Recall: Euclidean Alg: $n, m \in \mathbb{Z}$, $n > m > 0$.

$n = m \cdot q_1 + r_1$, $0 \le r_1 < m$. (How? Look at $r_{-1} = n$, $r_0 = m$)

$\{n - mq \mid q \in \mathbb{Z}\} = S \subseteq \mathbb{Z}$ takes positive vals,

Let r = least ≥ 0 val. Claim: $r < m$. If not,

$r \geq m$ and $n - mq = r \Rightarrow n - \underbrace{mq - m}_{m(q+1)} = r - m \in S$

$\ast$ since r is least such. $\Rightarrow r < m$ ✓ ≥ 0.

Continue $\exists q_j, r_j$ s.t. $r_{j-2} = r_{j-1} q_j + r_j$, $0 \le r_j < r_{j-1}$

Stops at some finite $J \le m$, where $r_J = 0$.

Thm: $r_{J-1} = \gcd(n, m)$.

∩

pf: If $\ell | n$ & $\ell | m \Rightarrow r_1 = n - mq_1$ has $\ell | r_1$.

If $\ell | r_{j-2}$ & $\ell | r_{j-1} \Rightarrow r_j = r_{j-2} - r_{j-1} q_j$ has $\ell | r_j$.

$\Rightarrow r_{J-1}$ has $\ell | r_{J-1} \Rightarrow \gcd(n,m) | r_{J-1}$.

Need to show: $r_{J-1} | \gcd(n,m)$. But

$r_{J-2} = r_{J-1} q_J + \cancel{r_J} \Rightarrow r_{J-2}$ has $r_{J-1} | r_{J-2}$

Follow backwards all r_j have $r_{J-1} | r_j$. $\forall j$,

$j=0 \Rightarrow r_{J-1} | \underbrace{m}_{r_0}$ & $j=-1 \Rightarrow r_{J-1} | \underbrace{n}_{r_{-1}} \Rightarrow r_{J-1} = \gcd$.

Given $n, m \neq 0$, looked at $S = \{xn + my \mid x, y \in \mathbb{Z}\}$

S is an ideal: (1) $z \in S \Rightarrow r \cdot z \in S \ \forall r \in \mathbb{Z}$.

(2) $z_1, z_2 \in S \Rightarrow z_1 \pm z_2 \in S$.

Exercise 1 ↑

Def Names: "group": set S with operation $+$
& identity & inverses. E.g. $(\mathbb{N},+)$? No. But $(\mathbb{Z},+)$ yes.

$\forall x \in S,\ x+0=x$ $\quad$ $\forall x \in S\ \exists y \in S : x+y=0$

"ring" set $(S,+,\times)$, $+,-,\times$. E.g. $(\mathbb{Z},+,\times)$ yes.

"field" set $(S,+,\times)$, $+,-,\times,\div$ i.e. $\forall x \in S \setminus \{0\}$,
$\exists y \in S$ s.t. $xy=1$

Thm: $(\mathbb{Z}/n\mathbb{Z},+,\times)$ is a field $\Leftrightarrow$ n = prime

What is $\frac{1}{2}$ in $\mathbb{Z}/11$? I.e. y s.t. $2\cdot y \equiv 1 \pmod{11}$.
$2\cdot 6 \equiv 1 \pmod{11}$. What is "$\frac{1}{3}$"? $3\cdot 4 \equiv 1$ so "$\frac{1}{3}$" $=4$

5^{-1}?

$\mathbb{Z}/11$	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

$\mathbb{Z}/12$	1	2	3	4	5	6	7	8	9	10	11
x^{-1}	1	X	X	X	5	X	7	X	X	X	11

$2 \cdot y \equiv 1 \ (12)$ i.e. $2y = 1 + 12m$.

$12m + 2y = 1$ X

$\varphi(12) = 4$.

Exercise: Table x vs x^{-1} in $\mathbb{Z}/17$.

Pf of Thm: If n = prime = p, Does $a \not\equiv 0 \ (p)$ have $\bar{a} = a^{-1}$? If $b = a^{-1}$, want $a \cdot b \equiv 1 \ (p)$. i.e. $ab - p \cdot m \overset{*}{=} 1$. But $(a, p) = 1$. so $\exists$ s, t $(\in \mathbb{Z})$ s.t. $\overset{*}{}$

Rmk: Use FLT! $a^{p-1} \equiv 1$, then $a^{p-2} \equiv \bar{a}$.

Ex: Find $\bar{5}$ mod 17. Want 5^{15}.

5^n	5^1	5^2	5^4	5^8
mod 17	5	8	13 $\equiv -4$	16 $\equiv -1$

$5^{15} = 5^8 \cdot 5^4 \cdot 5^2 \cdot 5^1$.

$\rightarrow 3 \cdot 8 = \boxed{7}$.

Pf of Thm cont'd: If $n \neq$ prime, let $a \not\equiv 0 \ (n)$ have $\gcd(a,n) > 1$. Then $a \cdot b + n \cdot m = 1$ has no solutions. $\Rightarrow$ $a \cdot b \equiv 1 \pmod{n}$ has no solutions.

Def: $(\mathbb{Z}/n\mathbb{Z})^\times = \{ a \bmod n \mid$ invertible "units" $\exists b : a \cdot b = 1 \}$

Euler totient $\varphi(n) \overline{=} \#(\mathbb{Z}/n)^*$

Exercise 3: Compute $(\mathbb{Z}/40)^\times$, $\varphi(40)$.

Thm: $\mathbb{Z}$ is a PID "principal ideal domain":

ideal $S \subset \mathbb{Z}$ s.t. ① $z_1, z_2 \in S \Rightarrow z_1 + z_2 \in S$.
& ② $z \in S, r \in \mathbb{Z} \Rightarrow r \cdot z \in S$.

Def: ideal S is **principal** if $\exists\, d \in \mathbb{Z}$ s.t.
$S = (d) = \{ d \cdot r \mid r \in \mathbb{Z} \} = d\mathbb{Z}$.

In general ideal looks like:
$S = (n_1, \ldots, n_k) = \{ n_1 x_1 + \cdots + n_k x_k \mid x_i \in \mathbb{Z} \}$.

Claim: $\exists\, d = \gcd(n_1, \ldots, n_k)$ s.t. $S = (d)$.

Ex: $(10, 14, 24) \supseteq 10, 14, 4, 20, 28, 8, 0,$
$6, 2, 18,$
$= (2).$

Ex: $(6, 18, 22, 5) \supseteq 1$
$\Rightarrow \mathbb{Z} = (1) = (-1)$

Ex: $(6, 10, 15) = (1) = (-1)$

pf of Claim: If $\ell \mid n_1$ & $n_2 \cdots n_k \Rightarrow \forall z \in S, \ell \mid z$.

$\Rightarrow d = \gcd(n_1, \ldots, n_k) \mid z \ \forall z \in S. \Rightarrow S \subseteq d\mathbb{Z}$.

For other direction, want $d \in S$. Let $r > 0$ be least element of S. Looking at $(n_1, n_2) = (d_1)$. Add more elements to $(n_1, \ldots, n_k) = (d_1) \cap (d_2) \cdots = (d)$.