MOE Advanced Level Higher 3 (H3) Math

Mathematical Proofs and Reasoning

Lecture 2

Telegram Chat

Conent

Truth Table

Given some (Mathematical) statements, we may form a truth table to list the truth value of some combinations of the statements depending on the truth value of the original statements.

Example

Modus Ponen: $P \Rightarrow Q$

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Question. Why is $P \Rightarrow Q$ true whenever P is false? This is known as vacuously true.

Negation

Definition

Let P be a (mathematical) statement. The negation of P, read as not P, denoted as $\neg P$, is true when P is false, and false when P is true.

P	$\neg P$
T	F
F	T

Example

P: n is an odd integer. $\neg P$: n is not an odd integer.

In this case, $\neg P$ is equivalent to n is an even number.

Exercise. $\neg(\neg P) \equiv P$.

Negation of Universal Statement

- Recall that universal statements are statements with the quantifier "for all", "for any".
- In standard form it is written as for all x in D, $P(x)$, or in the syntax is $\forall x \in D,\ P(x)$.
- The negation of a universal statement is an existential statement,

$$\neg(\forall x \in D,\ P(x)) \quad \Leftrightarrow \quad \exists x \in D,\ \neg P(x)$$

Example

$\forall x \in D,\ P(x)$: Everyone in class gets a chocolate.

$\exists x \in D,\ \neg P(x)$: Someone in class did not get a chocolate.

Example

Is the following statement true?

For all integer $n \geq 1$, $n^2 + 1$ is a prime number.

$P(n)$: $n^2 + 1$ is prime. D: integers ≥ 1. The statement is $\forall n \in D,\ P(n)$.

For $n = 1$, $1^2 + 1 = 2$ is prime.

For $n = 2$, $2^2 + 1 = 5$ is prime.

Negation of Existential Statements

The negation of an existential statement is a universal statement.

$$\neg(\exists x \in D,\ P(x)) \quad \Leftrightarrow \quad \forall x \in D,\ \neg P(x).$$

Example

$\exists x \in D,\ P(x)$: Some students in the class likes durian.
$\forall x \in D\ \neg P(x)$ Every student in the class does not like durian.
Equivalent to: No student in class likes durian.

Modus Tollen or Contrapositive

Theorem

If x^2 is an even integer, then x is an even integer.

Proof.

Let $x^2 = 2m$ for some integer m.

... cannot $x = \sqrt{2m}$

... required conclusion is $x = 2n$ for some integer n.

□

Modus Tollen or Contrapositive

Let P and Q be (mathematical) statements. Consider the statement $\neg Q \Rightarrow \neg P$.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Observe that the truth values for $P \Rightarrow Q$ are equal to those for $\neg Q \Rightarrow \neg P$. That is, $P \Rightarrow Q$ is logically equivalent to $\neg Q \Rightarrow \neg P$; denoted as $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$.

Example

$P \Rightarrow Q$: If you do well in your exam, then you will get a sweet.
$\neg Q \Rightarrow \neg P$: If you got did not get a sweet, then you did not do well in your exam.

Example

Theorem

If x^2 is an even integer, then x is an even integer.

Proof.

P: x^2 is an even integer. Q: x is an even integer.

$\neg Q$: x is an odd integer. $\neg P$: x^2 is an odd integer.

Prove instead: if x is an odd integer, then x^2 is an odd integer.

$x = 2k + 1$ for some integer k. Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

is an odd integer since $2k^2 + 2k$ is an integer.

□

Conjunction and Disjunction

Truth table for conjunction (and, denoted as $\wedge$) and disjunction (or, denoted as $\vee$).

P	Q	$P \wedge Q$	$P \vee Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Conjunction $\leftrightarrow$ intersection

$$\{x \mid P(x)\} \cap \{x \mid Q(x)\} = \{x \mid P(x) \wedge Q(x)\}.$$

Disjunction $\leftrightarrow$ union

$$\{x \mid P(x)\} \cup \{x \mid Q(x)\} = \{x \mid P(x) \vee Q(x)\}.$$

De Morgan's law

Truth table for negation of conjunction and disjunction.

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$	$(\neg P) \vee (\neg Q)$
T	T	T	T	F	F	F	F	F	F
T	F	F	T	F	T	T	F	F	T
F	T	F	T	T	F	T	F	F	T
F	F	F	F	T	T	T	T	T	T

Comparing the truth table,

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

Discussion

Show that

1. $\{x \mid \neg(P(x) \wedge Q(x))\} = \{x \mid P(x)\}^c \cup \{x \mid Q(x)\}^c$

2. $\{x \mid \neg(P(x) \vee Q(x))\} = \{x \mid P(x)\}^c \cap \{x \mid Q(x)\}^c$

where for a set A, A^c denotes the set complement of A.

Example

Theorem

For any real numbers x and y, if $x^2y + xy^2 < 30$, then $x < 2$ or $y < 3$.

Proof.

Theorem has the structure $P \Rightarrow (Q_1 \vee Q_2)$.

Consider proof by contrapositive, $\neg(Q_1 \vee Q_2) \Rightarrow \neg P$, or $(\neg Q_1) \wedge (\neg Q_2) \Rightarrow \neg P$.

$(\neg Q_1) \wedge (\neg Q_2) \Rightarrow \neg P$: If $x \geq 2$ and $y \geq 3$, then $(x^2y + xy^2 \geq 30$.

Since $x \geq 2$ and $y \geq 3$, then $x + y \geq 2 + 3 = 5$ and $xy \geq (2)(3) = 6$. Hence,

$$x^2y + xy^2 = xy(x + y) \geq (6)(5) = 30.$$

□

Example

Theorem

For integers a and b, if 3 does not divide ab, then 3 does not divide a and 3 does not divide b.

Proof.

Direct proof of the theorem requires considering cases.

Theorem has the structure $\neg P \Rightarrow (\neg Q_1 \wedge \neg Q_2)$.

Consider proof by contrapositive, $(Q_1 \vee Q_2) \Rightarrow P$.

$(Q_1 \vee Q_2) \Rightarrow P$: If $3 \mid a$ or $3 \mid b$, then $3 \mid ab$. Theorem now becomes obviously true.

Without lost of generality, suppose $a = 3n$ for some integer n. Then

$$ab = 3nb = 3(nb)$$

is a multiple of 3 since nb is an integer.

Rational Numbers

Definition

A real number r is a rational number if it can be written as

$$r = \frac{p}{q}, \quad q \neq 0,$$

for some integers p, called the numerator, and q, called the denominator.

The set of rational numbers is denoted as $\mathbb{Q}$. The complement of the set of rational numbers (in the set of reals) is the set of irrational numbers.

Example

- p and q might not be unique $\frac{28}{12} = \frac{14}{6} = \frac{7}{3}, \quad -\frac{1}{2} = \frac{-1}{2} = \frac{1}{-2}.$
- all integers are rational numbers, $\mathbb{Z} \subseteq \mathbb{Q}$. $3 = \frac{3}{1} = \frac{6}{2} = \frac{9}{3} = ..., \quad 49 = \frac{49}{1}.$

Unique Irreducible Expression

Definition

Two integers a and b are coprime if the only positive common divisor is 1. That is

$$r \mid a \ \wedge \ r \mid b \quad \Rightarrow \quad r = 1.$$

Example

Discussion. List some examples of coprime integers.

- Any 2 prime numbers are coprime.
- 6 and 25 are coprime.

Unique Irreducible Expression

Definition

Given a rational number $r = \frac{p}{q}$, we can divide p and q be their greatest common divisor, and multiply both p and q by -1 if necessary and assume that $q > 0$. This way, we can express a rational number as $r = \frac{p}{q}$ such that p and q are coprime, and $q > 0$. We call this expression irreducible.

Theorem

Every rational number has a unique irreducible expression.

Proof requires the uniqueness of prime factorization. The proof can be found in the appendix.

Properties of $\mathbb{Q}$

Theorem

(i) *(Closure under addition) If r_1 and r_2 are rational numbers, then so is $r_1 + r_2$.*

(ii) *(Additive Inverse) If r is a rational number, then so is $-r$.*

(iii) *(Closure under multiplication) If r_1 and r_2 are rational numbers, then so is $r_1 r_2$.*

(iv) *(Multiplicative inverse) If r is a nonzero rational number, then $\frac{1}{r}$ is a rational number.*

Proof.

Exercise. □

Remark. This theorem proves that the set $\mathbb{Q}$ is a field.
See https://en.wikipedia.org/wiki/Field_(mathematics)).

Biconditional

- Recall that $P \Leftrightarrow Q$, read as P is and only if Q, is $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.
- In some instances, we may instead prove $(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)$. That is, use direct prove for $P \Rightarrow Q$, and use contrapositive to prove $Q \Rightarrow P$.
- Or prove $(Q \Rightarrow P) \wedge (\neg Q \Rightarrow \neg P)$. That is, use direct prove for $Q \Rightarrow P$, and use contrapositive to prove $P \Rightarrow Q$.

Example

Theorem

For integers a and b, ab is odd if and only if a and b are odd.

Proof.

$(Q_1 \wedge Q_2) \Rightarrow P$: a and b are odd $\Rightarrow ab$ is odd $(Q_1 \wedge Q_2) \Rightarrow P$, and
$\neg Q_1 \vee \neg Q_2 \Rightarrow \neg P$: a **or** b even $\Rightarrow ab$ is even.

Suppose $a = 2n + 1$ and $b = 2m + 1$ for some integers n, m. Then

$$ab = (2n + 1)(2m + 1) = 4nm + 2n + 2m + 1 = 2(2mn + n + m) + 1$$

is odd since $2mn + n + m$ is an integer.

Conversely, suppose a or b is even. Without lost of generality, suppose $a = 2n$. Then

$$ab = 2nb = 2(nb)$$

is even since nb is an integer.

□

Proof by Contradiction

A proving technique where we want to prove that a statement is true by assuming that it is false, and arrive at a contradiction.

Example

Claim: *Not every statement can be proven.*

Suppose to a contradiction that this is false, that is every statement can be proven. Consider the statement

"This statement cannot be proven."

If this statement is true, then it cannot be proven, thus contradicting our assumption that every statement can be proven.
If this statement is false, then it can be proven, but that means it is true, which again leads to a contradiction.
Thus, our assumption that every statement can be proven must be false. Hence, it is true that not every statement can be proven.

Example

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose to a contradiction that $\sqrt{2}$ is rational. Write $\sqrt{2} = \frac{a}{b}$ in its irreducible expression. Then

$$2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \quad \Rightarrow \quad a^2 = 2b^2 \quad \Rightarrow \quad a^2 \text{ is even, since } b^2 \text{ is an integer.}$$

Hence, a is even too. Write $a = 2n$ for some integer n. Then $a^2 = (2n)^2 = 4n^2$. But then

$$4n^2 = a^2 = 2b^2 \quad \Rightarrow \quad b^2 = 2n^2 \quad \Rightarrow \quad b^2 \text{ and thus } b \text{ is even too.}$$

Write $b = 2m$ for some integer m. But that means that $\sqrt{2} = \frac{a}{b} = \frac{2n}{2m} = \frac{n}{m}$, a contradiction to $r = \frac{a}{b}$ being the (unique) irreducible expression of r. □

Example

Let L_1 to be the line passing through points $P_1(0,0,1)$ and $P_2(1,1,0)$, and L_2 be the line passing through points $Q_1(0,1,0)$ and $Q_2(1,0,0)$. Show that the lines never intersect.

A direction vector of L_1 is $\vec{v}_1 = (1,1,-1)$, and a direction vector for L_2 is $\vec{v}_2 = (1,-1,0)$. Suppose to the contradiction that the lines intersect. Then there exists some $\lambda_1, \lambda_2 \in \mathbb{R}$ such that

$$(0,0,1) + \lambda_1(1,1,-1) = (0,1,0) + \lambda_2(1,-1,0).$$

Comparing the coordinates, we obtain

$$\begin{cases} \lambda_1 = \lambda_2 \\ \lambda_1 = 1 - \lambda_2 \\ 1 - \lambda_1 = 0 \end{cases}$$

From the third equation, $\lambda_1 = 1$, and hence from the second, $\lambda_2 = 0$. But substituting this into equation 1, we have $1 = 0$, a contradiction. Hence, we conclude that the lines do not intersect.

Discussion

Suppose $x \neq 0$. Prove that x is irrational if and only if $\dfrac{1}{x}$ is irrational.

Prime and Composite (and 1)

Definition

An integer p is a prime number if $p \neq 1$ and its only divisor is 1 and itself. An integer that is neither 1 nor prime is called a composite number.

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 can be written as a product of primes in exactly one way, up to permutations of the prime.

Equivalently, for any integer $a > 1$, there are unique and distinct primes $p_1, p_2, ...p_k$, and unique positive integers $n_1, n_2, ..., n_k$ such that

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}.$$

This is called the prime decomposition or prime factorization of a.

Remark. This is a existence and uniqueness theorem.

Euclid Lemma

Theorem

Let p be a prime number. If p divides ab, then p divides a or p divides b.

$$p \mid ab \quad \Rightarrow \quad (p \mid a) \vee (p \mid b).$$

Proof.

Let $a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ and $b = q_1^{m_1} q_2^{m_2} \cdots q_l^{m_l}$ be the prime decomposition of a and b, respectively. Since $p \mid ab = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} q_1^{m_1} q_2^{m_2} \cdots q_l^{m_l}$, by the uniqueness of prime decomposition of $p = p_i$ for some $i = 1, ..., k$, or $p = q_j$ for some $j = 1, ..., l$. If $p = p_i$ for some $i = 1, ..., k$, then $p \mid a$. If $p = q_j$ $j = 1, ..., l$, then $p \mid b$. This shows that either $p \mid a$ or $p \mid b$. □

Exercise. We have seen in lecture 1 that the theorem is false if we replace p with a composite number n. Why does the proof not work in that case?

There are Infinitely Many Primes

Theorem

There are infinitely many prime numbers.

Proof.

Suppose there are finitely many primes. Let $p_1, p_2, ..., p_m$ be all the prime numbers. Consider the integer

$$a = p_1 p_2 \cdots p_m + 1.$$

Since $a > p_1, p_2, ..., p_m$, by hypothesis, it is a composite. Let $a = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$ be the prime factorization of a, where $n_i \geq 0$ are nonnegtaive integer. Then for each $i = 1, 2, ..., m$ such that $n_i > 0$,

$$p_i \mid a, \quad \text{and} \quad p_i \mid (a-1) = p_1 p_2 \cdots p_m.$$

This means that $p_i \mid (a - (a-1)) = 1$, which means that $p_i = 1$, a contradiction to p_i being a prime number. This shows that the assumption that there are finitely many primes is false, thus concluding that there must be infinitely many primes. □

Twin Prime Conjecture

Definition

A pair of prime numbers $p_1 < p_2$ is said to be a twin prime if $p_2 - p_1 = 2$.

Example

$(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, ..., $(41, 43)$, ...,
$(2\,996\,863\,034\,895 \times 2^{1\,290\,000} - 1, 2\,996\,863\,034\,895 \times 2^{1\,290\,000} + 1)$

Conjecture

There are infinitely many pair of twin primes.

Great Internet Mersenne Prime Search

- By the fundamental theorem of arithmetic, since primes are the fundamental building blocks of all integers, understanding them help us understand integers in general.
- Cryptography, in particular, RSA cryptography uses large primes (though not as large as the largest ones found recently).
- The great internet Merseene prime search https://www.mersenne.org/ allows people to download a free program on their computer to be used to search for the next largest prime known.
- Some prize money will be awarded to the person whose computer was used to find the next largest known prime.
- Current largest known prime is $2^{136279841} - 1$, total of $41,024,320$ digits, found in 21 October 2024. Click here https://www.mersenne.org/primes/digits/M136279841.zip to see all the digits on this prime.
- Such prime numbers are known as Mersenne primes.

Mersenne Prime

Definition

A prime number of the form $p = 2^n - 1$ for some positive integer n is known as a Mersenne prime.

Example

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 - 127$ are Mersenne primes
- $2^4 - 1 = 15$, $2^6 - 1 = 62$, $2^8 - 1 = 255$, $2^9 - 1 = 511 = 7 \times 73$ are not prime numbers.

Question. Based on the examples above, make a hypothesis.

Discussion

A false hypothesis is

$$\text{If } p \text{ is prime, then } 2^p - 1 \text{ is a Mersenne prime,}$$

A counterexample would be $2^{11} - 1 = 2047 = 23 \times 89$.

Prove the following statement.

$$\text{If } 2^n - 1 \text{ is prime, then } n \text{ is prime.}$$

Challenge

Theorem

If p is prime, then $\sqrt{p}$ is irrational.

Remark. If someone is being unreasonable or illogical, tell him/her that he/she is being the square root of some prime.

Appendix

Uniqueness of Irreducible Rational Expression

Theorem

Every rational number has a unique irreducible expression.

Proof.

Suppose $r = \frac{a}{b} = \frac{c}{d}$ are irreducible expression of a rational number. Then $ad = bc$. Let p be a prime factor of b. Then since a and b are coprime and $p \mid ad$, necessarily $p \mid d$. This is for all prime factors of b, and thus $b \mid b$. Analogously, every prime factor of d is a prime factor of b too. Hence, $d \mid b$ too. Since both $b, d > 0$, necessarily $b = d$. Thus, $a = c$. □