MOE Advanced Level Higher 3 (H3) Math

Mathematical Statements and Proofs

Lecture 1

Telegram Chat

Content

Some Nomenclature and Notations

The set of real numbers is denoted as $\mathbb{R}$. Unless stated otherwise, the universal set of numbers will be the set of real numbers.

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$: the set of **integers**. The set of numbers that can be obtained from 0 by adding or subtracting 1.
- $\mathbb{Z}^+ = \mathbb{Z}_{>0} = \{1, 2, 3, 4, 5, \dots\}$: the set of **positive integers**.
- $\mathbb{N} = \mathbb{Z}^+$, the set of **natural numbers**. (**Remark**. Some textbooks includes 0 in $\mathbb{N}$.)
- $\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\}$: the set of **rational numbers**.
- $\varnothing$: the **empty set**, the set containing no element.
- Similarly we can use $\mathbb{Z}^-$, $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{R}^+$, $\mathbb{R}^-$, ...
- $\mathbb{C}$ denoted the set of all complex numbers. Not discussed (formally).

Types of Statements (Structure)

Conditional statements

- In standard form: If P then Q
- Other forms: Q is necessary for P, or P is sufficient for Q
- Symbolic form: $P \Rightarrow Q$

Here P is called the hypothesis or assumption; Q is called the conclusion. No assumption that P is true. But when P is true, then Q is.

Example

If $n > 2$, then $n > 1$.

Type of Statements (Structure)

Biconditional Statements

(i) Standard form: P if and only if Q

(ii) Abbreviation: P iff Q

(iii) Other forms: P is necessary and sufficient for Q

(iv) Symbolic form: $P \Leftrightarrow Q$

(v) Means $P \Rightarrow Q$ and $Q \Rightarrow P$.

Example

n is odd if and only if $n + 1$ is even.

Types of Statements (Structure)

Existential Statement

(i) Standard form: There exists an x in D such that $P(x)$

(ii) Abbreviation: $\exists\, x \in D,\ P(x)$

(iii) D is the domain

(iv) Other forms: there is a ..., there exists ..., for some ..., we can find ..., ... has ...

Example

- There exists a real number x such that $x^2 = 2$.
- There is a tallest person in the world.

Type of Statements (Content)

Definition

A (mathematical) definition is a (true) mathematical statement that gives the precise meaning of a word or phrase that represents some object, property or other concepts.

To state a mathematical statement, we first need definitions.
"All zaxcillian has rizz" makes no sense.

Example (Negative Example)

From https://www.dictionary.com/.

- Definition of happy: being delighted, pleased, or glad, as over a particular thing.
- Definition of pleased: very happy or satisfied
- Examples: It's like when you win a match, or did well in your exam, or have an ice cream, ... etc.

Type of Statements (Content)

Definition

A (mathematical) definition is a (true) mathematical statement that gives the precise meaning of a word or phrase that represents some object, property or other concepts.

Example

- An integer a is even if there exists an integer n such that $a = 2n$.
- An integer a is odd if there exists an integer n such that $a = 2n + 1$.

Type of Statements (Content)

Theorem

A theorem is a true mathematical statement that can be proven mathematically.

Example

n is odd if and only if $n + 1$ is even.

Axiom

An axiom is a mathematical statement that does not require proof.

Example

If x and y are integers, then so is $x + y$.

Axioms

Some axioms of real numbers $\mathbb{R}$: See Appendix A for full list.

- Closure. For any real numbers x and y, $x + y$ and $x \cdot y$ are real numbers.
- Associative. For any x, y, z, $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Commutative. For any x and y, $x + y = y + x$, $x \cdot y = y \cdot x$.
- Identity. There exists 0 and 1 such that $x + 0 = x$ and $1 \cdot x = x$ for all x.
- Inverse. For any x, there is a $-x$ such that $x + (-x) = 0$. If $x \neq 0$, there is a $\frac{1}{x}$ such that $x \cdot \frac{1}{x} = 1$.
- Distributive. For any x, y, z, $x \cdot (y + z) = x \cdot y + x \cdot z$.

It depends on who you ask. Some would construct the set of real numbers instead. See
https://en.wikipedia.org/wiki/Construction_of_the_real_numbers

Some Other Axioms

Here are some axioms of mathematics.

- Zermelo-Fraenkel (ZF) Set Theory:
  https://plato.stanford.edu/entries/set-theory/zf.html.
- May include Axiom of choice (ZFC): https://plato.stanford.edu/entries/axiom-choice/.
  - Even with the axiom of choice, mathematicians are still unable to prove the continuum hypothesis.
  - This led to the birth of independence.
- Euclid Axioms of Geometry:
  https://plus.maths.org/content/maths-minute-euclids-axioms.
  - The fifth axiom gave Mathematicians some problems, "parallel lines" in a sphere do intersect.
  - This gives rise to non-euclidean geometry (manifold).

Axioms for H3

For this course (H3), we take the list of axioms in *Appendix A* as our foundational assumptions. These describe the basic properties of the real numbers $\mathbb{R}$, and we will accept them without proof.

We are also allowed to use any fact or result established in H2 Mathematics, unless stated otherwise.

Occasionally, we will revisit some H2 results and reprove them, not because they are in doubt, but to demonstrate proof techniques.

Remark

We begin by agreeing upon a set of axioms. Once accepted, these statements are treated as true without question. Questioning the axioms themselves belongs to another branch of mathematics, such as logic or foundations.

Proofs

(Mathematical) Proof

A deductive argument for a mathematical statement, showing that the stated assumptions logically guarantee the conclusion.

$$P \xrightarrow{\text{definitions, axioms, algebraic manipulations, and previously established facts}} Q.$$

Example

For $a \in \mathbb{Z}$, if a is odd, then $a+1$ is even.

- The hypothesis or assume is $P =$ (if a is odd). The conclusion is $Q = a+1$ is even.
- In short, we want to prove the condition statement

$$a \text{ is odd} \quad \Rightarrow \quad a+1 \text{ is even}$$

- May give a direct prove: Start with P, end in Q.

Example

Theorem

For $a \in \mathbb{Z}$, if a is odd, then $a + 1$ is even.

(Not) Proof.

3 is odd, 3+1=4 is even.

5 is odd, 5+1=6 is even.

97 is odd, 97+1=98 is even.

etc...

□

This is not a proof; only gave examples. It does not show that statement is true for all odd integers. This is a universal statement "for any", "for all" (notation $\forall$). It is impossible to prove by exhaustive search.

Example

Theorem

For $a \in \mathbb{Z}$, if a is odd, then $a + 1$ is even.

(Not) Proof.

You try search for an odd number a such that $a+1$ is not even. Cannot right? So, the theorem is true. □

Inability to find counter-example does not constitute a proof.

Example

All crows are black.

Example

Theorem

For $a \in \mathbb{Z}$, if a is odd, then $a + 1$ is even.

(Not) Proof.

Of course it's true since my professor said it is. This follows from deep algebraic structures that extend beyond elementary divisibility rules, touching on abstract algebra, modular arithmetic, and measure theory. Additionally, this result is a trivial corollary of the Generalized Parity Theorem, which is left as an exercise to the reader. □

This is called proof by intimidation, but Mathematicians should uphold truth and not be intimidated.

Example

Theorem

For $a \in \mathbb{Z}$, if a is odd, then $a + 1$ is even.

(Direct) Proof.

Suppose a is odd. Starting from the hypothesis.

There exists an integer n such that $a = 2n + 1$. Definition of odd number.

Then $a + 1 = 2n + 2 = 2(n + 1)$ Algebraic manipulation.

Since $m = n + 1$ is an integer Use Axiom, closure property.

so, $a + 1 = 2m$ for some integer m. Definition of even.

Hence, $a + 1$ is even. Conclusion.

□

Example

Theorem

For $a \in \mathbb{Z}$, if a is odd, then $a + 1$ is even.

Proof.

Suppose a is odd. There exists an integer n such that $a = 2n + 1$. Then

$$a + 1 = 2n + 2 = 2(n + 1) = 2m,$$

where $m = n + 1$. Since $m = n + 1$ is an integer, $a + 1 = 2m$ is even. □

The box at the bottom right symbolizes the end of the proof. May also use QED.

Direct Proof

A direct proof is an approach to prove a conditional statement $P \Rightarrow Q$.

(i) It is a series of valid argument that starts with the hypothesis P, and end with the conclusion Q.

(ii) In the process, may use definitions, properties, axioms, algebraic manipulations, and other known results.

$$P \quad \Rightarrow \quad P_1 \quad \Rightarrow \quad P_2 \quad \Rightarrow \quad \cdots \quad \Rightarrow \quad P_k \quad \Rightarrow \quad Q.$$

(iii) Keep an eye on the conclusion Q in every step, each statement P_i is "approaching" Q.

(iv) May "cheat" and work backwards from Q a little.

(v) May need to use existential instantiation.

Existential Instantiation $\exists$

- If we know something exists, may give it a name (label) and use it.
- However, do not give two a priori different objects the same name (label) in the current discussion.

Example

- Let a be an odd integer. Then there exists an integer n such that $a = 2n + 1$.

$$\exists\, n \in \mathbb{Z} \quad s.t. \quad a = 2n + 1$$

- Let a and b be odd integers. Then there exists an integer n such that $a = 2n + 1$ and $b = 2n + 1$.
  - This would imply that $a = b$, which might not be true.
  - Instead, there exists integers n and m such that $a = 2n + 1$ and $b = 2m + 1$.

$$\exists\, n, m \in \mathbb{Z} \quad s.t. \quad a = 2n + 1, \quad b = 2m + 1$$

Example

Theorem

The product of an even integer with an odd integer is even.

(Not) Proof.

Suppose m is even and n is odd. Then

$$mn = 2r = 2(p)(2q+1) = (2p)(2q+1)$$

So, let $m = 2p$ and $n = 2q+1$ shows that $mn = 2r$ is even. □

Question. What is wrong with the proof?

Example

Theorem

The product of an even integer with an odd integer is even.

Proof.

Suppose m is even and n is odd. Then

$$\exists\, p, q \in \mathbb{Z} \quad s.t. \quad m = 2p \text{ and } n = 2q + 1.$$

So,

$$mn = (2p)(2q + 1) = 2(p)(2q + 1) = 2r,$$

where $r = p(2q + 1)$ is an integer. Hence, mn is even. □

Divisibility

Example

- 3 divides 12, 3 is a factor of 12, 12 is divisible by 3.
  - $3 \times 4 = 12$.
- 7 divides 21, 7 is a factor of 21, 21 is divisible by 7.
  - $7 \times 3 = 21$.

Definition

Let n and d be integers such that $d \neq 0$. We say that n is divisible by d, or d divides n, denoted as $d \mid n$ if and only if there is an integer k such that

$$n = kd.$$

Otherwise, we say d does not divide n, and denote it as $d \nmid n$.

Caution. Not to be confused with n/d.

Example

Theorem

If x is an even integer, then x^2 is divisible by 4.

(Direct) Proof.

Since x is even, Starting from the hypothesis.

there exists an integer n such that $x = 2n$. Definition of even number.

Then $x^2 = (2n)^2 = 4n^2$. Algebraic manipulation.

Since $n^2 = n \times n$ is an integer q, Axiom of closure property of multiplication.

this means that $x^2 = 4q$ for some integer q. definition of divisibility.

Hence, x^2 is divisible by 4. Conclusion.

□

Example

Theorem

If x is an even integer, then x^2 is divisible by 4.

Proof.

Since x is even, there exists a integer n such that $x = 2n$. So,

$$x^2 = (2n)^2 = 4n^2 = 4q,$$

where $q = n^2$ is an integer. This shows that x^2 is divisible by 4. □

Example

Theorem

Let $a, b \in \mathbb{Z}$. If $a, b > 0$ and $a \mid b$, then $a \leq b$.

(Direct) Proof.

Suppose $a, b > 0$ and $a \mid b$. Start with hypothesis.

Then there exists an integer k such that $b = ka$. Definition of divisibility.

Since $a, b > 0$, necessarily $k > 0$. T25 of appendix A: $xy > 0 \Rightarrow x, y > 0$ or $x, y < 0$.

It follows that $1 \leq k$, since 1 is the smallest positive integer. Basic property of integer.

Then $a = a \times 1 \leq a \times k = b$. T20 of appendix A: $x < y$ and $z > 0 \Rightarrow xz < yz$.

Hence, $a \leq b$. Conclusion.

□

Idea of proof: $a = \cdots ? \cdots \leq ak = b$

Example

Theorem

Let $a, b \in \mathbb{Z}$. If $a, b > 0$ and $a \mid b$, then $a \leq b$.

Proof.

Suppose $a, b > 0$ and $a \mid b$. Then there exists an integer k such that $b = ka$. But since a and b are positive, k is positive too. This means that $1 \leq k$. Therefore

$$a = a \times 1 \leq a \times k = b,$$

which shows that $a \leq b$. □

Discussion

What is wrong with the following proof?

Theorem

2=1

Proof.

Let a and b be real numbers such that $a = b$. Then

$$
\begin{array}{rcll}
ab & = & b^2 & \text{multiply both sides by } b \\
a^2 - ab & = & a^2 - b^2 & \text{take the negative of both sides and add to } a^2 \\
a(a-b) & = & (a+b)(a-b) & \text{factorizing out } (a-b) \\
a & = & a+b & \text{canceling the common terms on both sides} \\
a & = & 2a & \text{since } a = b \\
1 & = & 2 & \text{canceling the common terms on both sides}
\end{array}
$$

Exercise

Prove the following theorem.

Theorem

For any $a, b, c \in \mathbb{Z}$,

$$a \mid b \quad \textit{and} \quad a \mid c \quad \Rightarrow \quad a \mid (b \pm c).$$

Counter-Example

- The theorems thus far are universal conditional statements ($\forall$).
- To disprove a universal conditional statement, that is, to show that it is false, provide a counter-example.

Example

All oranges (fruit) are orange in color.

False. Counter-example

Counter-Example

In providing a counter-example, it must fulfil the hypothesis, but not the conclusion. That is, to show that $P \Rightarrow Q$ is false,

$$P(\text{true}) \quad \text{and} \quad Q(\text{false}) \quad \text{then} \quad P \quad \not\Rightarrow \quad Q.$$

Example

Let $a, b, c \in \mathbb{Z}\backslash\{0\}$.

1. If $c \mid ab$, then $c \mid a$ or $c \mid b$.
2. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Congruence Modulo

- In 12hrs format, 7 hours after 10am is 5pm.
  $7 + 10 = 17 \equiv 5 \mod 12$, since $17 - 5 = 1 \times 12$.
- In 12hrs format, 5 hours after 8am is 1pm.
  $5 + 8 = 13 \equiv 1 \mod 12$, since $13 - 1 = 1 \times 12$.
- In 24hrs format, 12 hours after 1300hrs is 0100hrs the following day.
  $12 + 13 = 25 \equiv 1 \mod 24$, since $25 - 1 = 1 \times 24$.

Definition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that a is congruent to b modulo n, or a equals to b modulo n, denoted as

$$a \equiv b \mod n$$

if and only if n divides $a - b$, $n \mid (a - b)$.

Example

Example

- $24 \equiv 3 \mod 7$ since $24 - 3 = 21 = 3 \times 7$
- $31 \equiv -11 \mod 7$ since $31 - (-11) = 42 = 7 \times 6 \times 7$
- $25 \not\equiv 10 \mod 7$ since $25 - 10 = 15$ and $7 \nmid 15$
- Any multiple of 7 is congruent to 0 modulo 7.
- $\forall\, n$ even, $n \equiv 0 \mod 2$. $\forall\, n$ odd, $n \equiv 1 \mod 2$.
- All prime number except 2 is congruent to 1 modulo 2.

Equivalently, $a \equiv b \mod n$ iff $a = b + nk$ for some $k \in \mathbb{Z}$.

Properties of Congruence

Theorem (Congruence is an Equivalence Relation)

Let n be an integer with $n > 1$.

1. *For every integer a,*
$$a \equiv a \mod n \quad \textit{reflexive property}$$
2. *For all integers a and b,*
$$a \equiv b \mod n \iff b \equiv a \mod n \quad \textit{symmetric property}$$
3. *For all integers a, b, and c,*
$$a \equiv b \mod n \text{ and } b \equiv c \mod n \implies a \equiv c \mod n \quad \textit{transitive property}$$

Proof.

Exercise. □

Modular Arithmetic

Theorem

For all integers a, b, c and n, with $n > 1$, suppose $a \equiv b \mod n$ and $c \equiv d \mod n$. Then

1. $a \pm c \equiv b \pm d \mod n$. *preserved addition.*
2. $a \times c \equiv b \times d \mod n$. *preserved multiplication.*
3. $a + k \equiv b + k \mod n$ *for all* $k \in \mathbb{Z}$.
4. $k \times a \equiv k \times b \mod n$ *for all* $k \in \mathbb{Z}$.
5. $a^m \equiv b^m \mod n$ *for all* $m \in \mathbb{Z}^+$. *preserved power.*

Remark. That is, congruent modulo behaves like equality for addition, subtraction, and multiplication.

Question. Does congruent modulo preserve division? That is, if $c \mid a$ and $d \mid b$, then is it true that $\frac{a}{c} \equiv \frac{b}{d} \mod n$?

Partial Proof.

Only proof (2) as an example.

Given $a \equiv b \mod n$ and $c \equiv d \mod n$ direct proof, start with the hypothesis

then $a = b + nk$ for some $k \in \mathbb{Z}$ and $c = d + nl$ for some $l \in \mathbb{Z}$. definition

Multiplying them together,

$$ac = (b + nk)(d + nl) = \cdots = bd + n(bl + kd + lkn) \quad \text{algebraic manipulation}$$

So, $ac = bd + nm$ for some $m \in \mathbb{Z}$, definition

and thus $ac \equiv bd \mod n$. conclusion

□

Exercise. Prove the other statements.

Discussion

Theorem

Let n be a positive integer. Then for any m, there is a unique r with $0 \leq r < n$ such that

$$m \equiv r \mod n.$$

Equivalently, there is a q such that

$$m = qn + r, \qquad \text{for some } 0 \leq r < n.$$

Prove the existence theorem for $m, n > 0$.

Proof by Cases

Theorem

If n is an integer, then 3 divides $n^3 - n$.

Proof.

Every number either divides 3, or have remainder 1 or 2 when divided by 3 (every number is congruent to either 0, 1, or 2 modulo 3).

Case 1. Suppose $n = 3k$ for some integer k. Then

$$n^3 - n = (3k)^3 - 3k = 3(9k^3 - k) \quad \Rightarrow \quad 3 \mid n^3 - n \text{ since } 9k^3 - k \text{ is an integer.}$$

Case 2. Suppose $n = 3k + 1$ for some integer k. Then

$$n^3 - n = (3k+1)^3 - (3k+1) = 3(9k^3 + 9k^2 + 2k) \quad \Rightarrow \quad 3 \mid n^3 - n \text{ since } 9k^3 + 9k^2 + 2k \text{ is an integer.}$$

Case 3. **Exercise**.

□

Considering Cases

Usually, when a statement involves n divisibility by d or multiples of d, may consider cases,

Case 1. $n = kd$

Case 2. $n = kd + 1$

$\vdots$

Case d. $n = dk + (d - 1)$

Example

For cases involving odd or even, consider the parity of integer n.

Case 1. n is even, $n = 2k$ for some integer k.

Case 2. n is odd, $n = 2k + 1$ for some integer k.

If problem involves 2 numbers n and m, consider their whether they are have the same parity.

Case 1. m and n has the same parity.

Case 1a. $m = 2k$, $n = 2l$ for some integers k, l.

Case 1b. $m = 2k + 1$, $n = 2l + 1$ for some integers k, l.

Case 2. m and n has different parity.

Case 2a. $m = 2k$, $n = 2l + 1$ for some integers k, l.

Case 2b. $m = 2k + 1$, $n = 2l$ for some integers k, l.

Considering Cases

Theorem

For all integers a and b, if

$$3 \nmid a \text{ and } 3 \nmid b, \text{ then } 3 \nmid ab.$$

Question. What are the cases we should consider?

Discussion

Prove that for any integer $n \in \mathbb{Z}$,

1. $n^3 - n$ is even.

2. $6 \mid n^3 - n$.

Challenge

Theorem

The product of r consecutive terms is divisible by $r!$.

Appendix

Quotient Remainder Theorem

Theorem

Let n be a positive integer. Then for any m, there is a unique r with $0 \leq r < n$ such that

$$m \equiv r \mod n.$$

Equivalently, there is a q such that

$$m = qn + r, \qquad \text{for some } 0 \leq r < n.$$

Proof.

First suppose $m \geq 0$. If $m < n$, let $r = m$ and $q = 0$. Otherwise, if $m \geq n$, let q be the largest number such that $m \geq nq$ and let $r = m - nq \geq 0$. We claim that $r < n$. For if $r \geq n$, then $r = n + d$ for $d \geq 0$. Hence, $m = nq + n + d = n(q + 1) + d \geq n(q + 1)$, contradicting q being the largest choice. This proves that

$$m = qn + r \quad \text{for some } 0 \leq r < n.$$

Quotient Remainder Theorem

Continue.

Now suppose $m < 0$. If $-n \leq m$, let $r = n + m \geq 0$ and $q = -1$. Also, $r < n$ too since $m < 0$. So,

$$m = (-1)n + r, \qquad \text{for some } 0 \leq r < n.$$

Now suppose $m < -n$. Let q' be the smallest integer such that $-q'n \leq m$ and let $r = m + nq' \geq 0$. We claim that $r < n$. Suppose $r \geq n$. Then $r = n + d$ for $d \geq 0$. Hence,

$$m = -q'n + n + d = -n(q' - 1) + d \geq -n(q' - 1),$$

and since $(q' - 1) < q'$, it contradicts the choice of q' being the smallest. So, let $q = -q'$, we have

$$m = qn + r \quad \text{for some } 0 \leq r < n.$$

Quotient Remainder Theorem

Continue.

Finally, we will prove the uniqueness. Suppose there are q and q' such that

$$m = qn + r \quad \text{and} \quad m = q'n + r' \text{ for some } 0 \geq r, r' < n.$$

Without lost of generality, assume $r' \geq r$. Then

$$r' - r = (m - q'n) - (m - qn) = qn - q'n = n(q - q').$$

Since $r < n$ and $r' < n$, $0 \geq n(q - q') = r' - r < n$ tells us that necessarily $q - q' = 0$, and hence, $r' r'$. $\square$