1. Introduction, the natural numbers

- $\mathbb{N} = \{1, 2, 3, ...\}$
- $\mathbb{N}_0 = \{0, 1, 2, 3, ...\} = \mathbb{N} \cup \{0\}$
- **Peano's axioms**: three primitive terms: $\mathbb{N}_0$, 0 and **successor function**, S.
  - $0 \in \mathbb{N}_0$.
  - $\forall a \in \mathbb{N}_0, S(a) \neq 0$.
  - $S(a) = S(b) \Rightarrow a = b$.
  - If $X \subseteq \mathbb{N}_0$ and
    - $0 \in X$ and
    - $\forall a \in X, S(a) \in X$

    then $X = \mathbb{N}_0$.
- Last axiom applied to $X = \{n \in \mathbb{N}_0 : P(n) \text{ true}\}$ gives **Principle of Mathematical Induction (PMI)**: for statement $P(n)$, if $P(0)$ true and $\forall n \in \mathbb{N}_0, P(n) \Rightarrow P(n+1)$ then $P(n)$ true for every $n \in \mathbb{N}_0$.
- **PMI variants**:
  - If $P(0)$ true and if for every $n \in \mathbb{N}_0$, $P(x)$ for every $x < n$ implies $P(n)$, then $P(n)$ true for every $n \in \mathbb{N}_0$.
  - Same as two variants above but with base case $P(1)$ true leading to $P(n)$ true for every $n \in \mathbb{N}$.
- **Addition of natural numbers**: let $a \in \mathbb{N}_0$.
  - $a + 0 = a$.
  - $a + S(b) = S(a + b)$
- **Well ordering principle (WOP)**: let $S \subseteq \mathbb{N}_0$, $S \neq \emptyset$, then S has a smallest element.

2. Divisibility

- a **divides** b, $a \mid b$ if $\exists d \in \mathbb{Z}, b = ad$. If not, write $a \nmid b$.
- **Properties of divisibility**:
  - $a \mid 0$.
  - If $a \neq 0$, $0 \nmid a$.
  - $1 \mid a$ and $a \mid a$.
  - $a \mid b \Longrightarrow a \mid bc$.
  - $a \mid b$ and $b \mid c \Longrightarrow a \mid c$.
  - $a \mid b$ and $a \mid c \Longrightarrow a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.
  - $a \mid b$ and $b \mid a \Longrightarrow a = \pm\, b$.
  - $a \mid b, a > 0, b > 0 \Longrightarrow a \leq b$.
  - $a \mid b \Longrightarrow ac \mid bc$.
- **Division algorithm**: let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then exist unique q and r such that

$$a = qb + r, \quad 0 \leq r < b$$

- **Common divisor** d of a and b is such that $d \mid a$ and $d \mid b$.
- **Greatest common divisor (**$\gcd$**)** of a and b is maximal common divisor.
- $\gcd(0, 0)$ doesn't exist.
- **Properties of** $\gcd$:

  - $\gcd(a, b) = \gcd(b, a)$.
  - If $a > 0$, $\gcd(a, 0) = a$.
  - $\gcd(a, b) = \gcd(-a, b)$.
  - If $a > 0, b > 0$, $\gcd(a, b) \leq \min\{a, b\}$.
- For every $a, b, q \in \mathbb{Z}$,

$$\gcd(a, b) = \gcd(a, b - a) = \cdots = \gcd(a, b - qa)$$

- **Euclidean algorithm**: let $a, b \in \mathbb{N}$. Repeating the division algorithm:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \end{aligned}$$

  Then exists smallest n such that $r_n = 0$. Then if $n = 1$, $\gcd(a, b) = b$, else $\gcd(a, b) = r_{n-1}$. Also, exists $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by$$