Set Notations Modulo n

- For $n \in Z^*$:

- $Z_n = \{0,1, \ldots, n-1 \}$
  - Set of residues

- $Z_n^* = \{ a \in Z_n \mid \gcd(a,n) = 1\}$
  - Set of integers co-prime with n
  - E.g., $n = 15$
  - $Z_n = \{0,1, 2, \ldots,14\}$
  - $Z_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Groups

- Groups denoted by $|G, \cdot|$ are non-empty sets with a binary operation denoted by $\cdot$ defined over G such that for every $a, b \in G$, $a \cdot b \in G$
- Group Properties: Every group, G has to have the following properties:

Groups

1. Closure: For all $a,b \in G$, $a \cdot b \in G$
2. Associative: For all $a,b,c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Identity element: There exists an $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$
4. Inverse element: For all $a \in G$, there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$

Groups Example

- Identity element:
  - $Z_N = (\{0, 1, 2, 3, 4, 5, 6, 7, 8\}, +)$
  - Identity element $e \in Z_N$ such that $a+e = e+a = a$ is 0

- Inverse element:
  - For each $a \in Z_N$ there should be an a^{-1}, such that $(a + a^{-1}) \bmod N = (a^{-1} + a) \bmod N = 0 \bmod N$
  - Take a=5. We need an a^{-1} such that $5+a^{-1} \equiv 0 \bmod 9$ [1]
  - So, $a^{-1} = 4$

1: Why? $a \equiv b \pmod{n}$ iff $(a \bmod n) = (b \bmod n)$

Abelian Groups

1. Closure: For all $a,b \in G$, $a \cdot b \in G$
2. Associative: For all $a,b,c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Identity element: There exists an $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$
4. Inverse element: For all $a \in G$, there exists an $a' \in G$ such that $a \cdot a' = a' \cdot a = e$
5. Commutative: For all $a,b \in G$, $a \cdot b = b \cdot a$

Group Order

- Infinite group: Unlimited number of elements, e.g., Z, Z_+, N

- Finite group: Limited set of elements, e.g., Z_n, Z_n^*, where $n \in Z$ or Z_+ or N. The number of elements = *order* of group. Denoted by $| Z_n |$, $|Z_n^*|$, etc.

- Let $n = 9$, so $Z_n^* = \{1, 2, 4, 5, 7, 8\}$

- What is $| Z_n^* |$?
  - 6 – length of Z_n^*

Group Properties and Tricks

- If G is a group of order x and $a \in G$, then $a^y \bmod n = a^{y \bmod x} \bmod n$
- E.g., $n \in Z_+$, let n=9, so $Z_9^* = \{1, 2, 4, 5, 7, 8\}$

- Find $4^{50} \bmod 9$
- Here $G = Z_9^* = \{1, 2, 4, 5, 7, 8\}$, and $x = |Z_n^*| = 6$, $y = 50$
- $4^{50} \bmod 9 = 4^{50 \bmod 6} \bmod 9$

  $= 4^2 \bmod 9$

  $= 16 \bmod 9$

  $= 7$

Cyclic Group

- A group G is cyclic if every element of G is a power a^k, $k \in Z^+$, of a fixed element $a \in G$
- Element a is the *generator* of G

- G is cyclic group
- $k \geq 1$, every element of G is a^k, e.g., G = {2, 4, 8, 16, 32, 64, 128,…} — generator, a = 2
- If n is prime, Z_n^* is cyclic

- We'll revisit this in more detail in Number Theory IV slides