8/19/2026

Last Time:

Thm (Fundamental Thm of Arithmetic) Every $n>1$ can be written as a product primes, uniquely up to the order of the prime factors.

Thm (Division Algorithm). Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$, s.t.

$$a = q \cdot b + r.$$

(q: quotient, r: remainder)

Pf. Exercise.

E.g. 1. $a=100$, $b=13$: $100 = 13 \cdot \underset{q}{7} + \underset{r}{9}$

2. $a=100,\ b=-13 : 100 = -13 \cdot \underset{8}{-7} + \underset{7}{9}$

3. $a=-100,\ b=13 : -100 = 13 \cdot \underset{8}{-8} + \underset{7}{4}$

Recall :

Lem 1.1. Every $n>1$ has a prime divisor.

Pf of Existence Part of FTA : Let $n>1$. By Lem 1.1,

$$n = p_1 n_1,\ p_1 \text{ is prime},\ n > n_1.$$

$n_1 = 1$: $n = p_1 \cdot 1 = p_1$ ✓

$n_1 > 1$: By Lem 1.1 again,

$$n_1 = p_2 n_2,\ p_2 \text{ is prime},\ n_1 > n_2.$$

$n_2 = 1$: $n_1 = p_2 \cdot 1 = p_2$, $n = p_1 n_1 = p_1 p_2$. ✓

$n_2 > 1$! Continue until we get

$$n = p_1 p_2 \cdots p_k \underline{n_k}, \quad n_{k-1} > n_k = 1.$$

$n_k = 1$

We are done. □

Defn (Ideals) Let R be a comm ring. An ideal of R is a set I s.t:

(1) $0 \in I$

(2) $x, y \in I \Rightarrow x + y \in I$

(3) $r \in R, x \in I \Rightarrow rx \in I$.

E.g. (Ideals of $\mathbb{Z}$): $I = \{\text{even integers}\}$

$I_m = \{n : m \mid n\}$, $m \in \mathbb{Z}$ nonzero.

Defn (Principal Ideal) An ideal I of R is called principal if $I = \{rx : r \in R\}$ for some $x \in R$.

Defn (Principal Ideal Domain) A domain D is called a PID if every ideal of D is principal.

Prop 2.1. $\mathbb{Z}$ is a PID.

Pf. Let I be an ideal. Need to show $I = \{n : m \mid n\}$ for some m.

$I = \{0\}$: ✓

$I \neq \{0\}$: I contains some $m > 0$. We may assume m is the minimal positive element.

Claim : $I = \{n : m \mid n\}$.

$\{n : m \mid n\} \subseteq I$: ✓

$I \subseteq \{n : m \mid n\}$: Take any $n \in I$. By DA, can write

$$n = qm + r, \quad 0 \leq r < m.$$

$$r = n - qm \in I \implies r = 0 \implies m \mid n. \quad \square$$

($n \in I$, $qm \in I$)

Notation : $\langle m \rangle = \{n : m \mid n\}$.

Defn (GCD) Let $a, b \in \mathbb{Z}$, not both 0. Then the gcd of

a, b $\forall s$ a positive integer. d s.t.

(1) $d \mid a$, $d \mid b$

(2) $c \mid a$, $c \mid b \Rightarrow c \mid d$.

We write $\gcd(a,b) = d$ or simply $(a,b) = d$.

Lem (Bézout's lemma) Let $a, b \in \mathbb{Z}$, not both 0. Write $d = (a,b)$ and consider $I_{a,b} = \{ax+by : x, y \in \mathbb{Z}\}$. Then $I_{a,b}$ $\forall s$ an $\forall dea l$ and $I_{a,b} = \langle d \rangle$. Consequently, there are $x, y \in \mathbb{Z}$ s.t. $ax+by = d$.

Pf. $I_{a,b}$ $\forall s$ an $\forall dea l$ (Ex).

$I_{a,b} \subseteq \langle d \rangle$: $d \mid a$, $d \mid b \Rightarrow d \mid ax+by \Rightarrow ax+by \in \langle d \rangle$.

$\langle d \rangle \subseteq I_{a,b}$: By Prop 2.1, $I_{a,b} = \langle m \rangle$ for some $m \in \mathbb{Z}$.

Need to show $m \mid d$. Since $a, b \in I_{a,b}$, $m \mid a$, $m \mid b$.

So $m \mid d$. □

Lem (Euclid's lemma) Let $a, b \in \mathbb{Z}$ and let p be prime.

Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Pf. $p \mid a$ ✓

$p \nmid a$: $(a, p) = 1$ (Ex).

Bézout's lemma $\Rightarrow ax + py = 1$, for some $x, y \in \mathbb{Z}$.

$\Rightarrow abx + pby = b$.

$p \mid ab$, $p \mid p \Rightarrow p \mid ab \cdot x + p \cdot by \Rightarrow p \mid b$. □