Calculando logaritmos discretos en $\mathbb{F}_p$ usando el método de los cálculos de índices

ML

---

g raíz primitiva

Queremos resolver $g^x \equiv h \pmod{p}$.

- Elegimos B y resolvemos $g^x \equiv \ell \pmod{p}$ $\forall$ primo $\ell \le B$

★ o sea calculamos $\log_g(\ell)$ para cada primo $\ell \le B$

- miramos los productos

$$h \cdot g^{-k} \pmod{p} \quad k = 1, 2, \dots$$

hasta encontrar k t.q. $h \cdot g^{-k} \pmod{p}$ es B-liso

$$h \cdot g^{-k} \equiv \prod_{\ell \le B} \ell^{e_\ell} \pmod{p}$$

- concluimos

$$\log_g(h) \equiv k + \sum_{\ell \le B} e_\ell \cdot \log_g(\ell) \pmod{p-1}$$

↑ porque PLP es módulo $p-1$ por Fermat

¿Cómo hacemos el paso ★?

Para potencias al azar calculamos $g_i \equiv g^i \pmod{p}$ con $0 < g_i < p$.

Si g_i no es B-liso los descartamos. Si g_i es B-liso,

$$g_i = \prod_{\ell \le B} \ell^{u_\ell(i)}$$

$$\Rightarrow \quad i \equiv \log_g(g_i) = \sum_{\ell \le B} u_\ell(i) \log_g(\ell) \pmod{p-1}$$

Se ve que las únicas incógnitas son los $\log_g(\ell)$. Si encontramos más que $\pi(B)$ tales ecuaciones, como esto usando álgebra lineal (mód $p-1$) se puede hallar una solución. Para hacer álgebra lineal mód $p-1$ usamos CRT.

Ej: $p = 18443$

Resolver $37^x \equiv 211 \pmod{18443}$

$g = 37$ raíz prim módulo p.

Base de factores $= \{2, 3, 5\}$, $B = 5$

Al azar elegimos potencias para encontrar potencias que son B-lisas mód p:

Mod. intento

$$g^{12708} \equiv 2^3 \cdot 3^4 \cdot 5 \pmod p \qquad g^{11311} \equiv 2^3 \cdot 5^2 \pmod p$$

$$g^{15400} \equiv 2^3 \cdot 3^3 \cdot 5 \pmod p \qquad g^{2731} \equiv 2^3 \cdot 3 \cdot 5^4 \pmod p$$

$\Rightarrow$

$$12708 \equiv 3 \underbrace{\log_g 2}_{x_2} + 4 \underbrace{\log_g 3}_{x_3} + \underbrace{\log_g 5}_{x_5}$$

$\Rightarrow$

$$12708 \equiv 3x_2 + 4x_3 + x_5 \pmod{p-1}$$
$$11311 \equiv 3x_2 + 2x_5 \pmod{p-1}$$
$$15400 \equiv 3x_2 + 3x_3 + x_5 \pmod{p-1}$$
$$2731 \equiv 3x_2 + x_3 + 4x_5 \pmod{p-1}$$

$p-1 = 18442 = 2 \cdot 9221$

Soluciones son:

$$(x_2, x_3, x_5) \equiv (1,0,1) \bmod 2$$

$$(x_2, x_3, x_5) \equiv (5733, 6529, 6277) \bmod 9221$$

$$\underset{CRT}{\Rightarrow} \quad (x_2, x_3, x_5) = (5733, 15750, 6277) \bmod 18442$$

Nos acordamos que queremos resolver $37^x \equiv 211 \pmod p$. Entonces, calculamos $37^{-k} \cdot 211 \pmod p$ para k al azar hasta que encontremos un producto B-liso:

$$211 \cdot 37^{-9549} \equiv 2^5 \cdot 3^2 \cdot 5^2 \pmod p$$

$$\Rightarrow \quad \log_g(211) - 9549 = 5x_2 + 2x_3 + 2x_5 \pmod{p-1}$$

$$\Rightarrow \quad \log_g(211) \equiv 8500 \pmod{18442}$$

Obs: una estimación del tiempo que toma este procedimiento:

Base de factores $\{p \leq B\} \Rightarrow$ tenemos que encontrar $\approx \pi(B)$ números B-lisos de la forma $g^i \pmod p$

Se debería tomar $B = L(p)^{1/\sqrt{2}}$ y deberíamos calcular $\approx B^2 \approx L(p)^{\sqrt{2}}$ potencias i.

Reciprocidad cuadrática:

¿Cómo se sabe si a es un cuadrado mód p?

Def. ~~un residuo~~ p primo impar, a con $p \nmid a$

a es un residuo cuadrático módulo p si existe c t.q

$$c^2 \equiv a \pmod{p}.$$

Se dice que a es un no-residuo si no existe tal c.

Prop. p impar.

(a) $RC \times RC = RC$

(b) $NRC \times RC = NRC$

(c) $NRC \times NRC = RC$.

Dem.: Una demostración general que nos da los tres casos al mismo tiempo.

g^n un cuadrado $\Leftrightarrow \exists k.\ n = 2k$

g una raíz primitiva módulo p.

$n = 2k \Rightarrow g^n$ un cuadrado.

$n = 2k+1 \Rightarrow$ supongamos que $g^n = g^{2k+1} = c^2$. Tiene de

Fermat $\Rightarrow$ $$c^{p-1} \equiv 1 \pmod{p}$$

Pero, $c^{p-1} \equiv (c^2)^{\frac{p-1}{2}} \equiv (g^{2k+1})^{\frac{p-1}{2}} \equiv g^{k(p-1)} g^{\frac{p-1}{2}} \pmod{p}$.

$c^{\frac{p-1}{2}}$ $g^{k(p-1)} \equiv 1 \pmod p$ por Fermat y entonces (2)

$$g^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Pero g es una raíz primitiva $\cancel{X}$.

Entonces potencias impares de g son no-residuos

Hemos probado:

$$g^m \text{ es } \begin{cases} RC & \text{si } m \text{ par} \\ NRC & \text{si } m \text{ impar} \end{cases}$$

$\square$.

Y las tres afirmaciones se prueban así.

~~QR·QR=QR~~ , $\overset{+1}{RC} \cdot \overset{+1}{RC} = \overset{+1}{RC}$, $\overset{-1}{NRC} \cdot \overset{-1}{NRC} = \overset{+1}{RC}$

$\underset{-1}{NRC} \cdot \underset{+1}{RC} = \underset{-1}{NRC}$

<u>Def.</u> p impar. El símbolo de Legendre es

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ RC mód } p \\ -1 & a \text{ NRC mód } p) \\ 0 & \text{p/a.} \end{cases}$$

Entonces

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$ por la proposición anterior.

Algo completamente obvio pero súper útil:

$$a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Tma (Reciprocidad cuadrática):

p, q impar

(a) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases}$

(b) $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1,7 \ (8) \\ -1 & p \equiv 3,5 \ (8) \end{cases}$

(c) $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \ (4) \text{ o } q \equiv 1 \ (4) \\ -\left(\frac{q}{p}\right) & p \equiv 3 \ (4) \text{ o } q \equiv 3 \ (4). \end{cases}$

Ej: $\left(\frac{-15750}{37907}\right) = \left(\frac{-1}{37907}\right)\left(\frac{15750}{37907}\right)$

$15750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$

$= -\left(\frac{15750}{37907}\right)$

$= -\left(\frac{2}{37907}\right)\left(\frac{3}{37907}\right)^2\left(\frac{5}{37907}\right)^3\left(\frac{7}{37907}\right)$

$= -\left(\frac{2}{\underbrace{37907}_{3 \bmod 8}}\right)\left(\frac{5}{37907}\right)\left(\frac{7}{37907}\right)$

$= \left(\frac{5}{37907}\right)\left(\frac{7}{37907}\right)$

$= \left(\frac{37907}{5}\right) \cdot -\left(\frac{37907}{7}\right)$

$\begin{array}{r} 13 \\ 8. \\ \hline 4 \end{array}$

$$= -\left(\frac{2}{5}\right)\left(\frac{2}{7}\right)$$

$$= -(-1)\cdot(1)$$

$$= 1.$$

¿Cómo evitamos tener que factorizar?

<u>Def:</u> $a, b \in \mathbb{Z}$, b impar y positivo. $b = p_1^{e_1} \cdots p_t^{e_t}$

El símbolo de Jacobi: $\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p_i}\right)^{e_i}$

Aunque la definición parece precisar cómo factorizar b, de hecho el símbolo de Jacobi cumple lo mismo que cumple el símbolo de Legendre:

- $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$; $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\cdot\left(\frac{a}{b_2}\right)$

- $a_1 \equiv a_2 \Rightarrow \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$

- $\left(\frac{-1}{b}\right) = \begin{cases} 1 & b \equiv 1 \ (4) \\ -1 & b \equiv 3 \ (4) \end{cases}$

- $\left(\frac{2}{b}\right) = \begin{cases} 1 & b \equiv 1, 7 \ (8) \\ -1 & b \equiv 3, 5 \ (8) \end{cases}$

- $\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & a \equiv 1 \ (4) \text{ o } b \equiv 1 \ (4) \\ -\left(\frac{b}{a}\right) & a \equiv 3 \ (4) \text{ y } b \equiv 3 \ (4). \end{cases}$

Entonces se usa símbolo de Jacobi y sólo se tiene que factorizar por potencias de 2.

¿El símbolo de Jacobi, qué nos dice?

Supongamos $\left(\frac{a}{b}\right)=1$. Si $b=pq \Rightarrow \left(\frac{a}{p}\right)=1=\left(\frac{a}{q}\right)$

o

$\left(\frac{a}{p}\right)=-1=\left(\frac{a}{q}\right)$.

Ahora $\left(\frac{a}{p}\right)=1=\left(\frac{a}{q}\right) \Rightarrow \exists$ $c_1^2 \equiv a \pmod p$
$c_2^2 \equiv a \pmod q$

$\underset{CRT}{\Rightarrow} \exists c$ t.q. $c \equiv c_1 \pmod p$ y t.q. $c^2 \equiv a \pmod{}$
$c \equiv c_2 \pmod q$

Y si $\left(\frac{a}{p}\right)=-1=\left(\frac{a}{q}\right) \Rightarrow$ a es un no residuo mód (pq).

Probabilidad

Si $\left(\frac{a}{b}\right)=-1$ a es un no-residuo módulo b.

Encripción ~~probabilística~~ probabilística

Alice elige texto plano m y una cadena r de bits aleatorios y usa la clave pública para encriptar (m,r).

Para m_1, m_2 fijo, sean

$e(m_1,r)$ = texto cifrado encriptado desde m_1 con una cadena aleatoria r

$e(m_2,r)$ = " m_2 " r.

Las distribuciones de estos textos cifrados deberían ser distinguibles.

Para desencriptar Bob precisa hallar m solamente y no la cadena r.

Método de Goldwasser y Micali tiene como base el problema

> p, q primos secretos
> $N = pq$ dado, (público)
> Determinar si a es un RC mód N.

Si como Bob sabe factorizar $N = pq$

$$a \text{ es un RC módulo } pq \iff \underbrace{\left(\frac{a}{p}\right) = 1 \text{ y } \left(\frac{a}{q}\right) = 1}_{\text{fáciles}}$$

Eve puede calcular $\left(\frac{a}{N}\right)$ pero como ya vimos, eso no implica que sabe si a es un RC módulo N.

Goldwasser - Micali

	Bob	Alice
Claves	p, q secreto a t.q. $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$ Publica $N = pq$ y a	
Encriptar		$m \in \{0,1\}$, r al azar $1 < r < N$ Usando (N, a) publicado por Bob calcula $c = \begin{cases} r^2 \ (N) & \text{si } m = 0 \\ ar^2 \ (N) & \text{si } m = 1 \end{cases}$ Manda c a Bob
Desencriptar	Calcular $\left(\frac{c}{p}\right)$ $m = \begin{cases} 0 & \left(\frac{c}{p}\right) = 1 \\ 1 & \left(\frac{c}{p}\right) = -1 \end{cases}$	

Este procedimiento funciona porque

$$\left(\frac{c}{p}\right) = \begin{cases} \left(\frac{r^2}{p}\right) = \left(\frac{r}{p}\right)^2 = 1 & \text{si } m=0 \\ \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right) = -1 & \text{si } m=1. \end{cases}$$

Como r es aleatorio, Eve ve todos los posibles cuadrados módulo N si m=0. y ve todos los no cuadrados si m=1. Entonces parece más o menos aleatorio

¿Eve que sabe calcular?

$$\left(\frac{c}{N}\right) = \left(\frac{r^2}{N}\right) = \left(\frac{r}{N}\right)^2 = 1 \quad \text{si } m=0.$$

$$\left(\frac{c}{N}\right) = \left(\frac{ar^2}{N}\right) = \left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = (-1)(-1) = 1.$$

Entonces calculando el símbolo de Jacobi no le dice nada.

Este sistema no es práctico. ¿Por qué?

Queremos $N = pq \approx 2^{1000}$. ~~Si~~ Alice que encripta un mensaje de k bits

Entonces manda a Bob k números de ~1000 bits. O sea 1000 k bits.

En general, el sistema tiene una factor de expansión de $\log_2(N)$. ~~...~~

~~Si~~ ~~...~~ ElGamal es un método probabilístico porque el hecho que

hay una clave efímera.