Teoría de grupos

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.

Grupos

Muchos de los métodos criptográficos que están vigentes hoy en día consideran resultados de la teoría de grupos. Como ejemplo de estos pueden mencionarse desde el cifrado RSA o ElGamal, a implementaciones de protocolos de conocimiento cero como el propuesto por Fiat-Shamir y que ha sido la base de otros protocolos similares.

Recordamos que el par $\langle G, \oplus \rangle$ formado por el conjunto G y la operación $\oplus$ tiene estructura de grupo si la operación es cerrada en G y es asociativa, si existe un elemento e de G que es neutro para la operación, esto es, $a \oplus e = e \oplus a = a$ y si, para todo elemento a de G existe el inverso de a, esto es, un elemento a^{-1} tal que $a \oplus a^{-1} = a^{-1} \oplus a = e$.

Dado un grupo $\langle G, \oplus \rangle$, todo subconjunto de G que cumpla las propiedades para ser grupo se considera *subgrupo* de G.

Ejemplo 1. *Consideremos el par* $G = \langle [1, 12], \cdot \text{ mód } 13 \rangle$. *Puede comprobarse que* G *cumple las propiedades mencionadas y que por lo tanto que* G *es un grupo.*

Por otro lado, del mismo modo puede concluirse que $G' = \langle \{1, 3, 4, 9, 10, 12\}, \cdot \text{ mód } 13 \rangle$ *también es un grupo. Además, ya que* $\{1, 3, 4, 9, 10, 12\}$ *un subconjunto de* $[1, 12]$*, puede decirse que* G' *es un subgrupo de* G.

Dado $\langle G, \oplus \rangle$ un grupo y donde a es un elemento de G, se define la *potencia* como la composición de un elemento del conjunto un determinado número de veces, así:

$$a^k = \underbrace{a \oplus a \oplus \ldots \oplus a}_{k}.$$

Si el conjunto que considera un grupo es finito, entonces el grupo se dice que es finito. En criptografía, estos grupos finitos son ampliamente utilizados.

A partir de la operación potencia, el *subgrupo generado por* a se define como el conjunto de elementos de G que pueden obtenerse mediante composición de a un determinado número de veces, esto es:

$$< a >= \{a^i \ : \ i \geq 1\}$$

Otra noción muy importante y relacionada con la operación definida es el *orden de un elemento* a en G, que denotaremos con $ord(a)$, como el menor entero positivo t tal que $a^t = e$.

Ejemplo 2. *Dado el grupo* $\langle\{1, 2, 4, 5, 7, 8\}, \cdot \text{ mód } 9\rangle$*, la siguiente tabla muestra el orden de los elementos del grupo.*

elemento	1	2	4	5	7	8
orden	1	6	3	6	3	2

donde, por ejemplo, se puede comprobar que $5^6 \text{ mód } 9 = 1$.

Un resultado que relaciona los conceptos de orden y subgrupo generado por un elemento es el siguiente:

Teorema 1. *Dado cualquier grupo finito* $\langle G, \oplus\rangle$ *y cualquier elemento* a *en* G *se cumple que*

$$ord(a) = card(< a >)$$

Consideranto $ord(a) = t$, la prueba de este resultado tiene en cuenta que $a^t = e$, y por lo tanto, para todo $k > t$, el elemento a^k se puede obtener también como a^{k-t}. Un corolario de este resultado es el siguiente:

Corolario 1.1. *Dado cualquier grupo finito* $\langle G, \oplus\rangle$ *y cualquier elemento* a *en* G *tal que* $ord(a) = t$*, se cumple que* $a^i \equiv a^j$ *si y sólo si* $i \equiv j \pmod t$

La prueba del corolario considera que, independientemente del valor i considerado:

$$i = q_i t + i \text{ mód } t, \quad q_i \geq 0$$

de modo que:

$$\begin{aligned} a^i \equiv a^{q_i t + i \text{ mód } t} &\equiv a^{q_i t} \oplus a^{i \text{ mód } t} \equiv \\ &\equiv e^{q_i} \oplus a^{i \text{ mód } t} = a^{i \text{ mód } t} \end{aligned}$$

Actuando del mismo modo respecto a^j, obtenemos el resultado enunciado en el corolario.

Como consecuencia de estos resultados, es consistente definir:

$$a^0 = e$$

$$a^i = a^{i \bmod t}, \text{ para todo } i \geq 0$$

Grupo multiplicativo

Como se ha comentado en otras ocasiones, un conjunto de especial interés en criptografía es el que contiene todos los resíduos módulo un determinado entero positivo n, que habitualmente denotamos con $\mathbb{Z}_n$.

Otro conjunto interesante derivado de $\mathbb{Z}_n$ es aquel que contiene los elementos invertibles $\mathbb{Z}_n$ de acuerdo con una determinada operación que, si no se indica explicitamente otra, habitualmente consideraremos como un producto módulo n. Este conjunto de elementos invertibles lo denotaremos con $\mathbb{Z}_n^*$. Si la operación considerada es el producto módulo n, entonces $|\mathbb{Z}_n^*| = \phi(n)$. Al contener $\mathbb{Z}_n^*$, por definición, únicamente los elementos invertibles, el par $\langle \mathbb{Z}_n^*, \cdot \bmod n \rangle$ tiene estructura de grupo y suele denominarse *grupo multiplicativo.*

Ejemplo 3. *Considerando el conjunto* $\mathbb{Z}_{18}$ *y la operación producto módulo* 18*, El conjunto de elementos invertibles es:*

$$\mathbb{Z}_{21}^* = \{1, 2, 5, 7, 8, 10, 11, 13, 16, 17, 19, 20\}$$

Puede comprobarse que:

$$|\mathbb{Z}_{21}^*| = \phi(21) = (3^1 - 3^0)(7^1 - 7^0) = 12$$

y que el par $\langle \mathbb{Z}_{21}^*, \cdot \bmod n \rangle$ *tiene estructura de grupo.*

Dado un grupo $\langle G, \oplus \rangle$, un elemento α de G es un *generador* si el orden de α es $\phi(n)$. Si un grupo tiene un generador, se dice que el grupo es *cíclico*, además, como consecuencia, si α es un *generador*, se cumple que:

$$\mathbb{Z}_n^* = \{\alpha^i \ : \ 1 \leq i \leq \phi(n)\}$$

Ejemplo 4. *Dado* $\mathbb{Z}_{23}^* = [1, 22]$*, distintos generadores de* $\mathbb{Z}_{23}^*$ *son* 5*,* 7 *o* 10*. Esto es, el orden de todos ellos es* 22 *e igual al tamaño del grupo.*

Por otra parte, 2*,* 3*,* 8 *o* 13 *no son generadores del grupo multiplicativo, porque, como ejemplo, el orden de* 13 *es* 11*, esto es,* 13^{11} mód $23 = 1$*.*

El resultado siguiente establece una condición necesaria y suficiente sobre n para que el grupo multiplicativo $\mathbb{Z}_n^*$ sea cíclico.

Teorema 2. *El grupo multiplicativo* $\mathbb{Z}_n^*$ *es cíclico sí y sólo si* $n = 2, 4, p^e, 2p^e$*, donde* p *es primo impar y* e *un entero positivo.*

Una consecuencia de este resultado es que, para cualquier valor n primo, el grupo multiplicativo $\mathbb{Z}_n^*$ es cíclico.

Ejemplo 5. *El grupo multiplicativo* $\mathbb{Z}_{21}^*$ *no es cíclico ya que no existe ningún elemento cuyo orden sea* $\phi(21) = 12$*.*

Por otra parte, el grupo multiplicativo $\mathbb{Z}_{25}$ *sí es cíclico y, como ejemplo,* 2 *es un generador.*

Lagrange

Uno de los resultados más importantes en Teoría de Grupos, que utilizaremos en distintas ocasiones y que se enuncia sin demostración establece que dado cualquier subgrupo, su tamaño (número de elementos en el conjunto) es un divisor del tamaño del grupo en el que está incluído.

Teorema 3 (Lagrange)**.** *Sea* $\langle G, \oplus \rangle$ *un grupo finito y* $\langle G', \oplus \rangle$ *un subgrupo de* $\langle G, \oplus \rangle$*, entonces,* $card(G')|card(G)$*.*

Una consecuencia del Teorema de Lagrange es el siguiente:

Corolario 3.1. *Si* $\langle G, \oplus \rangle$ *es un grupo finito con identidad* e*, entonces, para todo*

$a \in G$ se cumple que:

$$a^{|G|} = e$$

La prueba del corolario considera que el tamaño de $< a >$ (subgrupo generado por a) es de un tamaño divisor del tamaño del grupo, por lo tanto:

$$|G| = kt,\ k \in \mathbb{Z},\ t = ord(a)$$

y por lo tanto:

$$a^{|G|} = a^{kt} = e^k = e$$

Ejemplo 6. *Consideremos el grupo* $\langle [1, 12], \cdot \text{ mód } 13 \rangle$ *de tamaño 12. El subgrupo generado por* 4*, esto es,* $< 4 >= \langle \{1, 3, 4, 9, 10, 12\}, \cdot \text{ mód } 13 \rangle$ *tiene tamaño* 6*. Nótese que* $4^6 \text{ mód } 13 = 1$ *y también que* $4^{12} \text{ mód } 13 = (4^6)^2 \text{ mód } 13 = 1$*.*

Otro ejemplo es el subgrupo generado por 3*, esto es,* $< 3 >= \langle \{1, 3, 9\}, \cdot \text{ mód } 13 \rangle$*. En este caso* $3^{12} \text{ mód } 13 = (3^3)^4 \text{ mód } 13 = 1$*.*

A partir del Teorema de Lagrange puede obtenerse un resultado que permite comprobar si un valor α en un grupo G es generador.

Teorema 4. *Sea* $\alpha \in \mathbb{Z}_n^*$*,* α *es un generador de* $\mathbb{Z}_n^*$ *si y sólo si, para todo* p *primo divisor de* $\phi(n)$ *se cumple que:*

$$\alpha^{\phi(n)/p} \not\equiv 1 \pmod{n}$$

Ejemplo 7. *Considerando el grupo multiplicativo* $\mathbb{Z}_{25}$*, un generador del grupo es* 2 *porque:*

- $\phi(25) = 20$*, cuyos divisores primos son* 2 *y* 5*.*
- $2^{20/2} \text{ mód } 25 = 24 \neq 1$
- $2^{20/5} \text{ mód } 25 = 16 \neq 1$

Otros resultados que pueden considerarse consecuencia del Teorema de Lagrange se deben a Euler y a Fermat y se enuncian a continuación. En especial, el Teorema de Fermat es ampliamente utilizado en la prueba de corrección de muchos algoritmos criptográficos.

Teorema 5 (Euler)**.** *Dado cualquier n mayor que 1, y dado cualquier elemento a del grupo multiplicativo $\mathbb{Z}_n^*$, se cumple que:*

$$a^{\phi(n)} = 1$$

Teorema 6 (Fermat (Little Theorem))**.** *Para todo p primo y todo elemento a del grupo multiplicativo $\mathbb{Z}_n^*$, se cumple que:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Una primera consecuencia del (Pequeño) Teorema de Fermat es que, para todo p primo, $\mathbb{Z}_p^*$ es cíclico, $\mathbb{Z}_p^* = \mathbb{Z}_p - 0$ y por lo tanto $a^p \equiv a \pmod{p}$.

Ejercicios

Ejercicio 1.

¿Cuales son los elementos del grupo multiplicativo $\mathbb{Z}_{39}$?

Ejercicio 2.

Considerando operaciones en el grupo multiplicativo $\mathbb{Z}_{39}$, ¿puede deducirse el orden de 2 si se sabe que $ord(16) = 3$ y que $16 = 2^4 \bmod 39$?

Ejercicio 3.

¿Cuál es el orden de los elementos del grupo multiplicativo $\mathbb{Z}_{36}$?

Ejercicio 4.

Dado el valor primo $n = 1999$*, sabiendo que* $n - 1 = 2 \cdot 3^3 \cdot 37$*, ¿Es* 2 *un generador de* $\mathbb{Z}_{1999}$*? ¿lo es* 11*? ¿lo es* 3*?.*

Ejercicio 5.

¿Qué dice el Teorema de Fermat acerca de la primalidad de $n = 1453$*? ¿y acerca de la de* $n = 2379$*?*
