Cyclic Groups

Tuesday, September 21, 2021 1:32 PM

Group Theory

- Building crypto on prime order cyclic groups.

- Def'n: A Group is a set G, and a binary operation $\cdot$

$$\cdot : G \times G \to G$$

Satisfying:

- Identity.

$$\exists e, \forall g \in G, \; e \cdot g = g \cdot e = g$$

- Inverses:

$$\forall g \in G \; \exists g^{-1} \text{ s.t. } g \cdot g^{-1} = g^{-1} \cdot g = e$$

- Associative:

$$\forall g,h,j \in G, \; g \cdot (h \cdot j) = (g \cdot h) \cdot j$$

Examples:

- $\mathbb{Z}^+$ integers under addition.

+ closed integers

0 id.

$(-X) + X = 0$

- $\mathbb{N}^+$?

closed ✓

assoc ✓

identity ✓ 0 $x \in \mathbb{N}$?

inverses $S + (x) = 0$

- $\mathbb{Z}_n^+$ integers mod n $n \in \mathbb{N}$

$\{0, 1, \ldots, n-1\}$

Inverse: $a + (n-a) = 0 \mod n$.

Q. next five:

$\{1,2,3,4,5\}$ under $\times \mod 6$.

integers from 1 to (G-1) under multiplication ∪.