El problema del logaritmo discreto

José Galaviz

1976, MIT.

Whitfield Diffie.

Martin Hellman.

Ralph Merkle.

La idea

- Poner de acuerdo a dos entidades en un secreto común.
- Intercambiando datos a través de un canal inseguro.
- Sin que el eventual espía que interviene al canal pueda saber el secreto.

El primero

- Gauss, C.F., *Disquisitiones Arithmeticae,* Leipzig, 1801, §57.
- *Index.*
- Si $r = b^e$ (mód n), e es el *index* de r base b módulo n.
- Logaritmo discreto.

Grupo

Un grupo (G, +) es un conjunto no vacío G, junto con una operación binaria “+”, en el que se satisfacen los siguientes requisitos.

- Cerradura. a,b en G significa que a+b está en G.
- Asociatividad. Si a,b,c en G entonces

$$a + (b + c) = (a + b) + c$$

- Identidad. Existe un único elemento distinguido e en G, tal que para toda a en G: a + e = e + a = a
- Inverso (simétrico). Para todo a en G, existe un elemento a’ en G tal que a + a’ = e

El número de elementos en el grupo es el **orden del grupo**

Convenciones

- Si la operación se denota con “+” suele llamarse grupo aditivo y entonces el neutro es 0 y el simétrico es… simétrico o inverso aditivo denotado -a.
- Si la operación se denota con * o punto o nada, entonces se llama grupo multiplicativo el neutro es 1, y el simétrico es inverso multiplicativo, denotado a^{-1}.
- Y esto NO es relevante. Es pura sintaxis.
- La operación no necesariamente es conmutativa, si lo és el grupo es abeliano.

Ejemplos

- $(\mathbb{N},+)$ no es grupo. Tampoco $(\mathbb{N},*)$.
- $(\mathbb{Z}, +)$ sí lo es, pero no $(\mathbb{Z}, *)$.
- $(\mathbb{Q}, +)$ sí lo es, y $(\mathbb{Q}, *)$ lo sería si quitamos al cero.
- $(\mathbb{Z}_m, +)$ sí lo es, pero $(\mathbb{Z}_m, *)$ sólo si m es primo (y le quitamos el cero), en cuyo caso de hecho es más que un grupo, como sabemos.

De orden 4

Hay dos, exactamente, grupos de orden 4:

($\mathbb{Z}_4$, +) y el 4-grupo de Klein.

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Grupos cíclicos

Son grupos especiales en los que todos los elementos pueden ser generados a partir de uno sólo de ellos usando la operación de grupo. Si G es un grupo cíclico entonces existe un elemento g, tal que cualquier otro elemento del grupo q se puede escribir como (grupo aditivo):

$q = g + g + \ldots + g$ (k veces) $= k\,g$.

o (grupo multiplicativo):

$q = g * g * \ldots * g$ (ka veces) $= g^k$.

g es un **generador** del grupo.

Ejemplos

- $(\mathbb{Z}_m, +)$ tiene al 1 como generador.
- $(\mathbb{Z}_7 \setminus \{0\}, *)$ es cíclico:

1	3^0
2	3^2
3	3^1
4	3^4
5	3^5
6	3^3

No todos lo son

- $(\mathbb{Z}_4, +)$ es cíclico.
- El 4-grupo de Klein no lo es.

Otro ejemplo, el 2 como generador o *raíz primitiva*

$x \in \mathbb{Z}_{11}^*$	Expresión	Valor nominal
1	2^{10}	1024
2	2^1	2
3	2^8	256
4	2^2	4
5	2^4	16
6	2^9	512
7	2^7	128
8	2^3	8
9	2^6	64
10	2^5	32

¿Y si usamos a 3?

$$3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 5,\ 3^4 = 4,\ 3^5 = 1,\ \ldots$$

Nomás generamos un subgrupo cíclico de orden 5

Veamos...

Si se nos proporcionan valores para g, m y s, donde m es el tamaño del módulo en un campo finito o un grupo cíclico generado por la raíz primitiva g y existe un exponente e tal que: $s \equiv g^e \pmod{m}$. Dado que:

- La secuencia de resultados para ge no tiene un patrón distinguible y
- Que la secuencia generada por g es del tamaño del orden del grupo.

Entonces no parece fácil encontrar el valor de e.

El problema del logaritmo discreto

Definición 2. Dados un grupo cíclico $(G, \cdot)$, un elemento generador $g \in G$ y un elemento $s \in G$, el *problema del logaritmo discreto en* G consiste en encontrar el valor de $e \in \mathbb{Z}$ tal que:

$$s = g^e$$

¿Qué tan difícil?

- No se ha encontrado un algoritmo (clásico) que resuelva el problema del logaritmo discreto en tiempo polinomial.
- Se cree que si P ≠ NP entonces el problema está en una clase que se ha llamado NPI (NP-intermedios).
- El algoritmo de Shor (1999) puede resolver el problema en tiempo polinomial en una computadora cuántica.

¿Qué tan difícil es encontrar un generador?

No son tan escasas

Teorema 1. *Si t es una raíz primitiva en el grupo cíclico de orden m, $\mathbb{Z}_m$, entonces*

$$t^{\frac{m-1}{2}} \equiv m-1 \pmod{m} \equiv -1 \pmod{m}$$

Están bien caracterizadas, así que se pueden buscar haciendo la prueba. Hay φ(φ(m)), si m es primo hay φ(m-1). φ(m) es la cantidad de números primos relativos con m menores que él.

Ejemplo

Ejemplo 2.0.4. 6 es raíz primitiva módulo 761:

$6^{760/2} \equiv 760 \pmod{761}$

Por otra parte $\varphi(760) = 288$, así que ese es el número de raíces primitivas módulo 761

Intercambio de llaves de Diffie-Hellman 1/2

Dos interlocutores A y B. Un canal que suponemos intervenido.

1. A y B escogen un número primo grande p y una raíz primitiva g $\in \mathbb{Z}_p^*$. Se pueden poner de acuerdo usando el canal.
2. A elige un entero aleatorio grande a: $0 < a < p-1$ y envía a B: $X = g^a \pmod p$
3. B elige un entero aleatorio grande b: $0 < b < p-1$ y envía a A: $X = g^b \pmod p$

Intercambio de llaves de Diffie-Hellman 2/2

4. A calcula $K_1 = Y^a \pmod p$.
5. B calcula $K_2 = X^b \pmod p$.

$K_1 = K_2 = g^{ab} \pmod p = \mathbf{K}$

Dificultad del criptoanálisis

Alguien que haya estado escuchando el canal posee p, g, X y Y. Para calcular K necesitaría:

- Obtener el logaritmo discreto de X o de Y en base g módulo p, para obtener a o b (con uno basta) y poder calcular $K = g^{ab} \pmod{p}$.
- Calcular $K = g^{ab} \pmod{p}$ de alguna otra manera.

Siendo precisos

La seguridad del protocolo de Diffie-Hellman se basa en DOS premisas:

1. Calcular el logaritmo discreto es un problema difícil computacionalmente hablando.
2. No hay otra manera de obtener K más que calculando el logaritmo discreto (hipótesis de Diffie-Hellman).