From Groups to Affine Ciphers

Yan Huang
Objectives

• Groups

• Greatest common divisors

• Euclidean algorithm

• Affine Ciphers
Group \((G, \star)\)

A group consists of a set \(G\) and a binary function \(\star\) that satisfy the following properties

- **Closure**: For all \(a, b \in G\), \(a \star b \in G\).
- **Identity**: There is an \(e \in G\) such that
  \[ e \star a = a \star e = a \]
  for every \(a \in G\).
- **Inverse**: For every \(a \in G\) there is a unique \(b \in G\) such that
  \[ a \star b = b \star a = e \]
  We denote such \(b\) as \(a^{-1}\).
- **Associativity**: For all \(a, b, c \in G\),
  \[ a \star (b \star c) = (a \star b) \star c \]
Example: $\mathbb{Z}_3^+ = (\{0, 1, 2\}, \ +_{\text{mod} \ 3})$

- Closure ✓
- Identity ✓
- Inverse ✓
- Associativity

\[ a \cdot (b + c) = a \cdot b + a \cdot c \]
Example: $\mathbb{Z}_7^+ = (\{0, 1, \ldots, 6\}, +_{\text{mod } 7})$

- Closure
- Identity
- Inverse
- Associativity
Example: $\mathbb{Z}_3^* = (\{1, 2\}, \ast_{\text{mod} \ 3})$

- Closure
- Identity
- Inverse
- Associativity
Example: $\mathbb{Z}_7^* = (\{1, \ldots, 6\}, \ast_{\text{mod } 7})$

- **Closure**

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

- **Identity**

- **Inverse**

- **Associativity**
How about \( \{1, 2, 3, 4, 5, 6, 7, 8\}, \ *_{\text{mod 9}} \)?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Closure**
- **Identity**
- **Inverse**
- **Associativity**
How about \( \{1, 2, 4, 5, 7, 8\}, \mod 9 \)?

<table>
<thead>
<tr>
<th>( *_{\text{mod } 9} )</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- Closure
- Identity \( 1 \) is the identity element.
- Inverse
- Associativity
Commutative Groups

If the $\star$ function of a group $G = (S, \star)$ additionally satisfies that
\[ \forall a, b \in S, \quad a \star b = b \star a \]

Then $G$ is called an *commutative* (or *abelian*) group.

Ex. \((\{0, 1, 2\}, \mod 3)

\((\{1, 2, 4, 5, 7, 8\}, \mod 9)\)
Greatest Common Divisor

• A common divisor of two integers $a$ and $b$ is a positive integer $d$ that divides both of them. The greatest common divisor of $a$ and $b$ is the largest of all common divisors.

- $\gcd(2, 4) = 2$
- $\gcd(6, 9) = 3$
- $\gcd(7, 5) = 1$
- $\gcd(8, 9) = 1$
- $\gcd(124, 72) = 4$
- $\gcd(748, 2024) = ?$

If $\gcd(a, b) = 1$, then $a$ and $b$ are said to be coprime.
Which integers belong to $\mathbb{Z}_n^*$?

• $\mathbb{Z}_n^*$ consists of *exactly* the set of integers that are coprime with $n$. Namely, $\mathbb{Z}_n^* = \{a \mid \gcd(a, n) = 1\}$.

- $\forall a \in \mathbb{N}$, $\gcd(a, n) = 1 \Rightarrow \exists b$ such that $ab = 1 \mod n$. 
Which integers belong to $\mathbb{Z}_n$?

- Given $a$ and $n$, the question of whether $a \in \mathbb{Z}_n^*$ reduces to computing $\gcd(a, n)$.
  - You don’t have to know how to factorize $a$ and $n$ to compute $\gcd(a, n)$.
  - $\gcd(823, 2939)$

$\text{gcd}(823, 2939) = \text{gcd}(2116, 823)$

If $d \mid 2116$ and $d \mid 823$.

So $d \mid (2939 - 823) = 2116$

If $d \mid 2116$ and $d \mid 823$. Note $d \mid 2939$. 

$\gcd(2939 - 2 \times 823) = 1293$

$\frac{470}{823}$
\[
gcd(823, 2939) = gcd(823, 2939 \mod 823) \\
= gcd(823, 470) \\
= gcd(823 \mod 470, 470) \\
= gcd(353, 470) \\
= gcd(353, 470 \mod 353) \\
= gcd(353, 117) \\
= gcd(353 \mod 117, 117) = gcd(2, 117) = gcd(2, 1) = 1
\]
\[ \text{gcd}(a, n) = \text{gcd} \left( a, n \mod a \right) \text{ if } n > a \]
\[ \text{if } n = aq + r \text{ (} 0 \leq r < a \text{)} \]
\[ = \text{gcd} \left( a, r \right) \]
Another Example: gcd(87,45)

\[
gcd(87, 45) = gcd(42, 45)
\]
\[
= gcd(42, 3)
\]
\[
= gcd(0, 3) = 3
\]
What is $\mathbb{Z}_{16}^*$?

\[ \mathbb{Z}_{16}^* = \{ a \mid \text{gcd}(a, 16) = 1, a \leq 16 \} \]
Implementing $\text{gcd}(a, n)$ with Haskell
Affine Cipher

To Encrypt:
\[ C = k_1 \times M + k_2 \mod 26 \]

To Decrypt:
\[ M = (C - k_2) \times k_1^{-1} \mod 26 \]
Affine Cipher

To Encrypt:
\[ C = k_1 \times M + k_2 \mod 26 \]

To Decrypt:
\[ M = (C - k_2) \times k_1^{-1} \mod 26 \]

What values can \( k_2 \) take?

What values can \( k_1 \) take?
Implementing Affine Cipher in Haskell