8/21/2026

Recall:

Prop 2.1. $\mathbb{Z}$ is a PID: Every ideal I of $\mathbb{Z}$ is

Principal (of the form $I = \langle m \rangle$).

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

$I_{a,b}$ is an ideal and $I_{a,b} = \langle d \rangle$. Consequently, there

are $x, y \in \mathbb{Z}$ s.t. $ax + by = d$.

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

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

Rmk 3.1. Applying Euclid's lemma repeatedly shows

$$p \mid a_1 a_2 \cdots a_k \implies p \mid a_i \text{ for some } 1 \le i \le k.$$

Moreover, if $a_1, \dots, a_k$ are primes, then

$$p \mid a_1 a_2 \cdots a_k \implies p = a_i \text{ for some } 1 \le i \le k.$$

Pf of Uniqueness Part of FTA: Let $n > 1$.

① n is prime: $n = n \cdot 1 = 1 \cdot n$ ✓

② n is composite: Suppose n is minimal s.t.

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l \quad (k \ge l)$$

are distinct factorizations. Since $p_1 \mid q_1 \cdots q_l$, Euclid's lemma $\implies$

p_1 divides some q_j. But q_j is prime. So $p_1 = q_j$.

Rearrange $q_1, \dots, q_l$ s.t. $q_j = q_1$. So $p_1 = q_1$.

$$n = p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_l$$

$$\Rightarrow \frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l .$$

Remember n is minimal and $1 < \frac{n}{p_1} < n$. A contradiction. $\square$

FTA can be restated as:

Thm (UF in $\mathbb{Z}$) Every nonzero, nonunit $n \in \mathbb{Z}$ can be written as a product of primes and units, uniquely up to the order of factors and multiplication by units.

Note: A domain with such a property is called a unique factorization domain (UFD).

Observation: The same proof shows that a domain equipped with a DA (called Euclidean domain) is both a PID and a UFD.

Thm. PID $\Rightarrow$ UFD.

How to find $\gcd(a,b)$?

Method 1. List all common divisors and take the largest. ☹

Method 2. Factorize a, b and combine. ☹ Factorizing is hard!

E.g. $a = 63 = 3 \cdot 3 \cdot 7 = 3^2 \cdot 7$
$b = 42 = 2 \cdot 3 \cdot 7$
$\Rightarrow (a,b) = 3 \cdot 7 = 21.$

Method 3. Euclidean algorithm. ☺

$$I_{a,b} = \{ax + by : x, y \in \mathbb{Z}\} = I_{a,a-b}$$
$$= I_{a,a-2b}$$
$$= \cdots$$

By DA, $a = q \cdot b + r$, $0 \le r < |b|$. Then

$$I_{a,b} = I_{a,a-q\cdot b} = I_{a,r} \quad (q \neq 0).$$

keep going for a, r until the remainder becomes 0.

E.g. Find $(1533, 1225)$.

$$1533 = 1225 \cdot 1 + 308$$

$$1225 = \underbrace{308 \cdot 3}_{924} + 301$$

$$308 = 301 \cdot 1 + 7$$

$$301 = 7 \cdot 43 + 0$$

$\uparrow$

gcd

Congruences.

Defn (Congruence) Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$. We say a is congruent to b modulo m if $m \mid (a-b)$.

Notation. $a \equiv b \pmod{m}$

"$\equiv$" is an equivalence relation:

(1) Reflexivity: $a \equiv a \pmod{m}$.

(2) Symmetry: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

(3) Transitivity: $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$

$\Rightarrow a \equiv c \pmod{m}$.

Properties :

1. $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$

$$\Rightarrow \begin{cases} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m \\ a_1 a_2 \equiv b_1 b_2 \pmod m \end{cases}$$

Special cases : ① $a \equiv b \pmod m \Leftrightarrow a \pm c \equiv b \pm c \pmod m$.

② $a \equiv b \pmod m \Rightarrow ka \equiv kb \pmod m$

③ $a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m$, $k \geq 0$.

2. $a \equiv b \pmod{mn} \Rightarrow a \equiv b \pmod m$, $a \equiv b \pmod n$.

3. $ka \equiv kb \pmod m \Leftrightarrow \frac{m}{d} \cdot a \equiv \frac{m}{d} \cdot b \pmod{\frac{m}{d}}$ $(d = (k, m))$

$(k \neq 0)$

$$\Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$$

Warning : $2 \cdot 2 \equiv 2 \pmod 2$, but $2 \not\equiv 1 \pmod 2$.