Lecture 15:

Last time: we proved:

- Every subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.
- Every subgroup of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

} Every subgroup of a cyclic group is cyclic.

↳ we proved this by showing that:

If $H \leq \mathbb{Z}/n\mathbb{Z}$ is a subgroup,

the smallest element in

$$\{\bar{1}, \bar{2}, \ldots, \overline{n-1}\} \cap H$$

is the generator.

Today, we will refine this. But we need to remember some things about g.c.d, the greatest common divisor.

For $a, b \in \mathbb{Z}$.

"equivalent characterizations of gcd"

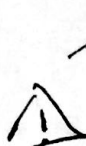
Proposition: The following numbers are equal:

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

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

where $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$; $\alpha_i, \beta_i \geq 0$.

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



We'll only prove $A = C$.

- If $d|a$ and $d|b$, then
  $\forall x, y$, $d \mid ax+by$.
  so $\gcd(a,b) \mid C$
  so $\underline{\gcd(a,b) \leq C}$.
- On the other hand. $C = \min\{c \in \mathbb{Z}_{>0} \mid c = ax+by \; x,y \in \mathbb{Z}\}$.
  We'll show $C|a$. By division algorithm:

$$a = qC + r \quad \text{for unique } q,\ r \in \{0,1,\dots,C-1\}.$$

Let $C = xa+yb$.

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

$$\underbrace{(-qx+1)}_{\in \mathbb{Z}} a - \underbrace{qy}_{\in \mathbb{Z}} b = r.$$

So r is an integer-linear combination of a and b.
But since $r < C$, we have $r = 0$
because C was minimal. $a = qC + 0$
So $C|a$. Similarly: $C|b$.
Since $C|a$ and $C|b$, and gcd is the greatest common divisor, $C \leq \gcd(a,b)$. Thus $C = \gcd(a,b)$

Proposition: In $\mathbb{Z}$,

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

proof: $\langle a \rangle = a\mathbb{Z} \qquad \langle b \rangle = b\mathbb{Z}$.

$$a\mathbb{Z} + b\mathbb{Z} = \{ xa + yb \mid x, y \in \mathbb{Z} \} \leq \mathbb{Z} .$$

We know, from our proof that subgroups of $\mathbb{Z}$ are (infinite cyclic) $\mathbb{Z}$, that $a\mathbb{Z}+b\mathbb{Z}$ is generated by its smallest positive element, which is

$$\min \{ c \in \mathbb{Z}_{>0} \mid c = xa+yb,\ x, y \in \mathbb{Z} \}$$

which is the $\gcd(a,b)$ by proposition above. □

Proposition: In $\mathbb{Z}/n\mathbb{Z}$

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

proof/exercise: Same idea as above.

What is ~~the~~ a generator? (the smallest element c in $\{0,1,2,\ldots,n-1\}$ of the form:

$$c + yn = x \cdot a \ (\ldots)$$

Exercise: What is the lattice of subgroups of $\mathbb{Z}/18\mathbb{Z}$?

Exercise: Prove that $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ iff a and n are relatively prime.