Math Tripos Part IA: Numbers and Sets

Michael Li

May 21, 2015

Introduction to number systems and logic
Overview of the natural numbers, integers, real numbers, rational and irrational numbers, algebraic and transcendental numbers. Brief discussion of complex numbers; statement of the Fundamental Theorem of Algebra.

Ideas of axiomatic systems and proof within mathematics; the need for proof; the role of counter-examples in mathematics. Elementary logic; implication and negation; examples of negation of compound statements. Proof by contradiction. [2]

Sets, relations and functions
Union, intersection and equality of sets. Indicator (characteristic) functions; their use in establishing set identities. Functions; injections, surjections and bijections. Relations, and equivalence relations. Counting the combinations or permutations of a set. The Inclusion-Exclusion Principle. [4]

The integers
The natural numbers: mathematical induction and the well-ordering principle. Examples, including the Binomial Theorem. [2]

Elementary number theory
Prime numbers: existence and uniqueness of prime factorisation into primes; highest common factors and least common multiples. Euclidfis proof of the infinity of primes. Euclidfis algorithm. Solution in integers of $ax + by = c$.

Modular arithmetic (congruences). Units modulo n. Chinese Remainder Theorem. Wilson's Theorem; the Fermat-Euler Theorem. Public key cryptography and the RSA algorithm.[8]

The real numbers
Least upper bounds; simple examples. Least upper bound axiom. Sequences and series; convergence of bounded monotonic sequences. Irrationality of $\sqrt{2}$ and e. Decimal expansions. Construction of a transcendental number. [4]

Countability and uncountability
Definitions of finite, infinite, countable and uncountable sets. A countable union of countable sets is countable. Uncountability of R. Non-existence of a bijection from a set to its power set. Indirect proof of existence of transcendental numbers. [4]

Contents

1 Sets, functions and relations

1.1 Sets

Definition. A *set* is a collection of stuff without order. Elements in a set are only counted once.

Definition. A *equal to* B, denoted $A = B$, if $\forall x(x \in A \Leftrightarrow x \in B)$ (they have the same elements).

Definition. A is a *subset* of B, written as $A \subseteq B$ or $A \subset B$, if all elements in A are in B.

Theorem. $(A = B) \Leftrightarrow (A \subseteq B \text{ and } B \subseteq A)$

Definition. For sets A and B, we define (other operations *must* be based upon these):

- *Intersection*: $A \cap B = \{x : x \in A \text{ and } x \in B\}$ (Operation Associative)
- *Union*: $A \cup B = \{x : x \in A \text{ or } x \in B\}$ (Operation Associative)
- *Set difference*: $A \setminus B = \{x \in A : x \notin B\}$
- *Symmetric difference*, $A \Delta B$, as the set in which elements are in exactly one of the two sets.
- *Power set*, $\mathcal{P}(x)$, as the set of all subsets.

Proposition. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Note. If A_α are sets then $\bigcap_{\alpha \in I} A_\alpha = \{x : \forall \alpha \in I(x \in A_\alpha)\}$ and $\bigcup_{\alpha \in I} A_\alpha = \{x : \exists \alpha \in I(x \in A_\alpha)\}$.

Definition. An *ordered pair* (a, b) is defined as $\{a, \{a, b\}\}$. $(a, b) = (a', b')$ iff $a = a'$ and $b = b'$.

Definition. Given sets A, B, the *Cartesian product* of A and B is $A \times B = \{(a, b) : a \in A, b \in B\}$. This can be extended to n products.

1.2 Functions

Definition. A *function* (or *map*) $f : A \to B$ is a "rule" that assigns, for each $a \in A$, exactly one element $f(a) \in B$, denoted $a \mapsto f(a)$.

Definition. A function f is *injective* if it hits everything at most once, or $\forall x, y \in X, f(x) = f(y) \Rightarrow x = y$. A function is *surjective* if it hits everything at least once, or $\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$.

A function is *bijective* if it is both injective and surjective. Only bijective functions have inverses.

Definition. A *permutation* of A is a bijection $A \to A$.

Definition. The *composition* of two functions is a function you get by applying one after another. For f, g, we have $g \circ f : X \to Z$ with $g \circ f(x) = g(f(x))$. This operation is associative.

Definition. $f(A) = \{f(a) : a \in A\}$ is the *image* of A. We have f is surjective iff $f(A) = B$.

For a set V, $f^{-1}(V) = \{a \in A : f(a) \in V\}$ is the *pre-image* of V.

Definition. The *identity map* $\mathrm{id}_A : A \to A$ is defined as the map $a \mapsto a$.

Definition. Given $f : A \to B$, a *left inverse* of f is a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$, a *right inverse* of f is a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$.

Theorem. The left inverse of A exists iff f is injective.

Proof. ($\Rightarrow$) If the left inverse g exists, then $\forall a, a' \in A, f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \Rightarrow a = a'$. ($\Leftarrow$) if f is injective, we can construct a left inverse g defined as

$$g : \begin{cases} g(b) = a & \text{if } b \in f(A), \text{ where } f(a) = b \\ g(b) = \text{anything} & \text{otherwise} \end{cases}.$$

□

Theorem. The right inverse of A exists iff f is surjective. (Equivalent to Axiom of Choice)

Proof. ($\Rightarrow$) We have $f(g(B)) = B$, thus f must be surjective since its image is B.

($\Leftarrow$) If f surjective, we construct g: for each $b \in B$, pick $a \in A$ with $f(a) = b$ and put $g(b) = a$.

□

Definition. An *inverse* of f is both a left inverse and a right inverse. It is written as $f^{-1} : B \to A$.

1.3 Relations

Definition. A *relation* R on A says some elements of A are related to others. Formally, $R \subseteq A \times A$. We write aRb iff $(a, b) \in R$.

Example. aRb iff a and b have the same final digit. e.g. $(37)R(57)$. [Equivalence Relation]

Definition. A relation R is *reflective* if $\forall a, aRa$. A relation R is *symmetric* iff $\forall a, b$, $aRb \Leftrightarrow bRa$. A relation R is *transitive* iff $\forall a, b, c$, $aRb \vee bRc \Rightarrow aRc$.

Definition. A relation is an *equivalence relation*, or $\sim$, if it is reflexive, symmetric and transitive. The *equivalence class* $[x]$ is the set of all elements related via $\sim$ to x.

Definition. A *partition* of a set X is a collection of subsets A_α of X such that each element of X is in exactly one of A_α.

Theorem. For a $\sim$ on A, the equivalence classes of $\sim$ define a partition of A and vice versa.

Proof. By reflexivity, we have $a \in [a]$. Thus the equivalence classes cover the whole set. We must now show that for all $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Suppose $[a] \cap [b] \neq \emptyset$. Then $\exists c \in [a] \cap [b]$. So we have $a \sim b$. For all $b' \in [b]$, we have $b \sim b'$. Thus by transitivity, we have $a \sim b'$. Thus $[b] \subseteq [a]$. By symmetry, $[a] \subseteq [b]$ and $[a] = [b]$. □

Definition. The *quotient map* q maps each element in A to the equivalence class containing a.

2 Division

2.1 Euclid's Algorithm

Definition (Factor of integers)**.** Given $a, b \in \mathbb{Z}$, we say a *divides* b/a is a *factor* of b/$a|b$ if $\exists c \in \mathbb{Z}(b = ac)$. For any b, ± 1 and $\pm b$ are always factors of b. The others are called *proper factors*.

Theorem (Division Algorithm)**.** Given $a, b \in \mathbb{Z}$, there are unique $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$.

Proof. Choose $q = \max\{q : qb \leq n\}$ (exists due to $\mathbb{Z}$). Now write $r = a - qb$. We have $0 \leq r < b$ and thus q and r are found. Suppose that $a = qb + r = q'b + r' \Rightarrow (q - q')b = (r' - r)$. From definition, $-b < r - r' < b$, but $r' - r$ is a multiple of b so $q - q' = r' - r = 0$. □

Definition. A *common factor* of a and b is a number $c \in \mathbb{Z}$ such that $c|a$ and $c|b$. A highest common factor or GCD of two numbers$a, b \in \mathbb{N}$, denoted $d = \gcd(a,b) = \mathrm{hcf}(a,b) = (a,b)$, is a number $d \in \mathbb{N}$ such that $d|a$ and $d|b$ and if $c|a$ and $c|b$ then $c|d$.

Note. You might think it is more natural to define $\gcd(a,b)$ to be the largest common factor and then show it has the property that all other common factors divide it-but the definition is superior. (application in non-ordered rings)

Theorem. Let a,b $\in \mathbb{N}$ Then $\gcd(a,b)$ exists.

Proof. let $S = \{ua + vb : u, v \in \mathbb{Z}\}$ be the set of all linear combinations of a, b. Let d be the smallest positive integer of S, say $d = xa + yb$. If $c|a$, $c|b$ then $c|d$. So we need only show that $d|a$ and $d|b$ for then $d = \mathrm{hcf}(a,b)$. By the division algorithm we have $q, r \in \mathbb{Z}$ with $a = qd + r$ with $0 \leq r < d$. Then $r = a - qd = a(1 - qx) - yb$ so r ∈ S. Since d is smallest positive member of S, and $0 \leq r < d$, we have $r = 0$. Hence $d|a$ and likewise $d|b$. □

Corollary (Bezout's Theorem)**.** Let $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ with $c = ua + vb$ iff $(a,b)|c$.

Proof. "⇒" let $d = (a,b)$ If $c = ua + vb$ then $d|c$ (because $d|a$ and $d|b$). "⇐" Conversely, suppose $d|c$, say $c = kd$. There exists $x, y \in \mathbb{Z}$ with $d = xa + yb$ Then $c = (kx)a + ky(b)$ □

Example. $a = 57, b = 42$ Find their GCD.
$(57,42) = (42,15) = (15,12) = (12,3) = 3$
Since $57 = 42 + 15$, $42 = 15 * 2 + 12$, $15 = 12 + 3$, $12 = 3 * 4 + 0$

This is Euclid's algorithm. It works because $(a,b) = (b,r_1) = (r_1,r_2) = ... = (r_{n-1},r_n)$ =factors of r_{n-1}. Note it gives an alternative proof that hcf exist. And it is fast. ($r_n \leq \frac{r_{n-2}}{2}$)

Can we express (a,b) as a linear combination of a and b? Yes! Reverse Engineer Euclid.

Example.

$$\begin{aligned} 3 &= 15 - 2 * 6 \\ &= 3 * 15 - 2 * 21 \\ &= 3 * 57 - 8 * 21 \end{aligned}$$

Comment. Is there a way to work out x, y as we go, without having to remember our steps and retrace? Write $A_{-1} = 0$, $A_0 = 1$ $B_{-1} = 1$ $B_0 = 0$ for j ≥ 1

$$A_j = q_j A_{j-1} + A_{j-2}, \text{ and } B_j = q_j B_j + B_{j-2}$$

Prove that : $aB_j - bA_j = (-1)^{j-1} r_j$ Hence $a * B_{n-1} - b * A_{n-1} = (-1)^{n-1}(a, b)$
Also $A_j B_{j-1} - B_j A_{j-1} = (-1)^j$ so $(A_j, B_j) = 1$

Comment.

$$\frac{57}{21} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}}$$

$2, 2 + \frac{1}{1} = 3, 2 + \frac{1}{1 + \frac{1}{2}} = \frac{8}{3}$ are called the *convergents*.

2.2 Primes

Definition. $p \in \mathbb{N}$ is *prime* if $p > 1$ and the only factors of p are $\pm 1, \pm p$.

Theorem. Every number can be written as a product of primes.

For if $n \in \mathbb{N}$ is not itself prime, it can be written as $n = ab$ and repeat until all are prime.

Note. This does *not* give uniqueness. There are fields in which prime factorization is not unique.

Theorem. There are infinitely many primes.

Euclid 300BC. Let $p_1, ..., p_k$ be some primes, Let $n = p_1 p_2 .... p_k + 1$. Then $p_i \nmid N$, else $p_i \mid 1$ $(i = 1, 2, \cdots, k)$ which is not true. But N is a product of primes, so there must be other primes. □

Erdős 1930. Let p_1,...p_k be some primes. Any number a product of these primes has form $p_1^{j_1} p_2^{j_2} .... p_k^{j_k} = m^2 p_1^{i_1} p_2^{i_2} .... p_k^{i_k}$ where $j_i \geq 0$, $m \in \mathbb{N}$ and i_k=0 or 1. Any number $\leq N$ of the above form has $m \leq \sqrt{N}$. Hence there are at most $\sqrt{N} * 2^k$ numbers of this kind. So if $N > \sqrt{N} * 2^k$, i.e. $N > 4^k$, there must be a number $\leq N$ not of this form, hence there is a prime $\leq N$ not amongst $p_1, ...p_k$. □

Note. Euclid shows $k^{th}\ prime < 2^{2^k}$ while Erdos shows $k^{th}\ prime < 4^k$. In fact k^{th} prime $\sim k \log k$ (Prime number Theorem).

Theorem. If $a|bc$ and a and b are coprime then $a|c$.

Proof. From Euclid's algorithm (or Bezout's Theorem) there exist $u, v \in \mathbb{Z}$ with ua+vb=1. So (multiply by c), uac+vbc=c. Now a divides LHS, so a divides RHS, so $a|c$. □

Corollary. If p is prime and $p|ab$ then $p|a$ or $p|b$.

Proof. $(p, a) = 1$ or p since p is prime. if it is p then $p|a$. If it is 1, then using the theorem, $p|b$. □

Theorem (Fundamental Theorem of Arithmetic)**.** Every natural number's prime factorization is unique. If $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ ($p_1 \cdots q_l$ prime) then $k = l$ and $q_1 ....q_l$ are $p_1 ...p_k$ in some order.

Proof. Let $p_1 ...p_k = q_1 ...q_l$ then $p_1 | q_1 ...q_k$ then p_1 divides q_1 or $p_1 | q_2 ...q_l$. Either $p_1 = q_1$ because q_1 prime or we repeat until we find some p_1 divides some q_m for $1 \leq m \leq l$ and thus $p_1 = q_m$. Repeat procedure for all p_n $1 \leq n \leq k$ and thus $l = k$ and $q_1 ....q_l$ are $p_1 ...p_k$ in some order. □

3 Counting and Integers

Proposition (Pigeonhole Principle)**.** Given $(m-1)n + 1$ pigeons in n pigeonholes, some pigeonhole has $\geq m$ pigeons.

Definition. Let X be a set. For each $A \subset X$ the *indicator* or *characteristic function* of A is the function $i_A : X \to \{0, 1\}$ where $i_A(x) = 1$ if $x \in A$ and 0 if $x \notin A$.

Proposition. (i) $i_A = i_B \Leftrightarrow A = B$

(ii) $i_{A \cap B} = i_A i_B$

(iii) $i_{\bar{A}} = 1 - i_A$

(iv) $i_{A \cup B} = i_A + i_B - i_{A \cap B}$

(v) $i_{A \setminus \bar{B}} = i_A i_{\bar{B}} = i_A(1 - i_B) = i_A - i_A i_B = i_A - i_{A \cap B}$

(vi) $i_{A \triangle B} = i_A + i_B \pmod 2$

This is very useful in proving set identities. (E.g.:$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$)

Note. Indicator functions are handy for computing the sizes of finite sets because if $A \subset X$ then $|A| = \sum_{x \in X} i_A(x)$. Clearly $|A \cup B| = |A| + |B| - |A \cap B|$ (Generalizable)

Proof.

$$\begin{aligned}|A \cup B| &= \sum_x A \cup B(x) \\ &= \sum i_A x + \sum i_B(x) - \sum i_{A \cap B}(x) \\ &= |A| + |B| - |A \cap B|\end{aligned}$$

□

Theorem (Inclusion-Exclusion Principle)**.** Suppose we have sets $A_1, A_2, ..., A_n$ be subsets of finite set X. Then

$$|\bar{A_1} \cap \bar{A_2} \cap \cdots \cap \bar{A_n}| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|$$

Proof. Proof 1 By induction on n. Proof 2 By induction on $|X|$. Proof 3. Observe

$$\begin{aligned}i_{\bar{A_1} \cap \bar{A_2} \cap \ldots \cap \bar{A_n}} &= i_{\bar{A_1}} i_{\bar{A_2}} i_{\bar{A_3}} \cdots i_{\bar{A_n}} = (1 - i_{A_1})(1 - i_{A_2}) \cdots (1 - i_{A_n}) \\ &= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i} i_{A_j} + \cdots + (-1)^n i_{A_1} i_{A_2} \cdots i_{A_n} \\ &= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i \cap A_j} + \cdots + (-1)^n i_{A_1 \cap A_2 \cap \cdots \cap A_n}\end{aligned}$$

$$\begin{aligned}|\bar{A_1} \cap \bar{A_2} \cap \cdots \cap \bar{A_n}| &= \sum_x 1(x) - \sum_i \sum_x i_{A_i}(x) + \sum_{i<j} \sum_x i_{A_i \cap A_j}(x) + \cdots + \sum_x (-1)^n i_{A_1 \cap A_2 \cap \cdots \cap A_n}(x)| \\ &= |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|\end{aligned}$$

□

3.1 Combinations

Definition. There are $\binom{n}{r}$ subsets of $\{1, 2, 3, \cdots, n\}$ of size r. The symbol is pronounced as "n choose r" and sometimes called "binomial coefficient".

Note. Some people write it as ${}^nC_r$, but DO NOT use that.

Proposition. By definition,

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

Theorem. For $n \in \mathbb{N}$ with $a, b \in \mathbb{R}$, we have

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{r}a^{n-r}b^r + \cdots + \binom{n}{n}a^0 b^n$$

Proof. We have $(a+b)^n = (a+b)(a+b)\cdots(a+b)$. We then choose r b's, and thus we have $\binom{n}{r}$ choices to do that. □

Proposition.

(i) $\binom{n}{r} = \binom{n}{n-r}$.

(ii) $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ (Pascal's identity)

(iii) $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$.

(iv) $\binom{a}{r}\binom{b}{0} + \binom{a}{r-1}\binom{b}{1} + \cdots + \binom{a}{r-k}\binom{b}{k} + \cdots \binom{a}{0}\binom{b}{r} = \binom{a+b}{r}$
(Vandermonde's convolution)

Proposition. $\binom{n}{r} = \dfrac{n!}{(n-r)!r!}$.

Proof. There are $n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$ to choose r elements in order. Each choice of subsets is chosen this way in $r!$ orders, so the number of subsets is $\frac{n!}{(n-r)!r!}$. □

We might write $x^{\underline{r}}$ for the polynomial $x(x-1)\cdots(x-r+1)$. We call this "x to the r falling". We can write $\binom{n}{r} = \dfrac{n^{\underline{r}}}{r!}$. Multiplying Vandermonde by $r!$, we obtain the "falling binomial theorem"

$$\binom{r}{0}a^{\underline{r}}b^{\underline{0}} + \binom{r}{1}a^{\underline{r-1}}b^{\underline{1}} + \cdots + \binom{r}{r}a^{\underline{0}}b^{\underline{r}} = (a+b)^{\underline{r}}.$$

Example. A bank prepares a letter for each of its n customers, saying how much it cares.There are $n!$ ways to put the letters in the envelopes. In how many ways can this be done so that no one gets the right letter?

We let X be the set of all envelopings (permutation of n). $|X| = n!$. For each i, let $A_i = \{x \in X : x \text{ assigns the correct letter to customer } i\}$. We want to

know $|\bigcap_i \bar{A}_i|$. We know that $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!, \cdots$. By the inclusion-exclusion formula, we have

$$|\bigcap_i \bar{A}_i| = |X| - \sum |A_i| + \sum |A_i \cap A_j| + \cdots$$

$$= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}\right) \approx n!e^{-1}$$

3.2 Well-ordering and Induction

Theorem ((Weak) Principle Of Induction)**.** Let $P(n)$ be a statement about the number $n \in N$ Suppose (i) $P(1)$ is true and (ii) $\forall n \in N$, if $P(n)$ is true then $P(n+1)$ is true Then $P(n)$ is true $\forall n \in N$.

Example (Tower of Hanoi)**.** n rings stacked on peg A. Our goal is to move it to peg B without a larger one stacked on top of a smaller one. We claim that it needs at least exactly $2^n - 1$ moves.

Proof. Using the Weak principle of Induction, let us prove $n = 1$. $P(1)$ is trivially true.

Suppose $n = k$ is true and try to prove $n = k + 1$ is true. We first move the top k rings to C, then bottom ring to B, then move the k rings from C to B.

Assuming $P(n)$, this needs $2^n - 1 + 1 + 2^n - 1 = 2^n * 2 - 1 = 2^{n+1} - 1$ moves.

Can we do it in fewer? We must free bottom ring, so must shift top n rings to another ring. That takes $\geq 2^n - 1$ moves by $P(n)$. Then we shift bottom ring and we have to shift the smaller n rings back, taking $\geq 2^n - 1$ moves by $P(n)$. So we nee at least $2^{n+1} - 1$ moves. Thus $n = k + 1$ is true when $n = k$ is true. Then by WPI, P(n) is true $\forall n$.

□

Theorem (Strong Principle of Induction)**.** let $P(n)$ be a statement about $n \in N$. Suppose (i) $P(1)$ true (ii) $\forall n \in N$ if $P(k)$ true $\forall k < n$ then $P(n)$ true. Then $P(n)$ is true for all $n \in N$.

Theorem. The Strong Principle of Induction is equivalent to the Weak Principle of Induction.

Proof. Clearly SPI⇒ WPI [Any proof using WPI can use SPI] To show that WPI ⇒ SPI, suppose P(1) true and ∀n $P(1) \wedge \cdots \wedge P(n-1) \Rightarrow P(n)$. We wish to show that $P(n)$ is true for all n. Let $Q(n)$="P(k) is true ∀ k ≤n" Then we can prove $Q(n)$ is true $\forall n$ using WPI, so $P(n)$ true ∀ n. □

Definition. A *partial order* on a set is a reflective, antisymmetric, transitive relation. A *total order* is a partial order where $\forall$ a $\neq$ b exactly one of aRb and bRa holds.

Example. Ordinary ordering of $\mathbb{N}$ $a \leq b$ (Total order)

Definition. A total order is *well-ordered* if every non-empty subset has a minimal element. i.e. if $S \neq \emptyset$, then $\exists m \in S$ s.t. if $x < m \Rightarrow x \notin S$.

Example. $\mathbb{N}$ with its usual order.

Theorem (Well-ordering principle (WOP))**.** $\mathbb{N}$ is well-ordered.

Theorem. SPI is equivalent to WOP.

Proof. To show that $WOP \Rightarrow SPI$, suppose $P(n)$ is given, $P(1)$ is true, and $P(n)$ true if $P(k)$ true $\forall k < n$. We want to show $P(n)$ true $\forall$ n. Suppose, contrary to SPI, that $P(n)$ is false for some n's. Let $C = \{n : P(n)$ false$\}$ "set of counterexamples". Then $C \neq \emptyset$ so has a minimal element $m \in C$ is the smallest counterexample m. Now $P(k)$ is true for all $k \leq m$, so $P(m)$ is true. Thus $WOP \Rightarrow SPI$.

Now we need to show SPI $\Rightarrow$ WOP, let $S \subseteq \mathbb{N}$ and suppose S has no minimal element. Let $P(n)$ be "$n \notin S$"

Certainly $1 \notin S$ so $P(1)$ true. Now suppose $P(k)$ is true $\forall k < n$. The $k \notin S$ $\forall k < n$. If $n \in S$ then n is the minimum element of S, so $n \notin S$, so $P(n)$ true. By SPI, $P(n)$ true $\forall$ n, so $S = \emptyset$. $\square$

Example. Consider total order on $\mathbb{N} \times \mathbb{N}$ by "lexicographic" order.

$$(a, b) \leq (c.d)$$

If $a < c$ or $a = c \wedge b \leq d$.

Example (Ackermann function)**.** $a : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}$ is defined by

$$a(0, , n) = n + 1$$

$$a(m, 0) = a(m - 1, 1) \text{ if } m > 0$$

$$a(m.n) = a(m - 1, a(m - n - 1)) \text{ if } m, n > 0$$

Is it well-defined?

Note. a(m,n) is expressed in terms of a at points (x,y)¡(m.n) in the order. So functions is well defined if lexicographic order is well-ordered: i.e. every subset non-empty has minimal element.

But $\mathbb{N}_0 \times \mathbb{N}_0$ is well-ordered: if $S \subset \mathbb{N}_0 \times \mathbb{N}_0$ is non-empty. let$S_x = \{x \in \mathbb{N}_0 : \exists y$ such that $(x, y) \in S\}$ (S_x has minimum element m by WOP). let $S_y = \{y \in \mathbb{N}_0 : \exists x$ such that $(x, y) \in S\}$ (S_y has minimum element n by WOP).

Then (m, n) is minimum element of S.

4 Modular Arithmetic

Definition. If A,B $\in \mathbb{Z}$ have the same remainder after division by m we say a and b are *congruent modulo m.* that is $a \equiv b \pmod{m}$ means $m|a - b$. i.e. a, b written in $\pmod{n}$ have same last digit.

Remark. Computer does arithmetic mod 2^{64}. ISBN uses modular arithmetic in check digits.

Note. if $a \equiv b \pmod{m}$ and $d|m$ then $a \equiv b \pmod{d}$.

If $a \equiv b \pmod{m}$ and $u \equiv v \pmod{m}$ then $a + u \equiv b + v \pmod{m}$ and $au \equiv bv \pmod{m}$. Formally, we are doing arithmetic with congruence classes in $\mathbb{Z}_m$.

Example. Show that $2a^2 + 3b^3 = 1$ has no solutions in $\mathbb{Z}$.

Proof. If soluble then $2a^2 \equiv 1 \pmod{3}$ But $2 \cdot 0^2 \equiv 0$, $2 \cdot 1^2 \equiv 2$, $2 \cdot 2^2 \equiv 2$, so no solution to the congruence, hence none to the original equation. □

Example. There are infinitely many primes $\equiv -1 \pmod{4}$

Proof. Suppose not, so let $p_1, \cdots, p_k$ be all primes $\equiv -1 \pmod{4}$ Let $N = 4p_1p_2....p_k - 1$. Then $N \equiv -1 \pmod{4}$ Now N is a product of primes, $N = q_1....q_l$ say. But $2 \nmid N$ and $p_i \nmid N$ for all i. Hence $q_i \equiv 1 \pmod{4}$ for all i. But then $N = q_1 \cdots q_l \equiv 1 \pmod{4}$, a contradiction. □

Definition. u is a *unit* modulo m if there exists v such that $uv \equiv 1 \pmod{m}$

Theorem. u is a unit modulo m iff $(u, m) = 1$.

Proof. Suppose u is a unit and let $d = (u, m)$. We have $uv \equiv 1$, so $m \mid uv - 1$ thus $d \mid uv - 1$. But $d \mid u$ so $d = 1$. Suppose conversely that $(u, m) = 1$. Then $\exists a, b \in \mathbb{Z}$ with $ua + mb = 1$. Thus $ua \equiv 1$. □

Remark. We can find a with $ua \pmod{1}$ efficiently.

Corollary. If $(a, m) = 1$ then $ax \equiv b \pmod{m}$ has a unique solution $\pmod{m}$.

Proof. $ax \equiv b \pmod{m}$ and $(a, m) = 1$ then $\exists w$ such that $aw \equiv 1 \pmod{m}$ by theorem so $wax \equiv wb \pmod{m}$ so $x \equiv wb \pmod{m}$. Conversely if $x \equiv wb \pmod{m}$, then $ax \equiv b \pmod{m}$. □

Theorem. There is a solution to $ax \equiv b \pmod{m}$ if and only if $(a, m)|b$.

If $d = (a, m)|b$, then the solution is the unique solution to $\frac{a}{d}x \equiv \frac{b}{d}x \pmod{\frac{m}{d}}$

Proof. If $(a, m) = d > 1$, then $d|b$ is a necessary condition for solution to exist as $d \mid ax - b$. If it satisfies this, then $a = da'$ and $b = db'$ and $m = dm'$ so $ax \equiv b \pmod{m}$ so $da'x \equiv db' \pmod{dm'}$ so $a'x \equiv b' \pmod{m}'$. We can solve that since a' and m' are corpime. □

4.0.1 Multiple Moduli

Theorem (Chinese Remainder Theorem)**.** Let $(m, n) = 1$ and $a, b \in \mathbb{Z}$. Then there is a unique solution $\pmod{mn}$ to:

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}$$

This means there is a number x satisfying both, and every other solution y satisfies $x \equiv y \pmod{mn}$.

Proof. Since m and n are coprime, we can express m, n in the form $um + vn = 1$ for integer u, v. Then notice $um \equiv 1 \pmod{n}$ and $vn \equiv 1 \pmod{m}$ let x=umb+vna. Then it is clear that x satisfies the equation set in the theorem. Moreover if $y \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, $m|y - x$ and $n|y - x \Leftrightarrow mn|y - x$ by FTA $\Leftrightarrow y \equiv x \pmod{mn}$. □

Remark. (i) We have a bijection $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$

(ii) Can be extended to more than two moduli by induction.

Note. x (the solution) is a unit $\pmod{mn}$ iff a is a unit $\pmod{m}$ and b is a unit $\pmod{n}$.

Proof. If $\exists\ u$ such that $xu \equiv 1 \pmod{mn}$, so $au \equiv xu \equiv 1 \pmod{m}$, likewise b is a unit mod n.

Conversely, if $au \equiv 1 \pmod{m}$ and $bv \equiv 1 \pmod{n}$, by CRT, there $\exists\ w$ such that $w \equiv u \pmod{m}$ and $w \equiv v \pmod{n}$. Thus $cw \equiv 1 \pmod{m}$ and $cw \equiv 1 \pmod{n}$. But $1 \equiv 1 \pmod{m}$ and $1 \equiv 1 \pmod{n}$, so by CRT (uniqueness) $cw \equiv 1 \pmod{mn}$. Thus c is a unit (mod mn) □

Definition (Euler's Totient Function)**.** We denote by $\phi(m)$ the number of integers a, $a \leq a \leq m$, such that $(a, m) = 1$, that is, a is a unit (modulo m).

Note. It follows from above that ϕ is *multiplicative*: that is

$$\phi(mn) = \phi(m)\phi(n) \ (m, n) = 1$$

$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. Thus if $m = p_1^{k_1} \cdots p_l^{k_l}$ (distinct primes), $\phi(m) = m \prod_{p|m}(1 - \frac{1}{p})$. (Proof possible by inclusion-exclusion).

Note. Let p be a prime. Then $1, 2, \ldots, p-1$ are units and come in pairs of inverses a, u plus self-inverses (if $x^2 \equiv 1 \pmod{p}$). Now

$$x^2 \equiv 1 \pmod{p} \Leftrightarrow p|x^2-1 = (x-1)(x+1) \Leftrightarrow x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p}$$

Thus 1 and -1 are the only self-inverse elements in multiplicative group mod p.

Theorem (Wilson's theorem)**.**

$$(p-1)! \equiv -1 \pmod{p} \text{ (if } p \text{ prime)}$$

Proof. $(p-1)!$ is the product of $\frac{p-3}{2}$ inverse pairs together with 1 and -1. □

Theorem (Fermat's Little Theorem)**.** let p be prime. Then $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof. a is a unit. So $ax \equiv ay$ iff $x \equiv y \pmod{p}$. Then $a, 2a, 3a, ..., (p-1)a$ are distinct (mod p) so they are congruent to $1, 2, ...p-1$ is some way. Then:

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$$

□

Theorem (Fermat-Euler)**.** Let $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. Let $U = \{x \in N : 0 < x < m, (x, m) = 1\}$ These are the $\phi(m)$ units. If $U = \{u_1, u_2, \cdots, u_{\phi(m)}\}$ then $au_1, \cdots, au_{\phi(m)}$ are distinct units (since a is), so are $u_1, \ldots, u_{\phi(m)}$ in some order. Hence

$$au_1 au_2 \ldots au_{\phi(m)} \equiv u_1 u_2 \ldots u_{\phi(m)} \pmod{m}$$

Then by the same reasoning as in proof of Fermat Little's Theorem, we have $a^{\phi(m)} \equiv 1 \pmod{m}$ □

4.0.2 Squares

Definition. $1^2, 2^2, 3^3 \ldots, (p-1)^2$ are squares mod p, and we call these numbers *quadratic residues*.

If $a^2 \equiv b^2 \pmod{p}$ then $p|(a^2 - b^2) = (a-b)(a+b)$. By FTA: $a \equiv \pm b \pmod{p}$. Thus every square is a square of exactly two numbers (p odd). So there are exactly $\frac{p-1}{2}$ quadratic residues.

Theorem. If p is a odd prime, then -1 is a quadratic residue if and only if $p = 4k+1$.

Proof. $-1 \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 2 \cdots \frac{p-1}{2}(-\frac{p-1}{2}) \cdots (-1) \equiv (-1)^{\frac{p-1}{2}}(\frac{p-1}{2}!)^2$. So if $p \equiv 1 \pmod{4}$ then -1 is a quadratic residue. For $4k+3$ primes, if $-1 \equiv z^2$ for some z, then Fermat says $1 \equiv z^{p-1} \equiv z^{4k+2} \equiv (z^2)^{2k+1} \equiv -1$, a contradiction. □

Fermat proved that a prime can be written as sum of two squares iff it is of form $4k+1$ using the theorem and "method of infinite descent".

Example. Using this theorem, we can prove there are infinitely many primes of form $4k+1$ easily.

Proof. Suppose not, Construct number $N = (2p_1p_2 \cdots p_k)^2 + 1$ in which the p_i are all the primes of form 4k+1. Then if q divides N, q is of form 4k+3. However, that means $N \equiv 0 \pmod{q}$ so $(2p_1p_2 \cdots p_k)^2 \equiv -1 \pmod{q}$. However we know -1 is not a quadratic residue of k, so contradiction. □

If $p \equiv 4k+3$ we can compute square roots using Fermat. Suppose $a \equiv z^2 \pmod{p}$

$$a^{2k+1} \equiv z^{4k+2} \equiv z^{p-1} \equiv 1 \Rightarrow a^{2k+2} \equiv a \pmod{p}$$

So $\pm a^{k+1}$ are square roots of a. We can compute powers efficiently by repeated squaring. as in

$$a^{37} \equiv ((((a^2)^2)^2)^2)^2 \cdot (a^2)^2 \cdot a$$

Which has efficiency $O(\log n)$ compared to $O(n)$.

4.1 Public Key Cryptography

Let us agree to write messages as sequences of numbers. You wish to safely transmit your message. We need an encryption scheme that everyone knows but only you can decrypt.

4.1.1 RSA Cryptography

You find two large primes p, q, Let $n = pq$. Pick e co-prime to $\phi(n) = (p-1)(q-1)$ Find d such that

$$de \equiv 1 \pmod{\phi(n)}$$

Publish pair n, e. To send you a message (sequence of numbers) split message into numbers $M < n$. Send you $M^e \pmod{n}$ To find M: $(M^e)^d \equiv M^{k\phi(n)+1} \equiv M \pmod{n}$.

To break this one can prime factorize or find $\phi(n)$, which is as hard as factorization. ($\phi(n)$ enables you to find p, q through quadratics) It is not known if RSA can be broken without factorizing.

5 Real Numbers

5.1 Natural Numbers

5.1.1 Peano's Axioms

$\mathbb{N}$ is a set with a special element 1 and map: $N \to N$ $n \to n^+$ "successor" such that

(i) $\forall n, n^+ \neq 1$

(ii) $\forall n, m, n \neq m \Rightarrow n^+ \neq m^+$

(iii) that's all: So If $A \subseteq \mathbb{N}$, and satisfies the two axioms, then $A = \mathbb{N}$

We can construct $\mathbb{Z}$ from $\mathbb{N}$ using subtraction. To construct $\mathbb{Q}$ from $\mathbb{Z}$, we can define a relation R on $\mathbb{Z} \times N$ by $(a, b)R(c, d)$ if $ad = bc$. R is a equivalence relation (check this). $\mathbb{Q}$ is the set of equivalence classes. We write $\frac{a}{b}$ for [(a,b)] Next define +, $\times$ on $\mathbb{Q}$ so when constructed has the properties of a *totally ordered field*.

Properties of Rationals

(i) $\mathbb{Q}$ is an additive abelian group with identity 0.

(ii) $\mathbb{Q}\backslash\{0\}$ is a multiplicative abelian group with identity 1.

(iii) Multiplication is distributive (over addition).

(iv) There is an order relation $\leq$ on Q which is antisymmetric and transitive.

(v) This relation is *total*, as in either $p < q$, p=q, or $p > q$. (trichotomy)

(vi) $\forall p, q, r \in \mathbb{Q}, p < q \Rightarrow p + r < q + r$,$p < q, 0 < r \Rightarrow pr < qr$

(i) to (ii) gives a field, (iv) and (v) gives total order, (vi) means the order respects the field. A totally ordered field satisfies all identities. Note that any ordered field $0 < 1$, for otherwise $1 < 0$:

$$1 < 0 \Rightarrow 0 < -1$$

$$0 < -1 \Rightarrow 0 < (-1)^2 = 1 \text{ (Contradiction)}$$

Note. Q is *dense*: If $p, q \in Q$, $\exists r \in Q$ such that $p < r < q$.

Theorem. There is no rational $\frac{a}{b} \in Q$ that solves $q^2 = 2$

Original Proof. The standard show 2 is both factor of a and b proof. □

Proof. Let p be a prime such that $p|b$. Then $a^2 = 2b^2$ so $p|a^2$. By FTA, $p|a$. □

Dirichlet. $\frac{a}{b} = \frac{2b}{a}$ So $\frac{au+2bv}{bu+av} = \frac{a}{b}$ $u = -1, v = 1$ gives $\frac{a}{b} = \frac{2b-a}{a-b}$ (contradicts minimal b) □

Bezout. Same as 3, but use u, v, so $bu + av = 1$. Then $\frac{a}{b}$ is an integer! □

5.2 Construction of real numbers

Definition. $s \in X$ is a *least upper bound* (or *supremum*) for the set $S \subseteq X$, denoted as $s = \sup X$, if

(i) s is an upper bound for S, i.e. $\forall x \in S(x \leq s)$.

(ii) if t is any upper bound for S, then $s \leq t$.

Similarly, a *greatest lower bound* is defined. By definition, the least upper/lower bound for S, if exists, is unique.

Definition. The *real numbers* is a totally ordered field containing $\mathbb{Q}$ that satisfies the least upper bound axiom.

Axiom (Least upper bound axiom)**.** Every non-empty set of the real numbers that has an upper bound has a least upper bound.

Corollary. Every non-empty set of the real numbers bounded below has an infimum.

Proof. $-S = \{-x : x \in S\}$ is a non-empty set bounded above, and $\inf S = -\sup(-S)$. □

Now the set $\{q \in Q : q < 0 \text{ or } q^2 < 2\}$ has a supremum in $\mathbb{R}$ (by definition). We now construct $\mathbb{R}$ from Dedekind cuts.

Definition. A *Dedekind cut* of $\mathbb{Q}$ is a set of partition of $\mathbb{Q}$ into L and R such that $\forall l \in L, r \in R, l < r$ and R has no minimum, i.e. a partition that splits $\mathbb{Q}$ into a "left" and "right" sets.

Given $\mathbb{Q}$, construct a set $\mathbb{R}$ from $\mathbb{Q}$ by letting $\mathbb{R}$ be the set of all Dedekind cuts. We can inject $\mathbb{Q} \to \mathbb{R}$ by $q \mapsto \{x \in q : x \leq q\}, \{x \in \mathbb{Q} : x > q\}$.

Definition. A *closed interval* $[a, b]$ with $a \leq b \in R$ is the set $\{x \in \mathbb{R} : a \leq x \leq b\}$ n An *open interval* (a, b) with $a \leq b \in R$ is the set $\{x \in \mathbb{R} : a < x < b\}$.

Theorem. (Axiom of Archimedes) Given $r \in \mathbb{R}$, there exists $n \in \mathbb{N}$ with $n > r$.

Proof. Assume the contrary. Then r is an upper bound for $\mathbb{N}$. $\mathbb{N}$ is not empty since $1 \in \mathbb{N}$. By the least upper bound axiom, $s = \sup \mathbb{N}$ exists. Since s is the least upper bound for $\mathbb{N}$, $s - 1$ is not an upper bound for $\mathbb{N}$. So $\exists m \in \mathbb{N}$ with $m > s - 1$. Then $m + 1 \in \mathbb{N}$ but $m + 1 > s$, which contradicts the statement that s is an upper bound. □

Theorem. $\mathbb{Q}$ is dense in $\mathbb{R}$, i.e. given $r, s \in \mathbb{R}$, with $r < s$, $\exists q \in \mathbb{Q}$ with $r < q < s$.

Proof. wlog assume first $r \geq 0$ (just multiply everything by -1 if $r < 0$). Since $s - r > 0$, $\exists n \in \mathbb{N}$, $\frac{1}{n} < s - r$. By the Axiom of Archimedes, $\exists N \in \mathbb{N}$ such that $N > sn$.

Let $T = \{k \in \mathbb{N} : \frac{k}{n} \geq s\}$. T is not empty, since $Nn \in T$. Then by the well-ordering principle, T has a minimum element m. Now $m \neq 1$ since $\frac{1}{n} < s - r \leq s$. Let $q = \frac{m-1}{n}$. Since $m - 1 \notin T$, $q < s$. If $q = \frac{m-1}{n} < r$, then $\frac{m}{n} < r + \frac{1}{n} < s$, so $m \notin T$, contradiction. So $r < q < s$. □

Theorem. There exists $x \in \mathbb{R}$ with $x^2 = 2$.

Proof. Let $S = \{r \in \mathbb{R} : r^2 \leq 2\}$. Then $0 \in S$ so $S \neq \emptyset$. Also $\forall r \in S (r \leq s)$. So S is bounded above. So $x = \sup S$ exists and $0 \leq x \leq 3$.

By trichotomy, either $x^2 < 2, x^2 > 2$ or $x^2 = 2$.

Suppose $x^2 < 2$. Let $0 < t < 1$. Then consider $(x + t)^2 = x^2 + 2xt + t^2 < x^2 + 6t + t \leq x^2 + 7t$. Pick $t < \frac{2-x^2}{7}$, then $(x + t)^2 < 2$. So $x + t \in S$. Contradiction. Now suppose $x^2 > 2$.Let $0 < t < 1$. Then consider $(x - t)^2 = x^2 - 2xt + t^2 \geq x^2 - 6t$. Pick $t < \frac{x^2-2}{6}$. Then $(x - t)^2 > 2$, so $x - t$ is an upper bound for S. Contradiction So by trichotomy, $x^2 = 2$. □

5.3 Sequences

Definition. A *sequence* is a function $\mathbb{N} \to \mathbb{R}$. If a is a sequence, instead of $a(1), a(2), \cdots$, we usually write $a_1, a_2, \cdots$.

Definition. The sequence $(a_n)_{n=1}^{\infty}$ *tends to* $l \in \mathbb{R}$ as n tends to infinity if and only if

$$\forall \epsilon > 0 \text{ there exists} N \in \mathbb{N} \text{ such that } \forall n \geq N(|a_n - l| < \epsilon)$$

If a_n tends to l as n tends to infinity, we write $\lim_{n\to\infty} a_n = l$; or a_n converges to l.

Intuitively, if $a_n \to l$, we mean given any ϵ, for sufficiently large n, a_n is always within $l \pm \epsilon$.

Definition. a_n *converges* if there is an l s.t. $a_n \to l$. The sequence *diverges* if it doesn't converge.

Example. Show that $a_n = 1 - \frac{1}{n} \to 1$.

Given $\epsilon > 0$, choose $N > \frac{1}{\epsilon}$, which exists by the Axiom of Archimedes. If $n \geq \mathbb{N}$, then $|a_n - 1| = \frac{1}{n} \leq \epsilon$. So $a_n \to 1$.

Theorem. Every bounded monotonic sequence converges.

Note. a_n is increasing if $a_m \leq a_n$ iff $m \leq n$. It is monotonic if it is increasing or decreasing. a_n is bounded if $\exists a \in \mathbb{R}$ such that $|a_n| \leq a$.

Proof. wlog assume a_n is increasing. The set $\{a_n : n \geq 1\}$ is bounded and non-empty. So it has a supremum l. Show that l is the limit: Given any $\epsilon > 0$, $l - \epsilon$ is not an upper bound of a_n. So $\exists N$ such that $a_N \geq l - \epsilon$. Since a_n is increasing, we know that $l \geq a_m \geq a_N > l - \epsilon$ for all $m \geq N$. So $\exists N$ such that $\forall n \geq N$, $|a_n - l| < \epsilon$. So $a_n \to l$. □

Definition. A *subsequence* of (a_n) is $a_{g(n)}$ where $g : \mathbb{N} \to \mathbb{N}$ is strictly increasing.

Theorem. Every sequence has a monotonic subsequence.

Proof. Call a point a_k a "peak" if $\forall m \geq k(a_m \leq a_k)$. If there are infinitely many peaks, then they form a decreasing subsequence. If there are only finitely many peaks, $\exists N$ such that no a_n with $n > N$ is a peak. Pick a_{N_1} with $N_1 > N$. Then pick a_{N_2} with $N_2 > N_1$ and $a_{N_2} > a_{N_1}$ (possible because not a peak). Then repeat*ad infinitum* and we have a monotonic subsequence. □

Theorem.

(i) If $a_n \to a$ and $a_n \to b$, then $a = b$ (i.e. limits are unique)

(ii) If $a_n \to a$ and $b_n = a_n$ for all but finitely many n, then $b_n \to a$.

(iii) If $a_n = a$ for all n, then $a_n = a$.

(iv) If $a_n \to a$ and $b_n \to b$, then $a_n + b_n \to a + b$

(v) If $a_n \to a$ and $b_n \to b$, then $a_n b_n \to ab$

(vi) If $a_n \to a \neq 0$, and $\forall n(a_n \neq 0)$. Then $1/a_n \to 1/a$.

(vii) If $a_n \to a$ and $b_n \to a$, and $\forall n(a_n \leq c_n \leq b_n)$, then $c_n \to a$. (Sandwich theorem)

Proof.

(i) Suppose instead $a < b$. Then choose $\epsilon = \frac{b-a}{2}$. By the definition of the limit, $\exists N_1$ s.t. $\forall n \geq N_1$, $|a_n - a| < \epsilon$. There also $\exists N_2$ s.t. $\forall n \geq N_2$, $|a_n - b| < \epsilon$. Let $N = \max\{N_1, N_2\}$. If $n \geq \max\{N_1, N_2\}$, then $|a - b| \leq |a - a_n| + |a_n - b| < 2\epsilon = b - a$. Contradiction. So $a = b$.

(ii) Given $\epsilon > 0$, there $\exists N_1$ s.t. $\forall n \geq N_1$, we have $|a_n - a| < \epsilon$. Since $b_n = a_n$ for all but finitely many n, there exists N_2 such that $\forall n \geq N_2$, $a_n = b_n$. Let $N = \max\{N_1, N_2\}$. Then $\forall n \geq N$, we have $|b_n - a| = |a_n - a| < \epsilon$. So $b_n \to a$.

(iii) $\forall \epsilon$, take $N = 1$. Then $|a_n - a| = 0 < \epsilon$ for all $n \geq 1$.

(iv) Given $\epsilon > 0$, $\exists N_1$ s.t. $\forall n \geq N_1$, we have $|a_n - a| < \epsilon/2$. Similarly, $\exists N_2$ s.t. $\forall n \geq N_2$, we have $|b_n - b| < \epsilon/2$. Let $N = \max\{N_1, N_2\}$. Then $\forall n \geq N$, $|(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b| < \epsilon$.

(v) Given $\epsilon > 0$, Then there exists N_1, N_2, N_3 s.t.

$$\forall n \geq N_1 : |a_n - a| < \frac{\epsilon}{2(|b| + 1)}$$
$$\forall n \geq N_2 : |b_n - b| < \frac{\epsilon}{2|a|}$$
$$\forall n \geq N_3 : |b_n - b| < 1 \Rightarrow |b_n| < |b| + 1$$

Then let $N = \max\{N_1, N_2, N_3\}$. Then $\forall n \geq N$,

$$\begin{aligned} |a_n b_n - ab| &= |b_n(a_n - a) + a(b_n - b)| \\ &\leq |b_n||a_n - a| + |a||b_n - b| \\ &< (|b| + 1)|a_n - a| + |a||b_n - b| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$

(vi) Given $\epsilon > 0$, then $\exists N_1, N_2$ s.t. $|a_n - a| < \frac{|a|^2}{2}\epsilon$ and $|a_n - a| < \frac{|a|}{2}$.
Let $N = \max\{N_1, N_2\}$. The $\forall n \geq N$,

$$\begin{aligned} \left|\frac{1}{a_n} - \frac{1}{a}\right| &= \frac{|a_n - a|}{|a_n||a|} \\ &< \frac{2}{|a|^2}|a_n - a| < \epsilon \end{aligned}$$

(vii) By (iii) to (v), we know that $b_n - a_n \to 0$. Let $\epsilon > 0$. Then $\exists N$ s.t. $\forall n \geq N$, we have $|b_n - a_n| < \epsilon$. So $|c_n - a_n| < \epsilon$. So $c_n - a_n \to 0$. So $c_n = (c_n - a_n) + a_n \to a$.

□

5.4 Series

Definition. Let a_n be a sequence. Then $s_m = \sum_{n=1}^{m} a_n$ is the *mth partial sum* of the *series* whose nth term is a_n. We write $\sum_{n=1}^{\infty} a_n = \lim_{m\to\infty} s_m$ If the limit exists.

Example. Suppose $a_n = r^n$, where $|r| < 1$. Then $s_m = r \cdot \frac{1-r^m}{1-r} \to \frac{r}{1-r}$ since $r^n \to 0$. So $\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$.

5.4.1 Decimal expansions

Definition. Let (d_n) be a sequence with $d_n \in \{0, 1, \cdots 9\}$. Then $\displaystyle\sum_{n=1}^{\infty} \frac{d}{10^n}$ converges to a limit r with $0 \leq r \leq 1$ since the partial sums s_m are increasing and bounded by $\sum \frac{9}{10^n} \to 1$ (geometric series). We say $r = 0.d_1 d_2 d_3 \cdots$, the *decimal expansion* of r.

Does every x with $0 \leq x < 1$ have a decimal expansion? Pick d_1 maximal such that $\frac{d_1}{10} \leq x < 1$. Then $0 \leq x - \frac{d_1}{10} < \frac{1}{10}$ since d_1 is maximal. Then pick d_2

maximal such that $\frac{d_2}{100} \le x - \frac{d_1}{10}$. By maximality, $0 \le x - \frac{d_1}{10} - \frac{d_2}{100} < \frac{1}{100}$. Repeat inductively, pick maximal

$$\frac{d_n}{10^n} \le x - \sum_{j=1}^{n-1} \frac{d_j}{10^j} \Rightarrow 0 \le x - \sum_{j=1}^{n} \frac{d_j}{10^j} < \frac{1}{10^n}.$$

Since both LHS and RHS $\to 0$, by sandwich, $x - \sum_{j=1}^{\infty} \frac{d_j}{10^j} = 0$, i.e. $x = 0.d_1 d_2 \cdots$.

Since we have shown that at least one decimal expansion, can the same number have two different decimal expansions? Now suppose that the a_j and b_j are equal until k, i.e. $a_j = b_j$ for $j < k$. wlog assume $a_k < b_k$. Then

$$\sum_{j=k+1}^{\infty} \frac{a_j}{10^j} \le \sum_{j=k+1}^{\infty} \frac{9}{10^j} = \frac{9}{10^j} \cdot \frac{1}{1 - 1/10} = \frac{1}{10^k}.$$

So we must have $b_k = a_k + 1$, $a_j = 9$ for $j > k$ and $b_j = 0$ for $j > k$. $(0.47999\cdots = 0.48000\cdots)$.

5.5 Irrational numbers

Definition. Numbers in $\mathbb{R} \setminus \mathbb{Q}$ are *irrational*. A decimal is *periodic* if after a finite number ℓ of digits, it repeats in blocks of k for some k. (it is rational)

Proof. Clearly a periodic decimal is rational.

Conversely, let $x \in \mathbb{Q}$. Then x has a periodic decimal. Suppose $x = \frac{p}{2^c 5^d q}$ with $(q, 10) = 1$. Then $10^{\max(c,d)} x = \frac{a}{q} = n + \frac{b}{q}$ for some $a, b, n \in \mathbb{Z}$ and $0 \le b < q$. However, since $(q, 10) = 1$, by Fermat-Euler, $10^{\phi(q)} \equiv 1 \pmod{q}$, i.e. $10^{\phi(q)} - 1 = kq$ for some k. Then

$$\frac{b}{q} = \frac{kb}{kq} = \frac{kb}{999\cdots 9} = kb\left(\frac{1}{10^{\phi(q)}} + \frac{1}{10^{2\phi(q)}} + \cdots\right).$$

Since $kb < kq$, write $kb = d_1 d_2 \cdots d_{\phi(q)}$. So $\frac{b}{q} = 0.d_1 d_2 \cdots d_{\phi(q)} d_1 d_2 \cdots$ and x is periodic. □

Example. $x = 0.01101010001010\cdots$, where 1s appear in prime positions, is irrational since the digits don't repeat.

5.6 Euler's number

Definition.

$$e = \sum_{j=0}^{\infty} \frac{1}{1!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

Proposition. e is irrational.

Proof. Is $e \in \mathbb{Q}$? Suppose $e = \frac{p}{q}$. We know $q \geq 2$ since e is not an integer (it is between 2 and 3). Then $q!e \in \mathbb{N}$. But

$$q!e = \underbrace{q! + q! + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{q!}}_{n} + \underbrace{\frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \cdots}_{x},$$

where $n \in \mathbb{N}$. We also have $x = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \cdots$. This is a contradiction since $q!e$ must be in $\mathbb{N}$ but it is a sum of an integer n plus a non-integer x. □

5.7 Algebraic numbers

Definition (Algebraic and transcendental numbers)**.** An *algebraic number* is a root of a polynomial with integer coefficients (or rational coefficients). A number is *transcendental* if it is not algebraic.

Theorem. (Liouville 1851; Non-examinable) L is transcendental, where

$$L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000100\cdots$$

with 1s in the factorial positions.

Proof. Suppose instead that $f(L) = 0$ where $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$, where $a_i \in \mathbb{Z}$, $a_k \neq 0$.

For any rational p/q, we have

$$f\left(\frac{p}{q}\right) = a_k \left(\frac{p}{q}\right)^k + \cdots + a_0 = \frac{\text{integer}}{q^k}.$$

So if p/q is not a root of f, then $f(p/q) \geq q^{-k}$.

For any m, we can write $L =$ first m terms + rest of the terms $= s + t$.

Now consider $|f(s)| = |f(L) - f(s)|$ (since $f(L) = 0$). We have

$$\begin{aligned} |f(L) - f(s)| &= \left|\sum a_i(L^i - s^i)\right| \leq \sum |a_i(L^i - s^i)| \\ &= \sum |a_i|(L-s)(L^{i-1} + \cdots + s^{i-1}) \leq \sum |a_i|(L-s)i, \\ &= (L-s)\sum i|a_i| = tC \end{aligned}$$

with $C = \sum i|a_i|$.

Writing s as a fraction, its denominator is at most $10^{m!}$. So $|f(s)| \geq 10^{-k\times m!}$. Combining with the above, we have $tC \geq 10^{-k\times m!}$.

We can bound t by

$$t = \sum_{j=m+1}^{\infty} 10^{-j!} \leq \sum_{\ell=(m+1)!}^{\infty} 10^{\ell} = \frac{10}{9} 10^{-(m+1)!}.$$

So $(10C/9)10^{-(m+1)!} \geq 10^{-k\times m!}$. Pick $m \in \mathbb{N}$ so that $m \geq k$ and $10^{m!} > \frac{10C}{9}$. This is always possible since both k and $10C/9$ are constants. Then the inequality gives $10^{-(m+1)} \geq 10^{-k}$, which is a contradiction since $m \geq k$. □

Note. Hermite (1873) showed that e is transcendental. Lindemann (1882) showed that π is transcendental.

6 Countability

Lemma. If $f : [n] \to [n]$ is injective then f is surjective.

Proof. By induction on n. It is true for n=1. Let $n > 1$, Let $J = f(n)$. let $g : [n] \to [n]$

$$g(j) = n, g(n) = j, g(i) = i(i \neq j, n)$$

The map $g \circ f$ fixes n. So the map $h : [n-1] \to [n-1]$ defined by $h(i) = g \circ f(i)$ is well defined and injective. By induction it is surjective, i.e. bijective. Hence $g \circ f$ is bijective. □

Corollary. If A is a set and A has a bijection to $[n]$ and a bijection to $[m]$. Then $n = m$.

Proof. We may assume $m \geq n$. Let $h : [n] \to [m]$ be the injective identity map. Then $[m] \to A \to [n] \to [m]$ is injective. By lemma it is also surjective. So h surjective so $n \geq m$. Hence n=m. □

Definition. The set A is *finite* if there exists $n \in N$ and a bijection $A \to [n]$ (or A is $\emptyset$). The *size* of A is n, written $|A|$. by corollary, it is well defined.

Lemma. Let $S \subseteq N$, then either S is finite or there is a bijection $g : \mathbb{N} \to S$.

Proof. If S is not empty, there is by WOP, a least element. Take out that element s_1 and if it is non-empty, take out the next least element s_2. Repeat. If it stops then $S = \{s_1, s_2, \ldots, s_n\}$ which is finite. If it goes on forever then the map from $\mathbb{N} \to S$ with $g(i) = s_i$ is well defined, and it is injective and surjective. (at most k elements of S less than k, so $k = s_i$ for some $i \leq k$) □

Definition. The set A is *countable* if A is finite or there is a bijection from $A \to \mathbb{N}$.

Theorem. The following are equivalent:

(i) A is countable.

(ii) there is an injection $A \to \mathbb{N}$

(iii) A = $\emptyset$ or there is a surjection from $\mathbb{N} \to A$.

Proof. Plainly $(i) \Rightarrow (ii)$. Conversely, if there is an injection $f : A \to \mathbb{N}$. then f gives bijection from A and f(A). If S is finite, so is A. If S is infinite, there is bijection from S to $\mathbb{N}$ so that $A \to S \to N$ is a bijection. So$(ii) \Rightarrow (i)$. Plainly $(i) \Rightarrow (iii)$. Conversely, if $A \neq \emptyset$ and $f : \mathbb{N} \to A$ is a surjection. Define a map $f : A \to \mathbb{N}$ by $g(a) = min f^{-1}(\{a\})$ which exists by WOP. Thus g is an injection, so by (ii) A is countable. Thus $(iii) \Rightarrow (i)$. □

Since $\mathbb{Z}$ is countable we have injection $\mathbb{Z} \to \mathbb{N}$. So injection

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

This shows hat rationals are countable ($\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$) By Induction $\mathbb{Z}^k$ is countable.

Theorem. A countable union of countable sets is countable.

Proof. Let I be a countable index set, and for each $\alpha \in I$, let A_α be a countable set. We need to show that $\bigcup_{\alpha \in I} A_\alpha$ is countable. It is enough to construct an injection $h : \bigcup_{\alpha \in I} A_\alpha \to \mathbb{N} \times \mathbb{N}$ because $\mathbb{N} \times \mathbb{N}$ is countable. We know that I is countable. So there exists an injection $f : I \to \mathbb{N}$. For each $\alpha \in I$, there exists an injection $g_\alpha : A_\alpha \to \mathbb{N}$.

For $a \in \bigcup A_\alpha$, pick $m = \min\{j \in \mathbb{N} : a \in A_\alpha \text{ and } f(\alpha) = j\}$. Then $h(a) = (m, g_\alpha(a))$ is an injection. □

Proposition. $\mathbb{Q}$ is countable.

Proof. $\mathbb{Q}$ can be mapped injectively to $\mathbb{Z} \times \mathbb{N}$ by $a/b \mapsto (a, b)$, where $b > 0$ and $(a, b) = 1$. □

Theorem. The set of algebraic numbers is countable.

Proof. Let $\mathcal{P}_k$ be the set of polynomials of degree k with integer coefficients. Then $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0 \mapsto (a_k, a_{k-1}, \cdots, a_0)$ is an injection $\mathcal{P}_k \to \mathbb{Z}^{k+1}$. Let $\mathcal{P}$ be the set of all polynomials with integer coefficients. Then clearly $\mathcal{P} = \bigcup \mathcal{P}_k$. So $\mathcal{P}$ is countable.

For each polynomial $p \in \mathcal{P}$, let R_p be the set of its roots. Then R_p is finite and thus countable. Hence $\bigcup_{p \in \mathcal{P}} R_p$, the set of all algebraic numbers, is countable. □

Theorem. The set of real numbers $\mathbb{R}$ is uncountable.

Proof. (Cantor's diagonal argument) Assume $\mathbb{R}$ is countable. Then we can list the reals as $r_1, r_2, r_3 \cdots$ so that every real number is in the list. Write each r_n in binary form:

$$\begin{aligned} r_1 &= n_1 \,.\, d_{11}\, d_{12}\, d_{13}\, d_{14} \cdots \\ r_2 &= n_2 \,.\, d_{21}\, d_{22}\, d_{23}\, d_{24} \cdots \\ r_3 &= n_3 \,.\, d_{31}\, d_{32}\, d_{33}\, d_{34} \cdots \\ r_4 &= n_4 \,.\, d_{41}\, d_{42}\, d_{43}\, d_{44} \cdots \end{aligned}$$

Define $r = 0 \,.\, d_1\, d_2\, d_3\, d_4 \cdots$ by $d_n = 1 - d_{nn} \pmod 2$ Then by construction, this differs from the nth number in the list by the nth digit, and is so different from every number in the list. Then r is a real number but not in the list. Contradiction. □

Corollary. There are uncountable many transcendental numbers.

Proof. If not, then the reals, being the union of the transcendentals and algebraic numbers, must be countable. But the reals is uncountable. □

Theorem. Let A be a set. Then there is no surjection from $A \to \mathcal{P}A$.

Proof. Suppose $f : A \to \mathcal{P}(A)$ surjectively. Let $S = \{a \in A : a \notin f(a)\}$. Since f is surjective, there must exist $s \in A$ such that $f(s) = S$. If $s \in S$, then $s \notin S$ by the definition of S. Conversely, if $s \notin S$, then $s \in S$. Contradiction. So f cannot exist. □

Theorem (Cantor-Schröder-Bernstein theorem)**.** Suppose there are injections $A \to B$ and $B \to A$. Then there's a bijection $A \leftrightarrow B$.

Continuum hypothesis. There is no set whose size lies between $\mathbb{N}$ and $\mathbb{R}$. In 1963, Paul Cohen proved that it is impossible to prove this or disprove this statement (in ZFC).