MATH 541 Lecture 03 30 January 2023

Modular Arithmetic

Last time: Dihedral group

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle$$

Example $n=4$ $R_i = \{1, r, r^2, r^3\} \subseteq D_8$

$\uparrow$ closed under the group multiplication

$\Rightarrow R$ is a subgroup of D_8

Linear algebra $W \overset{\text{subset}}{\subseteq} V$ = vector space

W is a subspace $\Leftrightarrow$ closed on $+$ and scalar multiplication

---

$r^2 \cdot r^3 = r^5 = r$ Look at powers

$r^3 \cdot r^3 = r^2$ $r^i \cdot r^j = r^{i+j}$

but for the exponents "$4 = 0$"

Def Let $a, b \in \mathbb{Z}$ Say "a divides b / b is divisible by a"

if $\exists k \in \mathbb{Z}$, s.t. $b = ak$ Notation: $a \mid b$

Exercise: If $a \mid b_1$, $a \mid b_2$, then $a \mid b_1 + b_2$

Pf By assumption, $\exists k_1, k_2 \in \mathbb{Z}$, s.t. $b_i = ak_i$ for $i = 1, 2$

$$b_1 + b_2 = \underbrace{(k_1 + k_2)}_{\mathbb{Z}} a \Rightarrow a \mid b_1 + b_2$$

Def Say "$p \in \mathbb{Z}_{>1}$ is a prime number", if the <u>only</u> $a \in \mathbb{Z}_{>1}$ that divides p is p itself

Ex: $2, 3, 5, 7, \dots$ prime $\quad 4, 6, 8, 9, 10, \dots$ composite numbers

Fun Fact: 57 is called the "Grothendieck prime" $(3 \cdot 19)$

Division w/ remainder

For any $a, b \in \mathbb{Z}$, $a \neq 0$, there exists a unique pair $(q, r) \in \mathbb{Z}^2$

s.t. $b = qa + r$ and $0 \leq r < |a|$

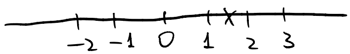
Exercise: $a = 9$, $b = 1373$ Find $\underset{\substack{\| \\ 152}}{q}$ and $\underset{\substack{\| \\ 5}}{r}$

Pf assume $a > 0$ ($a < 0$ exercise)

Consider $b/a \in \mathbb{Q}$

$\exists!$ $q \in \mathbb{Z}$, s.t. $q \leq b/a < q+1$

there exists a unique



$0 \leq b/a - q < 1 \quad \times a > 0$

$0 \leq \underbrace{a(b/a - q)}_{r = b - aq} < a$

Then we set $r = b - aq$

Def Let $a, b \in \mathbb{N} = \mathbb{Z}_{\geq 0}$

We say that "$d \in \mathbb{N}$ is the greatest common divisor of a, b"

if $\partial \leq d$ for every $\partial \in \mathbb{N}$, s.t. $\partial | a$, $\partial | b$

$d = \gcd(a, b)$

Ex $\gcd(12, 18) = 6 \quad \gcd(30, 31) = 1$

Well ordering principle

Let $S \subseteq \mathbb{Z}$ which is bounded below (resp. above)

Then $\exists!$ s_{min} (resp. s_{max}) in S s.t. $\forall s \in S$, $s \geq s_{min}$ (resp. $s \leq s_{max}$)

Ex $S \subseteq \mathbb{Q}$

$$S = \{q \in \mathbb{Q} \mid q < \sqrt{2}\}$$ does not have a max

Say $f_{max} \in S$ $\qquad q_{max} < q < \sqrt{2}$

Can always find $q \in S$

We write $a \equiv b \mod n$ (equivalent/congruent)

if $n \mid a-b$ $\quad$ E.g. $5 \equiv 3 \mod 2$

E.g. $n=4$ $\{\ldots, -8, -4, 0, 4, 8, \cdots\}$

$\overline{9} = \overline{-3} = \{-7, -3, 1, 5, 9, \ldots\}$

$\{-6, -2, 2, 6, 10, \ldots\}$

$\{-5, -1, 3, 7, 11, \ldots\}$

For $a \in \mathbb{Z}$, write $\bar{a}$ ~~for~~ its congruence class

$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\}$ is a group w/ $+$ defined by $\bar{a} + \bar{b} = \overline{a+b}$

Say $\bar{2} + \bar{3} = \bar{5}$

$(n=4)$ $\quad \overline{-10} + \bar{7} = \overline{-3}$

Need to check: $\forall a, b, a', b' \in \mathbb{Z}$

s.t. $a \equiv a' \bmod n$, $b \equiv b' \bmod n$

We have $a+b \equiv a'+b' \bmod n$ (exercise)

<u>Def</u> Two groups G, H are <u>isomorphic</u> if $\exists \varphi : G \to H$ bijection ~~of~~ sets

s.t. $\varphi(a)\varphi(b) = \varphi(ab)$, $\forall a, b \in G$

Then I can say $R \subseteq D_{2n}$

$\{1, r, r^2, \dots\}$

$R \cong \mathbb{Z}/n\mathbb{Z}$ isomorphic