Numbers.

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ natural numbers

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ integers.

$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \text{ are integers with } b \neq 0 \right\}$ rational numbers

$\mathbb{R}$: real numbers. $\sqrt{2}$ a non-rational but real.

$\mathbb{C}$: complex numbers

Notation: $\boxed{x \in \mathbb{Z}}$

"x is in $\mathbb{Z}$"

It is an integer.

Divisibility

Let $a, b \in \mathbb{Z}$. We say b divides a if there exists some $q \in \mathbb{Z}$ such that

$$a = b \cdot q.$$

We denote this by $b \mid a$.

In this context, we say b is a divisor or factor of a.

Ex: $2 \mid 10$ $(q = 5, a = 10, b = 2)$, $5 \mid 20$, $3 \mid 18$

Ex: For what $n \in \mathbb{Z}$ is the following true?

$$n \mid 0$$

In fact all integers n are valid!

$$0 = n \cdot q$$

(Find any $q \in \mathbb{Z}$) $q = 0$ works.

Ex: $1 \mid a \implies a = 1 \cdot q$ for some $q \in \mathbb{Z}$.

$$q = a.$$

Common divisors and GCD

Let $a, b \in \mathbb{N}$

Def: • A number $d \in \mathbb{N}$ is a common divisor of a and b if

$$d \mid a \quad \text{and} \quad d \mid b.$$

• The largest common divisor is the greatest common divisor (GCD), written

$$\gcd(a, b).$$

Ex: $\gcd(4, 6) = 2.$ $\gcd(12, 18) = 6.$

Prime and coprime (pairs)

- **Def:** A number $p \in \mathbb{N}$ is **prime** if $p > 1$ and its only (positive) divisors are 1 and p.

(Every integer has a unique prime factorization.)

- A pair $a, b \in \mathbb{N}$ are **coprime** if

$$\gcd(a,b) = 1.$$

Ex: Are 105 and 64 coprime?

$64 = 2^6$ $\quad 105 = 5 \cdot 21 = 3 \cdot 5 \cdot 7.$ No primes in common!

$\gcd(64, 105) = 1.$

Nonex: 64 and 32 are not coprime.

Euclid's algorithm and The remainder theorem

Theorem (remainder)

Let $a, b \in \mathbb{Z}$ with $b > 0$. ~~There exists a~~ There exists unique integers q and r such that

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

where $0 \leq r < b$.

Important for uniqueness!

We call q the quotient and r the remainder.

A GCD Fact

If $a = b \cdot q + r$ (same hypotheses as thm.)

then

$$\gcd(a,b) = \gcd(b,r).$$

Implies!

Reason: A number $d \in \mathbb{N}$ divides both a and b if and only if d divides both b and

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

If ⟶ then

then ⟵ If

P if and only if Q the same as If P, then Q and If Q, then P.

Assume $d|a$ & $d|b$. Convince you that $d|b$ and $d|r$.

easy

$a = dx$, $b = dy$ $x, y \in \mathbb{Z}$.

implies

$$r = a - b \cdot q = (dx) - (dy)q = d(x - y \cdot q)$$

Euclid's alg.

For positive integers $a > b$, we repeatedly apply the Remainder Theorem until we get zero remainder

$$a = bq_1 + r_1, \qquad 0 \le r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, \qquad 0 \le r_3 < r_2$$

$\vdots$ (Eventually, we get zero remainder)

$b > r_1 > r_2 > r_3 > \cdots$ all integers so eventually we hit zero.

The final non-zero integer r_k is ....

$$\gcd(a, b).$$