NATURAL NUMBERS
\[ \mathbb{N}, \mathbb{N}^+, +, \times, \cdot, < \]

+, \cdot are associative, commutative, distributive

Units:
\[ a + 0 = 0 + a = a \]
\[ a \cdot 1 = 1 \cdot a = a \]

\[ < \; a < b \Rightarrow a + c < b + c \]
\[ \Rightarrow a \cdot c < b \cdot c \; (c > 0) \]

For any \( a, b \in \mathbb{N} \)
\[ a < b \]
\[ a = b \]
\[ b < a \]

BASIC PROPERTIES

(i) any \( \emptyset \neq S \subseteq \mathbb{N} \) has a smallest element

(ii) Mathematical Induction
\[ 1 \in S \]
\[ a \in S \Rightarrow a + 1 \in S \]
\[ \Rightarrow S = \mathbb{N} \]

DIVISION RING
\[ a + c = b + c \Rightarrow a = b \]
\[ a \cdot c = b \cdot c \Rightarrow a = b \; \; \; c \neq 0 \]

\( \mathbb{Z} \) integers
Additive inverses \( (a) + (-a) = 0 \)
Q rationals

Multiplicative Inverses
\[ a \cdot (\frac{1}{a}) = 1 \quad a \neq 0 \]
\( \frac{1}{a} \) denoted \( \frac{1}{a} \)

R real numbers

Completion with respect to
\[ |a| = \begin{cases} \ a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases} \]

(will not use)

Any polynomial factors into quadratic terms

C complex numbers
\[ a + ib \quad a, b \in \mathbb{R} \]
\[(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + (b_1 + b_2)i \]
\[(a_1 + ib_1) \cdot (a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1) \]

\[ i^2 = -1 \]

\[ (a + ib)^{-1} = \frac{a}{a^2 + b^2} + \frac{b}{a^2 + b^2}i \]
\[ N(a + ib) = a^2 + b^2 \]
\[ \overline{(a + ib)} = a - ib \]

\( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) totally ordered for <

\( \mathbb{C} \) has NO reasonable <
We will study \( \mathbb{N} \) and its arithmetic properties.

**Definition:** We say \( a \mid b \) "\( a \) divides \( b \)" if \( b = ma \) for some \( m \in \mathbb{N} \).

A number is called **prime** if it cannot be expressed as \( p = a \cdot b \) with \( 1 < a, b \).

**Thm:** Any number is a product of primes.

**Pf:** By induction.

\( 1 \) is an exception; called a unit.

\( 2 \) is prime.

Suppose true for all \( a < N \).

Either \( N \) is prime, so done

or

\( N = a \cdot b \) with \( 1 < a, b \). By the induction step,

- \( a \) a product of primes
- \( b \) a product of primes

\( \Rightarrow a \cdot b \) is a product of primes

**Needed**

\( 1 < a \Rightarrow 1 \cdot b < a \cdot b = N \)

\( 1 < b \Rightarrow 1 \cdot a < b \cdot a = N \)

**Thm:** Any \( a \in \mathbb{N} \) is uniquely a product of primes, unique up to order.
This is much harder, or at least more awkward.

**Euclidean Algorithm**

\[ a, b \in \mathbb{N}, \quad b = ma + r \text{ for some } 0 \leq r < a. \]

**Proof:** \( b < a \quad b = 0 \cdot a + b \)

\[ b = a \quad b = 1 \cdot a + 0 \]

\( b > a \quad S = \{ m \mid b < ma, \ m \in \mathbb{N} \} \)

\( b \in S \quad b < ba \quad (b \leq a \text{ because } 1 = a \text{ is clear}) \)

So \( S \) has a smallest element.

\((m - 1)a \leq b < ma\)

\[ 0 \leq b - (m - 1)a = b - ma + a < a \]

**Lemma:** \( p \) prime, \( p \nmid a \). Then there exist \( m, n \in \mathbb{Z} \) such that

\[ mp + na = 1 \]

**Proof:** \( J = \{ x \in \mathbb{Z} \mid x \mid a \lor x \mid a \} \)

\( a, p \in S, \text{ so } S \neq \emptyset \)

\( x, y \in S \implies px + py \in S \text{ for any } x, y \in S \)

\( r, s \in \mathbb{Z} \)

\( a = mp + r_0 \text{ with } 0 < r_0 < p \)

\((r = 0 \implies p \nmid a) \)

So \( r_0 \in J \).

\[ p = m_1 r_0 + r_1 \quad 0 < r_1 < p \text{ so } r_1 \in J \]

\( r_0 = m_2 r_1 + r_2 \)

\[ \vdots \]

\[ r_i = m_i r_{i+1} + r_{i+2} \quad r_{i+2} \]

**Must stop:** \( r_{i+2} = 1 \)

So \( 1 = mp + ma \)
\[ n_{S-1} = m_S n_S + n_{S+1} \]

Stop at

\[ n_S = m_{S+1} n_{S+1} + 0 \]

\[ n_{S+1} \bigg| n_S \bigg| \cdots \bigg| p \bigg| \]

So \( n_{S+1} = 1 \) and

\[ 1 = \alpha p + \beta a \]
Prop: If \( p \mid a \cdot b \) then \( p \mid a \) or \( p \mid b \).

Pf: Say \( p \mid a \). Then \( \alpha p + \beta a = 1 \)
\[ \begin{align*}
\beta a &= 1 - \alpha p p^0 \\
\beta a b &= (1 - \alpha p) b = b - p \alpha b \\
mp &= a b = b - p \alpha b \\
b &= (m + \alpha b)p \Rightarrow p \mid b
\end{align*} \]

Pf of Unique factorization

By induction.

True for \( 1 \in \mathbb{N} \)

Suppose true for all \( a < N \).

Say \( N = \prod_{i=1}^{a} a_i \cdot \prod_{i=2}^{b} b_i \).

Suppose \( N = \prod_{i=1}^{a} a_i \cdot \prod_{i=2}^{b} b_i \).

Say \( N = \prod_{i=1}^{a} a_i \cdot \prod_{i=2}^{b} b_i \).

Pf of Unique factorization

Either way, \( p_i \) is one of the \( a \)'s.

Divide both sides by \( p_i \) and use the induction hypothesis

GCD: \((a, b)\) greatest common divisor.

Same proof as earlier shows

\[ \left\{ \alpha a + \beta b \right\} = \left\{ m \cdot (a, b) \right\} \]

in particular, \( \exists \alpha, \beta \in \mathbb{Z} \) \( (a, b) = \alpha a + \beta b \)
SO FAR EUCLID WOULDN'T UNDERSTAND

\[ (1 \cdot 2 = 2) \quad (1 \cdot 2 = 2) \quad (1 \cdot 2 = 2) \quad (1 \cdot 2 = 2) \quad (1 \cdot 2 = 2) \]

\[ (5 \cdot 2 = 10) \quad (5 \cdot 2 = 10) \quad (5 \cdot 2 = 10) \quad (5 \cdot 2 = 10) \quad (5 \cdot 2 = 10) \]

**THM:** \( \text{If } \gcd(m, n) = 1, \text{ then } \frac{1}{m} - \frac{1}{n} \]

\[ = \frac{1}{n} - \frac{1}{m} \]

\[ \text{Sum of divisors (modular)} \]

\[ (q_1 + 1)(q_2 + 1) \ldots (q_n + 1) = \phi(n) \]

\[ \text{Number of divisors (including 1)} \]

\[ n = q_1^a_1 \cdot q_2^a_2 \ldots q_r^a_r \]

**Some consequences**
\[ r = \{ x \in \mathbb{R} \mid x \neq 0 \} \text{ in coosed principort} \]
\[ \mathbb{Z}/a\mathbb{Z} \] on \( \mathbb{Z} \neq 0 \] in \( \mathbb{Z} \).

\[ \{ a, b \in \mathbb{Z} \mid a \neq 0 \} \]
\[ \ker \Rightarrow \ker = 0 \times \ker \rightarrow \ker = 0 \times \ker \)

\[ \text{An ideal } I \subseteq \mathbb{R} \text{ in a not centered } \]
\[ \text{units } 0, \text{ principal } \]
\[ \text{distributive, commutative (sometimes)} \]
\[ \text{two operations, associative}, (\mathbb{R}, +, \cdot) \]

\[ \text{A ring } R \text{ is a structure} \]
\[ \text{More Modern Language} \]
Define a ring \( \mathbb{Z}[x] \): \([a + bx, c + dx] + [e + fx, g + hx] = [a + e + (b + f)x, c + g + (d + h)x] \)

\[ x^2 + \frac{b}{h} = (x + \frac{b}{h})(x - \frac{b}{h}) \]

\[ x = h \quad \text{and the integer solution} \quad x = h \]

\[ \text{solution} \quad x = h + y \]

**Question:** Find the integers \( a, b, c, d, e, f, g, h \) in \( \mathbb{Z} \) such that the equation

\[ a + bx = cy + dx \]

is a prime number.
When $a$, $b$, and $c$ are integers, $N(\mathbf{a} \pm \mathbf{b} \pm \mathbf{c})$ is an integer when $\mathbf{a} = 0$ or $\mathbf{b} = 0$ or $\mathbf{c} = 0$.

The **Euclidean Algorithm** can be used to find the greatest common divisor (GCD) of two integers $a$ and $b$.

$$N(a + b + c) = \frac{a^2 + b^2}{c}$$

$$N(a + b - c) = \frac{a^2 + b^2}{c}$$

$$N(a + b + c) = \frac{a^2 + b^2}{c}$$

$$N(a + b - c) = \frac{a^2 + b^2}{c}$$

$$N(a + b + c) = \frac{a^2 + b^2}{c}$$

$$N(a + b - c) = \frac{a^2 + b^2}{c}$$