From Groups to Affine Ciphers

Yan Huang

Objectives

• Groups

• Greatest common divisors

• Euclidean algorithm

• Affine Ciphers

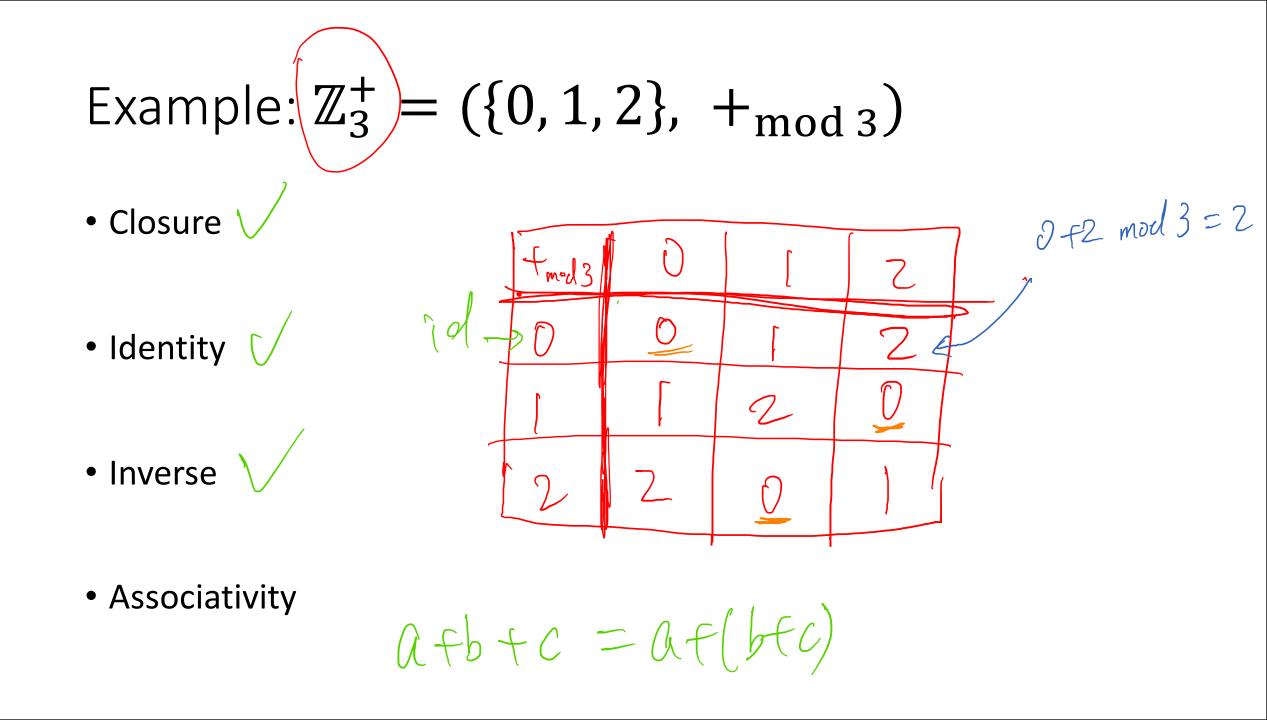
Group (G, *)

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

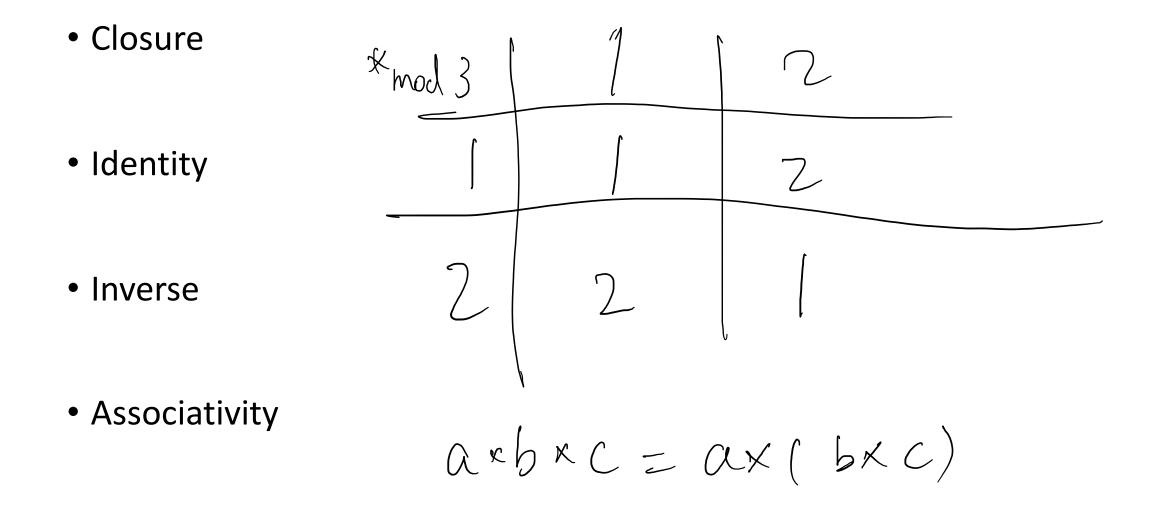
 $e \star a = a \star e = a$ for every $a \in G$.

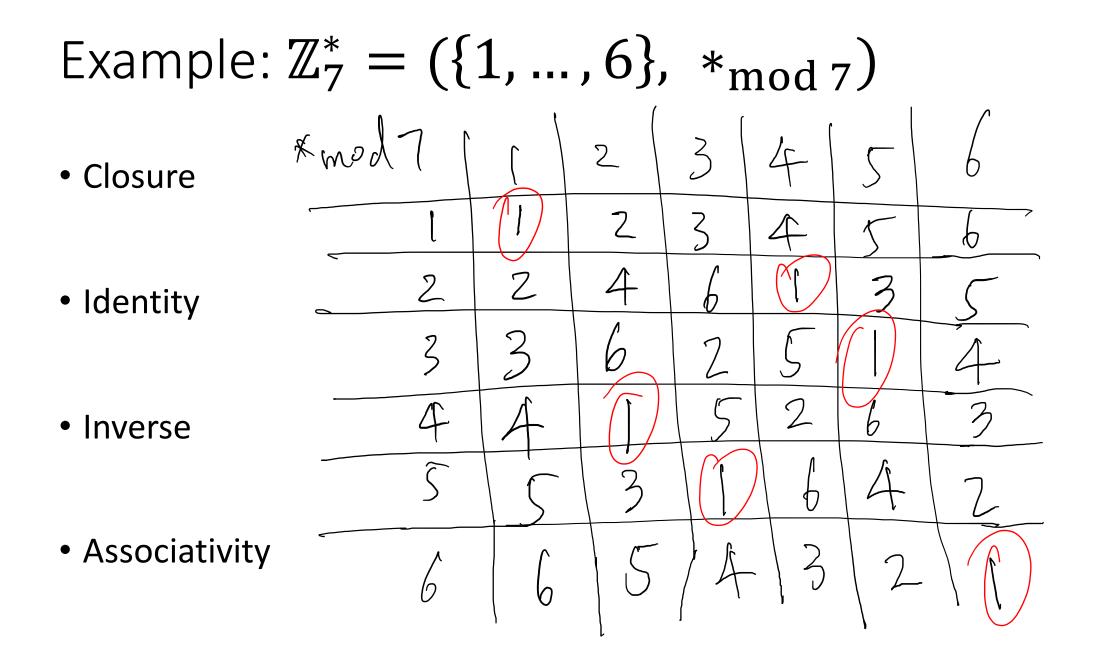
- Inverse: For every $a \in G$ there is a unique $b \in G$ such that $a \star b = b \star a = e$. We denote such b as a^{-1} .
- Associativity: For all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

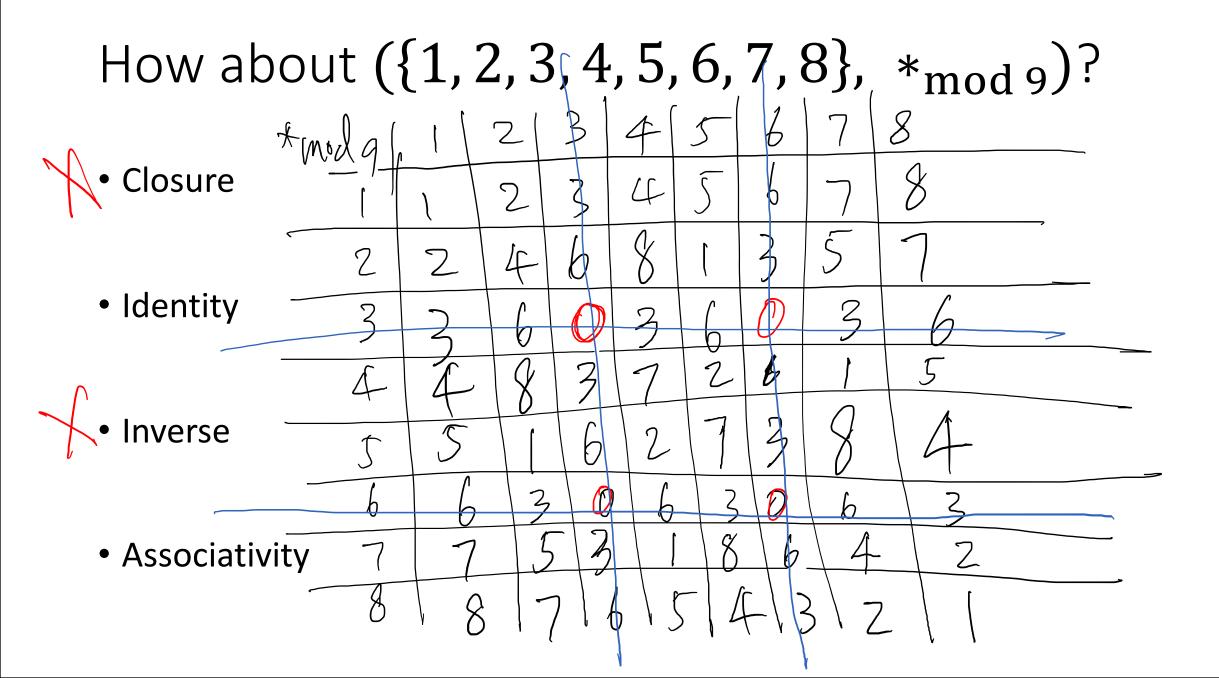


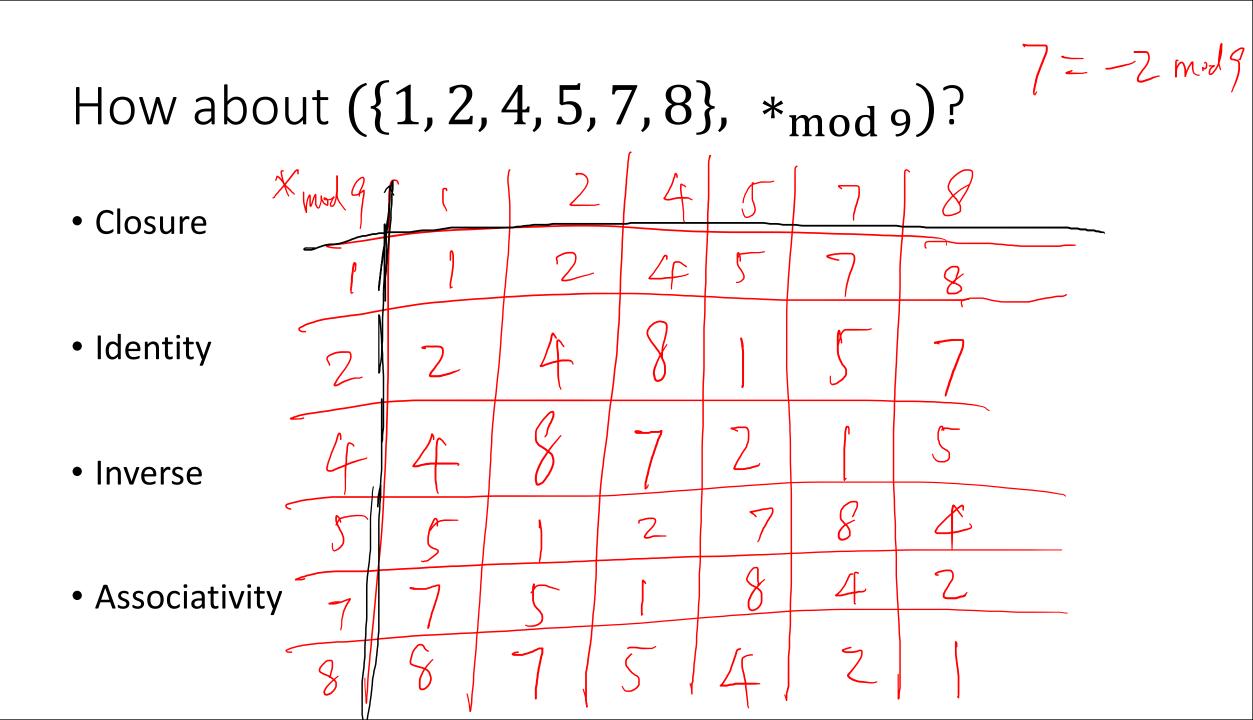
Example: $\mathbb{Z}_7^+ = (\{0, 1, \dots, 6\}, +_{\text{mod } 7})$ • Closure ()1232F5 Identity \mathbf{r} \mathcal{O} Inverse $\overline{1}$ h Associativity $\left[2\right]$

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









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. ({{,1,2}} foud 3) ({ {] , 2 , 4 , 5 , 7 , 8 } , Xmdq)

Greatest Common Divisor J g(dla, b)=1. then and b are said to be

- 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.
 - $\begin{array}{l} -\gcd(2,4) &= 2 \\ -\gcd(6,9) = 3 \\ -\gcd(7,5) = | \\ -\gcd(8,9) = 1 \\ -\gcd(124,72) = 4 \\ -\gcd(748,2024) = ? \end{array} \begin{array}{l} \end{tabular} \begin{tabular}{l} & \end{tabular} \end{tabular} \begin{tabular}{l} & \end{tabular} \end{tabular} \begin{tabular}{l} & \end{tabular} \end{tabular} \end{tabular} \begin{tabular}{l} & \end{tabular} \end{tabular} \end{tabular} \begin{tabular}{l} & \end{tabular} \e$

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) (megne d'is the gcd (823, 2929). then d | 823 d | 2939 d | 2939 d | (2939 - 823) = 2116

g(d(823, 2939) = g(d(2116, 823)) d(2939 - 2823) = [193)if d(2116, and d(823)) = 2d(2939 - 2823) = [193] = 2d(2939) = [293] = 823

 $g(d(823, 2939) = g(d(823, 2939) \mod 823)$ = g(d(823, 470)= 9cd (823 mod 470, 470) = 3cd(353,470)= gcd (353, 470 mod 353) = 962(353, 117) $= gcd(353 \mod 117, 117) = gcd(2, 117) = gcd(2, 1)$

gcd(a,n) = gcd(a, n mod a) if n > a

if $N = aqfr (o \leq r < a)$

= gcd(a, r)

Another Example: gcd(87,45) (87 mod 42 = 42 45 mod 42 = 3 $gcd(87, 45) = gcd(42, 45) 242 \mod 3=0$ = ged (42, 3) = gcd(0, 3) = 3

What is \mathbb{Z}_{16}^* ? $\{a \mid gcd(a, b) = 1, a < b\}$

 $Z_{6}^{*} = \{1, 3, 5, 7, 9, 11, 13, \\ 15, \}$

Implementing 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:

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

To Decrypt:

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

What values can k_2 take?

What values can k_1 take?

Implementing Affine Cipher in Haskell