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

$+_{\text{mod } 3}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

id → 0

$0 + 2 \bmod 3 = 2$

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

Example: $\mathbb{Z}_7^+ = (\{0, 1, \ldots, 6\},\ +_{\mathbf{mod}\ 7})$

- Closure
- Identity
- Inverse
- Associativity

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Example: $\mathbb{Z}_3^* = (\{1, 2\},\ *_{\mathbf{mod\ 3}})$

- Closure
- Identity
- Inverse
- Associativity

$*_{\text{mod } 3}$	1	2
1	1	2
2	2	1

$a \times b \times c = a \times (b \times c)$

Example: $\mathbb{Z}_7^* = (\{1, \dots, 6\}, *_{\bmod 7})$

- Closure
- Identity
- Inverse
- Associativity

*mod7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

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

- Closure
- Identity
- Inverse
- Associativity

$*_{\text{mod } 9}$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

$7 = -2 \bmod 9$

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

- Closure
- Identity
- Inverse
- Associativity

$*_{\text{mod } 9}$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Commutative Groups

If the $\star$ function of a group $G = (S, \star)$ additionally satisfies that

$$\forall a, b \in S, \qquad a \star b = b \star a$$

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

Ex. $(\{0, 1, 2\}, +_{\text{mod } 3})$

$(\{1, 2, 4, 5, 7, 8\}, \times_{\text{mod } 9})$

Greatest Common Divisor

if $gcd(a, b) = 1$. then
a and b are said to be
coprime.

- 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)=?

$6 = 2 \times 3$. $9 = 3 \times 3$

divisors 6 $= \{1, 2, 3, 6\}$
divisors 9 $= \{1, 3, 9\}$.

divisors 124 $= [1, 2, 4, 31, 62, 124]$.
divisors 72 $= [\ldots]$

Which integers belong to $\mathbb{Z}_{\boldsymbol{n}}^*$?

- $\mathbb{Z}_n^*$ 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 $ab = 1 \bmod n$.

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) imagine d is the gcd(823, 2939). then

$d \mid 823 \quad d \mid 2939$. so $d \mid (2939 - 823) = 2116$

$\gcd(823, 2939) = \gcd(2116, 823)$. $\quad d \mid (2939 - 2\cdot 823) = 1293$

if $d \mid 2116$, and $d \mid 823$: $\Rightarrow \cancel{d \mid 2939}$ ✓

$$\begin{array}{r} 1293 \\ -\ 823 \\ \hline 470 \end{array}$$

$$\gcd(823, 2939) = \gcd(823, 2939 \bmod 823)$$
$$= \gcd(823, 470)$$
$$= \gcd(823 \bmod 470, 470)$$
$$= \gcd(353, 470)$$
$$= \gcd(353, 470 \bmod 353)$$
$$= \gcd(353, 117)$$
$$= \gcd(353 \bmod 117, 117) = \gcd(2, 117) = \gcd(2, 1)$$
$$= 1$$

$\gcd(a, n) = \gcd(a, n \bmod a)$ if $n > a$

if $n = aq + r$ $(0 \le r < a)$

$= \gcd(a, r)$

Another Example: gcd(87,45)

$$87 \bmod 45 = 42$$
$$45 \bmod 42 = 3$$
$$42 \bmod 3 = 0$$

$$\gcd(87, 45) = \gcd(42, 45)$$
$$= \gcd(42, 3)$$
$$= \gcd(0, 3) = 3$$

What is $\mathbb{Z}_{16}^*$?

$\{a \mid \gcd(a, 16) = 1, a < 16\}$

$\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$

Implementing $\mathbf{gcd}(a, n)$ with Haskell

Affine Cipher

To Encrypt:

$$C = k_1 * M + k_2 \mod 26$$

To Decrypt:

$$M = (C - k_2) * k_1^{-1} \mod 26$$

Affine Cipher

To Encrypt:

$$C = k_1 * M + k_2 \qquad \mod 26$$

To Decrypt:

$$M = (C - k_2) * k_1^{-1} \quad \mod 26$$

What values can k_2 take?

What values can k_1 take?

Implementing Affine Cipher in Haskell