Lecture 14:

- Last time: we proved that a cyclic group (i.e. a group that is generated by a single one of its elements), ie $G = \langle g \rangle$ for some $g \in G$) is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$.
- We also looked at $|g| = \min_{k \in \mathbb{Z}_{>0}} \{ \cancel{} \mid g^k = 1 \}$ 'order' of g. And proved:

Lemma: If $g^k = 1$, then $n = |g| \mid k$.

Today: Subgroups of cyclic groups.

Let's remember some things from basic number theory: Greatest common divisor

Definition: If $a, b \in \mathbb{Z}$, $g.c.d(a, b)$ is the largest integer that divides both a and b.

Proposition: The following numbers are equal

(1) $A = gcd(a, b) = \max \{ d \in \mathbb{Z} \mid d \mid a \text{ and } d \mid b \}$

(2) $B = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)}$.

where $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ $(\alpha_i, \beta_i \geqslant 0)$

(3) $C = \min \{ c \in \mathbb{Z}_{>0} \mid c = x \cdot a + y \cdot b,\ x, y \in \mathbb{Z} \}$

"smallest positive integer-linear combination of a and b".

part of proof:

$A = C \quad ((1) = (3))$.

. If $d \mid a$ and $d \mid b$ then $\forall x, y$ $d \mid ax+by$.

since $\gcd(a,b)$ divides both $\gcd(a,b) \mid C$.

so $\gcd(a,b) \leq C$.

- On the other hand, $C = \min\{c \in \mathbb{Z}_{\geq 0} \mid c = xa + yb,\ x, y \in \mathbb{Z}\}$.

then $C \mid a$ because:

$$a = qC + r \quad C > r \geq 0,$$

but if $r > 0$, then $a - qC = r < C$

is $a - q(xa + yb) = r$

$$(-qx+1)a - qyb = r$$

is a smaller positive integer-linear combination of a and b.

So $C \mid a$, similarly $C \mid b$.

since $\gcd(a,b) =$ max of all divisors,

$= \max\{d \in \mathbb{Z}_{\geq 1} \mid d \mid a \text{ and } d \mid b\}$

$$C \leq \gcd(a,b).$$

Proposition: Every subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

proof: Let $H \leq \mathbb{Z}$ be a subgroup.

Let $c = \min H \cap \mathbb{Z}_{\geq 1}$.

be the smallest positive element of H.

Then we claim $H = \langle c \rangle$.

Since $c \in H$, $\langle c \rangle \subset H$.

On the other hand, if $b \in H$,

then $\exists!\, q, r$ st

$$b = qc + r \quad c > r \geq 0$$

but then

$$\underbrace{b}_{\in H} - \underbrace{qc}_{\in H} = r \in H.$$

but $r < c$, so $r = 0$ since c was minimal. Hence $\langle c \rangle \supset H$.

Since $\langle c \rangle$ is an infinite cyclic group $\langle c \rangle = H \cong \mathbb{Z}$.

$\square$

Subgroups of $\mathbb{Z}/n\mathbb{Z}$:

Proposition: Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $\langle d \rangle$ for $d \mid n$. (and $\langle 0 \rangle$).

proof: Let H be a subgroup of $\mathbb{Z}/n\mathbb{Z}$. represent each element of H by an $\bar{h}$ s.t. $n > h \geq 0$.

Let a be the smallest $h > 0$ s.t $\bar{h} \in H$. (If there is no such h, then $H = \langle 0 \rangle$)

Let $\bar{h} \in H$. By division algorithm:

$$h = qa + r \qquad 0 \leq r < a$$

But since $h \in H$ and $a \in H$,

$$h - qa = r \in H.$$

But $r < a$ and a was minimal, so $r = 0$ and $a \mid h$.

Since $\underset{\overset{\shortparallel}{\bar{n}}}{\bar{0}} \in H$, $a \mid n$ also. $\square$

But how many of these subgroups coincide? none

If I have $\langle b \rangle$, which $\langle d \rangle$ does it correspond to?

Proposition: If $b \in \mathbb{Z}$,

$$\langle \bar{b} \rangle = \langle \overline{\gcd(b,n)} \rangle.$$

proof: Since $\gcd(b,n) \mid b$,

$\bar{b} \in \langle \overline{\gcd(b,n)} \rangle$ so

$$\langle \overline{\gcd(b,n)} \rangle \supseteq \langle \bar{b} \rangle.$$

On the other hand:

$$\gcd = xb + yn$$

so $\overline{\gcd} = x\bar{b}$

so $\gcd(a,b) \in \langle b \rangle$

So $\langle \gcd(a,b) \rangle \subseteq \langle b \rangle$

Thus: $\langle \gcd(a,b) \rangle = \langle b \rangle$. $\square$

Exercise: Prove that

$$\langle a \rangle + \langle b \rangle = \langle \gcd(a,b) \rangle$$