Un tercer ejemplo: verificación de primalidad

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

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

Un tercer ejemplo: verificación de primalidad

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

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

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

- Vamos a repasar algunos conceptos y resultados fundamentales sobre ella

Para recordar: aritmética modular

Dados dos números $a, b \in \mathbb{Z}$, si $b > 0$ entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que $0 \leq \beta < b$ y

$$a = \alpha \cdot b + \beta$$

Además, estos números α, β son únicos

β es llamado el resto de la división entera entre a y b, y es denotado como $a \bmod b$

- Por ejemplo, $8 \bmod 3 = 2$, $9 \bmod 3 = 0$ y $(-8) \bmod 3 = 1$

Para recordar: aritmética modular

Definición

$b \equiv c \bmod n$ *si* n *divide a* $(c - b)$

Usamos la notación $n|m$ para indicar que n divide a m

- $b \equiv c \bmod n$ si $n|(c - b)$

Para recordar: algunas propiedades básicas

Proposición

1. $a \equiv b \bmod n$ *si y sólo si* $a \bmod n = b \bmod n$
2. $a \equiv (a \bmod n) \bmod n$
3. *Si* $a \equiv b \bmod n$ *y* $c \equiv d \bmod n$, *entonces:*

$$\begin{aligned} (a + c) &\equiv (b + d) \quad \bmod n \\ (a \cdot c) &\equiv (b \cdot d) \quad \bmod n \end{aligned}$$

Para recordar: algunas propiedades básicas

Proposición

1. $a \equiv b \bmod n$ *si y sólo si* $a \bmod n = b \bmod n$
2. $a \equiv (a \bmod n) \bmod n$
3. *Si* $a \equiv b \bmod n$ *y* $c \equiv d \bmod n$, *entonces:*

$$\begin{aligned} (a + c) &\equiv (b + d) \bmod n \\ (a \cdot c) &\equiv (b \cdot d) \bmod n \end{aligned}$$

Ejercicios

1. Demuestre la proposición
2. Demuestre que un número n es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3

Para recordar: una propiedad fundamental

Teorema (Fermat)

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

Para recordar: una propiedad fundamental

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:

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

Para recordar: una propiedad fundamental

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:

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

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

Para recordar: una propiedad fundamental

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

- Concluimos que $p | \binom{p}{k}$ □

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

Para recordar: una propiedad fundamental

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

- Concluimos que $p | \binom{p}{k}$ □

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

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

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

Aritmética modular: una propiedad fundamental

Corolario (Fermat)

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

Aritmética modular: una propiedad fundamental

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

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

Aritmética modular: una propiedad fundamental

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 $a^{p-1} \equiv 1 \bmod p$ □

Otra noción importante: máximo común divisor

Sea MCD(a, b) el máximo común divisor de los números a y b

- ¿Cómo podemos calcular MCD(a, b)?

Otra noción importante: máximo común divisor

Sea MCD(a, b) el máximo común divisor de los números a y b

- ¿Cómo podemos calcular MCD(a, b)?

Proposición

Si $b > 0$, *entonces* $MCD(a, b) = MCD(b, a \bmod b)$

Otra noción importante: máximo común divisor

Sea MCD(a, b) el máximo común divisor de los números a y b

- ¿Cómo podemos calcular MCD(a, b)?

Proposición

Si $b > 0$, *entonces* $MCD(a, b) = MCD(b, a \bmod b)$

Demostración: Vamos a demostrar que un número c divide a a y b si y sólo si c divide a b y $a \bmod b$

- De esto se concluye que MCD$(a, b) =$ MCD$(b, a \bmod b)$

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$

($\Rightarrow$) Suponga que $c|a$ y $c|b$.

Dado que $(a \bmod b) = a - \alpha \cdot b$, concluimos que $c|(a \bmod b)$.

($\Leftarrow$) Suponga que $c|b$ y $c|(a \bmod b)$.

Dado que $a = \alpha \cdot b + (a \bmod b)$, tenemos que $c|a$ $\square$

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad para $a > 0$:

$$\text{MCD}(a, b) = \begin{cases} a & b = 0 \\ \text{MCD}(b, a \bmod b) & b > 0 \end{cases}$$

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad para $a > 0$:

$$\text{MCD}(a, b) = \begin{cases} a & b = 0 \\ \text{MCD}(b, a \bmod b) & b > 0 \end{cases}$$

Usamos esta identidad para generar un algoritmo para calcular el máximo común divisor:

MCD(a, b)
    if $a = 0$ **and** $b = 0$ **then return** error
    else if $a = 0$ **then return** b
    else if $b = 0$ **then return** a
    else if $a \geq b$ **then return** **MCD**(b, $a \bmod b$)
    else return **MCD**(a, $b \bmod a$)

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad para $a > 0$:

$$\text{MCD}(a, b) = \begin{cases} a & b = 0 \\ \text{MCD}(b, a \bmod b) & b > 0 \end{cases}$$

Usamos esta identidad para generar un algoritmo para calcular el máximo común divisor:

MCD(a, b)
    if $a = 0$ **and** $b = 0$ **then return** error
    else if $a = 0$ **then return** b
    else if $b = 0$ **then return** a
    else if $a \geq b$ **then return MCD**(b, $a \bmod b$)
    else return MCD(a, $b \bmod a$)

¿Cuál es la complejidad del algoritmo?

La complejidad del algoritmo

Lema

Si $a \geq b$ *y* $b > 0$, *entonces* $(a \bmod b) < \frac{a}{2}$

La complejidad del algoritmo

Lema

Si $a \geq b$ *y* $b > 0$, *entonces* $(a \bmod b) < \frac{a}{2}$

Demostración: Si $b > \frac{a}{2}$:

$$a \bmod b \;=\; a - b \;<\; a - \frac{a}{2} \;=\; \frac{a}{2}$$

La complejidad del algoritmo

Si $b < \frac{a}{2}$, existe k tal que $\frac{a}{2} < k \cdot b \leq a$.

Por lo tanto:

$$a \bmod b \;\leq\; a - k \cdot b \;<\; a - \frac{a}{2} \;=\; \frac{a}{2}$$

Si $b = \frac{a}{2}$ (a debe ser par):

$$a \bmod b \;=\; 0 \;<\; b \;\leq\; a$$

□

La complejidad del algoritmo

Ejercicio

Suponga que la operación básica para el algoritmo **MCD** es el cálculo de la función $x \bmod y$. Muestre entonces que el algoritmo en el peor caso es $O(\log_2(\text{máx}\{a, b\}))$, suponiendo que la entrada es (a, b)

- Vale decir, **MCD** es de orden lineal en el tamaño de la entrada en el peor caso

Una identidad útil

Identidad de Bézout

Para cada $a, b \in \mathbb{N}$ tales que $a \neq 0$ o $b \neq 0$, existen $s, t \in \mathbb{Z}$ tales que:

$$\text{MCD}(a, b) \quad = \quad s \cdot a + t \cdot b$$

Una identidad útil

Identidad de Bézout

Para cada $a, b \in \mathbb{N}$ tales que $a \neq 0$ o $b \neq 0$, existen $s, t \in \mathbb{Z}$ tales que:

$$\text{MCD}(a, b) \quad = \quad s \cdot a + t \cdot b$$

Demostración: Sea

$$D \quad = \quad \{n \in \mathbb{N} \mid n > 0 \text{ y existen } s, t \in \mathbb{Z} \text{ tal que } n = s \cdot a + t \cdot b\}$$

Dado que $a \neq 0$ o $b \neq 0$, se tiene que $D \neq \emptyset$ y, por lo tanto, D tiene un menor elemento

- Sea d este elemento, y suponga que $d = s_0 \cdot a + t_0 \cdot b$

Una identidad útil

Existen $\alpha, \beta \in \mathbb{N}$ tales que $0 \leq \beta < d$ y $a = \alpha \cdot d + \beta$

Una identidad útil

Existen $\alpha, \beta \in \mathbb{N}$ tales que $0 \leq \beta < d$ y $a = \alpha \cdot d + \beta$

Como $d = s_0 \cdot a + t_0 \cdot b$, tenemos que $\alpha \cdot d = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

- Concluimos que $a - \beta = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

Una identidad útil

Existen $\alpha, \beta \in \mathbb{N}$ tales que $0 \leq \beta < d$ y $a = \alpha \cdot d + \beta$

Como $d = s_0 \cdot a + t_0 \cdot b$, tenemos que $\alpha \cdot d = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

- Concluimos que $a - \beta = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

Entonces tenemos que $\beta = (1 - \alpha \cdot s_0) \cdot a + (-\alpha \cdot t_0) \cdot b$

Una identidad útil

Existen $\alpha, \beta \in \mathbb{N}$ tales que $0 \leq \beta < d$ y $a = \alpha \cdot d + \beta$

Como $d = s_0 \cdot a + t_0 \cdot b$, tenemos que $\alpha \cdot d = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

- Concluimos que $a - \beta = \alpha \cdot s_0 \cdot a + \alpha \cdot t_0 \cdot b$

Entonces tenemos que $\beta = (1 - \alpha \cdot s_0) \cdot a + (-\alpha \cdot t_0) \cdot b$

Dado que $0 \leq \beta < d$ y d es el menor elemento en D, concluimos que $\beta = 0$

- Por lo tanto $d|a$

Una identidad útil

De la misma forma concluimos que $d|b$

Una identidad útil

De la misma forma concluimos que $d|b$

Sea $c \in \mathbb{N}$ tal que $c|a$ y $c|b$

Una identidad útil

De la misma forma concluimos que $d|b$

Sea $c \in \mathbb{N}$ tal que $c|a$ y $c|b$

Se tiene entonces que $c|(s_0 \cdot a + t_0 \cdot b)$

- Por lo tanto $c|d$, lo cual implica que $c \leq d$

Una identidad útil

De la misma forma concluimos que $d|b$

Sea $c \in \mathbb{N}$ tal que $c|a$ y $c|b$

Se tiene entonces que $c|(s_0 \cdot a + t_0 \cdot b)$

- Por lo tanto $c|d$, lo cual implica que $c \leq d$

Concluimos que $d|a$, $d|b$ y para todo c tal que $c|a$ y $c|b$, se tiene que $c \leq d$

- Por lo tanto $d = \text{MCD}(a, b)$ □

Una última noción importante: inverso modular

Definición

b es inverso de a en módulo n si $a \cdot b \equiv 1 \bmod n$

Una última noción importante: inverso modular

Definición

b es inverso de a en módulo n si $a \cdot b \equiv 1 \bmod n$

Ejemplo

37 es inverso de 13 en módulo 60

Una última noción importante: inverso modular

Definición

b es inverso de a en módulo n si $a \cdot b \equiv 1 \bmod n$

Ejemplo

37 es inverso de 13 en módulo 60

¿Todo número tiene inverso modular?

Una última noción importante: inverso modular

Definición

b es inverso de a en módulo n si $a \cdot b \equiv 1 \bmod n$

Ejemplo

37 es inverso de 13 en módulo 60

¿Todo número tiene inverso modular?

- No, 2 no tiene inverso en módulo 4

Una última noción importante: inverso modular

Definición

b es inverso de a en módulo n si $a \cdot b \equiv 1 \, mod \, n$

Ejemplo

37 es inverso de 13 en módulo 60

¿Todo número tiene inverso modular?

- No, 2 no tiene inverso en módulo 4

¿Bajo qué condiciones *a* tiene inverso en módulo *n*?

Una última noción importante: inverso modular

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$

Una última noción importante: inverso modular

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$

Demostración: ($\Rightarrow$) Suponga que b es inverso de a en módulo n

- Entonces: $a \cdot b \equiv 1 \bmod n$

Se deduce que $a \cdot b = \alpha \cdot n + 1$, por lo que $1 = a \cdot b - \alpha \cdot n$

Concluimos que si $c|a$ y $c|n$, entonces $c|1$

- Por lo tanto c debe ser igual a 1, de lo que concluimos que $\text{MCD}(a, n) = 1$

Inverso modular: existencia

($\Leftarrow$) Suponga que $\text{MCD}(a, n) = 1$

Por la identidad de Bézout existen $s, t \in \mathbb{Z}$ tales que:

$$1 \quad = \quad s \cdot n + t \cdot a$$

Por lo tanto: $a \cdot t \equiv 1 \bmod n$

- Concluimos que a tiene inverso en módulo n $\square$

Test de primalidad: primer ingrediente

El test de primalidad que vamos a estudiar está basado en estas propiedades ($n \geq 3$):

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: primer ingrediente

El test de primalidad que vamos a estudiar está basado en estas propiedades ($n \geq 3$):

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 □

Test de primalidad: primer ingrediente

Para $n \geq 2$, sea:

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

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

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

Test de primalidad: primer ingrediente

Para $n \geq 2$, sea:

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

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

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

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

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 un número compuesto n, el conjunto $\mathbb{Z}_n^*$ puede tener un gran número de elementos.

- No podemos basar nuestro test en los elementos del conjunto $(\{1, \ldots, n-1\} \setminus \mathbb{Z}_n^*)$

Test de primalidad: segundo ingrediente

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: segundo ingrediente

¿Cómo funcionaría el test de primalidad?

- ¿Con que salidas se podría equivocar? ¿Cuál sería la probabilidad de error?

Test de primalidad: segundo ingrediente

¿Cómo funcionaría el test de primalidad?

- ¿Con que salidas se podría equivocar? ¿Cuál sería la probabilidad de error?

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

Test de primalidad: segundo ingrediente

¿Cómo funcionaría el test de primalidad?

- ¿Con que salidas se podría equivocar? ¿Cuál sería la probabilidad de error?

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

- Teoría de grupos juega también 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 $c = b$

Subgrupos: demostración de las propiedades básicas

- Suponga que e_1 es el neutro en $(G, \circ)$ y e_2 es el neutro de $(H, \circ)$
  - Vamos a demostrar que $e_1 = e_2$

Dado que e_1 es el neutro en $(G, \circ)$: $e_2 \circ e_1 = e_2$

Dado que e_2 es el neutro en $(H, \circ)$: $e_2 \circ e_2 = e_2$

- Nótese que usamos la misma operación en H y G

Concluimos que $e_2 \circ e_1 = e_2 \circ e_2$

Subgrupos: demostración de las propiedades básicas

Sea e_2^{-1} el inverso de e_2 en $(G, \circ)$. Entonces:

$$
\begin{aligned}
e_2 \circ e_1 = e_2 \circ e_2 \quad &\Rightarrow \quad e_2^{-1} \circ (e_2 \circ e_1) = e_2^{-1} \circ (e_2 \circ e_2) \\
&\Rightarrow \quad (e_2^{-1} \circ e_2) \circ e_1 = (e_2^{-1} \circ e_2) \circ e_2 \\
&\Rightarrow \quad e_1 \circ e_1 = e_1 \circ e_2 \\
&\Rightarrow \quad e_1 = e_2
\end{aligned}
$$

Por lo tanto: $e_1 = e_2$

Subgrupos: demostración de las propiedades básicas

- Sea $a \in H$, y suponga que b es el inverso de a en $(G, \circ)$ y c es el inverso de a en $(H, \circ)$
  - Vamos a demostrar que $c = b$

Sea e el neutro en $(G, \circ)$ y $(H, \circ)$

- Por la primera propiedad, sabemos que $(G, \circ)$ y $(H, \circ)$ tienen el mismo neutro

Dado que b es el inverso de a en $(G, \circ)$: $a \circ b = e$

Dado que c es el inverso de a en $(H, \circ)$: $a \circ c = e$

Subgrupos: demostración de las propiedades básicas

Concluimos que: $a \circ b = a \circ c$

Sea a^{-1} el inverso de a en $(G, \circ)$. Entonces:

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

Por lo tanto: $b = c$ □

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* $|G|$

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: $c \circ a^{-1} \in H$ □

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:

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

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:

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

Teorema de Lagrange: demostración del segundo lema

f es sobre:

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

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: segundo ingrediente (continuación)

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

Test de primalidad: segundo ingrediente (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: segundo ingrediente (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 $a \in (\mathbb{Z}_n^* \setminus J_n)$, entonces $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$

Test de primalidad: segundo ingrediente (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 $a \in (\mathbb{Z}_n^* \setminus J_n)$, entonces $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$

¿Tenemos entonces nuestro test de primalidad?

Test de primalidad: segundo ingrediente (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 $a \in (\mathbb{Z}_n^* \setminus J_n)$, 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: segundo ingrediente (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 $a \in (\mathbb{Z}_n^* \setminus J_n)$, entonces $|J_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$

¿Tenemos entonces nuestro test de primalidad?

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

Test de primalidad: segundo ingrediente (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: segundo ingrediente (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: tercer ingrediente

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

Test de primalidad: tercer ingrediente

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

¿Qué hacemos entonces?

Test de primalidad: tercer ingrediente

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?

□

La estructura de S_n y las raíces modulares

Definition

b es una raíz cuadrada de a en módulo n si $b^2 \equiv a \bmod n$

Ejemplo

3 es una raíz cuadrada de 9 en módulo 16, y 3 es una raíz cuadrada de 4 en módulo 5.

Vamos a ver que hay una relación estrecha entre S_n y las raíces cuadradas modulares.

- Esta relación es fundamental para el test de primalidad

La estructura de S_n y las raíces modulares

Teorema

Sea $n \geq 3$ un primo y $a \in \{1, \ldots, n-1\}$. Entonces a tiene raíz cuadrada en módulo n si y sólo si $a^{\frac{n-1}{2}} \equiv 1 \, mod \, n$

La estructura de S_n y las raíces modulares

Teorema

Sea $n \geq 3$ un primo y $a \in \{1, \ldots, n-1\}$. Entonces a tiene raíz cuadrada en módulo n si y sólo si $a^{\frac{n-1}{2}} \equiv 1 \, mod \, n$

Demostración: ($\Rightarrow$) Suponga que a tiene raíz cuadrada en módulo n

- Sea $b \in \{1, \ldots, n-1\}$ tal que $b^2 \equiv a \bmod n$

Se tiene que:

$$\begin{aligned} a^{\frac{n-1}{2}} &\equiv (b^2)^{\frac{n-1}{2}} && \bmod n \\ &\equiv b^{n-1} && \bmod n \\ &\equiv 1 && \bmod n \end{aligned}$$

Existencia de raíces modulares: demostración

($\Leftarrow$) Para demostrar esta dirección del teorema, 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 $p(a) \equiv 0 \bmod n$

Existencia de raíces modulares: demostración

Lema

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

Existencia de raíces modulares: demostración

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

Existencia de raíces modulares: demostración

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

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

De la propiedad anterior se concluye que el lema es cierto.

- ¿Por qué?

Existencia de raíces modulares: demostración

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

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

De la propiedad anterior se concluye que el lema es cierto.

- ¿Por qué?

Definimos $q(x)$ como:

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

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

Existencia de raíces modulares: 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:

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

Existencia de raíces modulares: 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:

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

Existencia de raíces modulares: 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:

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

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

Tenemos entonces que:

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

Existencia de raíces modulares: demostración

Volvemos a la demostración inicial:

- Queremos demostrar que si $a^{\frac{n-1}{2}} \equiv 1 \bmod n$, entonces a tiene raiz en módulo n

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

Como $b^2 \equiv (n-b)^2 \bmod n$, se tiene que:

a tiene raiz en módulo n si y sólo si $a \in R$

Existencia de raíces modulares: demostración

Por ($\Rightarrow$) sabemos 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

Obtenemos una contradicción puesto que $1 \leq (c-b) \leq \frac{n-1}{2}$

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

Existencia de raíces modulares: demostración

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

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

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:

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

Así, si $a^{\frac{n-1}{2}} \equiv 1 \bmod n$, se tiene que a tiene raíz en módulo n $\square$

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

Si $n \geq 3$ es primo, dado que $S_n = \mathbb{Z}_n^*$, obtenemos por el teorema:

- Si a no tiene raíz en módulo n, entonces $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

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

Si $n \geq 3$ es primo, dado que $S_n = \mathbb{Z}_n^*$, obtenemos por el teorema:

- Si a no tiene raíz en módulo n, entonces $a^{\frac{n-1}{2}} \equiv -1 \bmod n$

Así, obtenemos el siguiente corolario de los resultados anteriores.

Corolario

Si $n \geq 3$ es primo:

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

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* $MCD(n_1, n_2) = 1$. *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:*

$$c \equiv a \mod m$$
$$c \equiv b \mod n$$

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 $\text{MCD}(m, n) = 1$, 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:

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

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:

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

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:

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

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

- Por lo tanto 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:

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

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

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

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

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 e implementar algoritmos eficientes para:

- Una función que determina si un número n es la potencia (no trivial) de otro número
- Una función para calcular $a^b \bmod n$

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

Verificando si un número es la potencia de otro

Finalmente, la siguiente función calcula n^k

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

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

Calculando la función $a^b \bmod n$

En general, no podemos invocar a **Exp**(a, b) y luego sacar módulo n para calcular $a^b \bmod n$

- El valor de $a^b \bmod n$ está acotado por n, mientras que a^b puede tener un valor demasiado grande

Calculando la función $a^b \bmod n$

En general, no podemos invocar a **Exp**(a, b) y luego sacar módulo n para calcular $a^b \bmod n$

- El valor de $a^b \bmod n$ está acotado por n, mientras que a^b puede tener un valor demasiado grande

Utilizamos entonces la siguiente función para calcular $a^b \bmod n$:

Exp(a, b, n)
  if $b = 1$ **then return** $a \bmod n$
  else if b es par **then**
    $val := \textbf{Exp}(a, \frac{b}{2}, n)$
    return $(val \cdot val) \bmod n$
  else
    $val := \textbf{Exp}(a, \frac{b-1}{2}, n)$
    return $(val \cdot val \cdot a) \bmod n$

La complejidad de **Exp**

Ejercicio

Considerando la multiplicación de enteros y el cálculo de la función $x \bmod y$ como las operaciones básicas a contar, demuestre que **Exp**(a, b, n) en el peor caso es $O(\log_2(b))$