Solución del logaritmo discreto por el cálculo del índice

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

Aunque no es aplicable a todos los grupos, el método del *cálculo del índice* (index-calculus) es el más eficiente que se conoce para resolver el problema del logaritmo discreto.

La idea detrás del algoritmo se debe a Kraitchik en 1922 y la formulación actual a Adleman en 1979. El algoritmo para el cálculo del índice ha inspirado soluciones para otros problemas como la criba cuadrática para la factorización de enteros.

Index-calculus

Como todo problema del logaritmo discreto, consideraremos un grupo finito cíclico, un generador α del grupo (de orden m) y un valor modular n. Utilizaremos la notación asociada al trabajo con el grupo $(\mathbb{Z}_n^*, \cdot \text{ mód } n)$.

Recordamos que el objetivo es, dado un elemento β del grupo, obtener el entero t tal que $\alpha^t \text{ mód } n = \beta$.

El Algoritmo 1 resume el proceso que puede verse como una sucesión de tres fases:

- Elección de una base de primos S que permita la representación de la *mayoría* de elementos del grupo como producto de elementos en S (la mayoría de los elementos sean S-smooth).
- Obtención de una serie de ecuaciones lineales que permitan obtener eficientemente los logaritmos discretos de los valores en la base.
- Búsqueda de un entero p tal que $\beta \cdot \alpha^p \text{ mód } n$

Ejemplo 1. *Consideremos el entero $n = 1109$ y $\alpha = 19$ el generador del subgrupo de $\mathbb{Z}_n^*$ de orden $m = 277$. Para calcular el logaritmo discreto de $\beta = 274$ en base α de acuerdo con el cálculo del índice consideraremos la base:*

$$S = \{2, 3, 5, 7, 11, 13\}.$$

Algoritmo 1 Cálculo del logaritmo discreto mediante el cálculo del índice.

Entrada: Un grupo finito cíclico $(G, \cdot \text{ mód } n)$
Entrada: Un generador α del grupo
Entrada: El orden m del grupo generado por α
Entrada: El valor β del cual quiere calcularse el logaritmo discreto.
Salida: t tal que $\alpha^t \text{ mód } n = \beta$

Método
Selecionar una base $S = \{p_1, p_2, \ldots, p_k\}$ tal que una *mayoría* de elementos c del grupo pueden descomponerse con los factores en S.
Mientras no se disponga de suficientes relaciones lineales **hacer**
  Generar aleatoriamente r y calcular $\alpha^r \text{ mód } n$
  Descomponer $\alpha^r \text{ mód } n$ como:

$$\alpha^r = \prod_{i=1}^{k} p_i^{e_i}, \quad e_i \geq 0$$

  Si es posible (α^r es S-smooth) **entonces**
    Aplicar logaritmos para obtener una relación lineal:

$$r = \sum_{i=1}^{k} e_i \log_\alpha p_i \text{ mód } m, \quad e_i \geq 0$$

  FinSi
FinMientras
Resolver el sistema para obtener los valores de los logaritmos de los elementos en S
Mientras no se haya encontrado solución **hacer**
  Generar aleatoriamente r
  Si $\beta \cdot \alpha^r \text{ mód } n$ es S-smooth **entonces**
    Obtener:

$$\beta\alpha^r = \prod_{i=1}^{k} p_i^{d_i} \text{ mód } n, \quad d_i \geq 0$$

    Obtener:

$$\log_\alpha \beta + r = \sum_{i=1} d_i \log p_i \text{ mód } m, \quad d_i \geq 0$$

    y despejar $t = \log_\alpha \beta$
    Devolver t
  FinSi
FinMientras
FinMétodo.

Primero generamos enteros r aleatorios que conduzcan a valores $\alpha^r \bmod n$ que puedan descomponerse en S (valores S- smooth):

$$\begin{aligned}
\alpha^{83} &\equiv 2^5 \cdot 7 \pmod{1109} \\
\alpha^{235} &\equiv 3^4 \cdot 13 \pmod{1109} \\
\alpha^{324} &\equiv 3^2 \cdot 7^2 \pmod{1109} \\
\alpha^{497} &\equiv 2^2 \cdot 7^2 \pmod{1109} \\
\alpha^{739} &\equiv 7^2 \cdot 11 \pmod{1109} \\
\alpha^{741} &\equiv 2^3 \cdot 3^2 \cdot 7 \pmod{1109} \\
\alpha^{936} &\equiv 2^6 \cdot 5 \pmod{1109} \\
\alpha^{1085} &\equiv 2^3 \cdot 3^3 \pmod{1109}
\end{aligned}$$

que, aplicando logaritmos, dan lugar a relaciones lineales módulo el orden del grupo:

$$\begin{aligned}
83 &\equiv 5\log_\alpha 2 \cdot \log_\alpha 7 \pmod{277} \\
235 &\equiv 4\log_\alpha 3 \cdot \log_\alpha 13 \pmod{277} \\
324 &\equiv 2\log_\alpha 3 \cdot 2\log_\alpha 7 \pmod{277} \\
497 &\equiv 2\log_\alpha 2 \cdot 2\log_\alpha 7 \pmod{277} \\
739 &\equiv 2\log_\alpha 7 \cdot \log_\alpha 11 \pmod{277} \\
741 &\equiv 3\log_\alpha 2 \cdot 2\log_\alpha 3 \cdot \log_\alpha 7 \pmod{277} \\
936 &\equiv 6\log_\alpha 2 \cdot \log_\alpha 5 \pmod{277} \\
1085 &\equiv 3\log_\alpha 2 \cdot 3\log_\alpha 3 \pmod{277}
\end{aligned}$$

A partir de este punto (linea 10 del algoritmo) podemos resolver el sistema de ecuaciones para calcular los valores de los logaritmos discretos (incógnitas en el sistema), obteniendo:

$$\begin{aligned}
log_\alpha 2 &= 201 \quad log_\alpha 7 = 186 \\
log_\alpha 3 &= 253 \quad log_\alpha 11 = 90 \\
log_\alpha 5 &= 7 \qquad log_\alpha 13 = 54
\end{aligned}$$

La elección de la base y del número de relaciones lineales en el sistema tiene que garantizar que todos los factores en la base aparecen al menos una vez y que se disponen de ecuaciones suficientes para obtener un sistema determinado. El cálculo eficiente de los logaritmos discretos de los p_i en la base permite en la última fase el cálculo del logaritmo discreto que se plantea como problema.

En la última fase el algoritmo itera (linea 11 del algoritmo) buscando un valor t tal que $\beta\alpha^t \bmod n$ sea S-smooth. Por ejemplo:

$$\beta\alpha^{17} = 2^8 \bmod 1109,$$

a partir de este punto se puede obtener:

$$\log_\alpha \beta + 17 = 8\log_\alpha 2 \bmod 277,$$

en este caso es suficiente conocer el logaritmo discreto de 2 para despejar el $\log_\alpha \beta$*:*

$$\log_\alpha \beta = 8 \log_\alpha 2 - 17 \bmod 277 = 206,$$

En efecto:

$$\alpha^{206} \bmod 1109 = 274.$$

Ejemplo 2. *Consideremos el primo de 16 bits* $n = 55243$ *y* $\alpha = 22$ *el generador del subgrupo de* $\mathbb{Z}_n^*$ *de orden* $m = 27621$*. Para calcular el logaritmo discreto de* $\beta = 37205$ *en base* α *de acuerdo con el cálculo del índice consideraremos la base:*

$$S = \{2, 3, 5, 7, 11, 13, 17\}.$$

El primer paso es considerar enteros r *aleatorios que conduzcan a valores* $\alpha^r \bmod n$ *que puedan descomponerse en* S *(valores* S*- smooth):*

$$\begin{aligned}
\alpha^{2992} &\equiv 2 \cdot 13^3 \pmod{55243} \\
\alpha^{17460} &\equiv 2^3 \cdot 3^3 \cdot 11^2 \pmod{55243} \\
\alpha^{17645} &\equiv 2^2 \cdot 3^4 \cdot 5 \cdot 13 \pmod{55243} \\
\alpha^{26378} &\equiv 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13 \pmod{55243} \\
\alpha^{28565} &\equiv 2^2 \cdot 5^3 \cdot 13 \pmod{55243} \\
\alpha^{28805} &\equiv 2^3 \cdot 5 \cdot 7^3 \pmod{55243} \\
\alpha^{47581} &\equiv 3 \cdot 5 \cdot 7 \pmod{55243} \\
\alpha^{51958} &\equiv 2^5 \cdot 3^3 \cdot 7^2 \pmod{55243} \\
\alpha^{54756} &\equiv 2^8 \cdot 3 \cdot 17 \pmod{55243}
\end{aligned}$$

que, aplicando logaritmos, transformamos en:

$$\begin{aligned}
2992 &\equiv \log_\alpha 2 + 3 \log_\alpha 13 \pmod{27621} \\
17460 &\equiv 3 \log_\alpha 2 + 3 \log_\alpha 3 + 2 \log_\alpha 11 \pmod{27621} \\
17645 &\equiv 2 \log_\alpha 2 + 4 \log_\alpha 3 + \log_\alpha 5 + \log_\alpha 13 \pmod{27621} \\
26378 &\equiv 2 \log_\alpha 2 + \log_\alpha 3 + 2 \log_\alpha 5 + \log_\alpha 7 + \log_\alpha 13 \pmod{27621} \\
28565 &\equiv 2 \log_\alpha 2 + 3 \log_\alpha 5 + \log_\alpha 13 \pmod{27621} \\
28805 &\equiv 3 \log_\alpha 2 + 3 \log_\alpha 5 + 3 \log_\alpha 7 \pmod{27621} \\
47581 &\equiv \log_\alpha 3 + \log_\alpha 5 + \log_\alpha 7 \pmod{27621} \\
51958 &\equiv 5 \log_\alpha 2 + 3 \log_\alpha 3 + 2 \log_\alpha 7 \pmod{27621} \\
54756 &\equiv 8 \log_\alpha 2 + \log_\alpha 3 + \log_\alpha 17 \pmod{27621}
\end{aligned}$$

A partir de este punto (linea 10 del algoritmo) podemos resolver el sistema de ecuaciones

para calcular los valores de los logaritmos discretos (incógnitas en el sistema), obteniendo:

$$\begin{array}{ll} log_\alpha 2 = 15943 & log_\alpha 11 = 11679 \\ log_\alpha 3 = 9712 & log_\alpha 13 = 4890 \\ log_\alpha 5 = 24884 & log_\alpha 17 = 363 \\ log_\alpha 7 = 12985 & \end{array}$$

Es necesario asegurarse en la construcción del sistema que todos los factores en la base aparecen al menos una vez y que se disponen de ecuaciones suficientes para obtener un sistema determinado.

A partir de los logaritmos discretos calculados el algoritmo itera (linea 11 del algoritmo) buscando un valor t tal que $\beta\alpha^t \bmod n$ sea S-smooth. Por ejemplo:

$$\beta\alpha^{35913} = 2^5 \cdot 3^5 \cdot 7 \bmod 55243,$$

a partir de donde se puede obtener:

$$\log_\alpha \beta + 35913 = 5\log_\alpha 2 + 5\log_\alpha 3 + \log_\alpha 7 \bmod 27621,$$

de donde, al haber calculado previamente los logaritmos discretos de 2, 3 y 7 puede despejarse el $\log_\alpha \beta$:

$$\log_\alpha \beta = 5\log_\alpha 2 + 5\log_\alpha 3 + \log_\alpha 7 - 35913 \bmod 27621 = 22484.$$

Aplicabilidad y límites

La dificultad para establecer (incluso definir) una base en determinados grupos hace que esta aproximación no sea aplicable en todos los casos.

Como ejemplo, no se conoce la forma de establecer una base que permita la descomposición de los elementos de un grupo generados en base a una curva elíptica (puntos de la curva), por lo que no es posible utilizar esta aproximación en ese caso.

Ejercicios

Ejercicio 1.

Resolver el problema del logaritmo discreto en base $\alpha = 3$ de $\beta = 12470$ módulo $p = 43577$ utilizando el algoritmo del cálculo del índice.

Solución:

$12470 = 3^{38997}$ mód 43577*, por lo que el logaritmo discreto en base* $\alpha = 3$ *de* β *módulo* 43577 *es* 38997*.*

Para resolver el problema es suficiente una base que contenga los 10 primeros primos.

Ejercicio 2.

Utilizar el algoritmo del cálculo del índice para resolver el problema del logaritmo discreto en base $\alpha = 2$ *de* $\beta = 1522407915$ *módulo* $p = 3094892893$*.*

Solución:

$1522407915 = 2^{571229561}$ mód 3094892893*, por lo que el logaritmo discreto es* 571229561*.*

Para resolver el problema es suficiente una base que contenga los 10 primeros primos.
