Numbers and Sets IA Mich

- Purpose of proofs, methods of proof (esp contradiction), non-valid proofs: other way round, assume something that does not exist (e.g. minimum element)

1 Elementary Number Theory

- Natural numbers
  - Peano Axioms: define $\mathbb{N}$
    1. Starting element (1 or 0) $\in \mathbb{N}$
    2. Incrementation is closed in $\mathbb{N}$
    3. Different elements increment to give different elements ($n \neq m \implies n+1 \neq m+1$)
    4. Axiom of induction: $P(1) \wedge [P(n) \implies P(n+1)] \implies P(n)\ \forall n \in \mathbb{N}$
  - Define addition and multiplication inductively
- Weak and strong principles of induction
- Constructing $\mathbb{Z}$, and $\mathbb{Q}$ from $\mathbb{N}$
- Divisibility ($a \mid b \iff \exists\, c \in \mathbb{N} : ac = b$), prime ($a \mid p \implies a = p$ or $a = 1$) and composites, prime factorisation, existence of infinitely many primes
- Highest common factor, division algorithm, Euclid's algorithm
- HCF as smallest positive linear combination of the two numbers
- Bezout's Theorem: Integer solutions to the equation $ax + by = c \iff \text{hcf}(a, b) \mid c$
- For all prime p, and $a, b \in \mathbb{Z}$, $p \mid ab \implies p \mid a$ or $p \mid b$
- Fundamental Theorem of Arithmetic: unique prime factorisation; does not hold in some other number systems, no unique factorisation into 'primes'

- Modulo arithmetic
  - Two views: as integers on the number line, or as points on the clock $\mathbb{Z}_n$
  - Inverses don't always exist, but if they do, they are unique, inverse of a in $\mathbb{Z}_n$ exists $\iff$ $\text{hcf}(a, n) = 1$, i.e. coprime
- Euler totient function ϕ:
  - $\phi(n)$ = number of invertible integers (units) in $\mathbb{Z}_n$
  - $\phi(p) = p-1$; $\phi(pq) = pq-p-q+1 = (p-1)(q-1)$; $\phi(p^k) = p^k-p^{k-1}$ (p, q prime)
- Fermat Little Theorem: for p prime and any integer $a \neq 0$, $a^{p-1} = 1$ in $\mathbb{Z}_p$
- Fermat-Euler Theorem: for a invertible in $\mathbb{Z}_n$, $a^{\phi(n)} = 1$
- In $\mathbb{Z}_p$, $x^2 = 1 \iff x = \pm 1$
- Show existence of infinitely many primes in the form $4k+1$ and $4k+3$
- Wilson's Theorem: $(p-1)! = -1$ in $\mathbb{Z}_p$
- $x^2 = -1$ in $\mathbb{Z}_p$ has a solution $\iff$ $p = 1 \pmod 4$
- Linear congruences, uniqueness of solutions (each line if and only if)
- Simultaneous linear congruences: Chinese remainder theorem, existence and uniqueness
- RSA encoding
  - Have $n = pq$, product of two large distinct primes, we know $\phi(n)$ easily
  - Have message x, encode it by taking x^e in $\mathbb{Z}_n$, for some exponent e (the coding exponent) coprime to $\phi(n)$
  - Decode: need d with$(x^e)^d = x$ in $\mathbb{Z}_n$
  - Fermat-Euler: $x^{\phi(n)} = 1 \pmod n$, so need $ed = k\phi(n) + 1$, i.e. solving $ed \equiv 1 \pmod{\phi(n)}$, easy by Euclid
  - Hard to decode: to get $\phi(n)$, need to factorise n

2 The Reals

- Rationals are not complete: no square roots; have gaps, least upper bounds not guaranteed
- Upper bound and least upper bound definitions
- Real numbers: special property called 'least upper bound axiom': any non-empty set bounded above has a least upper bound, the supremum/lub
- Least upper bound of a set need not be in the set
- Axiom of Archimedes: $\mathbb{N}$ has no upper bound in $\mathbb{R}$,i.e. $\forall r \in \mathbb{R}, \exists n \in \mathbb{N} : n > r$
  - Corollary: $\forall t \in \mathbb{R}, \exists n \in \mathbb{N} : \frac{1}{n} < t$
- A set has a greatest element implies supremum of the set is in the set, vice versa
- Greatest lower bound comes 'for free'
- Show that the supremum of a set equals square root of something, etc.
- The rationals are dense in the reals (given any two real numbers, there must be some rational number in between); and some irrational between any two real number
- Infinite sum defined to be the limit of sequence of partial sums
- Limit of a sequence: $\lim_{n\to\infty} x_n = x \iff \forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |x_n - x| < \epsilon$
- Convergent, divergent (limit does not exist, does not mean go to infinity)
- Limit of a sequence is unique, limits add and multiply
- Every bounded monotonic sequence converges: (say for increasing sequence) the set $S = \{x_i : i \in \mathbb{N}\}$ has a supremum, can get arbitrarily close to $\sup S$ (no smaller upper bound) and stay close to the $\sup S$ (since increasing)
- Bound terms of sequence by powers of two for easy evaluation

- Decimal expansion
- e is irrational (proved), and transcendental (out-syl). Liouville number is transcendental
- Complex numbers as operations defined on $\mathbb{R}^2$

3 Sets and Functions

- Constructing sets: subsets, unions, intersections, ordered pairs, power sets
- No universal set: Russel's paradox
- Finite size: can list elements
- Binomial coefficients, binomial theorem
- Inclusion exclusion formula
- Functions as rule of assigning elements of a set to another (formal definition as subset of Cartesian product)
- Injective, surjective, bijective
- Composition of functions, left/right inverse, invertible $\iff$ $\exists$ bijection
- Equivalence relation: (reflexive, symmetric, transitive) $\iff$ partition a set the set into equivalence classes
- Quotient (the set of equivalence classes) and quotient/projection map

4 Countability

- A set A is countable $\iff$ A is finite or bijects with $\mathbb{N}$ $\iff$ $\exists$ injection $f : A \to \mathbb{N}$
- Countable union of countable sets is countable
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable, $P(\mathbb{N}), \mathbb{R}$ are uncountable

- No bijection exists from any set X to $P(X)$
- To show a set X is uncountable:
  - Copy diagonal argument
  - Inject uncountable set into X
- To show a set X countable:
  - List its elements
  - Inject into a countable set (e.g. $\mathbb{N}$)
  - Use 'countable union of countable sets is countable'
  - If the set is related to $\mathbb{R}$, look at $\mathbb{Q}$
- A injects into $B \iff B$ surjects to A
- Schröder-Bernstein Theorem: A injects into B and B injects into $A \iff A$ bijects with B