Groups in Cryptography

Çetin Kaya Koç

http://cs.ucsb.edu/~koc/cs178
koc@cs.ucsb.edu

Joseph Louis Lagrange

Joseph-Louis Lagrange, born Giuseppe Luigi Lagrancia was an Italian-born French mathematician and astronomer born in Turin, Piedmont, who lived part of his life in Prussia and part in France. Wikipedia

Born: January 25, 1736, Turin
Died: April 10, 1813, Paris
Education: École Polytechnique
Parents: Maria Theresa Gros, Giuseppe Francesco Lodovico Lagrange
A set $S$ and a binary operation $\oplus$ together is called a group $G = (S, \oplus)$ if the operation and the set satisfy the following rules:

- **Closure**: If $a, b \in S$ then $a \oplus b \in S$.
- **Associativity**: For $a, b, c \in S$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
- **Neutral element**: There exists a neutral element $e \in S$ such that $a \oplus e = e \oplus a = a$.
- **Inverse element**: Every element $a \in S$ has an inverse $\text{inv}(a) \in S$:
  \[
  a \oplus \text{inv}(a) = \text{inv}(a) \oplus a = e
  \]
- **Commutativity**: If $a \oplus b = b \oplus a$, then the group $G$ is called an a commutative group or an Abelian group.

In cryptography we deal with Abelian groups.
The operation $\oplus$ is a multiplication “$\cdot$”

The neutral element is generally called the unit element $e = 1$

Multiplication of an element $k$ times by itself is denoted as

$$a^k = a \cdot a \cdot \ldots \cdot a$$

The inverse of an element $a$ is denoted as $a^{-1}$

Example: $(\mathbb{Z}_n^*, \ast \mod n)$; note that $\mathbb{Z}_n^*$ is the set $\{1, 2, \ldots, n - 1\}$ when $n$ is prime, and the operation is multiplication mod $n$

When $n$ is not a prime, $\mathbb{Z}_n^*$ is the set of invertible elements modulo $n$, since $a \in \mathbb{Z}_n^*$ implies $\gcd(a, n) = 1$, and thus $a$ is invertible mod $n$
Consider the multiplication tables mod 5 and 6, respectively, below:

<table>
<thead>
<tr>
<th>* mod 5</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* mod 6</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- Mod 5 multiplication operation on the set $\mathbb{Z}_5 = \{1, 2, 3, 4\}$ forms the group $\mathbb{Z}_5^*$.
- Mod 6 multiplication operation on the set $\mathbb{Z}_6 = \{1, 2, 3, 4, 5\}$ does not form a group since 2, 3 and 4 are not invertible.
- Mod 6 multiplication operation on the set of invertible elements forms a group: $(\mathbb{Z}_6^*, \ast \mod 6) = (\{1, 5\}, \ast \mod 6)$. 

Koç (http://cs.ucsb.edu/~koc)
Additive Groups

- The operation $\oplus$ is an addition “$+$”
- The neutral element is generally called the zero element $e = 0$
- Addition of an element $a$ $k$ times by itself, denoted as
  $$[k] a = a + \cdots + a$$
- The inverse of an element $a$ is denoted as $-a$
- Example: $(\mathbb{Z}_n, + \mod n)$ is a group; the set is
  $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ and the operation is addition mod $n$
Consider the addition tables mod 4 and 5, respectively, below

\[
\begin{array}{c|cccc}
+ \mod 4 & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{c|cccc}
+ \mod 5 & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}
\]

- Mod 4 addition operation on set \( \mathbb{Z}_4 = \{0, 1, 2, 3\} \) forms the group \((\mathbb{Z}_4, + \mod 4)\)
- Mod 5 addition operation on set \( \mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \) forms the group \((\mathbb{Z}_5, + \mod 5)\)
The order of a group is the number of elements in the set

The order of \( (\mathbb{Z}_{11}^*, \ast \mod 11) \) is 10, since the set \( \mathbb{Z}_{11}^* \) has 10 elements: \( \{1, 2, \ldots, 10\} \)

The order of group \( (\mathbb{Z}_p^*, \ast \mod p) \) is equal to \( p - 1 \); since \( p \) is prime, the group order \( p - 1 \) is not prime

The order of \( (\mathbb{Z}_{11}, + \mod 11) \) is 11, since the set \( \mathbb{Z}_{11} \) has 11 elements: \( \{0, 1, 2, \ldots, 10\} \)

The order of \( (\mathbb{Z}_n, + \mod n) \) is \( n \), since the set \( \mathbb{Z}_n \) has \( n \) elements: \( \{0, 1, 2, \ldots, n - 1\} \); here \( n \) could be prime or composite
The order of an element $a$ in a multiplicative group is the smallest integer $k$ such that $a^k = 1$ (where 1 is the unit element of the group)

- $\text{order}(3) = 5$ in $(\mathbb{Z}_{11}^*, \ast \mod 11)$ since
  $$\{ 3^i \mod 11 \mid 1 \leq i \leq 10 \} = \{3, 9, 5, 4, 1\}$$

- $\text{order}(2) = 10$ in $(\mathbb{Z}_{11}^*, \ast \mod 11)$ since
  $$\{ 2^i \mod 11 \mid 1 \leq i \leq 10 \} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$$

- Note that $\text{order}(1) = 1$
Order of an Element

- **The order of an element** $a$ in an additive group is the smallest integer $k$ such that $[k]a = 0$ (where 0 is the zero element of the group).

- $\text{order}(3)$ in $(\mathbb{Z}_{11}, + \mod 11)$ is computed by finding the smallest $k$ such that $[k]3 = 0$, which is obtained by successively computing

$$3 = 3, \quad 3 + 3 = 6, \quad 3 + 3 + 3 = 9, \quad 3 + 3 + 3 + 3 = 1, \quad \cdots$$

until we obtain the zero element.

- If we proceed, we find $\text{order}(3) = 11$ in $(\mathbb{Z}_{11}, + \mod 11)$

$$\{[i]3 \mod 11 \mid 1 \leq i \leq 11\} = \{3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 0\}$$

- Note that $\text{order}(0) = 1$
Lagrange’s Theorem

- Theorem: The order of an element divides the order of the group.
- Lagrange’s theorem applies to any group, and any element in the group.
- The order of the group \((\mathbb{Z}_{11}^*, \ast \mod 11)\) is equal to 10, while \(\text{order}(3) = 5\) in \((\mathbb{Z}_{11}^*, \ast \mod 11)\), and 5 divides 10, i.e., \(5|10\).
- \(\text{order}(2) = 10\) in \((\mathbb{Z}_{11}^*, \ast \mod 11)\), and 10 divides 10, i.e., \(10|10\).
- Similarly, \(\text{order}(1) = 1\) in \((\mathbb{Z}_{11}^*, \ast \mod 11)\), and 1 divides 10, i.e., \(1|10\).
- Since the order of the group \((\mathbb{Z}_{11}^*, \ast \mod 11)\) is 10, and the divisors of 10 are 1, 2, 5, and 10, the element orders can only be 1, 2, 5, or 10.
On the other hand, order(3) = 11 in \((\mathbb{Z}_{11}, + \text{ mod } 11)\), and 11\mid 11

Similarly, order(2) = 11 in \((\mathbb{Z}_{11}, + \text{ mod } 11)\)

We also found order(0)=1

Since the order of the group \((\mathbb{Z}_{11}, + \text{ mod } 11)\) is 11, and 11 is a prime number (divisors are 1 and 11), the order of any element in this group can be either 1 or 11

It turns out 0 is the only element in \((\mathbb{Z}_{11}, + \text{ mod } 11)\) whose order is 1; all other elements have the same order 11 which is the group order
An element whose order is equal to the group order is called **primitive**.

The order of the group \((\mathbb{Z}_{11}^*, \times \mod 11)\) is 10 and order(2) = 10, therefore, 2 is a primitive element of the group.

order(2) = 11 and order(3) = 11 in \((\mathbb{Z}_{11}, + \mod 11)\), which is the order of the group, therefore 2 and 3 are both primitive elements — in fact all elements of \((\mathbb{Z}_{11}, + \mod 11)\) are primitive except 0.

Theorem: The number of primitive elements in \((\mathbb{Z}_p^*, \times \mod p)\) is \(\phi(p - 1)\).

There are \(\phi(10) = 4\) primitive elements in \((\mathbb{Z}_{11}^*, \times \mod 11)\), they are: 2, 6, 7, 8; all of these elements are of order 10.
Cyclic Groups and Generators

- We call a group **cyclic** if all elements of the group can be generated by repeated application of the group operation on a **single element**.
- This element is called a **generator**.
- Any primitive element is a generator.
- For example, 2 is a generator of \((\mathbb{Z}_{11}^*, \ast \mod 11)\) since
  \[
  \{2^i \mid 1 \leq i \leq 10\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \mathbb{Z}_{11}^*
  \]
- Also, 2 is a generator of \((\mathbb{Z}_{11}, + \mod 11)\) since
  \[
  \{[i] 2 \mod 11 \mid 1 \leq i \leq 11\} = \{2, 4, 6, 8, 10, 1, 3, 5, 7, 9, 0\} = \mathbb{Z}_{11}
  \]