Week 1 (Wed.)

Division

$b > 0$

For any $a, b \in \mathbb{Z}$, there is a unique pair $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, $0 \leq r < b$.

(q: quotient, r: remainder)

$r = 0$ we say $b \mid a$

b is a divisor of a

$a \text{ div } b = q$

$a \text{ mod } b = r$

e.g., $53 \text{ div } 10 = 5$

$53 \text{ mod } 10 = 3$

congruence mod n

We say $a \equiv b \pmod{n}$ iff

$a \text{ mod } n = b \text{ mod } n$

e.g., $9 \text{ mod } 4 = 1$, $17 \text{ mod } 4 = 1$

$9 \equiv 17 \pmod{4}$

$a = bq + r$

$-11 = 3(-4) + r$

$-11 \text{ div } 3$

$= \left\lfloor \frac{-11}{3} \right\rfloor$

$= -4$

$-11 \text{ mod } 3$

$= -11 + 12$

$= 1$

Greatest Common Divisor (gcd)

gcd(a, b) is the largest $d \in \mathbb{Z}$ s.t. $d \mid a$ and $d \mid b$.

Naive: List all divisors of a, all divisors of b, find the largest value of d that shows up in both lists.

Fundamental Theorem of Arithmetic

Every integer > 1 can be uniquely written as either a prime or as a product of primes.

eg., $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 3^0 \cdot 5^1$

$384 = 2^7 \cdot 3^1 \cdot 5^0$

$80 = 2^4 \cdot 3^0 \cdot 5^1$

$\gcd(20, 384) = 2^2 = 4$

$\gcd(20, 80) = 2^2 \cdot 5^1 = 20$

Least Common Multiple (lcm)

lcm(a, b) is the smallest $m \in \mathbb{Z}$ s.t. $a \mid m$, $b \mid m$

$\text{lcm}(384, 80) = 2^7 \cdot 3^1 \cdot 5^1 = 1920$