Complejidad Probabilística

IIC3242

Complejidad probabilística

En esta capítulo vamos a estudiar algoritmos que utilizan una fuente de números aleatorios para resolver problemas.

El uso de aleatoriedad puede llevar a distintas situaciones:

- El algoritmo puede retornar una respuesta incorrecta con cierta probabilidad
- El algoritmo puede no dar una respuesta con cierta probabilidad
- ...

Complejidad probabilística

Esto da origen a la noción de clase de complejidad probabilística

- Clase de problemas que pueden ser resueltos con cierto tipo de algoritmos que usan aleatoriedad

Para empezar: Vamos a estudiar uno de los problema que motivó el estudio de este tipo de algoritmos.

Criptografía de clave pública

Se tiene dos funciones E y D:

- E sirve para encriptar y D para desencriptar: $D(E(M)) = M$
- E no puede usarse para desencriptar: $E(E(M)) \neq M$
- E y D están relacionadas, pero es difícil descubrir D a partir de E

Vamos a ver un ejemplo de este tipo de sistemas: RSA

El sistema criptográfico RSA

Algoritmo:

1. Adivine dos números primos distintos P y Q
2. Sean $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$
3. Sean e y d dos números tales que $e \cdot d \bmod \phi(N) = 1$
4. Entonces:

$$\begin{aligned} E(M) &= M^e \bmod N \\ D(M) &= M^d \bmod N \end{aligned}$$

Decimos que (e, N) es la clave pública y (d, N) es la clave privada

El sistema criptográfico RSA

Ejemplo

Sean $P = 7$ y $Q = 11$

- Se tiene que $N = 77$ y $\phi(N) = 60$

Sean $e = 13$ y $d = 37$

- Se tiene que $13 \cdot 37 \bmod 60 = 1$

Entonces: $E(M) = M^{13} \bmod 77$ y $D(M) = M^{37} \bmod 77$

Para $M = 5$:

$$\begin{array}{lcll} E(5) & = & 5^{13} \bmod 77 & = & 26 \\ D(E(5)) & = & 26^{37} \bmod 77 & = & 5 \end{array}$$

¿Por qué funciona RSA?

¿Qué propiedades debemos demostrar que son ciertas?

- $D(E(M)) = M$ para todo $M \in \{0, \ldots, N-1\}$

¿Qué problemas debemos demostrar que pueden ser resueltos de manera eficiente?

- Generar primos P y Q: Verificar si un número es primo
- Generar números e y d tales que $e \cdot d \bmod \phi(N) = 1$
- Calcular funciones E y D

¿Qué problemas no pueden ser resueltos de manera eficiente?

- Dado (e, N) calcular d: Encontrar los divisores de N

¿Por qué funciona RSA?

Vamos a responder las preguntas anteriores.

- Componente esencial para demostrar que RSA funciona: Aritmética modular
- Componente esencial para implementar RSA: Algoritmos probabilísticos

Vamos a estudiar estas dos áreas.

Aritmética modular

Definición

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

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

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

Vamos a estudiar algunas propiedades fundamentales de $\equiv$.

Aritmética modular: Propiedades básicas

Proposición

$a \equiv b \bmod n$ *si y sólo si* $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{aligned} a &= \alpha \cdot n + \beta & 0 \leq \beta < n \\ b &= \gamma \cdot n + \delta & 0 \leq \delta < n \end{aligned}$$

Por hipótesis: $\beta = \delta$

- Puesto que $a \bmod n = \beta$ y $b \bmod n = \delta$

Tenemos que: $(b - a) = (\gamma - \alpha) \cdot n$

- Por lo tanto: $n | (b - a)$

Aritmética modular: Propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$)

Sin perdida de generalidad suponemos que $\beta < \delta$

Se tiene que:

$$b - a \quad = \quad (\gamma - \alpha) \cdot n + (\delta - \beta)$$

Pero: $1 \leq (\delta - \beta) \leq \delta < n$

- Por lo tanto: $n \not| (b - a)$

Aritmética modular: Propiedades básicas

Corolario

$\equiv$ *es una relación de equivalencia.*

Corolario

$a \equiv (a \bmod n) \bmod n$

Ejercicio

Demuestre los corolarios

Aritmética modular: Propiedades básicas

Proposición

Si $a \equiv b \bmod n$ *y* $c \equiv d \bmod n$, *entonces:*

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

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
3. De una regla de división para el número 11

Aritmética modular: 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:

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

Aritmética modular: 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

Aritmética modular: 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 $a^{p-1} \equiv 1 \, mod \, p$.

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 $a^{p-1} \equiv 1 \bmod p$ □

RSA funciona correctamente

Sean E y D construidas como fue mencionado en las transparencias anteriores.

- $N = P \cdot Q$, $E(M) = M^e \bmod N$ y $D(M) = M^d \bmod N$

Teorema (Rivest-Shamir-Adleman)

Para cada $M \in \{0, \ldots, N-1\}$, se tiene que $D(E(M)) = M$.

Demostración: Sabemos que

$$\begin{aligned} D(E(M)) &= (M^e \bmod N)^d \bmod N \\ &= (M^e)^d \bmod N \\ &= M^{e \cdot d} \bmod N \end{aligned}$$

Por lo tanto, tenemos que demostrar que $M^{e \cdot d} \equiv M \bmod N$

RSA funciona correctamente: Demostración

Sabemos que $e \cdot d \equiv 1 \bmod \phi(N)$

- Por lo tanto: $e \cdot d = k \cdot \phi(N) + 1$

Tenemos que demostrar que $M^{k \cdot \phi(N)+1} \equiv M \bmod N$

- El siguiente lema es fundamental para la demostración

Lema

$M^{k \cdot \phi(N)+1} \equiv M \bmod P$ y $M^{k \cdot \phi(N)+1} \equiv M \bmod Q$

Demostración: Primero suponemos que $P|M$.

RSA funciona correctamente: Demostración

Entonces:
$$\begin{aligned} M^{k\cdot\phi(N)+1} \bmod P &= (M \bmod P)^{k\cdot\phi(N)+1} \bmod P \\ &= 0^{k\cdot\phi(N)+1} \bmod P \\ &= 0 \end{aligned}$$

Por lo tanto: $M^{k\cdot\phi(N)+1} \equiv M \bmod P$

En segundo lugar, suponemos que $P \not| M$.

- Sea $R = M \bmod P$

Dado que $R \in \{1, \ldots, P-1\}$, por teorema de Fermat:

$$R^{P-1} \equiv 1 \bmod P$$

Por lo tanto, dado que $R \equiv M \bmod P$:

$$M^{P-1} \equiv 1 \bmod P$$

RSA funciona correctamente: Demostración

De esto concluimos que:

$$\begin{aligned} M^{k\cdot\phi(N)+1} \bmod N &= ((M^{P-1})^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= ((M^{P-1} \bmod P)^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= (1^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= M \bmod P \end{aligned}$$

Concluimos que $M^{k\cdot\phi(N)+1} \equiv M \bmod P$

- De la misma forma se demuestra que $M^{k\cdot\phi(N)+1} \equiv M \bmod Q$

RSA funciona correctamente: Demostración

Del lema concluimos que:

$$M^{k\cdot\phi(N)+1} - M = \alpha \cdot P$$
$$M^{k\cdot\phi(N)+1} - M = \beta \cdot Q$$

Por lo tanto: $\alpha \cdot P = \beta \cdot Q$

Entonces, dado que P y Q son primos distintos tenemos que $P|\beta$

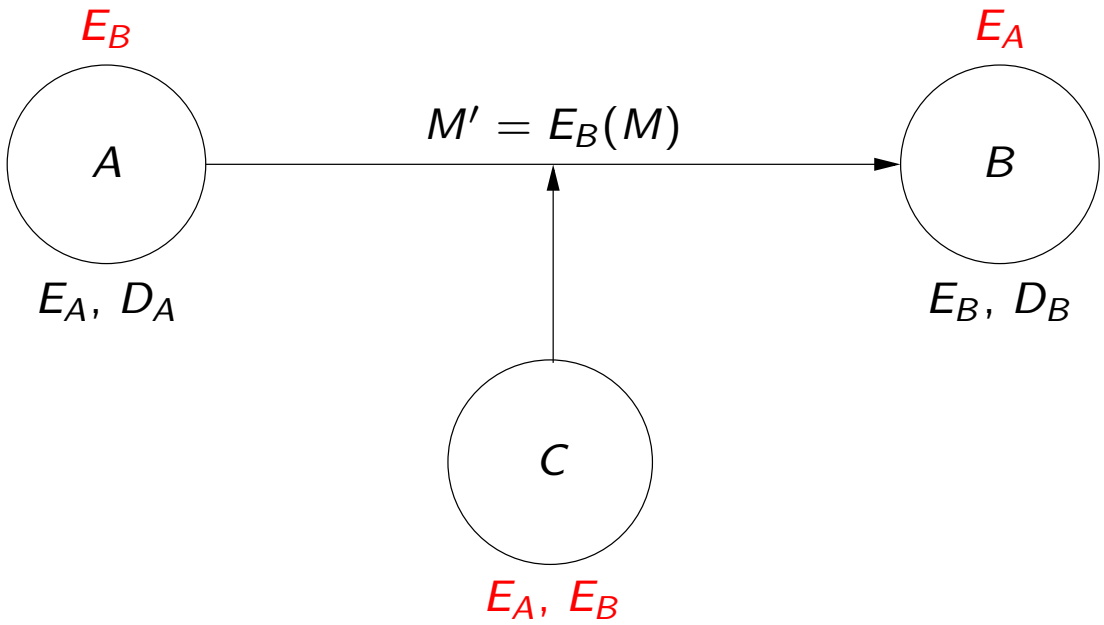
- $\beta = \gamma \cdot P$

Concluimos que $M^{k\cdot\phi(N)+1} - M = \gamma \cdot P \cdot Q$

- Vale decir: $M^{k\cdot\phi(N)+1} \equiv M \bmod N$ □

RSA: Autentificación y firma digitales

Escenario usual para RSA:



Dos preguntas a responder:

- Autentificación: ¿Cómo puede saber A si E_B es efectivamente la clave pública de B?
- Firma digital: ¿Cómo puede saber B si el mensaje M' fue efectivamente enviado por A?

RSA: Autentificación y firma digitales

Una propiedad fundamental de RSA: $E(D(M)) = M$

- Usamos esta propiedad para resolver los problemas de autentificación y firma digital

Autentificación: Suponemos que existe una organización certificadora I

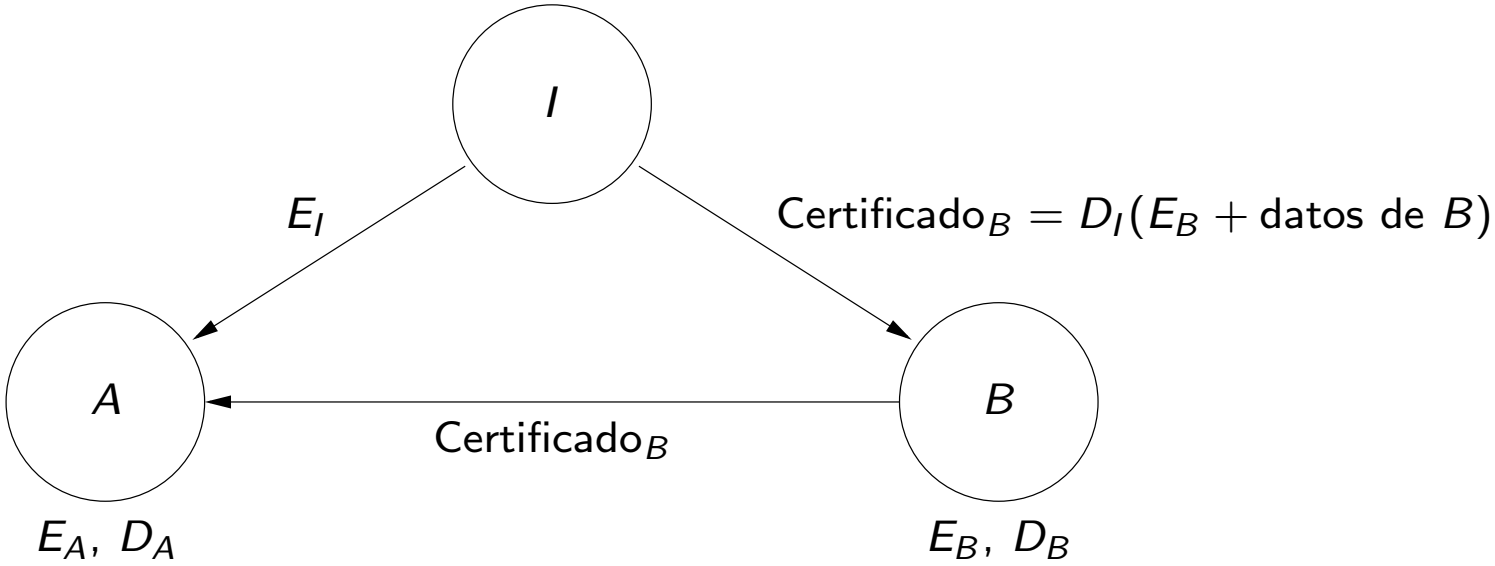
- Todos tienen acceso seguro a E_I

¿Cómo puede ser implementada la organización certificadora?

- ¿Por qué podemos suponer que tenemos acceso seguro a E_I?

RSA: Autentificación

Organización certificadora funciona de la siguiente forma:

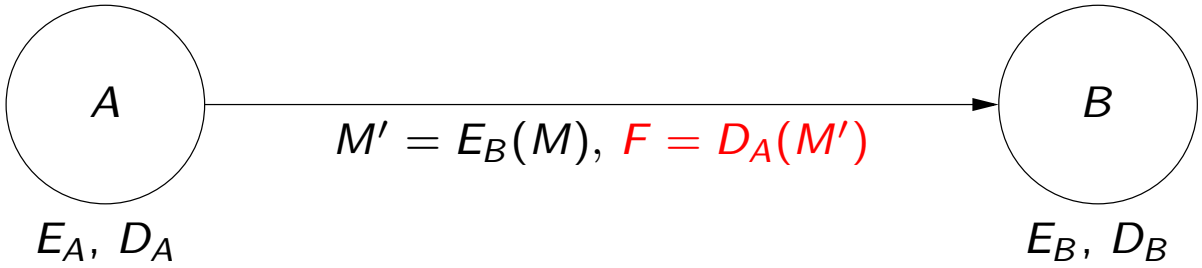


Tenemos entonces el siguiente protocolo:

- I entrega a B un certificado Certificado$_B$
- Para saber la clave pública de B (y los datos relevantes de B), A utiliza E_I(Certificado$_B$)

RSA: Firma digital

Envío de mensajes firmados: A envía tanto el mensaje M' como una firma F:



B recibe M' y F:

- Verificación: ¿Es cierto que $M' = E_A(M')$?
- Mensaje a leer: $D_B(M')$

RSA: Implementación

Para poder implementar RSA necesitamos algoritmos eficientes para los siguientes problemas:

(1) Generar primos P y Q

(2) Generar números e y d tales que $e \cdot d \bmod \phi(N) = 1$

(3) Calcular funciones E y D

Ya resolvimos (3), ahora vamos a resolver (2).

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:

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

Podemos usar esta identidad para generar un algoritmos recursivo para calcular el máximo común divisor.

- ¿Cuál es la complejidad del algoritmo?

Cálculo de máximo común divisor

Lema

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

Demostración: Si $b > \frac{a}{2}$:

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

Cálculo de máximo común divisor

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):

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

Cálculo de máximo común divisor

Concluimos que el algoritmo basado en la identidad calcula $\text{MCD}(a, b)$ en tiempo $O(\log a)$.

¡Pero este algoritmo puede hacer más!

- Puede ser extendido para calcular s y t tales que $\text{MCD}(a, b) = s \cdot a + t \cdot b$

Vamos a usar este algoritmo para calcular los coeficiente d y e usados en RSA.

- Vamos a usar este algoritmo para calcular *inversos modulares*

Algoritmo extendido para calcular el máximo común divisor

Suponga que $a \geq b$, y defina la siguiente sucesión:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{i+1} &= r_{i-1} \bmod r_i \qquad (i \geq 2) \end{aligned}$$

Calculamos esta sucesión hasta un número k tal que $r_k = 0$

- Tenemos que $\text{MCD}(a, b) = r_{k-1}$

Algoritmo extendido para calcular el máximo común divisor

Al mismo tiempo calculamos sucesiones s_i, t_i tales que:

$$r_i = s_i \cdot a + t_i \cdot b$$

Tenemos que: $\text{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

Sean:

$$s_0 = 1 \qquad t_0 = 0$$
$$s_0 = 0 \qquad t_0 = 1$$

Se tiene que:

$$r_0 = s_0 \cdot a + t_0 \cdot b$$
$$r_1 = s_1 \cdot a + t_1 \cdot b$$

Algoritmo extendido para calcular el máximo común divisor

Dado que $r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i-1} \bmod r_i$, tenemos que:

$$r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i+1}$$

Por lo tanto:

$$s_{i-1} \cdot a + t_{i-1} \cdot b = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot (s_i \cdot a + t_i \cdot b) + r_{i+1}$$

Concluimos que:

$$r_{i+1} = (s_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot s_i) \cdot a + (t_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot t_i) \cdot b$$

Definimos entonces:

$$s_{i+1} = s_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot s_i$$

$$t_{i+1} = t_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot t_i$$

Algoritmo extendido para calcular el máximo común divisor

Ejemplo

Vamos a usar el algoritmo para $a = 60$ y $b = 13$.

Inicialmente:

$$\begin{array}{lll} r_0 = 60 & s_0 = 1 & t_0 = 0 \\ r_1 = 13 & s_1 = 0 & t_1 = 1 \end{array}$$

Entonces tenemos que:

$$\begin{aligned} r_2 &= r_0 \bmod r_1 \\ s_2 &= s_0 - \lfloor \frac{r_0}{r_1} \rfloor \cdot s_1 \\ t_2 &= t_0 - \lfloor \frac{r_0}{r_1} \rfloor \cdot t_1 \end{aligned}$$

Algoritmo extendido para calcular el máximo común divisor

Example (Continuación)

Por lo tanto:

$$r_2 = 8 \qquad s_2 = 1 \qquad t_2 = -4$$

Y el proceso continua:

$$\begin{array}{lll} r_3 = 5 & s_3 = -1 & t_3 = 5 \\ r_4 = 3 & s_4 = 2 & t_4 = -9 \\ r_5 = 2 & s_5 = -3 & t_5 = 14 \\ r_6 = 1 & s_6 = 5 & t_6 = -23 \\ r_7 = 0 & s_7 = -13 & t_7 = 60 \end{array}$$

Tenemos que: $1 = 5 \cdot 60 + (-23) \cdot 13$

Inverso modular

Definición

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

Para el caso de RSA: d es inverso de e en módulo $\phi(N)$

- En el 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?

- ¿Cómo podemos calcular este inverso?

Inverso modular: Existencia

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 MCD$(a, n) = 1$

Inverso modular: Existencia

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

Ejecutando el algoritmo extendido para el cálculo del máximo común divisor obtenemos s y t 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

Pregunta final: ¿Es necesario suponer que $n \geq a$ en esta parte de la demostración? □

Cálculo de exponentes e y d en RSA

Recuerde que en RSA: $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$

- Tenemos que generar e y d tales que $e \cdot d \equiv 1 \bmod \phi(N)$

Tenemos los ingredientes necesarios para generar e y d:

genere al azar un número e
while $\text{MCD}(e, \phi(N)) > 1$ **do**
    genere al azar un número e
calcule s y t tales que $1 = s \cdot \phi(N) + t \cdot e$
sea $d \in \{0, \ldots, \phi(N) - 1\}$ tal que $d \equiv t \bmod \phi(N)$
return (e, d)

RSA: Implementación (continuación)

Como mencionamos anteriormente, para poder implementar RSA necesitamos algoritmos eficientes para los siguientes problemas:

(1) Generar primos P y Q

(2) Generar números e y d tales que $e \cdot d \bmod \phi(N) = 1$

(3) Calcular funciones E y D

Ya resolvimos (2) y (3), ahora vamos a resolver (1).

- Aquí vamos a necesitar algoritmos probabilísticos

Generación de números primos

Para generar un primo P usamos un enfoque simple:

- Generamos P al azar
- Usamos un test de primalidad para verificar si P es primo
  - Si P no es primo, lo generamos de nuevo

Para que este enfoque funcione, necesitamos:

- que la probabilidad de encontrar un primo sea alta
- un test de primalidad eficiente

Generación de números primos

Sea $\pi(n)$: Cantidad de números primos menores o iguales a n

- Ejemplo: $\pi(2) = 1$ y $\pi(10) = 4$

El siguiente teorema entrega una aproximación de $\pi(n)$.

Teorema (Hadamard-de la Vallée Poussin)

$$\lim_{n \to \infty} \frac{\pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

Generación de números primos

Concluimos que la probabilidad de encontrar un primo en el intervalo $\{m, \ldots, n\}$ $(m \leq n)$ es aproximadamente:

$$\frac{\pi(n) - \pi(m-1)}{n - (m-1)} \approx \frac{\left(\frac{n}{\ln n}\right) - \left(\frac{m-1}{\ln(m-1)}\right)}{n - (m-1)}$$

Entonces: La probabilidad de encontrar un primo es alta.

- Por ejemplo, la probabilidad de encontrar un primo de 200 dígitos es aproximadamente:

$$\frac{\left(\frac{10^{200}-1}{\ln(10^{200}-1)}\right) - \left(\frac{10^{199}-1}{\ln(10^{199}-1)}\right)}{10^{200} - 10^{199}} \approx 0{,}00217 > \frac{1}{500}$$

Por lo tanto: ¡Sólo nos falta un test de primalidad eficiente!

Test de primalidad

Ingrediente esencial para determinar primos P y Q usados en RSA: Tests de primalidad

Estos tests usan aleatoriedad.

- Hay una probabilidad de error asociada al resultado

Vamos a estudiar uno de estos tests.

Test de primalidad: Primer componente

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 componente

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 $n \geq 2$

Necesitamos saber cuál es el valor de $\phi(n)$

Función de Euler

Propiedades simples:

- Si p es primo: $\phi(p) = p - 1$
- Si p es primo y $k > 1$: $\phi(p^k) = p^k - p^{k-1}$

¿Cuál es el valor de $\phi(n)$ en general?

- Necesitamos teoría de grupos

Teoría de grupos

Para recordar

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 $b = c$

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. $(\mathbb{Z}_m^* \times \mathbb{Z}_n^*, \cdot)$, donde $(a_1, b_1) \cdot (a_2, b_2) = ((a_1 \cdot a_2) \bmod m, (b_1 \cdot b_2) \bmod n)$

Teoría de grupos: Noción de isomorfismo

Definition

Grupos $(G_1, \circ_1)$, $(G_2, \circ_2)$ son isomorfos si existe una biyección $f : G_1 \to G_2$ tal que para todo $a, b \in G_1$:

$$f(a \circ_1 b) \quad = \quad f(a) \circ_2 f(b)$$

Notación: $(G_1, \circ_1) \cong (G_2, \circ_2)$ indica que estos grupos son isomorfos.

La noción de isomorfismo es muy útil para el estudio de la función de Euler.

Noción de isomorfismo y la función de Euler

Teorema

Si $m, n \geq 2$ *y* $MCD(m, n) = 1$, *entonces* $(\mathbb{Z}^*_{m \cdot n}, \cdot) \cong (\mathbb{Z}^*_m \times \mathbb{Z}^*_n, \cdot)$

Para demostrar este teorema, necesitamos un teorema muy útil.

Teorema (Chino del Resto)

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

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

Teorema Chino del Resto: 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:

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

Noción de isomorfismo y la función de Euler (continuación)

Veamos ahora la demostración que $(\mathbb{Z}^*_{m\cdot n}, \cdot) \cong (\mathbb{Z}^*_m \times \mathbb{Z}^*_n, \cdot)$

- Recuerde que $m, n \geq 2$ y $\text{MCD}(m, n) = 1$

Sea $f(x) = (x \bmod m,\ x \bmod n)$

Tenemos que:

- $f : \mathbb{Z}^*_{m\cdot n} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n$

  Si $a \in \mathbb{Z}^*_{m\cdot n}$, entonces $\text{MCD}(a, m \cdot n) = 1$

  Por lo tanto: $\text{MCD}(a, m) = 1$ y $\text{MCD}(a, n) = 1$

  - Así, $\text{MCD}(a \bmod m, m) = 1$ y $\text{MCD}(a \bmod n, n) = 1$

  Concluimos que $f(a) = (a \bmod m,\ a \bmod n) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$.

Noción de isomorfismo y la función de Euler (continuación)

- f es 1-1

Si $a, b \in \mathbb{Z}^*_{m \cdot n}$ y $f(a) = f(b)$, entonces:

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

Por lo tanto: $(b - a) = \alpha \cdot m$ y $(b - a) = \beta \cdot n$

- Así, $\alpha \cdot m = \beta \cdot n$

Dado que $m|(\beta \cdot n)$ y $\text{MCD}(m, n) = 1$, se tiene que $\beta = \gamma \cdot m$

Concluimos que $(b - a) = \gamma \cdot m \cdot n$

- Se tiene que $a \equiv b \mod m \cdot n$, lo cual implica que $a = b$ (dado que $1 \leq a, b \leq m \cdot n - 1$)

Noción de isomorfismo y la función de Euler (continuación)

- f es sobre

Si $(a, b) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, por Teorema Chino del Resto tenemos que existe c tal que:

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

Dado que $(a - c) = \alpha \cdot m$ y $\text{MCD}(a, m) = 1$, concluimos que $\text{MCD}(c, m) = 1$.

- De la misma forma concluimos que $\text{MCD}(c, n) = 1$

Se tiene que $\text{MCD}(c, m \cdot n) = 1$.

- Por lo tanto: $(c \bmod m \cdot n) \in \mathbb{Z}_{m \cdot n}^*$ ya que $\text{MCD}(c, m \cdot n) = \text{MCD}(c \bmod m \cdot n, m \cdot n)$

Noción de isomorfismo y la función de Euler (continuación)

Sea $d = (c \bmod m \cdot n)$

Dado que $c = \alpha \cdot m \cdot n + d$, se tiene que:

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

Por lo tanto, d es el elemento buscado:

$$\begin{aligned} f(d) &= (d \bmod m, d \bmod n) \\ &= (c \bmod m, c \bmod n) \\ &= (a, b) \end{aligned}$$

Noción de isomorfismo y la función de Euler (continuación)

- f es un isomorfismo de $\mathbb{Z}^*_{m\cdot n}$ en $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$

Dados $a, b \in \mathbb{Z}^*_{m\cdot n}$:

$$\begin{aligned} f(a \cdot b) &= ((a \cdot b) \bmod m,\ (a \cdot b) \bmod n) \\ &= (((a \bmod m) \cdot (b \bmod m)) \bmod m, \\ &\quad\ ((a \bmod n) \cdot (b \bmod n)) \bmod n) \\ &= (a \bmod m,\ a \bmod n) \cdot (b \bmod m,\ b \bmod n) \\ &= f(a) \cdot f(b) \end{aligned}$$

Función de Euler (continuación)

Corolario

Si $m, n \geq 2$ *y* $MCD(m, n) = 1$, *entonces* $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

Ejemplo

Si $N = P \cdot Q$ con P y Q primos distintos (como en RSA), entonces $\phi(N) = (P - 1) \cdot (Q - 1)$

Función de Euler (continuación)

Corolario

Si $n = \prod_{i=1}^{\ell} p_i^{k_i}$, *donde* $p_1 < p_2 < \cdots < p_\ell$ *son números primos y* $1 \leq k_1, k_2, \ldots, k_\ell$, *entonces:*

$$\phi(n) = \prod_{i=1}^{\ell} \left(p_i^{k_i} - p_i^{k_i - 1} \right)$$

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 componente

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 componente

¿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 n compuesto)?

- Nuevamente teoría de grupos nos va a ayudar

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.

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 $c = b$

Ejercicio

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

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 $(H, \circ)$ tiene 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: Tamaño de un subgrupo

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

Demostración del 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

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* $a, b \in G$*:* $|[a]_\sim| = |[b]_\sim|$

Del lema se concluye el teorema.

- Puesto que las clases de equivalencia de $\sim$ particionan G

Teorema de Lagrange: Demostración

Demostración del 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

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

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

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 componente (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 encontrar el test

Test de primalidad: Segundo componente (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 componente

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 $S_n = \mathbb{Z}_n^*$

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 $a^{\frac{n-1}{2}} \equiv -1 \bmod n$. □

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

Existencia de 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 $a^{\frac{n-1}{2}} \equiv 1 \bmod n$.

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.

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?

Definimos $q(x)$ como:

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

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

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 $a_k \cdot a^k + \cdots + a_1 \cdot a + a_0 \equiv 0 \bmod n$.

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. □

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* $a^{\frac{n-1}{2}} \equiv -1 \, mod \, n$, *entonces:*

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

Demostración: 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:

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

Una propiedad fundamental de S_n para n compuesto: Demostración

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

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

Además, tenemos que:

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

Por lo tanto:

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

Una propiedad fundamental de S_n para n compuesto: Demostración

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

Finalmente: Un test aleatorio de primalidad

Input: Número impar $n \geq 3$ y número $k \geq 1$

El test realiza los siguiente pasos:

(1) Si $n = m^{\ell}$ donde $\ell \geq 2$, entonces retorna COMPUESTO. En caso contrario pasa a (2)

(2) Elije al azar $a_1, \ldots, a_k \in \{1, \ldots, n-1\}$

(3) Si para algún a_i $(1 \leq i \leq k)$ se tiene que $\text{MCD}(a_i, n) > 1$, entonces retorna COMPUESTO. En caso contrario pasa a (4)

Finalmente: Un test aleatorio de primalidad

(4) Calcula $b_i = (a_i^{\frac{n-1}{2}} \bmod n)$, para cada $i \in \{1, \ldots, k\}$

(5) Si para algún b_i $(1 \leq i \leq k)$ se tiene que $b_i \not\equiv 1 \bmod n$ y $b_i \not\equiv -1 \bmod n$, entonces retorna COMPUESTO. En caso contrario pasa a (6)

(6) Si $b_i \equiv 1 \bmod n$ para cada $i \in \{1, \ldots, n-1\}$, entonces retorna COMPUESTO. En caso contrario retorna PRIMO

Finalmente: Un test aleatorio de primalidad

El test de primalidad puede ser implementado de manera eficiente.

- ¿Cómo se implementa el paso (1) de manera eficiente?

Hay una probabilidad de error asociada a la salida del test.

- Vamos a calcular una cota superior para esta probabilidad

Test de primalidad: Probabilidad de error

El test se puede equivocar de dos formas:

- Suponga que n es primo. En este caso el test 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 sacada al azar 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 el test diga COMPUESTO para n primo es $\frac{1}{2^k}$

Test de primalidad: Probabilidad de error

- Suponga que n es compuesto. En este caso el test da una respuesta incorrecta si:
  - n no es de la forma m^ℓ con $\ell \geq 2$
  - $\text{MCD}(a_i, n) = 1$ para cada $i \in \{1, \ldots, k\}$
  - $b_i \equiv 1 \bmod n$ ó $b_i \equiv -1 \bmod n$ para todo $i \in \{1, \ldots, k\}$
  - $b_\ell \equiv -1 \bmod n$ para algún $\ell \in \{1, \ldots, k\}$

Por lo tanto, la probabilidad de error está acotada por:

$$\sum_{i=1}^{k} \left(\prod_{j \in (\{1,\ldots,k\} \setminus \{i\})} P((b_j \equiv 1 \bmod n \text{ ó } b_j \equiv -1 \bmod n) \mid b_i \equiv -1 \bmod n) \right) \cdot P(b_i \equiv -1 \bmod n)$$

Test de primalidad: Probabilidad de error

Dado que $n \geq 3$, n es impar, compuesto y no es de la forma m^ℓ con $\ell \geq 2$, se tiene que $|S_n| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$

- Puesto que existe $\ell \in \{1, \ldots, k\}$ tal que $b_\ell \equiv -1 \bmod n$

Por lo tanto, para $i \neq j$:

$$P((b_j \equiv 1 \bmod n \text{ ó } b_j \equiv -1 \bmod n) \mid b_i \equiv -1 \bmod n) \quad \leq \quad \frac{1}{2}$$

Concluimos que la probabilidad de que el test diga PRIMO para n compuesto está acotada por:

$$\frac{k}{2^{k-1}}$$