Summary Quiz 2

January 24, 2023 21:31

3.1 Well-Defined Operations

An operation $\cdot$ is well defined when if $\left.\begin{matrix} x \sim y \\ w \sim z \end{matrix}\right\} \to (x \cdot w) \sim (y \cdot z)$

Note: $x \sim y \leftrightarrow [x] = [y]$

3.2 Number Theory

- Any non-empty set $S \subseteq \mathbb{N}$ has a unique $d \in S$ such that $\forall x \in S,\ d \leq x$
- For $a, b \in \mathbb{Z},\ b > 0$, then $\exists!\, q, r \in \mathbb{Z}$ such that $a = bq + r$, $0 \leq r < b$

5.1 Divisibility and Modulo

$m \mid n$ means $\exists x \in \mathbb{Z}$ such that $n = mx$

$a \equiv b \bmod n$ means $n \mid (a - b) \to \dfrac{a-b}{n} \in \mathbb{Z}$

5.2 Properties of Arithmetic Modulo n

- Commutative: $a + b \equiv b + a \pmod{n}$
- Commutative: $ab \equiv ba \pmod{n}$
- Associative: $(a + b) + c \equiv a + (b + c) \pmod{n}$
- Association: $(ab)c \equiv a(bc) \pmod{n}$
- Distributive: $a(b + c) \equiv ab + ac \pmod{n}$
- 0 Identity for $+$: $a + 0 \equiv a \pmod{n}$
- 1 Identity for $\cdot$: $1a \equiv a \pmod{n}$
- Additive Inverses: $a + (-a) \equiv 0 \pmod{n}$

+ Theorems

Congruence modulo n is an equivalence relation

5.3 GCD and LCM

- $d = \mathrm{GCD}(a, b)$ if and only if:
  - $d \mid a$ and $d \mid b$
  - If $c \mid a$ and $c \mid b$, then $c \mid d$
- $m = \mathrm{LCM}(a, b)$ if and only if:
  - $a \mid m$ and $b \mid m$
  - If $a \mid n$ and $b \mid n$, then $m \mid n$

+ Theorems

- $\forall a, b \in \mathbb{Z},\ \exists!\, \mathrm{GCD}\ d$ and $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$
- $\forall a, b \in \mathbb{Z},\ \exists!\ \mathrm{LCM}\ m$
- If $\mathrm{GCD}(a, b) = 1$, then $\exists x, y$ such that $ax + by = 1$
- If $\mathrm{GCD}(a, b) = d$, then $\{ax + by : x, y \in \mathbb{Z}\} = d \times \mathbb{Z}$

5.4 Prime and Irreducible

For $p \in \mathbb{Z}$ where $p > 1$:

- p is irreducible if the only divisors of p are 1 and p
- p is prime if whenever $p \mid ab$, then $p \mid a$ and $p \mid b$

+ Theorems

- p is prime $\leftrightarrow$ p is irreducible
- For any $n \in \mathbb{Z}$ where $n > 1$, $\exists!\, p_1, \dots, p_s$ primes, $e_1, \dots, e_s$ positive integers such that $n = p_1^{e_1} \times \cdots \times p_s^{e_s}$

6.1 Prime and Irreducible

For some set S and an operation $\cdot$, $(S, \cdot)$ is a group if:

- Closure: $ab \in S$
- Associativity: $(ab)c = a(bc)$
- Identity: $\exists \epsilon \in S$ such that $x\epsilon = \epsilon x = x$
- Inverses: $\forall x \in S, \exists y \in S$ such that $xy = yx = \epsilon$