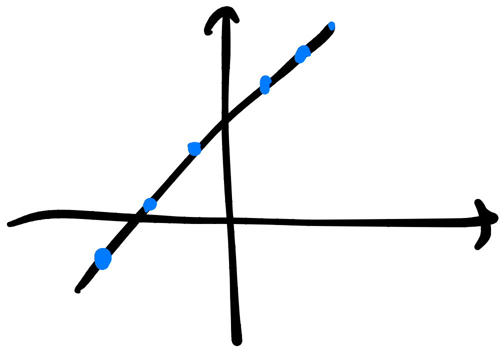
# Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

Google Slides

App: Good Notes



Q: Can we prove $(\mathbb{Z}/n\mathbb{Z})^\times = \{a : \gcd(a,n)=1\}$ ?

Yes. $\boxed{\text{The equation } ax+ny=c \text{ has integer solutions } (x,y) \text{ iff } \gcd(a,n)\mid c}$

The equation

$$ax + ny = c$$ has integer solutions $(x, y)$ iff $\gcd(a,n) \mid c$

If $\gcd(a,n) = 1$, then can solve $ax + \overset{0 \bmod n}{\overset{\shortparallel}{ny}} = 1$

$$\Rightarrow ax \equiv 1 \bmod n$$

$$\Rightarrow x \equiv a^{-1} \bmod n$$

For the other direction

if $ax \equiv 1 \mod n$

$\Rightarrow \exists y \in \mathbb{Z}$ with $ax = 1 + yn$

$\Rightarrow$ $ax - yn = 1 \quad x, y \in \mathbb{Z}$

so $\gcd(a, n) \mid 1$

Solve $4,6$ $4x+6y=1$

this has no sol. because $2 \mid (4x+6y)$

always if $x,y \in \mathbb{Z}$

$4x+6y=2$ $6=4+2$ gcd

$4=2\cdot 2+0$

$4(-1)+6(1)=2$

$$4\overset{-5}{x}+6\overset{5}{y}=10$$

# Chinese Remainder Theorem

$R = \mathbb{Z}$ $\quad n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $\quad p_i$ prime, $p_i \neq p_j$ $i \neq j$

$e_i > 0$

$$(a_1, a_2, \ldots, a_r$$

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_2^{e_2} \times \cdots \times \mathbb{Z}/p_r^{e_r}$$

$$x \equiv a_1 \mod p_1^{e_1}$$
$$x \equiv a_2 \mod p_2^{e_2}$$
$$\vdots$$
$$x \equiv a_r \mod p_r^{e_r}$$

# Quiz 9

That's all for today!