1 Elementary number theory

1.1 The Peano Axioms

- The natural numbers $\mathbb{N}$ are defined by the peano axioms:
  - For all $n, n+1 \neq 1$
  - If $m \neq n$, then $m+1 \neq n+1$
  - For any property $P(n)$: If $P(1)$ is true and $P(n) \Rightarrow P(n+1)$ for all n, then $P(n)$ true $\forall n$. This is the induction axiom.
- Strong induction: If $P(1)$ and for all n, $P(m)\ \forall m \leq n \Rightarrow P(n+1)$, then $P(n)$ true for all n. This can be shown by applying ordinary induction to $Q(n) =' P(m) \forall m \leq n'$.

1.2 Highest common factors

- For natural numbers a, b, a natural number c is the <u>hcf</u> of a and b if:
  1. $c|a$ and $c|b$
  2. If $d|a$ and $d|b$ then $d|c$
- Euclids Algorithm: for finding the hcf of a and b (wlog let $a \geq b$)
  - $a = q_1 b + r_1$
    $b = q_2 r_1 + r_2$
    $r_1 = q_3 r_2 + r_3$
    $\vdots$
    $r_{n-1} = q_{n+1} r_n + 0$
  - Then the output is r_n
  - Sequence terminates since $b > r_1 > r_2 \dots$
- Bezout's Lemma
  - For all $a, b \in \mathbb{N}$ we can write $xa + yb = \text{hcf}(a, b)$ for some $x, y \in \mathbb{Z}$
  - Can solve for x, y by reversing Euclid on a, b
  - Bezout can be used to show that $\forall x \in \mathbb{Z}_p$ with $x \neq 0$, x is invertible in $\mathbb{Z}_p$

1.3 Modular Arithmetic

- We say that $x \in \mathbb{Z}_k$ is invertible if $(x, k) = 1$. This can be shown simply using Bezout
- Fermat's Little Theorem and Euler-Fermat
  - By considering some non-zero $a \in \mathbb{Z}_p$ and the elements $a, a \cdot 2, a \cdot 3, \dots, a \cdot (p-1)$ it may be shown by pigeonhole that $a^{p-1}(p-1)! = (p-1)!$
  - Noting that $(p-1)!$ is invertible as a product of invertibles, $a^{p-1} = 1$
  - More generally by considering the set $\{a \cdot j : (j, k) = 1\}$ in $\mathbb{Z}_k$ we see that $a^{\phi(k)} = 1$ where $\phi(k)$ is the <u>Euler totient function</u>
- Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$
  - Follows simply from pairing each element in $\mathbb{Z}_p$ with its inverse. Then only 1 and -1 are left since they are their own inverse. Hence we have $(p-1)! = 1 \cdot 1 \cdot (-1) = -1$ $\square$

1.4 Solving Congruence Equations

- Chinese Remainder Theorem: Let u and v be comprime. Then for any a, b, there is an x with $x \equiv a \pmod{u}$ and $x \equiv b \pmod{v}$. Such an x is unique $\pmod{uv}$
  - Existence: Follows from setting $su + tv = 1$ for some $s, t \in \mathbb{Z}$, then $tv \equiv 1 \pmod{u}$ and $su = 1 \pmod{v}$. Finally consider $x = a(tv) + b(su)$ and we have such an x
  - Uniqueness: Suppose $x' \equiv a \equiv x \pmod{u}$ and $x' \equiv b \equiv x \pmod{v}$. Then $u|(x - x')$ and $v|(x - x')$ so $uv|(x - x')$ since $(u, v) = 1$. Therefore $x' \equiv x \pmod{uv}$

- An application: RSA Coding
  - Pick two primes p and q and let $n = pq$
  - Fix a 'coding exponent' e
  - To encode a message $x \in \mathbb{Z}_n$, raise it to the power of e in $\mathbb{Z}_n$ i.e $x \to x^e$
  - To decode we wish to find a d such that $(x^e)^d = x$. Since $x^{\phi(n)} = 1$, $x^{k\phi(n)+1} = x$ for all $k \in \mathbb{Z}$
  - Hence we wish to find d such that $de = k\phi(n) + 1$, i.e $ed \equiv 1 \pmod{\phi(n)}$
  - To do this we can run Euclid on e and $\phi(n)$, assuming they are comprime
  - If we know p and q then $\phi(n) = pq - p - q - 1$ and this is easy. If we don't know the primes, it is very hard - even when we know what n is.

2 The Reals

- The Least Upper Bound Property
  - The field $\mathbb{Q}$ is not complete - this means that there are 'gaps'. For example the sequence:
    $\{3, 3.1, 3.14, 3.141, 3.1415, \ldots\}$ does not converge in $\mathbb{Q}$
  - The Real numbers $\mathbb{R}$ 'fix' this issue by having the Least Upper Bound Property: For any non-empty subset S of $\mathbb{R}$ which is bounded above, there exists a least upper bound, denoted $\sup(S)$ such that $\forall s \in S, \sup(S) \geq s$

2.1 Sequences and Convergence

- For a sequence $(a_n)_{n=1}^{\infty}$ we say that the sequence converges to a if:

  $$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ s.t } \forall n \geq N, |a - a_n| < \varepsilon$$

- There are some key theorems which may help to determine whether a sequence converges:
  - If a sequence is monotonic and bounded above, it converges.
  - Comparison test
- For example the series:
  $$\sum_{n=0}^{\infty} \frac{1}{n!} \text{ converges by comparison with } \sum_{n=0}^{\infty} \frac{1}{2^n} = 2$$

2.2 Irrational and Transcental Numbers

- We say that a number x is irrational if $x \in \mathbb{R} \setminus \mathbb{Q}$
- We say that a number x is transcendental if $\nexists$ a polynomial f with integer coefficients such that $f(x) = 0$
  - The number $c = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental. To show this we need two facts:
    1. For all polynomials with integer coefficients and for all $x, y \in [0, 1]$, there exists k such that
       $$|P(x) - P(y)| \leq k|x - y|$$
    2. A non-zero polynomial of degree d has at most d roots
  - Suppose c is a root of a degree d polynomial $P(x)$, i.e $P(c) = 0$. Then it can be shown that $|c - c_n| \leq \dfrac{2}{10^{(n+1)!}}$
  - It may then be shown that for sufficiently large n $|P(c_n) - P(c)| \geq \dfrac{1}{10^{d \cdot n!}}$
  - Hence by fact 1, $\dfrac{1}{10^{d \cdot n!}} \leq \dfrac{2k}{10^{(n+1)!}}$, for some k which is false for sufficiently large n $\square$

3 Sets and functions

- The Inclusion-Exclusion Principle:

  For finite sets $S_1, S_2, \dots S_n$:

  $|S_1 \cup S_2 \cup \ldots \cup S_n| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \ldots + (-1)^{n+1} \sum_{|A|=n} |S_A|$

  Where $S_A = \bigcap_{i \in A} S_i$ and summation is taken over all k-subsets of $\{1, 2, \dots, n\}$

  - The theorem may be proven by seeing how many times each x is counted in the LHS and RHS

- Equivalence relations:

  - We say that a relation R on a set X is an <u>equivalence relation</u> if:
    1. R is <u>reflexive</u> - $xRx \ \forall x \in X$
    2. R is <u>symmetric</u> - $xRy \iff yRx \ \forall x, y \in X$
    3. R is <u>transitive</u> - $xRy \wedge yRz \implies xRz \ \forall x, y, z \in X$
  - The equivalance classes of an equivalence relation on a set X partitions X

4 Countability

- We say that a set X is <u>countable</u> if:
  - $\exists$ a injection $f : X \to \mathbb{N}$
  - $\exists$ a surjection $f : \mathbb{N} \to X$
  - $\exists$ a bijection $f : X \to \mathbb{N}$ or X is finite

- Some examples of countable sets are:
  - $\mathbb{N}$ - by definition
  - $\mathbb{N}^k$ - consider the injection $f : \mathbb{N}^k \to \mathbb{N}$ defined by $(n_1, n_2, \dots n_k) \mapsto p_1^{n_1} \cdot p_2^{n_2} \dots p_k^{n_k}$ for primes p_i

- A countable union of countable sets is countable - this may be shown by 'diagonally' counting the elements of countable sets $A_1, A_2, \dots$

- We say a set is <u>uncountable</u> if it is not countable. Some examples of uncountable sets are:
  - $\mathbb{R}$ - can be shown by Cantor's diagonalisation argument
  - $\mathbb{R} \setminus \mathbb{A}$ - consider $(\mathbb{R} \setminus \mathbb{A}) \cup \mathbb{A} = \mathbb{R}$
  - $\mathbb{P}(\mathbb{N})$ - shown by diagonalisation or a surjection into $\mathbb{R}$

- Schroder-Bernstein Theorem:

  If $f : A \to B$ and $g : B \to A$ are injections then $\exists$ bijection $h : A \to B$

  - To see why this is, consider the <u>ancestor sequence</u> of $a \in A$: $g^{-1}(a), f^{-1}g^{-1}(a), g^{-1}f^{-1}g^{-1}(x), \ldots$. Partition the sequences based on whether or not they terminate in even time, odd time or dont terminate. Then we can biject between these sets and their analogue in B.