H3 Mathematics

Methods of proof

- Direct proof, proof by cases
- Proof by mathematical induction
- Disproof by counterexample
- Proof by contradiction
- Proof of existence, uniqueness
- Proof by construction
- Pigeonhole principle
- Symmetry principle
- Combinatorial arguments and proofs

1 Functions

Functions and graphs

- Injectivity, surjectivity, bijectivity
- Odd and even functions
- f is **strictly monotonic increasing** if

  $$\forall x_1, x_2 \in D_f, \quad x_2 > x_1 \iff f(x_2) > f(x_1)$$

  f is **strictly monotonic decreasing** if

  $$\forall x_1, x_2 \in D_f, \quad x_2 > x_1 \iff f(x_2) < f(x_1)$$

  For a differentiable function, we can show it is strictly increasing on an interval I by showing $f'(x) > 0$ for all $x \in I$, and vice versa.

- f is **convex** in I if for any $x_1, x_2 \in I$ and $0 \le t \le 1$,

  $$f\left(tx_1 + (1-t)x_2\right) \le tf(x_1) + (1-t)f(x_2).$$

  f is **concave** in I if for any $x_1, x_2 \in I$ and $0 \le t \le 1$,

  $$f\left(tx_1 + (1-t)x_2\right) \ge tf(x_1) + (1-t)f(x_2).$$

Differentiation

- **Rolle's Theorem**: if f is continuous on $[a,b]$ and differentiable on (a,b), and $f(a) = f(b)$, then there exists $c \in (a,b)$ such that

  $$f'(c) = 0.$$

- **Mean Value Theorem**: if f is continuous on $[a,b]$ and differentiable on (a,b), then there exists $c \in (a,b)$ such that

  $$f'(c) = \frac{f(b)-f(a)}{b-a}.$$

- **Cauchy's Generalised Theorem of the Mean**: if f is continuous on $[a,b]$ and differentiable on (a,b), where $g(x) \ne 0$, then there exists $c \in (a,b)$ such that

  $$\frac{f'(c)}{g'(c)} = \frac{f(b)-f(a)}{g(b)-g(a)}.$$

- **L'Hopital's Rule**: if f and g are differentiable on an open interval I except possibly at a point c, $g'(x) \ne 0$, and $\lim_{x\to c} \frac{f(x)}{g(x)}$ is in indeterminate form, then

  $$\lim_{x\to c} \frac{f(x)}{g(x)} = \lim_{x\to c} \frac{f'(x)}{g'(x)}. \tag{1}$$

Integration

- **splitting the numerator**
- **substitution**
- **integration by parts**
- **using symmetry** (consider odd/even functions)
- **reducing to integrals with known solution**
- **reduction formula** (recurrence relation involving integrals of form I_n)

Differential equations (1st order)

- **Separation of variables**

  $\frac{\mathrm{d}y}{\mathrm{d}x} = f(x)g(y)$ can be written into

  $$\int \frac{1}{g(y)}\,\mathrm{d}y = \int f(x)\,\mathrm{d}x\,.$$

- **Integrating factor**

  $\frac{\mathrm{d}y}{\mathrm{d}x} + P(x)y = Q(x)$ can be dealt with by multiplying both sides by integrating factor $e^{\int P(x)\mathrm{d}x}$ to give

  $$e^{\int P(x)\mathrm{d}x}\frac{\mathrm{d}y}{\mathrm{d}x} + e^{\int P(x)\mathrm{d}x}P(x)y = e^{\int P(x)\mathrm{d}x}Q(x)$$
  $$\frac{\mathrm{d}}{\mathrm{d}x}\left(ye^{\int P(x)\mathrm{d}x}\right) = e^{\int P(x)\mathrm{d}x}Q(x)$$

  which can then be solved via direct integration.

- **Substitution**

  May need to come up with one by yourself.

2 Sequences and series

Limiting behaviour of sequences

- Take limits (L Hopital's rule is useful)
- **Monotone Convergence Theorem**: A monotone sequence of real numbers is convergent if and only if it is bounded.

Convergence of (infinite) series

- By definition, sequence of partial sums converges
- **Divergence Theorem**:

  If $u_n \not\to 0$ as $n \to \infty$, then $\sum u_n$ diverges.

  [The inverse is not true; a counterexample is the harmonic series.]

- **Bounded Convergence**:

  Suppose $u_n \ge 0$. Then $\sum u_n$ converges if and only if its sequence of partial sums (S_n) is bounded.

- **Comparison Test**:

  Suppose $u_n \ge 0$ and $v_n \ge 0$, and that there exists a positive integer m for which $u_k \le v_k$ for all integers $k \ge m$. Then

  - if $\sum v_n$ converges, then $\sum u_n$ converges
  - if $\sum u_n$ diverges, then $\sum v_n$ diverges

  Example: the harmonic series diverges.

- **Absolute Convergence**:

  If $\sum |u_n|$ converges, then $\sum u_n$ converges.

3 Inequalities

- **AM–GM inequality**:

  $$\frac{x_1 + x_2 + \cdots + x_n}{n} \ge \sqrt[n]{x_1 x_2 \cdots x_n} \tag{2}$$

  Equality holds iff $x_1 = x_2 = \cdots = x_n$.

- **Cauchy–Schwarz inequality**:

  $$\left(\sum_{i=1}^{n} u_i v_i\right) \le \left(\sum_{i=1}^{n} {u_i}^2\right)\left(\sum_{i=1}^{n} {v_i}^2\right) \tag{3}$$

  Equality holds iff there exists nonzero constant k such that $u_i = kv_i$ for all $i = 1, 2, \ldots, n$.

- **Triangle inequality**:

  $$|x_1 + x_2 + \cdots + x_n| \le |x_1| + |x_2| + \cdots + |x_n| \tag{4}$$

  Equality holds iff $x_1, x_2, \ldots, x_n$ are all nonnegative.

4 Number Theory

- A **rational number** can be expressed as $\frac{p}{q}$, where $p, q \in \mathbb{Z}$.
- **Greatest common divisor**: $d = \gcd(a, b)$ if

  (i) $d \mid a$ and $d \mid b$;

  (ii) if $k \mid a$ and $k \mid b$, then $k \leq d$.

  Bezout's Lemma: $\gcd(a, b)$ is a linear combination of a and b; that is, there exist integers s and t such that

  $$\gcd(a, b) = sa + tb. \tag{5}$$

  Corollary: if a and b are coprime, there exist integers s and t such that $sa + tb = 1$.

- **Euclid's Lemma**: if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- **Division Algorithm**
- If q and r are integers such that $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

  Euclidean Algorithm: to find $\gcd(a, b)$.
- **Fundamental Theorem of Arithmetic**: every integer $n > 1$ can be expressed as a product of primes in a unique way apart from the order of the prime factors.
- Euclid: there exist infinitely many primes.

  Prove by contradiction.
- Modular arithmetic, modular inverse
- **Fermat's Little Theorem**:

  $$a^{p-1} \equiv 1 \pmod{p}. \tag{6}$$

5 Combinatorics

Counting

- **Principle of inclusion and exclusion**:

  $$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - \cdots \\ &\quad + (-1)^{n+1} |A_1 \cap \cdots \cap A_n| \\ &= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1\leq i_1<\cdots<i_k\leq n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right)\end{aligned} \tag{7}$$

  To use PIE, specify the sets that you are counting across.

- **Bijection Principle**: if there exists a bijection $f : A \to B$, then $|A| = |B|$.

  Use Bijection Principle to transform problems to equivalent problems and resolve the equivalent problem and hence tackle the original problem. To employ Bijection Principle,

  1. State two sets A and B, one of which should be the set that you are trying to enumerate in the original problem.
  2. Define a mapping from A to B.
  3. Show that the mapping defined is bijective (both injective and surjective).
  4. Apply Bijection Principle: $|A| = |B|$.

- **Pigeonhole Principle**: if $n = km + 1$ objects are distributed among m boxes, then at least one of the boxes will contain at least $k + 1$ objects.

Distribution problems

- Distinct Objects into Distinct Boxes

  Number of ways of distributing r distinct objects into n distinct boxes such that each box can hold

  (i) at most one object is ${}^nP_r$

  (ii) any number of objects is n^r

- Identical Objects into Distinct Boxes

  Number of ways of distributing r identical objects into n distinct boxes is $\binom{r+n-1}{n-1}$.

- Distinct Objects into Identical Boxes

  Stirling number of the second kind, denoted by $S(r, n)$, is the number of ways of distributing r distinct objects into n identical boxes such that no box is empty.

  $$S(r, n) = S(r-1, n-1) + nS(r-1, n) \tag{8}$$

- Identical Objects into Identical Boxes

  A **partition** of a positive integer r into n parts, denoted by $P(r, n)$, is a set of n positive integers whose sum is r (order does not matter).

  $$P(r, n) = P(r-1, n-1) + P(r-n, n) \tag{9}$$

  where $1 < n \leq r$.

Recurrence relations

- Relate a_n to the previous terms
- Consider the extreme element (first / last / longest etc.)
- Specify initial conditions, if needed
- List out for small numbers to find pattern