Tutorial 0

Modular arithmetic

a is congruent b modulo n $\quad a, b \in \mathbb{Z} \quad n \in \mathbb{N}$

$$a \equiv b \pmod n \iff \exists k \in \mathbb{Z} : k \cdot n = a - b \iff n \mid a - b$$

n divides a − b

Example: $a = 14,\ b = 23,\ n = 3$ for $k = -3$

$-3 \cdot 3 = 14 - 23 \Rightarrow a \equiv b \pmod n$

Let $n = 7$ $a = 15$, then $a = 2 \cdot 7 + 1$

For $a \in \mathbb{Z}$, $n \in \mathbb{N}$, there is always a unique pair $k \in \mathbb{Z}$ and $r \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with $a = k \cdot n + r$

r is called the <u>remainder</u> of a modulo n.

$r = a \bmod n$

Examples: $x + 7 \equiv 3 \pmod{17}$

$x \equiv 3 - 7 = -4 \pmod{17}$

$x \equiv 13 \pmod{17}$

- $2x + 7 \equiv 3 \pmod{17}$

  $2x \equiv -4 \pmod{17}$

  $x \equiv -2 \pmod{17}$

  $x \equiv 15 \pmod{17}$

- $5x + 6 \equiv 13 \pmod{11}$

  $5x \equiv 7 \pmod{11}$

Let see: $5x \equiv 7 \equiv 18 \equiv 29 \equiv 40 \Rightarrow x \equiv 8 \pmod{11}$

Alternatively: $5 \nmid 1$; $5 \nmid 11 + 1$; $5 \nmid 22 + 1$; $5 \nmid 33 + 1$; $5 \mid 44 + 1$

$5 \cdot 9 \equiv 1 \pmod{11}$

$\Rightarrow 9 \cdot 5 \cdot x \equiv 9 \cdot 7 \pmod{11} \Rightarrow x \equiv 8 \pmod{11}$

Algebra / group G: a set G and operator $\circ : G \times G \to G$
$(a,b) \mapsto a \circ b$ is called a group, if

- $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a,b,c \in G$
- $\exists e \in G : a \circ e = e \circ a = a \quad \forall a \in G$ e is unit element
- $\forall a \in G : \exists a' \in G$ s.t. $a \circ a' = a' \circ a = e$

If $a \circ b = b \circ a \quad \forall a,b \in G$ it is called commutative or Abelian

$H \subset G$ and $(H, \circ)$ is a group, then h is called subgroup of G.

Let $ord(g) = \min \{ n \in \mathbb{N} \mid g^n = e \}$ // n-times executing of $\circ$
be the order of g

Let $\langle g \rangle = \{ g^n \mid 1 \le n \le ord(g) \}$

If $\langle g \rangle = G$ then g is called generator.

Lagrange's Theorem: $(G, \circ)$ finite group, H subgroup of G,
and $g \in G$
$\Rightarrow |H| \mid |G|$ and $ord(g) \mid |G|$

Ring: set R, operator $+ : R^2 \to R$, operator $\cdot : R^2 \to R$

- $(R, +)$ is Abelian
- $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a,b,c \in R$
- $\exists u \quad a \cdot u = u \cdot a = a \quad \forall a \in R$
- $(a+b) \cdot c = a \cdot c + b \cdot c$ and $c(a+b) = c \cdot a + c \cdot b \quad \forall a,b,c$

$a \cdot b = b \cdot a \quad \forall a,b \in R$ then R is called commutative

Fields: F with $+$ and $\cdot$ is called field if

- $(F, +)$ Abelian group
- $(F \setminus \{0\}, \cdot)$ Abelian group
- $c(a+b) = c \cdot a + c \cdot b$