Part IA — Numbers and Sets

Theorems with proof

Based on lectures by A. G. Thomason

Notes taken by Dexter Chua

Michaelmas 2014

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. Euclid's proof of the infinity of primes. Euclid's 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

0 Introduction

1 Proofs and logic

1.1 Proofs

1.2 Examples of proofs

Proposition. For all natural numbers n, $n^3 - n$ is a multiple of 3.

Proof. We have $n^3 - n = (n-1)n(n+1)$. One of the three consecutive integers is divisible by 3. Hence so is their product. □

Proposition. If n^2 is even, then so is n.

Proof. If n is even, then $n = 2k$ for some integer k. Then $n^2 = 4k^2$, which is even. □

Proof. Suppose n is odd. Then $n = 2k + 1$ for some integer k. Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2) + 1$, which is odd. This contradicts our assumption that n^2 is even. □

Proposition. The solutions to $x^2 - 5x + 6 = 0$ are $x = 2$ and $x = 3$.

Proof.

(i) If $x = 2$ or $x = 3$, then $x - 2 = 0$ or $x - 3 = 0$. So $(x - 2)(x - 3) = 0$.

(ii) If $x^2 - 5x + 6 = 0$, then $(x - 2)(x - 3) = 0$. So $x - 2 = 0$ or $x - 3 = 0$. Then $x = 2$ or $x = 3$.

Note that the second direction is simply the first argument reversed. We can write this all in one go:

$$\begin{aligned} x = 3 \text{ or } x = 2 &\Leftrightarrow x - 3 = 0 \text{ or } x - 2 = 0 \\ &\Leftrightarrow (x - 3)(x - 2) = 0 \\ &\Leftrightarrow x^2 - 5x - 6 = 0 \end{aligned}$$

Note that we used the "if and only if" sign between all lines. □

Proposition. Every positive number is ≥ 1.

Proof. Let r be the smallest positive real. Then either $r < 1$, $r = 1$ or $r > 1$.

If $r < 1$, then $0 < r^2 < r$. Contradiction. If $r > 1$, then $0 < \sqrt{r} < r$. Contradiction. So $r = 1$. □

1.3 Logic

2 Sets, functions and relations

2.1 Sets

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

Proposition.

- $(A \cap B) \cap C = A \cap (B \cap C)$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.2 Functions

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

Proof. ($\Rightarrow$) If the left inverse g exists, then $\forall a, a' \in A, f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \Rightarrow a = a'$. Therefore f is injective.

($\Leftarrow$) If f is injective, we can construct a g defined as

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

Then g is a left inverse of f. □

Theorem. The right inverse of f exists iff f is surjective.

Proof. ($\Rightarrow$) We have $f(g(B)) = B$ since $f \circ g$ is the identity function. Thus f must be surjective since its image is B.

($\Leftarrow$) If f is surjective, we can construct a g such that for each $b \in B$, pick one $a \in A$ with $f(a) = b$, and put $g(b) = a$. □

2.3 Relations

Theorem. If $\sim$ is an equivalence relation on A, then the equivalence classes of $\sim$ form a partition of A.

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 $a \sim c, b \sim c$. By symmetry, $c \sim b$. By transitivity, 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 $[a] = [b]$. □

3 Division

3.1 Euclid's Algorithm

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

Proof. Choose $q = \max\{q : qb \leq a\}$. This maximum exists because the set of all q such that $qb \leq a$ is finite. Now write $r = a - qb$. We have $0 \leq r < b$ and thus q and r are found.

To show that they are unique, suppose that $a = qb + r = q'b + r'$. We have $(q - q')b = (r' - r)$. Since both r and r' are between 0 and b, we have $-b < r - r' < b$. However, $r' - r$ is a multiple of b. Thus $q - q' = r' - r = 0$. Consequently, $q = q'$ and $r = r'$. □

Proposition. If $c \mid a$ and $c \mid b$, $c \mid (ua + vb)$ for all $u, v \in \mathbb{Z}$.

Proof. By definition, we have $a = kc$ and $b = lc$. Then $ua + vb = ukc + vlc = (uk + vl)c$. So $c \mid (ua + vb)$. □

Theorem. Let $a, b \in \mathbb{N}$. Then (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 member of S. Say $d = xa + yb$. Hence if $c \mid a, c \mid b$, then $c \mid d$. So we need to show that $d \mid a$ and $d \mid b$, and thus $d = (a, b)$.

By the division algorithm, there exist numbers $q, r \in \mathbb{Z}$ with $a = qd + r$ with $0 \leq r < d$. Then $r = a - qd = a(1 - qx) - qyb$. Therefore r is a linear combination of a and b. Since d is the smallest positive member of S and $0 \leq r < d$, we have $r = 0$ and thus $d \mid a$. Similarly, we can show that $d \mid b$. □

Corollary. (from the proof) Let $d = (a, b)$, then d is the smallest positive linear combination of a and b.

Corollary (Bézout's identity)**.** Let $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then there exists $u, v \in \mathbb{Z}$ with $c = ua + vb$ iff $(a, b) \mid c$.

Proof. ($\Rightarrow$) Let $d = (a, b)$. If c is a linear combination of a and b, then $d \mid c$ because $d \mid a$ and $d \mid b$.

($\Leftarrow$) Suppose that $d \mid c$. Let $d = xa + yb$ and $c = kd$. Then $c = (kx)a + (ky)b$. Thus c is a linear combination of a and b. □

Proposition (Euclid's Algorithm)**.** If we continuously break down a and b by the following procedure:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

then the highest common factor is r_{n-1}.

Proof. We have (common factors of a, b) = (common factors of b, r_1) = (common factors of r_1, r_2) = $\cdots$ = (factors of r_{n-1}). □

3.2 Primes

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

Proof. If $n \in \mathbb{N}$ is not a prime itself, then by definition $n = ab$. If either a or b is not prime, then that number can be written as a product, say $b = cd$. Then $n = acd$ and so on. Since these numbers are getting smaller, and the process will stop when they are all prime. □

Theorem. There are infinitely many primes.

Proof. (Euclid's proof) Suppose there are finitely many primes, say $p_1, p_2 \cdots p_n$. Then $N = p_1 p_2 \cdots p_n + 1$ is divisible by none of the primes. Otherwise, $p_j \mid (N - p_1 p_2 \cdots p_n)$, i.e. $p_j \mid 1$, which is impossible. However, N is a product of primes, so there must be primes not amongst $p_1, p_2 \cdots p_n$. □

Proof. (Erdös 1930) Suppose that there are finitely many primes, $p_1, p_2 \cdots p_k$. Consider all numbers that are the products of these primes, i.e. $p_1^{j_1} p_2^{j_2} \cdots p_k^{j_k}$, where $j_i \geq 0$. Factor out all squares to obtain the form $m^2 p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$, where $m \in \mathbb{N}$ and $i_j = 0$ or 1.

Let $N \in \mathbb{N}$. Given any number $x \leq N$, when put in the above form, we have $m \leq \sqrt{N}$. So there are at most $\sqrt{N}$ possible values of m. For each m, there are 2^k numbers of the form $m^2 p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$. So there are only $\sqrt{N} \times 2^k$ possible values of x of this kind.

Now pick $N \geq 4^k$. Then $N > \sqrt{N} \times 2^k$. So there must be a number $\leq N$ not of this form, i.e. it has a prime factor not in this list. □

Theorem. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Proof. From Euclid's algorithm, there exist integers $u, v \in \mathbb{Z}$ such that $ua + vb = 1$. So multiplying by c, we have $uac + vbc = c$. Since $a \mid bc$, $a \mid$LHS. So $a \mid c$. □

Corollary. If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. (True for all p, a, b)

Proof. We know that $(p, a) = p$ or 1 because p is a prime. If $(p, a) = p$, then $p \mid a$. Otherwise, $(p, a) = 1$ and $p \mid b$ by the theorem above. □

Corollary. If p is a prime and $p \mid n_1 n_2 \cdots n_i$, then $p \mid n_i$ for some i.

Theorem (Fundamental Theorem of Arithmetic)**.** Every natural number is expressible as a product of primes in exactly one way. In particular, if $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, where p_i, q_i are primes but not necessarily distinct, then $k = l$. $q_1, \cdots q_l$ are $p_1, \cdots p_k$ in some order.

Proof. Since we already showed that there is at least one way above, we only need to show uniqueness.

Let $p_1 \cdots p_k = q_1 \cdots q_l$. We know that $p_1 \mid q_1 \cdots q_l$. Then $p_1 \mid q_1(q_2 q_3 \cdots q_l)$. Thus $p_1 \mid q_i$ for some i. wlog assume $i = 1$. Then $p_1 = q_1$ since both are primes. Thus $p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l$. Likewise, we have $p_2 = q_2, \cdots$ and so on. □

Corollary. If $a = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r}$ and $b = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}$, where p_i are distinct primes (exponents can be zero). Then $(a, b) = \prod p_k^{\min\{i_k, j_k\}}$. Likewise, $\mathrm{lcm}(a, b) = \prod p_k^{\max\{i_k, j_k\}}$. We have $\mathrm{hcf}(a, b) \times \mathrm{lcm}(a, b) = ab$.

4 Counting and integers

4.1 Basic counting

Theorem (Pigeonhole Principle)**.** If we put $mn + 1$ pigeons into n pigeonholes, then some pigeonhole has at least $m + 1$ pigeons.

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) $i_{A\cup B} = 1 - i_{\overline{A\cup B}} = 1 - i_{\bar{A}\cap\bar{B}} = 1 - i_{\bar{A}}i_{\bar{B}} = 1 - (1 - i_A)(1 - i_B) = i_A + i_B - i_{A\cap B}$.

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

Proposition. $|A \cup B| = |A| + |B| - |A \cap B|$

Proof.

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

Theorem (Inclusion-Exclusion Principle)**.** Let A_i be subsets of a finite set X, for $1 \le i \le n$. Then

$$|\bar{A}_1 \cap \cdots \cap \bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^n |A_1 \cap \cdots A_n|.$$

Equivalently,

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

The two forms are equivalent since $|A_1 \cup \cdots \cup A_n| = |X| - |\bar{A}_1 \cap \cdots \cap \bar{A}_n|$.

Proof. Using indicator functions,

$$\begin{aligned}i_{\bar{A}_1\cap\bar{A}_2\cap\cdots\cap\bar{A}_n} &= \prod_j i_{\bar{A}_j}\\ &= \prod_j (1 - i_{A_j})\\ &= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i} i_{A_j} - \cdots + (-1)^n i_{A_1} i_{A_2} \cdots i_{A_n}\\ &= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i\cap A_j} - \cdots + (-1)^n i_{A_1\cap A_2\cap A_3\cap\cdots\cap A_n}\end{aligned}$$

Thus

$$\begin{aligned}|\bar{A}_1 \cap \cdots \cap \bar{A}_n| &= \sum_{x\in X} i_{\bar{A}_1\cap\bar{A}_2\cap\cdots\cap\bar{A}_n}(x)\\ &= \sum_x 1 - \sum_i\sum_x i_{A_i}(x) + \sum_{i<j}\sum_x i_{A_i\cap A_j}(x) - \cdots\\ &+ \sum_x (-1)^n i_{A_1\cap A_2\cap A_3\cap\cdots\cap A_n}(x)\\ &= |X| - \sum_i |A_i| + \sum_{i<j}|A_i\cap A_j|\\ &- \sum_{i<j<k}|A_i\cap A_j\cap A_k| + \cdots + (-1)^n|A_1\cap A_2\cap\cdots A_n| \qquad \square\end{aligned}$$

4.2 Combinations

Proposition. By definition,

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

Theorem (Binomial 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 $(a+b)^n = (a+b)(a+b)\cdots(a+b)$. When we expand the product, we get all terms attained by choosing b from some brackets, a from the rest. The term $a^{n-r}b^r$ comes from choosing b from r brackets, a from the rest, and there are $\binom{n}{r}$ ways to make such a choice. $\square$

Proposition.

(i) $\binom{n}{r} = \binom{n}{n-r}$. This is because choosing r things to keep is the same as choosing $n-r$ things to throw away.

(ii) $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ (Pascal's identity) The RHS counts the number of ways to choose a team of r players from $n+1$ available players, one of whom is Pietersen. If Pietersen is chosen, there are $\binom{n}{r-1}$ ways to choose the remaining players. Otherwise, there are $\binom{n}{r}$ ways. The total number of ways is thus $\binom{n}{r-1} + \binom{n}{r}$.

Now given that $\binom{n}{0} = \binom{n}{n} = 1$, since there is only one way to choose nothing or everything, we can construct *Pascal's triangle*:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
\end{array}$$

where each number is the sum of the two numbers above it, and the rth item of the nth row is $\binom{n}{r}$ (first row is row 0).

(iii) $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$. We are counting the number of pairs of sets (Y, Z) with $|Y| = k$ and $|Z| = r$ with $Z \subseteq Y$. In the LHS, we first choose Y then choose $Z \subseteq Y$. The RHS chooses Z first and then choose the remaining $Y \setminus Z$ from $\{1, 2, \cdots n\} \setminus Z$.

(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) Suppose we have a men and b women, and we need to choose a committee of r people. The right hand side is the total number of choices. The left hand side breaks the choices up according to the number of men vs women.

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

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

4.3 Well-ordering and induction

Theorem (Weak Principle of Induction)**.** Let $P(n)$ be a statement about the natural number n. Suppose that

(i) $P(1)$ is true

(ii) $(\forall n)\, P(n) \Rightarrow P(n+1)$

Then $P(n)$ is true for all $n \geq 1$.

Theorem. Inclusion-exclusion principle.

Proof. Let $P(n)$ be the statement "for any sets $A_1 \cdots A_n$", we have $|A_1 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots \pm |A_i \cap A_2 \cap \cdots \cap A_n|$".

$P(1)$ is trivially true. $P(2)$ is also true (see above). Now given $A_1 \cdots A_{n+1}$, Let $B_i = A_i \cap A_{n+1}$ for $1 \leq i \leq n$. We apply $P(n)$ both to the A_i and B_i.

Now observe that $B_i \cap B_j = A_i \cap A_j \cap A_{n+1}$. Likewise, $B_i \cap B_j \cap B_k = A_i \cap A_j \cap A_k \cap A_{n+1}$. Now

$$\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_{n+1}| &= |A_1 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup \cdots \cup A_n) \cap A_{n+1}| \\
&= |A_1 \cup \cdots \cup A_n| + |A_{n+1}| - |B_1 \cup \cdots \cup B_n| \\
&= \sum_{i \leq n} |A_i| - \sum_{i<j \leq n} |A_i \cap A_j| + \cdots + |A_{n+1}| \\
&\quad - \sum_{i \leq n} |B_i| + \sum_{i<j \leq n} |B_i \cap B_j| - \cdots
\end{aligned}$$

Note $\sum_{i\le n} |B_i| = \sum_{i\le n} |A_i \cap A_{n+1}|$. So $\sum_{i<j\le n} |A_i \cap A_j| + \sum_{i\le n} |B_i| = \sum_{i<j\le n+1} |A_i \cap A_j|$, and similarly for the other terms. So

$$= \sum_{i\le n+1} |A_i| - \sum_{i<j\le n+1} |A_i \cap A_j| + \cdots$$

So $P(n) \Rightarrow P(n+1)$ for $n \ge 2$. By WPI, $P(n)$ is true for all n. □

Theorem (Strong principle of induction)**.** Let $P(n)$ be a statement about $n \in \mathbb{N}$. Suppose that

(i) $P(1)$ is true

(ii) $\forall n \in N$, if $P(k)$ is true $\forall k < n$ then $P(n)$ is 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 the strong principle implies the weak principle since if $P(n) \Rightarrow P(n+1)$, then $(P(1) \wedge P(2) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1)$.

Now show that the weak principle implies the strong principle. Suppose that $P(1)$ is true and $(\forall n)\, P(1) \wedge P(2) \wedge \cdots \wedge P(n-1) \Rightarrow P(n)$. We want to show that $P(n)$ is true for all n using the weak principle.

Let $Q(n) =$ "$P(k)$ is true $\forall k \le n$". Then $Q(1)$ is true. Suppose that $Q(n)$ is true. Then $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ is true. So $P(n+1)$ is true. Hence $Q(n+1)$ is true. By the weak principle, $Q(n)$ is true for all n. So $P(n)$ is true for all n. □

Theorem (Well-ordering principle)**.** $\mathbb{N}$ is well-ordered under the usual order, i.e. every non-empty subset of $\mathbb{N}$ has a minimal element.

Theorem. The well-ordering principle is equivalent to the strong principle of induction.

Proof. First prove that well-ordering implies strong induction. Consider a proposition $P(n)$. Suppose $P(k)$ is true $\forall k < n$ implies $P(n)$.

Assume the contrary. Consider the set $S = \{n \in \mathbb{N} : \neg P(n)\}$. Then S has a minimal element m. Since m is the minimal counterexample to P, $P(k)$ is true for all $k < m$. However, this implies that $P(m)$ is true, which is a contradiction. Therefore $P(n)$ must be true for all n.

To show that strong induction implies well-ordering, let $S \subseteq \mathbb{N}$. Suppose that S has no minimal element. We need to show that S is empty. Let $P(n)$ be the statement $n \notin S$.

Certainly $1 \notin S$, or else it will be the minimal element. So $P(1)$ is true. Suppose we know that $P(k)$ is true for all $k < n$, i.e. $k \notin S$ for all $k < n$. Now $n \notin S$, or else n will be the minimal element. So $P(n)$ is true. By strong induction, $P(n)$ is true for all n, i.e. S is empty. □

5 Modular arithmetic

5.1 Modular arithmetic

Proposition. If $a \equiv b \pmod m$, and $d \mid m$, then $a \equiv b \pmod d$.

Proof. $a \equiv b \pmod m$ if and only if $m \mid (a-b)$, hence $d \mid (a-b)$, i.e. $a \equiv b \pmod d$. □

Proposition. If $a \equiv b \pmod m$ and $u \equiv v \pmod m$, then $a+u \equiv b+v \pmod m$ and $au \equiv bv \pmod m$.

Proof. Since $a \equiv b \pmod m$ and $u \equiv v \pmod m$, we have $m \mid (a-b)+(u-v) = (a+u)-(b+v)$. So $a+u \equiv b+v \pmod m$

Since $a \equiv b \pmod m$ and $u \equiv v \pmod m$, we have $m \mid (a-b)u+b(u-v) = au-bv$. So $au \equiv bv \pmod m$. □

Theorem. There are infinitely many primes that are $\equiv -1 \pmod 4$.

Proof. Suppose not. So let $p_1, \cdots p_k$ be all primes $\equiv -1 \pmod 4$. Let $N = 4p_1p_2\cdots p_k - 1$. Then $N \equiv -1 \pmod 4$. Now N is a product of primes, say $N = q_1q_2\cdots q_\ell$. But $2 \nmid N$ and $p_i \nmid N$ for all i. So $q_i \equiv 1 \pmod 4$ for all i. But then that implies $N = q_1q_2\cdots q_\ell \equiv 1 \pmod 4$, which is a contradiction. □

Theorem. u is a unit modulo m if and only if $(u, m) = 1$.

Proof. ($\Rightarrow$) Suppose u is a unit. Then $\exists v$ such that $uv \equiv 1 \pmod m$. Then $uv = 1 + mn$ for some n, or $uv - mn = 1$. So 1 can be written as a linear combination of u and m. So $(u, m) = 1$.

($\Leftarrow$) Suppose that $(u, m) = 1$. Then there exists a, b with $ua + mb = 1$. Thus $ua \equiv 1 \pmod m$. □

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

Proof. If $ax \equiv b \pmod m$, and $(a, m) = 1$, then $\exists a^{-1}$ such that $a^{-1}a \equiv 1 \pmod m$. So $a^{-1}ax \equiv a^{-1}b \pmod m$ and thus $x \equiv a^{-1}b \pmod m$. Finally we check that $x \equiv a^{-1}b \pmod m$ is indeed a solution: $ax \equiv aa^{-1}b \equiv b \pmod m$. □

Proposition. There is a solution to $ax \equiv b \pmod m$ if and only if $(a, m) \mid b$.

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

Proof. Let $d = (a, m)$. If there is a solution to $ax \equiv b \pmod m$, then $m \mid ax - b$. So $d \mid ax - b$ and $d \mid b$.

On the contrary, if $d \mid b$, we have $ax \equiv b \pmod m \Leftrightarrow ax - b = km$ for some $k \in Z$. Write $a = da'$, $b = db'$ and $m = dm'$. So $ax \equiv b \pmod m \Leftrightarrow da'x - db' = dkm' \Leftrightarrow a'x - b' = km' \Leftrightarrow a'x \equiv b' \pmod{m'}$. Note that $(a', m') = 1$ since we divided by their greatest common factor. Then this has a unique solution modulo m'. □

5.2 Multiple moduli

Theorem (Chinese remainder theorem)**.** Let $(m, n) = 1$ and $a, b \in \mathbb{Z}$. Then there is a unique solution (modulo mn) to the simultaneous congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases},$$

i.e. $\exists x$ satisfying both and every other solution is $\equiv x \pmod{mn}$.

Proof. Since $(m, n) = 1$, $\exists u, v \in \mathbb{Z}$ with $um + vn = 1$. Then $vn \equiv 1 \pmod{m}$ and $um \equiv 1 \pmod{n}$. Put $x = umb + vna$. So $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

To show it is unique, suppose both y and x are solutions to the equation. Then

$$\begin{aligned} & y \equiv a \pmod{m} \text{ and } y \equiv b \pmod{n} \\ \Leftrightarrow\ & y \equiv x \pmod{m} \text{ and } y \equiv x \pmod{n} \\ \Leftrightarrow\ & m \mid y - x \text{ and } n \mid y - x \\ \Leftrightarrow\ & mn \mid y - x \\ \Leftrightarrow\ & y \equiv x \pmod{mn} \end{aligned}$$

□

Proposition. Given any $(m, n) = 1$, c is a unit mod mn iff c is a unit both mod m and mod n.

Proof. ($\Rightarrow$) If $\exists u$ such that $cu \equiv 1 \pmod{mn}$, then $cu \equiv 1 \pmod{m}$ and $cu \equiv 1 \pmod{n}$. So c is a unit mod m and n.

($\Leftarrow$) Suppose there exists u, v such that $cu \equiv 1 \pmod{m}$ and $cv \equiv 1 \pmod{n}$. Then by CRT, $\exists w$ with $w \equiv u \pmod{m}$ and $w \equiv v \pmod{n}$. Then $cw \equiv cu \equiv 1 \pmod{m}$ and $cw \equiv cv \equiv 1 \pmod{n}$.

But we know that $1 \equiv 1 \pmod{m}$ and $1 \equiv 1 \pmod{n}$. So 1 is a solution to $cw \equiv 1 \pmod{m}$, $cw \equiv 1 \pmod{n}$. By the "uniqueness" part of the Chinese remainder theorem, we must have $cw \equiv 1 \pmod{mn}$. □

Proposition.

(i) $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$, i.e. ϕ is multiplicative.

(ii) If p is a prime, $\phi(p) = p - 1$

(iii) If p is a prime, $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$

(iv) $\phi(m) = m \prod_{p|m}(1 - 1/p)$.

Proof. We will only prove (iv). In fact, we will prove it twice.

(i) Suppose $m = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$. Then

$$\begin{aligned} \phi(m) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_\ell^{k_\ell}) \\ &= p_1^{k_1}(1 - 1/p_1)p_2^{k_2}(1 - 1/p_2) \cdots p_\ell^{k_\ell}(1 - 1/p_\ell) \\ &= m \prod_{p|m}(1 - 1/p) \end{aligned}$$

(ii) Let $m = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$. Let $X = \{0, \cdots m - 1\}$. Let $A_j = \{x \in X : p_j \mid x\}$. Then $|X| = m$, $|A_j| = m/p_j$, $|A_i \cap A_j| = m/(p_i p_j)$ etc. So $\phi(m) = |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \bar{A}_\ell| = m \prod_{p|m}(1 - 1/p)$. □

5.3 Prime moduli

Theorem (Wilson's theorem)**.** $(p-1)! \equiv -1 \pmod{p}$ if p is a prime.

Proof. If p is a prime, then $1, 2, \cdots, p-1$ are units. Among these, we can pair each number up with its inverse (e.g. 3 with 4 in modulo 11). The only elements that cannot be paired with a different number are 1 and -1, who are self-inverses, as show below:

$$\begin{aligned} & x^2 \equiv 1 \pmod{p} \\ \Leftrightarrow\ & p \mid (x^2 - 1) \\ \Leftrightarrow\ & p \mid (x-1)(x+1) \\ \Leftrightarrow\ & p \mid x-1 \text{ or } p \mid x+1 \\ \Leftrightarrow\ & x \equiv \pm 1 \pmod{p} \end{aligned}$$

Now $(p-1)!$ is a product of $(p-3)/2$ inverse pairs together with 1 and -1. So the product is -1. □

Theorem (Fermat's little theorem)**.** Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Equivalently, $a^{p-1} \equiv 1 \pmod{p}$ if $a \not\equiv 0 \pmod{p}$.

Proof. Two proofs are offered:

(i) The numbers $\{1, 2, \cdots p-1\}$ are units modulo p and form a group of order $p-1$. So $a^{p-1} \equiv 1$ by Lagrange's theorem.

(ii) If $a \not\equiv 0$, then a is a unit. So $ax \equiv ay$ iff $x \equiv y$. Then $a, 2a, 3a, \cdots (p-1)a$ are distinct mod p. So they are congruent to $1, 2, \cdots p-1$ in some order. Hence $a \cdot 2a \cdots 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$. So $a^{p-1}(p-1)! \equiv (p-1)!$. So $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem (Fermat-Euler Theorem)**.** Let a, m be coprime. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof. Lagrange's theorem: The units mod m form a group of size $\phi(m)$.

Alternatively, let $U = \{x \in \mathbb{N} : 0 < x < m, (x, m) = 1\}$. These are the $\phi(m)$ units. Since a is a unit, $ax \equiv ay \pmod{m}$ only if $x \equiv y \pmod{m}$. So if $U = \{u_1, u_2, \cdots, u_{\phi(m)}\}$, then $\{au_1, au_2, \cdots au_{\phi(m)}\}$ are distinct and are units. So they must be $u_1, \cdots u_{\phi(m)}$ in some order. Then $au_1 au_2 \cdots au_{\phi(m)} \equiv u_1 u_2 \cdots u_{\phi(m)}$. So $a^{\phi(m)} z \equiv z$, where $z = u_1 u_2 \cdots u_{\phi(m)}$. Since z is a unit, we can multiply by its inverse and obtain $a^{\phi(m)} \equiv 1$. □

Proposition. If p is an odd prime, then -1 is a quadratic residue if and only if $p \equiv 1 \pmod{4}$.

Proof. If $p \equiv 1 \pmod{4}$, say $p = 4k+1$, then by Wilson's theorem, $-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \cdots (-2)(-1) \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!^2 = (-1)^{2k}(2k!)^2 \equiv (2k!)^2$. So -1 is a quadratic residue.

When $p \equiv -1 \pmod{4}$, i.e. $p = 4k+3$, suppose -1 is a square, i.e. $-1 \equiv z^2$. Then by Fermat's little theorem, $1 \equiv z^{p-1} \equiv z^{4k+2} \equiv (z^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1$. Contradiction. □

Proposition. (Unproven) A prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proposition. There are infinitely many primes $\equiv 1 \pmod 4$.

Proof. Suppose not, and $p_1, \cdots p_k$ are all the primes $\equiv 1 \pmod 4$. Let $N = (2p_1 \cdots p_k)^2 + 1$. Then N is not divisible by 2 or $p_1, \cdots, p_k$. Let q be a prime $q \mid N$. Then $q \equiv -1 \pmod 4$. Then $N \equiv 0 \pmod q$ and hence $(2p_1 \cdots p_k)^2 + 1 \equiv 0 \pmod q$, i.e. $(2p_1 \cdots p_k)^2 \equiv -1 \pmod q$. So -1 is a quadratic residue mod q, which is a contradiction since $q \equiv -1 \pmod 4$. □

Proposition. Let $p = 4k + 3$ be a prime. Then if a is a quadratic residue, i.e. $a \equiv z^2 \pmod p$ for some z, then $z = \pm a^{k+1}$.

Proof. By Fermat's little theorem, $a^{2k+1} \equiv z^{4k+2} \equiv z^{p-1} \equiv 1$. If we multiply by a, then $a^{2k+2} \equiv a \pmod p$. So $(\pm a^{k+1})^2 \equiv a \pmod p$. □

5.4 Public-key (asymmetric) cryptography

Theorem (RSA Encryption)**.** We want people to be able to send a message to Bob without Eve eavesdropping. So the message must be encrypted. We want an algorithm that allows anyone to encrypt, but only Bob to decrypt (e.g. many parties sending passwords with the bank).

Let us first agree to write messages as sequences of numbers, e.g. in ASCII or UTF-8.

After encoding, the encryption part is often done with RSA encryption (Rivest, Shamier, Adleman). Bob thinks of two large primes p, q. Let $n = pq$ and pick e coprime to $\phi(n) = (p-1)(q-1)$. Then work out d with $de \equiv 1 \pmod{\phi(n)}$ (i.e. $de = k\phi(n) + 1$). Bob then publishes the pair (n, e).

For Alice to encrypt a message, Alice splits the message into numbers $M < n$. Alice sends $M^e \pmod n$ to Bob.

Bob then computes $(M^e)^d = M^{k\phi(n)+1} \equiv M \pmod n$ by Fermat-Euler theorem.

How can Eve find M? We can, of course, factorize n, find d efficiently, and be in the same position as Bob. However, it is currently assumed that this is hard. Is there any other way? Currently we do not know if RSA can be broken without factorizing (cf. RSA problem).

6 Real numbers

6.1 Construction of numbers

Proposition. $\mathbb{Q}$ is a totally ordered-field.

Proposition. $\mathbb{Q}$ is densely ordered, i.e. for any $p, q \in \mathbb{Q}$, if $p < q$, then there is some $r \in \mathbb{Q}$ such that $p < r < q$.

Proof. Take $r = \frac{p+q}{2}$. □

Proposition. There is no rational $q \in \mathbb{Q}$ with $q^2 = 2$.

Proof. Suppose not, and $(\frac{a}{b})^2 = 2$, where b is chosen as small as possible. We will derive a contradiction in four ways.

(i) $a^2 = 2b^2$. So a is even. Let $a = 2a'$. Then $b^2 = 2a'^2$. Then b is even as well, and $b = 2b'$. But then $\frac{a}{b} = \frac{a'}{b'}$ with a smaller b'. Contradiction.

(ii) We know that b is a product of primes if $b \neq 1$. Let $p \mid b$. Then $a^2 = 2b^2$. So $p \mid a^2$. So $p \mid a$. Contradict b minimal.

(iii) (Dirichlet) We have $\frac{a}{b} = \frac{2b}{a}$. So $a^2 = 2b^2$. For any, u, v, we have $a^2v = 2b^2v$ and thus $uab + a^2v = uab + 2b^2v$. So $\frac{a}{b} = \frac{au+2bv}{bu+av}$. Put $u = -1, v = 1$. Then $\frac{a}{b} = \frac{2b-a}{a-b}$. Since $a < 2b, a - b < b$. So we have found a rational with smaller b.

(iv) Same as 3, but pick u, v so $bu + av = 1$ since a and b are coprime. So $\frac{a}{b}$ is an integer. □

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

Proof. Let S be non-empty and bounded below. Let L be the set of all lower bounds of S. Since S is bounded below, L is non-empty. Also, L is bounded above by any member of S. So L has a least upper bound $\sup L$.

For each $x \in S$, we know x is an upper bound of L. So we have $\sup L \leq x$ by definition. So $\sup L$ is indeed a lower bound of S. Also, by definition, every lower bound of S is less than (or equal to) $\sup L$. So this is the infimum. □

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. □

Proposition. $\inf\{\frac{1}{n} : n \in \mathbb{N}\} = 0$.

Proof. Certainly 0 is a lower bound for S. If $t > 0$, there exists $n \in \mathbb{N}$ such that $n \geq 1/t$. So $t \geq 1/n \in S$. So t is not a lower bound for S. □

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 $r < 0$ and swap r and s). Since $s - r > 0$, there is some $n \in \mathbb{N}$ such that $\frac{1}{n} < s - r$. 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 $N \in T$. 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 for every $r \in S$, we have $r \leq 3$. 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 $x + t \in S$. This contradicts the fact that x is an upper bound of S.

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. This contradicts the fact that x is the least upper bound of S.

So by trichotomy, $x^2 = 2$. □

6.2 Sequences

Theorem. Every bounded monotonic sequence converges.

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 (least upper bound axiom). Show that l is the limit:

Given any $\varepsilon > 0$, $l - \varepsilon$ is not an upper bound of a_n. So $\exists N$ such that $a_N \geq l - \varepsilon$. Since a_n is increasing, we know that $l \geq a_m \geq a_N > l - \varepsilon$ for all $m \geq N$. So $\exists N$ such that $\forall n \geq N$, $|a_n - l| < \varepsilon$. So $a_n \to l$. □

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 $a_{N_2} > a_{N_1}$. This is possible because a_{N_1} is not a peak. The pick a_{N_3} with $N_3 > N_2$ and $a_{N_3} > a_{N_2}$, *ad infinitum.* Then 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 $a_n \to a$.

(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 $\varepsilon = \frac{b-a}{2}$. By the definition of the limit, $\exists N_1$ such that $\forall n \geq N_1$, $|a_n - a| < \varepsilon$. There also $\exists N_2$ st. $\forall n \geq N_2$, $|a_n - b| < \varepsilon$.

Let $N = \max\{N_1, N_2\}$. If $n \geq \max\{N_1, N_2\}$, then $|a - b| \leq |a - a_n| + |a_n - b| < 2\varepsilon = b - a$. Contradiction. So $a = b$.

(ii) Given $\varepsilon > 0$, there $\exists N_1$ st. $\forall n \geq N_1$, we have $|a_n - a| < \varepsilon$. 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 $|b_n - a| = |a_n - a| < \varepsilon$. So $b_n \to a$.

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

(iv) Given $\varepsilon > 0$, $\exists N_1$ such that $\forall n \geq N_1$, we have $|a_n - a| < \varepsilon/2$. Similarly, $\exists N_2$ such that $\forall n \geq N_2$, we have $|b_n - b| < \varepsilon/2$.

Let $N = \max\{N_1, N_2\}$. Then $\forall n \geq N$, $|(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b| < \varepsilon$.

(v) Given $\varepsilon > 0$, Then there exists N_1, N_2, N_3 such that

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

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

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

(vi) Given $\varepsilon > 0$, then $\exists N_1, N_2$ such that $|a_n - a| < \frac{|a|^2}{2}\varepsilon$ and $|a_n - a| < \frac{|a|}{2}$.

Let $N = \max\{N_1, N_2\}$. The $\forall n \geq N$,

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

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

6.3 Series

6.4 Irrational numbers

Proposition. A number is periodic iff it is rational.

Proof. Clearly a periodic decimal is rational: Say $x = 0.7413157157157\cdots$. Then

$$\begin{aligned} 10^\ell x &= 10^4 x \\ &= 7413.157157\cdots \\ &= 7413 + 157\left(\frac{1}{10^3} + \frac{1}{10^6} + \frac{1}{10^9} + \cdots\right) \\ &= 7413 + 157 \cdot \frac{1}{10^3} \cdot \frac{1}{1 - 1/10^3} \in \mathbb{Q} \end{aligned}$$

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 $0 \leq b < q$. 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 $kb < kq < 10^{\phi(q)}$, 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. □

6.5 Euler's number

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

$$x = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \cdots.$$

We can bound it by

$$0 < x < \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots = \frac{1}{q+1} \cdot \frac{1}{1 - 1/(q+1)} = \frac{1}{q} < 1.$$

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. □

6.6 Algebraic numbers

Proposition. All rational numbers are algebraic.

Proof. Let $x = \frac{p}{q}$, then x is a root of $qx - p = 0$. □

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

Theorem. (Hermite 1873) e is transcendental.

Theorem. (Lindermann 1882) π is transcendental.

7 Countability

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

Proof. Perform induction on n: It is true for $n = 1$. Suppose $n > 1$. Let $j = f(n)$. Define $g : [n] \to [n]$ by

$$g(j) = n, \quad g(n) = j, \quad g(i) = i \text{ otherwise.}$$

Then g is a bijection. So the map $g \circ f$ is injective. It fixes n, i.e. $g \circ f(n) = n$. So the map $h : [n-1] \to [n-1]$ by $h(i) = g \circ f(i)$ is well-defined and injective. So h is surjective. So h is bijective. So $g \circ f$ is bijective. So is f. □

Corollary. If A is a set and $f : A \to [n]$ and $g : A \to [m]$ are both bijections, then $m = n$.

Proof. wlog assume $m \geq n$. Let $h : [n] \to [m]$ with $h(i) = i$, which is injective. Then the map $h \circ f \circ g^{-1} : [m] \to [m]$ is injective. Then by the lemma this is surjective. So h must be surjective. So $n \geq m$. Hence $n = m$. □

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

Proof. If $S \neq \emptyset$, by the well-ordering principle, there is a least element $s_1 \in S$. If $S \setminus \{s_1\} \neq \emptyset$, it has a least element s_2. If $S \setminus \{s_1, s_2\}$ is not empty, there is a least element s_3. If at some point the process stops, then $S = \{s_1, s_2, \cdots, s_n\}$, which is finite. Otherwise, if it goes on forever, the map $g : \mathbb{N} \to S$ given by $g(i) = s_i$ is well-defined and is an injection. It is also a surjection because if $k \in S$, then k is a natural number and there are at most k elements of S less than k. So k will be mapped to s_i for some $i \leq k$. □

Theorem. The following are equivalent:

(i) A is countable

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

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

Proof. (i) ⇒ (iii): If A is finite, there is a bijection $f : A \to S$ for some $S \subseteq \mathbb{N}$. For all $x \in \mathbb{N}$, if $x \in S$, then map $x \mapsto f^{-1}(x)$. Otherwise, map x to any element of A. This is a surjection since $\forall a \in A$, we have $f(a) \mapsto a$.

(iii) ⇒ (ii): If $A \neq \emptyset$ and $f : \mathbb{N} \to A$ is a surjection. Define a map $g : A \to \mathbb{N}$ by $g(a) = \min f^{-1}(\{a\})$, which exists by well-ordering. So g is an injection.

(ii) ⇒ (i): If there is an injection $f : A \to \mathbb{N}$, then f gives a bijection between A and $S = f(A) \subseteq \mathbb{N}$. If S is finite, so is A. If S is infinite, there is a bijection g between S and $\mathbb{N}$. So there is a bijection $g \circ f$ between A and $\mathbb{N}$. □

Proposition. The integers $\mathbb{Z}$ are countable.

Proof. The map $f : \mathbb{Z} \to \mathbb{N}$ given by

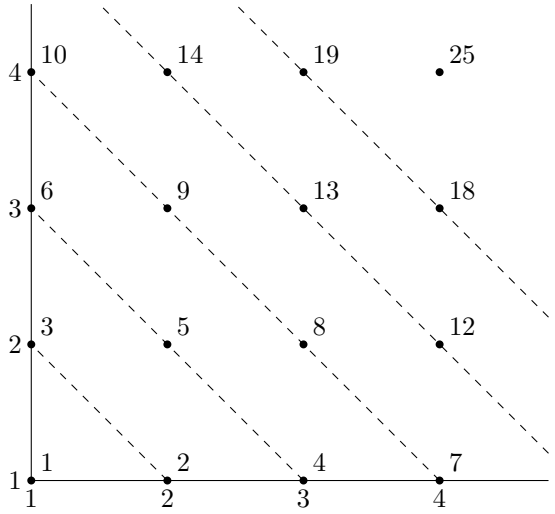
$$f(n) = \begin{cases} 2n & n > 0 \\ 2(-n) + 1 & n \leq 0 \end{cases}$$

is a bijection. □

Proposition. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. We can map $(a, b) \mapsto 2^a 3^b$ injectively by the fundamental theorem of arithmetic. So $\mathbb{N} \times \mathbb{N}$ is countable.

We can also have a bijection by counting diagonally: $(a, b) \mapsto \binom{a+b}{2} - a + 1$:



□

Proposition. If $A \to B$ is injective and B is countable, then A is countable (since we can inject $B \to \mathbb{N}$).

Proposition. $\mathbb{Z}^k$ is countable for all $k \in \mathbb{N}$

Proof. Proof by induction: $\mathbb{Z}$ is countable. If $\mathbb{Z}^k$ is countable, $\mathbb{Z}^{k+1} = \mathbb{Z} \times \mathbb{Z}^k$. Since we can map $\mathbb{Z}^k \to \mathbb{N}$ injectively by the induction hypothesis, we can map injectively $\mathbb{Z}^{k+1} \to \mathbb{Z} \times \mathbb{N}$, and we can map that to $\mathbb{N}$ injectively. □

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 $m = \min\{j \in \mathbb{N} : a \in A_\alpha \text{ and } f(\alpha) = j\}$, and let α be the corresponding index such that $f(\alpha) = m$. We then set $h(a) = (m, g_\alpha(a))$, and this is an injection. □

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

Proof. It can be proved in two ways:

(i) $\mathbb{Q} = \bigcup_{n \geq 1} \frac{1}{n}\mathbb{Z} = \bigcup_{n \geq 1} \left\{ \frac{m}{n} : m \in \mathbb{Z} \right\}$, which is a countable union of countable sets.

(ii) $\mathbb{Q}$ 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 $\mathcal{P}_k \to \mathbb{Z}^{k+1}$. Since $\mathbb{Z}^{k+1}$ is countable, so is $\mathcal{P}_k$.

Let $\mathcal{P}$ be the set of all polynomials with integer coefficients. Then clearly $\mathcal{P} = \bigcup \mathcal{P}_k$. This is a countable union of countable sets. 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 uniquely in decimal form (i.e. without infinite trailing '9's). List them out vertically:

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

Define $r = 0\,.\,d_1\, d_2\, d_3\, d_4 \cdots$ by $d_n = \begin{cases} 0 & d_{nn} \neq 0 \\ 1 & d_{nn} = 0 \end{cases}$. 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 $f : A \to \mathcal{P}(A)$ is surjective. 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 $A \leftrightarrow B$.