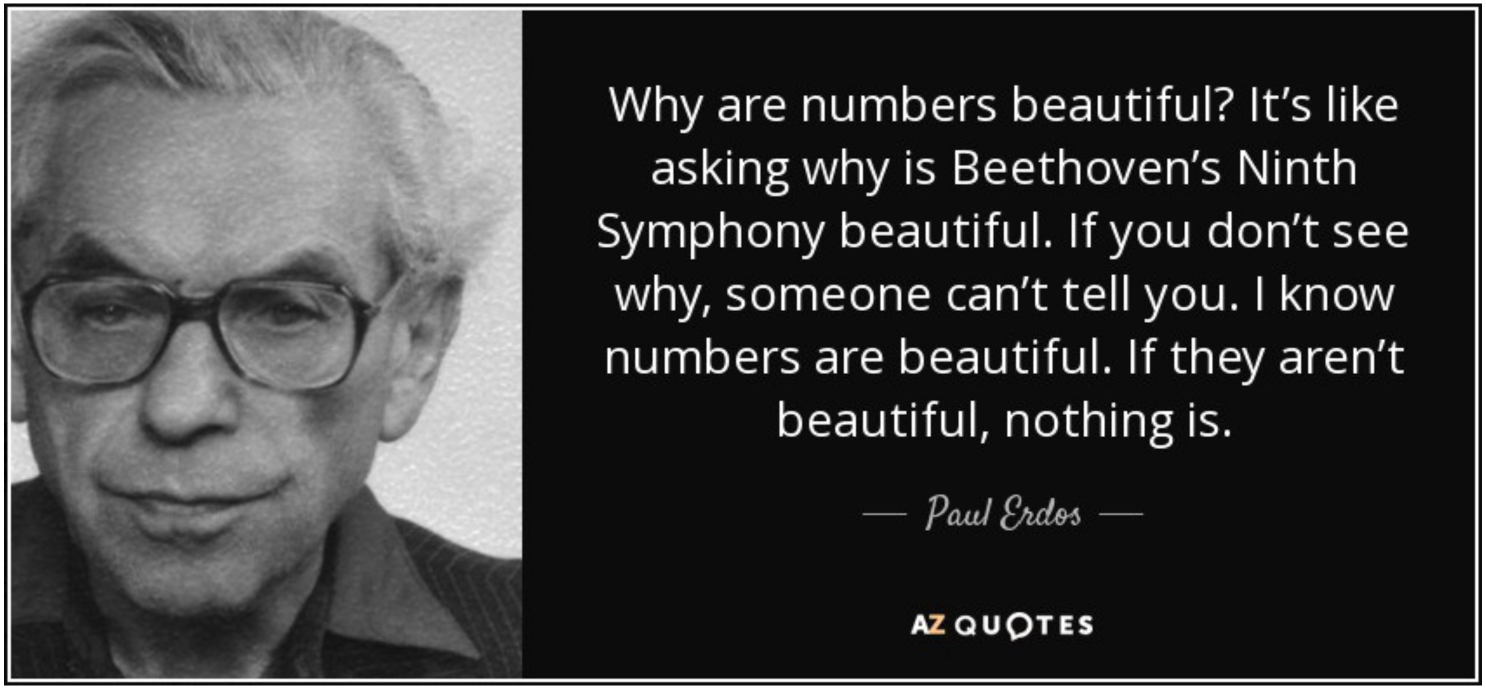
Teorema (Lagrange)

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

Teoría de grupos: una propiedad fundamental

Teorema (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

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

Teorema de Lagrange: 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:

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

Teorema de Lagrange: 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

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

- Suponga que $a \sim b$
  - Tenemos que demostrar que $b \sim a$

Dado que $a \sim b$: $b \circ a^{-1} \in H$

- Tenemos que demostrar que $a \circ b^{-1} \in H$

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

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 $(G, \circ)$

- 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

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

Lema

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

Teorema de Lagrange: 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

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

Se tiene que:

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

Por lo tanto: $f : [a]_\sim \to [b]_\sim$

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

Teorema de Lagrange: demostración del segundo lema

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

f es sobre:

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

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

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

$\square$

Test de primalidad: segunda versión (continuación)

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

Test de primalidad: segunda versión (continuación)

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

- ¡Usamos el Teorema de Lagrange!

Test de primalidad: segunda versión (continuación)

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

- ¡Usamos el Teorema de Lagrange!

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

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

Test de primalidad: segunda versión (continuación)

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

- ¡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)

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

- ¡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?

- Lamentablemente no todavía: números de Carmichael

Test de primalidad: segunda versión (continuación)

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

- ¡Usamos el Teorema de Lagrange!

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

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

¿Tenemos entonces nuestro test de primalidad?

- Lamentablemente no todavía: números de Carmichael
- Pero lo que hemos aprendido va a ser fundamental para desarrollar el test de primalidad

Test de primalidad: segunda versión (continuación)

Definition

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.

Test de primalidad: segunda versión (continuación)

Definition

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.

Test de primalidad: tercera version

Conclusión: el test basado en J_n no va a funcionar.

Test de primalidad: tercera version

Conclusión: el test basado en J_n no va a funcionar.

¿Qué hacemos entonces?

Test de primalidad: tercera version

Conclusión: el test basado en J_n no va a funcionar.

¿Qué hacemos entonces?

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

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

¡Esto sí funciona!

Test de primalidad: un intento exitoso

Vamos a diseñar un test de primalidad considerando los conjuntos:

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

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

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

Una propiedad fundamental de S_n para n primo

Proposición

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

Demostración: Si $a \in \{1, \ldots, n-1\}$, tenemos que $a^{n-1} \equiv 1 \bmod n$

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

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

Así, dado que n es primo se concluye que $a^{\frac{n-1}{2}} \equiv 1 \bmod n$ ó $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

- ¿Por qué? $\square$

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

Proposición

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

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

Proposición

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

Demostración: Para demostrar la proposición, usamos el siguiente lema.

Sea $p(x)$ el polinomio:

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

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

Decimos que a es una raíz de $p(x)$ en módulo n si $p(a) \equiv 0 \bmod n$

Número de raíces de un polinomio

Lema

$p(x)$ *tiene a lo más* k *raíces en módulo* 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 $a \in \{0, \ldots, n-1\}$:

$$p_1(a) \equiv p_2(a) \mod n$$

Notación

$p_1(x) \equiv p_2(x) \mod n$

Sea a una raíz de $p(x)$ en módulo n

Número de raíces de un polinomio

Vamos a demostrar que existe un polinomio $q(x)$ de grado $k-1$ tal que:

$$p(x) \quad \equiv \quad (x-a)\cdot q(x) \mod n$$

Pero antes de demostrar esto, vamos a mostrar que de esta propiedad se concluye que el lema es cierto.

Número de raíces de un polinomio

Vamos a demostrar que existe un polinomio $q(x)$ de grado $k - 1$ tal que:

$$p(x) \quad \equiv \quad (x - a) \cdot q(x) \mod n$$

Pero antes de demostrar esto, vamos a mostrar que de esta propiedad se concluye que el lema es cierto.

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

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

Número de raíces de un polinomio

Vamos a demostrar que existe un polinomio $q(x)$ de grado $k - 1$ tal que:

$$p(x) \equiv (x - a) \cdot q(x) \mod n$$

Pero antes de demostrar esto, vamos a mostrar que de esta propiedad se concluye que el lema es cierto.

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

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

Dado que n es primo, si $d \cdot e \equiv 0 \bmod n$, entonces $d \equiv 0 \bmod n \;$ o $\; e \equiv 0 \bmod n$

Número de raíces de un polinomio

Vamos a demostrar que existe un polinomio $q(x)$ de grado $k - 1$ tal que:

$$p(x) \quad \equiv \quad (x - a) \cdot q(x) \mod n$$

Pero antes de demostrar esto, vamos a mostrar que de esta propiedad se concluye que el lema es cierto.

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

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

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

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

Número de raíces de un polinomio

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

Número de raíces de un polinomio

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

Número de raíces de un polinomio

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

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

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

Número de raíces de un polinomio

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

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

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

Número de raíces de un polinomio

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

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

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 $5 \cdot 7 \equiv 0 \bmod 35$, pero $5 \not\equiv 0 \bmod 35$ y $7 \not\equiv 0 \bmod 35$

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

- Ya que $1^2 \equiv 1 \bmod 35$, $6^2 \equiv 1 \bmod 35$, $29^2 \equiv 1 \bmod 35$ y $34^2 \equiv 1 \bmod 35$

Número de raíces de un polinomio

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

$$p(x) \quad \equiv \quad (x - a) \cdot q(x) \mod n$$

Número de raíces de un polinomio

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

$$p(x) \equiv (x-a) \cdot q(x) \mod n$$

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

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

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

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

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

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:

$$a_0 \equiv -a \cdot b_0 \mod n,$$

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

Tenemos entonces que:

$$(x - a) \cdot q(x) \equiv p(x) \mod n$$

$\square$

Demostración de la proposición: continuación

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

Por el Teorema de Fermat, tenemos que:

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

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

$$(c - b) \cdot (c + b) \equiv 0 \bmod n$$

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

- Dado que n es primo

Demostración de la proposición: continuación

Pero $b \equiv c \bmod n$ 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: $|\{a \in \{1, \ldots, n-1\} \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n\}| \leq \frac{n-1}{2}$

Demostración de la proposición: continuación

Concluimos que:

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

Por lo tanto:

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

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

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

$\square$

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* $MCD(n_1, n_2) = 1$*. Si existe* $a \in \mathbb{Z}_n^*$ *tal que* $a^{\frac{n-1}{2}} \equiv -1 \bmod n$*, entonces:*

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

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* $MCD(n_1, n_2) = 1$*. Si existe* $a \in \mathbb{Z}_n^*$ *tal que* $a^{\frac{n-1}{2}} \equiv -1 \bmod n$*, entonces:*

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

Para demostrar el teorema necesitamos el Teorema Chino del resto

Para recordar: un teorema muy útil

Teorema (Chino del Resto)

Suponga que $MCD(m, n) = 1$*. Para todo* a *y* b*, existe* c *tal que:*

$$\begin{aligned} c &\equiv a \mod m \\ c &\equiv b \mod n \end{aligned}$$

Para recordar: un teorema muy útil

Teorema (Chino del Resto)

Suponga que $MCD(m,n) = 1$. *Para todo a y b, existe c tal que:*

$$\begin{aligned} c &\equiv a \mod m \\ c &\equiv b \mod n \end{aligned}$$

Demostración: Dado que $\mathrm{MCD}(m,n) = 1$, existen d y e tales que:

$$\begin{aligned} n \cdot d &\equiv 1 \mod m \\ m \cdot e &\equiv 1 \mod n \end{aligned}$$

Sea $c = a \cdot n \cdot d + b \cdot m \cdot e$

Se tiene que:

$$\begin{aligned} c &\equiv a \mod m \\ c &\equiv b \mod n \end{aligned}$$

$\square$

La demostración del teorema inicial

Suponga que $a \in \mathbb{Z}_n^*$ y $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

La demostración del teorema inicial

Suponga que $a \in \mathbb{Z}_n^*$ y $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

Por Teorema Chino del Resto, existe b tal que:

$$\begin{aligned} b &\equiv a \mod n_1 \\ b &\equiv 1 \mod n_2 \end{aligned}$$

La demostración del teorema inicial

Suponga que $a \in \mathbb{Z}_n^*$ y $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

Por Teorema Chino del Resto, existe b tal que:

$$\begin{array}{rcll} b & \equiv & a & \bmod n_1 \\ b & \equiv & 1 & \bmod n_2 \end{array}$$

Entonces: $a = \alpha \cdot n_1 + b$ y $1 = \beta \cdot n_2 + b$

- Por lo tanto $\mathrm{MCD}(b, n) = 1$, ya que $n = n_1 \cdot n_2$ y $a \in \mathbb{Z}_n^*$

La demostración del teorema inicial

Además, tenemos que:

$$\begin{aligned} b^{\frac{n-1}{2}} \quad \equiv \quad a^{\frac{n-1}{2}} & \quad \equiv \quad -1 \quad \mod n_1 \\ b^{\frac{n-1}{2}} & \quad \equiv \quad 1 \quad \mod n_2 \end{aligned}$$

Dado que $n = n_1 \cdot n_2$ concluimos que:

$$\begin{aligned} b^{\frac{n-1}{2}} & \quad \not\equiv \quad 1 \quad \mod n \\ b^{\frac{n-1}{2}} & \quad \not\equiv \quad -1 \quad \mod n \end{aligned}$$

La demostración del teorema inicial

Sea $c = (b \bmod n)$. Concluimos que $c \notin S_n$ y $c \in \mathbb{Z}_n^*$

- Por lo tanto: $S_n \subsetneq \mathbb{Z}_n^*$

Pero se tiene que $(S_n, \cdot)$ es un subgrupo de $(\mathbb{Z}_n^*, \cdot)$

- ¿Por qué?

Por Teorema de Lagrange: $|S_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$ $\square$

Un test de primalidad aleatorizado

Ya tenemos los ingredientes esenciales para el test de primalidad

- Sólo nos falta implementar algunas funciones auxiliares

Un test de primalidad aleatorizado

Ya tenemos los ingredientes esenciales para el test de primalidad

- Sólo nos falta implementar algunas funciones auxiliares

Necesitamos desarrollar un algoritmo eficiente para determinar si un número n es la potencia (no trivial) de otro número.

Verificando si un número es la potencia de otro

Primero necesitamos una función para calcular n^k

- Usamos el algoritmo de exponenciación rápida pero sin considerar el módulo

Verificando si un número es la potencia de otro

Primero necesitamos una función para calcular n^k

- Usamos el algoritmo de exponenciación rápida pero sin considerar el módulo

EXP(n, k)
    if $k = 1$ **then return** n
    else if k es par **then**
        $val :=$ **EXP**$(n, \frac{k}{2})$
        return $val \cdot val$
    else
        $val :=$ **EXP**$(n, \frac{k-1}{2})$
        return $val \cdot val \cdot n$

Verificando si un número es la potencia de otro

Dado un número natural $n \geq 2$, la siguiente función verifica si existen $m, k \in \mathbb{N}$ tales que $k \geq 2$ y $n = m^k$

EsPotencia(n)
    if $n \leq 3$ **then return** no
    else
        for $k := 2$ **to** $\lfloor \log_2(n) \rfloor$ **do**
            if TieneRaízEntera(n, k, 1, n) **then return** sí
        return no

Verificando si un número es la potencia de otro

La siguiente función verifica si existe $m \in \{i, \ldots, j\}$ tal que $n = m^k$

- Vale decir, la llamada **TieneRaízEntera**$(n,\ k,\ 1,\ n)$ verifica si n tiene raíz k-ésima entera

TieneRaízEntera$(n,\ k,\ i,\ j)$
    if $i = j$ **then**
        if EXP$(i, k) = n$ **then return** sí
        else return no
    else if $i < j$ **then**
        $p := \lfloor \frac{i+j}{2} \rfloor$
        $val :=$ **EXP**(p, k)
        if $val = n$ **then return** sí
        else if $val < n$ **then return TieneRaízEntera**$(n,\ k,\ p+1,\ j)$
        else return TieneRaízEntera$(n,\ k,\ i,\ p-1)$
    else return no

La complejidad de **EsPotencia**

Consideramos la multiplicación de números enteros como la operación básica a contar

Tenemos que:

La complejidad de **EsPotencia**

Consideramos la multiplicación de números enteros como la operación básica a contar

Tenemos que:

- En el peor caso **EsPotencia**(n) realiza ($\lfloor \log_2(n) \rfloor$ - 1) llamadas a la función **TieneRaízEntera**

La complejidad de **EsPotencia**

Consideramos la multiplicación de números enteros como la operación básica a contar

Tenemos que:

- En el peor caso **EsPotencia**(n) realiza $(\lfloor \log_2(n) \rfloor$ - $1)$ llamadas a la función **TieneRaízEntera**
- Existe $c \in \mathbb{N}$ tal que la llamada **TieneRaízEntera**$(n, k, 1, n)$ realiza en el peor caso a lo más $c \cdot \log_2(n)$ llamadas a la función **EXP**

La complejidad de **EsPotencia**

Consideramos la multiplicación de números enteros como la operación básica a contar

Tenemos que:

- En el peor caso **EsPotencia**(n) realiza $(\lfloor \log_2(n) \rfloor$ - $1)$ llamadas a la función **TieneRaízEntera**
- Existe $c \in \mathbb{N}$ tal que la llamada **TieneRaízEntera**$(n, k, 1, n)$ realiza en el peor caso a lo más $c \cdot \log_2(n)$ llamadas a la función **EXP**
- **EXP**(n, k) en el peor caso es $O(\log_2(k))$

La complejidad de **EsPotencia**

Concluimos que **EsPotencia**(n) en el peor caso es $O([\log_2(n)]^3)$

Vale decir, **EsPotencia** en el peor caso es de orden polinomial en el tamaño de la entrada

La complejidad de **EsPotencia**

Concluimos que **EsPotencia**(n) en el peor caso es $O([\log_2(n)]^3)$

Vale decir, **EsPotencia** en el peor caso es de orden polinomial en el tamaño de la entrada

- Se puede llegar a la misma conclusión si consideramos todas las operaciones realizadas por **EsPotencia**

Un test de primalidad aleatorizado

El siguiente algoritmo aleatorizado determina si un número entero $n \geq 2$ es primo.

El algoritmo recibe como entrada un valor entero $k \geq 1$ que es usado para controlar la probabilidad de error.

Un test de primalidad aleatorizado

TestPrimalidad(n, k)
    if $n = 2$ **then return** PRIMO
    else if n es par **then return** COMPUESTO
    else if EsPotencia(n) **then return** COMPUESTO
    else
        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 $b_i :=$ **EXP**($a_i, \frac{n-1}{2}, n$)
        $neg := 0$
        for $i := 1$ **to** k **do**
            if $b_i \equiv -1 \bmod n$ **then** $neg := neg + 1$
            else if $b_i \not\equiv 1 \bmod n$ **then return** COMPUESTO
        if $neg = 0$ **then return** COMPUESTO
        else return PRIMO

Test de primalidad: probabilidad de error

TestPrimalidad se puede equivocar de dos formas:

Test de primalidad: probabilidad de error

TestPrimalidad se puede equivocar de dos formas:

- Suponga que $n \geq 3$ es primo. En este caso **TestPrimalidad** da una respuesta incorrecta si $b_i \equiv 1 \bmod n$ para todo $i \in \{1, \ldots, k\}$

Test de primalidad: probabilidad de error

TestPrimalidad se puede equivocar de dos formas:

- Suponga que $n \geq 3$ es primo. En este caso **TestPrimalidad** da una respuesta incorrecta si $b_i \equiv 1 \bmod n$ para todo $i \in \{1, \ldots, k\}$

  Dado que $|S_n^+| = |S_n^-| = \frac{n-1}{2}$:

  - La probabilidad de que para un número a elegido con distribución uniforme desde $\{1, \ldots, n-1\}$ se tenga que $a^{\frac{n-1}{2}} \equiv 1 \bmod n$ es $\frac{1}{2}$

Test de primalidad: probabilidad de error

TestPrimalidad se puede equivocar de dos formas:

- Suponga que $n \geq 3$ es primo. En este caso **TestPrimalidad** da una respuesta incorrecta si $b_i \equiv 1 \bmod n$ para todo $i \in \{1, \ldots, k\}$

Dado que $|S_n^+| = |S_n^-| = \frac{n-1}{2}$:

- La probabilidad de que para un número a elegido con distribución uniforme desde $\{1, \ldots, n-1\}$ se tenga que $a^{\frac{n-1}{2}} \equiv 1 \bmod n$ es $\frac{1}{2}$

Por lo tanto, la probabilidad de que **TestPrimalidad** diga COMPUESTO para $n \geq 3$ primo es $\left(\frac{1}{2}\right)^k$

Test de primalidad: probabilidad de error

- Suponga que n es compuesto, n es impar y n no es de la forma m^ℓ con $\ell \geq 2$
  - Si n es par o n es de la forma m^ℓ con $\ell \geq 2$, entonces **TestPrimalidad** da la respuesta correcta COMPUESTO

Tenemos entonces que $n = n_1 \cdot n_2$ con $n_1 \geq 3$, $n_2 \geq 3$ y $\text{MCD}(n_1, n_2) = 1$

Test de primalidad: probabilidad de error

- Suponga que n es compuesto, n es impar y n no es de la forma m^ℓ con $\ell \geq 2$
  - Si n es par o n es de la forma m^ℓ con $\ell \geq 2$, entonces **TestPrimalidad** da la respuesta correcta COMPUESTO

Tenemos entonces que $n = n_1 \cdot n_2$ con $n_1 \geq 3$, $n_2 \geq 3$ y $\text{MCD}(n_1, n_2) = 1$

Además debe existir $a \in \{1, \ldots, n-1\}$ tal que $\text{MCD}(a, n) = 1$ y $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

Test de primalidad: probabilidad de error

- Suponga que n es compuesto, n es impar y n no es de la forma m^ℓ con $\ell \geq 2$
  - Si n es par o n es de la forma m^ℓ con $\ell \geq 2$, entonces **TestPrimalidad** da la respuesta correcta COMPUESTO

Tenemos entonces que $n = n_1 \cdot n_2$ con $n_1 \geq 3$, $n_2 \geq 3$ y $\text{MCD}(n_1, n_2) = 1$

Además debe existir $a \in \{1, \ldots, n-1\}$ tal que $\text{MCD}(a, n) = 1$ y $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

  - Si esto no es cierto **TestPrimalidad** retorna COMPUESTO, dado que si **TestPrimalidad** logra llegar a la última instrucción **if** entonces *neg* necesariamente es igual a 0

Test de primalidad: probabilidad de error

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

- Por la caracterización que dimos de S_n para n compuesto

Test de primalidad: probabilidad de error

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

- Por la caracterización que dimos de S_n para n compuesto

Vamos a utilizar este resultado para acotar la probabilidad de error:

$$\Pr\Bigg(\bigg(\bigwedge_{i=1}^{k} \mathrm{MCD}(a_i, n) = 1 \wedge (b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n)\bigg) \wedge \\ \bigg(\bigvee_{j=1}^{k} b_j \equiv -1 \bmod n\bigg)\Bigg)$$

Test de primalidad: probabilidad de error

Tenemos que:

$$\Pr\Bigg(\bigg(\bigwedge_{i=1}^{k} \mathrm{MCD}(a_i, n) = 1 \wedge (b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n)\bigg) \wedge \bigg(\bigvee_{j=1}^{k} b_j \equiv -1 \bmod n\bigg)\Bigg) \leq$$

$$\Pr\bigg(\bigwedge_{i=1}^{k} \mathrm{MCD}(a_i, n) = 1 \wedge (b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n)\bigg)$$

Por lo tanto sólo necesitamos una cota superior para la última expresión.

Test de primalidad: probabilidad de error

Tenemos que:

$$
\begin{aligned}
\Pr\Big(\bigwedge_{i=1}^{k} \mathrm{MCD}(a_i, n) = 1 \wedge (b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n)\Big) \\
= \prod_{i=1}^{k} \Pr(\mathrm{MCD}(a_i, n) = 1 \wedge (b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n)) \\
= \prod_{i=1}^{k} \Pr((b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n) \mid \mathrm{MCD}(a_i, n) = 1) \cdot \\
\Pr(\mathrm{MCD}(a_i, n) = 1) \\
\leq \prod_{i=1}^{k} \Pr((b_i \equiv 1 \bmod n \vee b_i \equiv -1 \bmod n) \mid \mathrm{MCD}(a_i, n) = 1) \\
= \prod_{i=1}^{k} \Pr(a_i \in S_n \mid a_i \in \mathbb{Z}_n^*) \ \leq \ \prod_{i=1}^{k} \frac{1}{2} \ = \ \frac{1}{2^k}
\end{aligned}
$$

Test de primalidad: probabilidad de error

Concluimos que la probabilidad de que el test diga PRIMO para el valor compuesto n está acotada por $\left(\frac{1}{2}\right)^k$

Test de primalidad: probabilidad de error

Concluimos que la probabilidad de que el test diga PRIMO para el valor compuesto n está acotada por $\left(\frac{1}{2}\right)^k$

En ambos casos (si n es primo o compuesto) la probabilidad de error del algoritmo está acotada por $\left(\frac{1}{2}\right)^k$

Test de primalidad: probabilidad de error

Concluimos que la probabilidad de que el test diga PRIMO para el valor compuesto n está acotada por $\left(\frac{1}{2}\right)^k$

En ambos casos (si n es primo o compuesto) la probabilidad de error del algoritmo está acotada por $\left(\frac{1}{2}\right)^k$

- ¡Si $k = 100$, está probabilidad está acotada por $\left(\frac{1}{2}\right)^{100} \approx 7.9 \times 10^{-31}$!