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.
- **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

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

3. Primes, composite numbers, and the FTA

- $n \in \mathbb{N}$ **prime** if $n > 1$ and if $d \mid n$ then $d = n$ or $d = 1$. If $n > 1$ not prime, n **composite**.
- There are infinitely many primes.
- There are infinitely many primes of form $4n - 1$.
- **Dirichlet's theorem**: Let a, b coprime. Then exist infinitely many primes of form $an + b$.
- **Euclid's lemma**: Let $p > 1$. p prime iff for every $a, b \in \mathbb{Z}$, $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$.
- Let p prime. If $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some i.
- **Fundamental theorem of arithmetic (FTA)**: let $n > 1$, then n can be written as product of primes, unique up to reordering. So exist distinct primes $p_1, \ldots, p_r$ and $e_1, \ldots, e_r \in \mathbb{N}$ such that

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

  and if $n = q_1^{f_1} \cdots q_s^{f_s}$ for distinct primes q_i, then $r = s$ and up to reordering, $p_i = q_i$ and $e_i = f_i$ for every i.

4. Classical equations and integer solutions

- **Pythagorean triple** $(x, y, z) \in \mathbb{N}^3$: solution to $x^2 + y^2 = z^2$. **Primitive** if $\gcd(x, y, z) = 1$.
- Every primitive Pythagorean triple (x, y, z), with $2 \mid x$, given by

$$\begin{cases} x = 2st \\ y = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

  with $s > t \geq 1$, $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.
- **Fermat's theorem**: no integer solutions exist to $x^4 + y^4 = z^2$.

- **Diophantine equation**: equation where integer or rational solutions are sought.

5. Modular arithmetic and congruences

- a **congruent to** b **modulo** $\boldsymbol{n}$, $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
- **Residue (congruence) class**: set of integers congruent $\operatorname{mod} n$.
- If $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$ then:
  - $a + a' \equiv b + b' \pmod{n}$ and
  - $aa' \equiv bb' \pmod{n}$.
- If $\gcd(c, n) = 1$, then $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$.
- **Complete set of residues mod $\boldsymbol{n}$**: subset $R \subset \mathbb{Z}$ of size n whose remainders $\operatorname{mod} n$ are distinct.
- Let R be complete set of residues mod n and let $\gcd(a, n) = 1$, then

  $$aR := \{ax : x \in \mathbb{R}\}$$

  is also complete set of residues mod n.
- **Linear congruence**: $ax \equiv b \pmod{n}$.
- If $\gcd(a, n) = 1$, linear congruence has solution, unique up to adding multiples of n (solutions lie in same congruence class).
- **Method for solving linear congruence** (if $\gcd(a, n) = 1$):
  - Use Euclidean algorithm to find u, v such that $1 = au + nv$.
  - $au \equiv 1 \pmod{n}$ so $a(ub) \equiv b \pmod{n}$ so solutions are

    $$x \equiv ub \pmod{n}$$

- Linear congruence solvable iff $\gcd(a, n) \mid b$.
- **Chinese remainder theorem (CRT)**: let $m, n \in \mathbb{N}$ coprime, $a, b \in \mathbb{Z}$. Then exists solution to

  $$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

  Any solutions are congruent $\operatorname{mod} mn$ and exists unique solution x with $0 \leq x < mn$.
- **Method to solve CRT problem**:
  - Use Euclidean algorithm to find r, s such that $1 = rm + sn$, so $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$.
  - So $brm \equiv b \pmod{n}$ and $asn \equiv a \pmod{m}$.
  - So $asn + brm \equiv b \pmod{n}$ and $asn + brm \equiv a \pmod{m}$.
  - So $x = brm + asn$ is solution.
- **Euler $\boldsymbol{\varphi}$-function**: $\varphi : \mathbb{N} \to \mathbb{N}$:

  $$\varphi(n) := |\{r \in \mathbb{N} : r \leq n \text{ and } \gcd(r, n) = 1\}|$$

- $\varphi(p) = p - 1$ for prime p.
- For prime p, $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$.
- If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.
- Let n have prime factorisation $n = \prod_{i=1}^{r} p_i^{e_i}$. Then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

- Let $n \in \mathbb{N}$, then

$$\sum_{d|n} \varphi(d) = n$$

where sum is over positive divisors of n.
- **Euler's theorem**: For $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $\gcd(a, n) = 1$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- **Fermat's little theorem**: let p prime, $a \in \mathbb{Z}$, $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

6. Primitive roots

- Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $\gcd(a, n) = 1$. **(Multiplicative) order** of $a \bmod n$, $\operatorname{ord}_n(a) = \operatorname{ord}(a)$, is smallest $d \in \mathbb{N}$ such that

$$a^d \equiv 1 \pmod{n}$$

- If $a^d \equiv 1 \pmod{n}$ for some d, then $\operatorname{ord}(a) \mid d$. So $\operatorname{ord}(a) \mid \varphi(n)$.
- Let $\gcd(a, n) = 1$, a is **primitive root mod $\boldsymbol{n}$** if $\operatorname{ord}_n(a) = \varphi(n)$.
- Let p prime, $f(x)$ polynomial with integer coefficients of degree n. Then f has at most n roots $\bmod p$, so $f(x) \equiv 0 \pmod{p}$ has at most n solutions $\bmod p$.
- Let p prime, $d \mid p - 1$. Then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions $\bmod p$ by Fermat's little theorem.
- Let p prime, then there are $\varphi(p - 1)$ primitive roots $\bmod p$.
- Let g primitive root $\bmod p$, $\gcd(a, p) = 1$. Then for some $r \in \mathbb{N}$,

$$a \equiv g^r \pmod{p}$$

($g, g^2, \ldots, g^{p-1}$ are distinct).
- Primitive roots $\bmod n$ exist iff $n = 2, 4, p^k$ or $2p^k$ for odd prime p, $k \in \mathbb{N}$.

7. Quadratic residues

- Let p prime, $a \in \mathbb{Z}$, $\gcd(a, p) = 1$. a is **quadratic residue (QR) mod $\boldsymbol{p}$** if for some $x \in \mathbb{Z}$, $x^2 \equiv a \pmod{p}$. If not, a is **quadratic non-residue (NQR) mod $\boldsymbol{p}$**.
- For p odd prime, there are $\frac{p-1}{2}$ QR's and QNR's $\bmod p$.
- Products of QR's and NQR's satisfy:

$$QR \times QR = QR$$
$$QR \times NR = NR$$
$$NR \times NR = QR$$

- Let p prime, $a \in \mathbb{Z}$, **Legendre symbol** is

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ QR} \\ -1 & \text{if } a \text{ NQR} \\ 0 & \text{if } p \mid a \end{cases}$$

- $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
- $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod{p}$.
- **Euler's criterion**: Let p odd prime, $a \in \mathbb{Z}$, $\gcd(a, p) = 1$, then

  $$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$
- -1 is QR if $p \equiv 1 \pmod{4}$ and is NQR if $p \equiv 3 \pmod{4}$.
- **Quadratic reciprocity law (QRL)**: let $p \neq q$ odd primes, then

  $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

  If $p = 2$,

  $$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$
- **Algorithm for computing Legendre symbol** $\left(\frac{a}{p}\right)$:
  - Divide a by p to get $a = tp + r$ so $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$.
  - If $r = 0$, $\left(\frac{r}{p}\right) = 0$ so stop.
  - If $r = 1$, $\left(\frac{r}{p}\right) = 1$ so stop.
  - If $r \neq 0, 1$ factorise into primes $r = q_1^{e_1} \cdots q_k^{e_k}$ so $\left(\frac{r}{p}\right) = \prod_{i=1}^{k} \left(\frac{q_i}{p}\right)^{e_i}$.
  - $r < p$ so $q_i < p$, so calculate $\left(\frac{q_i}{p}\right)$ for each i.
    - If $q_i = 2$, use $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
    - If $q_i > 2$, use $\left(\frac{q_i}{p}\right) = (-1)^{\frac{(q_i-1)(p-1)}{4}}\left(\frac{p}{q_i}\right)$ and go to step 1 to calculate $\left(\frac{p}{q_i}\right)$.
- **Note**: to evaluate $\left(\frac{-1}{p}\right)$, easier to use Euler's criterion.
- There are infinitely many primes of form $4n + 1$.

8. Sums of two squares

- If m and n are sums of two squares, then so is mn since $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac + bd)^2 + (ad - bc)^2$.
- Let p odd prime. Then p sum of two squares iff $p \equiv 1 \pmod{4}$ (and if $p \equiv 1 \pmod{4}$, this sum of two squares is unique).
- Let $n > 1$, $n = p_1 p_2 \cdots p_k N^2$, p_i distinct primes, $N \in \mathbb{N}$. Then n sum of two squares iff $p_i = 2$ or $p_i \equiv 1 \pmod{4}$ for all i.

9. Continued fractions

- **Finite continued fraction (CF)**:

$$[a_0; a_1, ..., a_n] = a_0 + \cfrac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_n}}}$$

- **Simple** CF: $a_0 \in \mathbb{Z}$, $a_1, ..., a_n \in \mathbb{N}$.
- Any rational number can be written as finite simple continued fraction.
- ***k*th convergent** of CF $[a_0; a_1, ..., a_n]$:

$$C_k := [a_0; a_1, ..., a_k]$$

- $C_n = p_n \,/\, q_n$, where

$$\begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}$$

  so $p_1 = a_0 a_1 + 1$, $p_0 = a_0$, $q_1 = a_1$, $q_0 = 1$ and $p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$
- If $[a_0; a_1, ..., a_n]$ is simple CF, then $q_{k-1} \leq q_k$ and $q_{k-1} < q_k$ if $k > 1$.
- $$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$$
- $\gcd(p_k, q_k) = 1$.
- Let $\alpha = [a_0; a_1, ..., a_n]$, $k = 0, ..., n-1$, then even numbered convergents increasing: $C_0 < C_2 < \cdots < C_{2m}$, odd numbered convergents decreasing $C_{2m+1} < \cdots < C_3 < C_1$ and for every k with $2k + 1 \leq n$,

$$\frac{p_{2k}}{q_{2k}} < \alpha \leq \frac{p_{2k+1}}{q_{2k+1}}$$

  and

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}}$$

- **Infinite CF** $[a_0; a_1, ...]$ is limit of convergents $C_n = [a_0; a_1, ..., a_n]$.
- For simple infinite CF, limit always exists.
- **Pell's equation**: $x^2 - dy^2 = 1$, $d \in \mathbb{N}$ not square.
- **Negative Pell's equation**: $x^2 - dy^2 = -1$.
- Infinite CF **periodic** if of form

$$[a_0; a_1, ..., a_m, a_{m+1}, ..., a_{m+n}, a_{m+1}, ..., a_{m+n}, ...]$$

  $a_0; a_1, ..., a_m$ is initial part, $a_{m+1}, ..., a_{m+n}, a_{m+1}, ..., a_{m+n}, ...$ is periodic part. In periodic part, $a_i = a_j$ if $i \equiv j \pmod{n}$. Write as

$$[a_0; a_1, ..., a_m, \overline{a_{m+1}, ..., a_{m+n}}]$$

  n is **period**.
- If d not square, CF of $\sqrt{d}$ is periodic with initial part only a_0.
- Let $p_k \,/\, q_k$ be convergents of simple CF expansion of $\sqrt{d}$ with period n, then for all $k \geq 1$,

$$p_{kn-1}^2 - d q_{kn-1}^2 = (-1)^{kn}$$

- So if n even or k even, $(x, y) = \left(p_{kn-1}, q_{kn-1}\right)$ are solution to Pell's equation. Else $(x, y) = \left(p_{kn-1}, q_{kn-1}\right)$ are solution to negative Pell's equation. **All** positive solutions to (negative) Pell equation given by above.