Q1. Let $A=\{(x,y): 0\le x\le 1,\ x\le y\le 1\}$ and $B=\{(x,y): 0\le y\le 1,\ 0\le x\le y\}$. Prove that $A=B$.

We need only to prove that $A\subseteq B$, and $B\subseteq A$

Proof: For any $(x,y)\in A$, we have $0\le x\le y\le 1$. So, $0\le y\le 1$ and $0\le x\le y$

$\Rightarrow (x,y)\in B \Rightarrow A\subseteq B$

When $(x,y)\in B$, we have $0\le x\le y\le 1$

So, $0\le x\le 1$ and $x\le y\le 1$, $\Rightarrow (x,y)\in A$

$\Rightarrow B\subseteq A$

This proves $A=B$ ※

Q2. Let $n \geq 1$ be an integer. Evaluate $\sum_{k=1}^{n} \binom{n}{k}$. Recall:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \quad \text{for any } x \in \mathbb{R}.$$

Sol: Let $x = 1$ to have

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

$$\Rightarrow \sum_{k=1}^{n} \binom{n}{k} = 2^n - 1 \quad \ddot{\smile}$$

Note: $0! = 1$

$(n+1)! = (n+1)(n!)$

$1! = 1 \cdot (0!)$

$\binom{k}{0} = \frac{k!}{0!\,(k-0)!} = 1$

$\forall\, k \geq 0$

(Q2. prac2) Use Gauss-Jordan method to invert

$$A = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}$$

Sol.

$$[A \quad I_{3\times 3}] = \begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ -1 & 2 & -1 & 0 & 1 & 0 \\ 0 & -1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$\frac{1}{2}R_1 + R_2 \to R_2$

$$\begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & 3/2 & -1 & 1/2 & 1 & 0 \\ 0 & -1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$\frac{2}{3}R_2 + R_3 \to R_3$

$$\begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & 3/2 & -1 & 1/2 & 1 & 0 \\ 0 & 0 & 4/3 & 1/3 & 2/3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\sim$

$\tilde{A}$ not invertible.

$A \neq 0$ invertible

$\frac{3}{4}R_3 + R_2 \to R_2$

$$\begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & 3/2 & 0 & 3/4 & 3/2 & 3/4 \\ 0 & 0 & 4/3 & 1/3 & 2/3 & 1 \end{bmatrix}$$

$\frac{2}{3}R_2 + R_1 \to R_1$

$$\begin{bmatrix} 2 & 0 & 0 & \frac{3}{2} & 1 & \frac{1}{2} \\ 0 & 3/2 & 0 & 3/4 & 3/2 & 3/4 \\ 0 & 0 & 4/3 & 1/3 & 2/3 & 1 \end{bmatrix}$$

$\frac{1}{2}R_1 \to R_1,\ \frac{2}{3}R_2 \to R_2,\ \frac{3}{4}R_3 \to R_3$

$$\begin{bmatrix} 1 & 0 & 0 & 3/4 & 1/2 & 1/4 \\ 0 & 1 & 0 & 1/2 & 1 & 1/2 \\ 0 & 0 & 1 & 1/4 & 1/2 & 3/4 \end{bmatrix}$$

A^{-1}.

(Q4/prac2) Let $W = \begin{bmatrix} A & 0 \\ B & C \end{bmatrix}$ where

$A \in \mathbb{R}^{n \times n}$ and $C \in \mathbb{R}^{m \times m}$ are both invertible

$0 \in \mathbb{R}^{n \times m}$ is a zero matrix. Find W^{-1}

Sol. $\left[\begin{array}{cccc} A & 0 & I_{n\times n} & 0 \\ B & C & 0 & I_{m\times m} \end{array}\right]$ $\xrightarrow{\substack{A^{-1}R_1 \to R_1 \\ C^{-1}R_2 \to R_2}}$

Note: $A^{-1}R_1$, not R_1A^{-1}

$A^{-1}R_1$: row operation

$R_1 A^{-1}$ ($n \times (2n+2m)$ $\quad$ $n \times n$) column operation of R_1

matrix product not defined

$$\begin{bmatrix} I & 0 & A^{-1} & 0 \\ C^{-1}B & I & 0 & C^{-1} \end{bmatrix} \xrightarrow{R_2 - C^{-1}BR_1 \to R_2}$$

$$= \begin{pmatrix} A^{-1} & \underset{n\times m}{0} \\ 0 & C^{-1} \end{pmatrix} \begin{pmatrix} A & 0 & I & 0 \\ \underset{m\times n}{B} & C & 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} \underset{n\times n}{A^{-1}A} + \underset{n\times n}{0B} & 0 & A^{-1} & 0 \\ C^{-1}B & I & 0 & C^{-1} \end{pmatrix}$$

$$\begin{bmatrix} I & 0 & A^{-1} & 0 \\ 0 & I & \underbrace{-C^{-1}BA^{-1}} & C^{-1} \end{bmatrix}$$

W^{-1}

break: 1750 ~ 1800.

(Q6. prac2) Show that

$$A_n := \begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & -1 & 2 & \ddots & & \\ & & \ddots & \ddots & -1 & \\ & & & -1 & 2 & -1 \\ & & & & -1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & & & & \\ -\frac{1}{2} & 1 & & & & \\ & -\frac{2}{3} & 1 & & & \\ & & \ddots & \ddots & & \\ & & -\frac{i-1}{i} & 1 & \cdots & 0 \\ & & & \ddots & \ddots & \\ & & & -\frac{n-1}{n} & 1 & \end{pmatrix} \begin{pmatrix} 2 & -1 & & & & \\ & \frac{3}{2} & -1 & & & \\ & & \frac{4}{3} & \ddots & & \\ & & & -1 & \leftarrow (j-1) & \\ & & & \frac{j+1}{j} & (1) & \\ & & & & \ddots & -1 \\ & & & & & \frac{n+1}{n} \end{pmatrix}$$

(i-1) (i) j

Proof: The first row of RHS is $(2, -1, 0, 0, \cdots, 0)$

The first column of RHS is $(2, -1, 0, \cdots, 0)^T$

For any $2 \le i \le n$, $2 \le j \le n$, the (i,j) entry of RHS is

$$\Big(0, \cdots 0, \underbrace{-\frac{i-1}{i}}_{(i-1)}, \underbrace{1}_{(i)}, 0, \cdots, 0\Big)$$

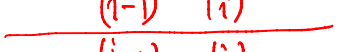
$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ -1 \leftarrow (j-1) \\ \frac{j+1}{j} \leftarrow (j) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Case 1:

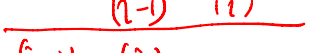
$i < j-1$, $j < i-1$

Case 2.

Case 3



Case 4



3 Foundations in logic

3.1 Proof methods

In this section we will focus on the basic structure of simple mathematical proofs, and see how to disprove a mathematical statement using a counterexample.

To illustrate these proof techniques we will use the properties of *even* and *odd* integers, and of *prime* and *composite* integers.

- An integer n is **even** if and only if n is equal to two times some integer.
- An integer n is **odd** if and only if n is equal to two times some integer plus 1.
- An integer n is **prime** if and only if $n > 1$, and for all positive integers r and s, if we have $n = r \cdot s$, then $r = 1$ or $s = 1$.
- An integer is **composite** if and only if $n > 1$, and $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Example 43. *Prove that for all* $x \in \{0, 1, 2, 3, 4, 5\}$, *the integer* $x^2 + x + 41$ *is a prime number.*

Method of Direct Proof:

To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **true**:

1. Suppose for a particular but *arbitrarily chosen* element x of D that the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
2. Show that the conclusion $Q(x)$ is true using definitions, previously established results, and the rules for logical inference.

Example 44. *Prove that for all integers* a, b, c *and* m, *if*

$$a - b = rm \quad \textit{and} \quad b - c = sm, \quad \textit{then} \quad a - c = tm$$

for some integers r, s *and* t.

The following are common **mistakes** that are often made in proofs; they should be avoided.

- Arguing from examples.
- Using the same letter to mean two different things.
- Jumping to a conclusion.
- Begging the question (assuming the thing you are trying to prove).

- Misusing the word 'if'.

Example 45. *Consider the statement that the product of any two odd integers is an odd integer. The following "proof" of this statement is incorrect as it is 'begging the question'.*

NOT a Proof:

Suppose that m and n are odd integers.
If mn is odd, then $mn = 2k + 1$ for some integer k.
By the definition of odd, $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b.

Thus $mn = (2a + 1)(2b + 1) = 2k + 1$, which is by definition odd. This is the statement which was to be shown.

what if mn is even? This proof doesn't cover all the cases.

Example 46. *Correctly prove the statement: the product of any two odd integers is an odd integer.*

proof. Let $m = 2k+1$, $n = 2r+1$, then
$mn = (2k+1)(2r+1) = 2(2kr+r+k) + 1$
is an odd number. ※

Disproof by Counterexample:

To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **false**, find a value of $x \in D$ for which $P(x)$ is true and $Q(x)$ is false.

$P(x)$: shorthand of a statement, e.g. "x is a prime number"

Example 47. Disprove the following statement:
If n is an even integer then $1 + 2 + 3 + \ldots + (n - 1) = kn$ for some integer k.
(Note that this statement is true for odd integers).

In this example, we write $D = \{2n : n \in \mathbb{Z}\}$ as the set of even integers.
$P(x) := "1+2+\cdots+(x-1) = kx$ for some $k \in \mathbb{Z}"$

How to format a proof:

1. Write the theorem to be proved. The claim/statement is: $\forall x \in D,\ P(x)$.
2. Clearly mark the beginning of the proof with the word "**Proof**".
3. Make your proof self-contained.
4. Write proofs in complete English sentences. (incomplete sentences may be confusing.)
5. Conclude by stating what it is you have proved. "The proof is completed." / or just write "※"

We disprove the statement by pointing out when $x = 2 \in D$.
$1 + 2 + \cdots (x-1) = 1 \neq k \cdot 2$ for any $k \in \mathbb{Z}$.

We continue our discussion of proof techniques now by considering the study of the rational numbers, that is, quotients of integers.

A real number is **rational** if and only if it can be expressed as a quotient of two integers with a *nonzero* denominator.

The set of all rational numbers is denoted by $\mathbb{Q}$. $\mathbb{Q}$

A real number that is not rational is **irrational**.

Break: 1902–1912.

$$r \text{ is rational} \iff \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

Example 48. *Determine the truth values of the following statements:*

(a) (0 is rational) $\wedge$ (0.377777... is rational). 0.37̇

(b) ($\sqrt{7}$ is rational) $\vee$ ($\sqrt{25}$ is rational).

(c) $\forall x \in \mathbb{R}$, if $3 \leqslant x \leqslant 4$ then x is rational.

Example 49. *Prove that the product of two rational numbers is a rational number.*

Example 50. *Prove that every rational number r has an additive inverse. (In other words, prove that for every rational number r, there exists another rational number s such that $r + s = 0 = s + r$.)*

Example 51. *Prove for $a \in Q$ has a unique representative with $\gcd(p, q) = 1$.*

Example 52. *Prove that every non-zero rational number r has a multiplicative inverse.*

We now describe exactly what it means to say that one integer **divides** another integer. One of the most important theorems in number theory will also be introduced, the **Unique Factorization Theorem**.

- If n and d are integers and $d \neq 0$, then n is **divisible** by d if and only if there exists some integer k such that $n = dk$.

  Alternatively, we say that:

  n is a **multiple of** d, or
  d is a **factor of** n, or
  d is a **divisor of** n, or
  d **divides** n.

- The notation $d \mid n$ is used to represent the predicate "d divides n".
- d **does not divide** n (denoted $d \nmid n$) if and only if $\frac{n}{d}$ is not an integer.

Warning: Note the difference between "$d \mid n$" and "d/n". → $\frac{d}{n}$

Example 53. Explain your answers to the questions below:

(a) *Is it true that* $4 \mid 72$*?* yes.

(b) *Is* 24 *a multiple of* 48*?* no. 48 is a multiple of 24

(c) *Is it true that* $0 \mid 5$*?* no

(d) *Is* -3 *a factor of* 9*?* yes. a divisor can be either positive or negative.

Is it true that $6 \mid 2a(3b+3)$, for all $a, b \in \mathbb{Z}$? Explain.

Is $2a(4b+1)$ a multiple of 4, for all $a, b \in \mathbb{Z}$? Explain.

- An alternative definition of a prime number is:

  An integer $n > 1$ is **prime** if and only if
  its only positive integer divisors are 1 and itself.

Theorem 8 (Unique Factorization for the Integers)**.** *Given any integer $n > 1$, there exist: a positive integer k; distinct prime numbers $p_1, p_2, \ldots, p_k$; and positive integers $e_1, e_2, \ldots, e_k$, such that*

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

and such expression is unique.

and any other expression of n as a product of prime numbers is identical to this, except perhaps for the order in which the terms are written.

Example 54. *Find the unique factorization of the following integers by trial division.*

(a) 5440

(b) 43560

for Exam, factorizing n for $1 \leq n \leq 100$ is enough

how? test $\frac{n}{2}, \frac{n}{3}, \frac{n}{5}, \frac{n}{7}$

because if $n = pq$ with $p \leq q$ then $p \leq \sqrt{n}$.

Suppose that k, a and b are integers.
If $k \mid a$ and $k \mid b$, prove that $k \mid (a+b)$.

Division into cases and the quotient-remainder theorem

In this section, we describe another important theorem in number theory: the **Quotient-Remainder Theorem**. We shall also encounter situations where it's easier to prove a statement by splitting the statement into cases.

Theorem 9 (Quotient-Remainder Theorem)**.** *Given any integer n and a positive integer d, there exist unique integers q and r such that*

$$n = dq + r \text{ and } 0 \leqslant r < d.$$

- Given an integer n and a positive integer d such that $n = dq + r$, where $0 \leqslant r < d$, we define

  $$n \textbf{ mod } d = r.$$

- For integers a and b, and a positive integer d, if $a \equiv r \pmod{d}$ and $b \equiv r \pmod{d}$ (so if a and b leave the same remainder upon division by d), then we say that "a is **congruent** to b **modulo** d " and write

  $$a \equiv b \pmod{d}.$$

  Note that this is the same as saying $a - b = kd$ for some integer k,
  or equivalently, $d \mid (a-b)$.

  Note: Working "$\pmod{d}$" we always assume that $d > 0$.

- $\mathbb{Z}$ denotes the set of integers. These are the positive and negative whole numbers and zero: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- We use $\mathbb{Z}^+$ to denote the positive integers, $\{1, 2, 3, \ldots\}$.
- $\mathbb{Q}$ denotes the set of rational numbers. These are the numbers that can be written as a quotient of integers, a/b, where a and b are integers and b *is nonzero*. All terminating or repeating decimals are rational numbers.
- $\mathbb{R}$ denotes the set of all real numbers. This includes all the rational numbers and all the irrational numbers (non-terminating and non-repeating decimals).

A **predicate** is a sentence that contains a finite number of variables; it becomes a statement when the variables are replaced with specific values.

Example 60. *In the following, x, a and b are integers. Which of the following are predicates?*

- *x is a positive integer.*
- *Please don't eat that.*
- *a is a factor of b.*
- *2 divides x and x divides 6.*
- *My toy elephant is grey.*
- *Paul is 20 years old.*

Predicates are often denoted by an upper case letter followed by variables listed within brackets. For example, the predicate "x is a multiple of 10" might be denoted by $P(x)$.

- The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable. The set of all such elements that make the predicate true is called the **truth set** of the predicate.

Example 61. *Let $Q(n)$ be the predicate:*
n is a factor of 15.
Find the truth set of $Q(n)$ if the domain of n is the set of integers $\mathbb{Z}$.

One way to make a predicate into a statement is to substitute a value for each variable. Another way is to add quantifiers.

- The symbol $\forall$ denotes "for all" (or for each, or for every), and is called the **universal quantifier**. Let $Q(x)$ be a predicate and D be the domain of x. The **universal statement**

$$\forall\, x \in D,\ Q(x)$$

is true if and only if $Q(x)$ is true for every x in D.
It is false if and only if $Q(x)$ is false for at least one x in D.

☆ "$Q(n)$" shorthand of a statement

e.g. $Q(n)$:= "n is an even number",

Then, $Q(1)$ is false, $Q(2)$ is true.

e.g. $Q(n)$:= "$k^2 > 0$ for all $k \geq n$":

Then $Q(5)$ is true, $Q(-3)$ is false

e.g. $Q(m,n)$:= "there exists an integer k, s.t $n < k < m$"

Then, $Q(5,2)$ is true, $Q(2,5)$ is false.

☆: → "$\forall$": for all / for any / for every / for each

→ "$\exists$" there exists / there is / there are.

→ "$\in$" belongs to / in

→ "$\sim$" NOT.

e.g. $\forall\, x$ even, $\exists\, k \in \mathbb{Z}$, s.t. $x = 2k$

e.g. $Q(n) \overset{\text{def}}{=}$ "n is even"

Then $\sim Q(n)$ = "n is not even".

About Exam: translate statements with symbols into English and avoid specific symbols.

e.g. "$\forall x \in \mathbb{Z},\ x \in \mathbb{R}$" avoid "$\forall, \in, \mathbb{Z}, \mathbb{R}$"

Sol: For any integer x, x is a real number.

e.g "$\forall x \in \mathbb{R},\ \forall \varepsilon > 0,\ \exists \delta > 0$ s.t $\forall |x-t| < \delta$, $|\sin x - \sin t| < \varepsilon$", avoid "$\forall, \in, \mathbb{R}, \exists$".

Sol For any real number x and positive number ε, there exists some $\delta > 0$, such that for any t, when ever $|x-t| < \delta$, one has $|\sin x - \sin t| < \varepsilon$. ※

☆ "$\Rightarrow$" implies

"$\Leftrightarrow$" equivalent.

e.g. $x \in \mathbb{Z} \Rightarrow x \in \mathbb{R}$

x even $\Leftrightarrow \exists\, k \in \mathbb{Z}$ s.t. $x = 2k$.

☆ Proof by Contradiction.

→ To prove Q

→ Assume $\sim Q$

→ Show that $\sim Q$ leads to a contradiction

→ **Conclude that Q is true.**

---

e.g. Let $A \in \mathbb{R}^{n \times n}$ be invertible. Prove $\det(A^{-1}) \neq 0$.

Proof. Assume $\det(A^{-1}) = 0$. From $AA^{-1} = I$

We have $1 = \det(I) = \det(A)\det(A^{-1}) = 0$.

The contradiction completes the proof. ※

e.g. $\forall n \in \mathbb{Z}$ when n^2 is odd, prove that n is odd.

Proof: Assume n is even.

The $n = 2k$ for some $k \in \mathbb{Z}$. So,

$n^2 = 2(2k^2)$ is even

The contradiction completes the proof. ※