MOE H3 Math

Numbers and Proofs

Lecture 2

- Prove by contrapositive
- Prove by contradiction

When Direct Proof fails

Theorem

For every integer a, if $3a^2 + 1$ is even, then a is odd.

Direct proof

Since $3a^2 + 1$ is even

there exist an integer n such that $3a^2 + 1 = 2n$

Not easy to go on from here to get:

$$a = 2q + 1$$

Try indirect proof

Hence a is odd.

Negation

Standard form: not P Symbolic form: ~P

Example

P: It is raining $\xrightarrow{\text{negation}}$ ~P: It is not raining

Q: N is an odd integer $\xrightarrow{\text{negation}}$ ~Q: N is not an odd integer

N is an even integer

When P is true, ~P is false, and vice versa

truth values

Negation

Example

N is either a square or a cube   P or Q

Negation

N is neither a square nor a cube

N is not a square and not a cube

N is not a square or not a cube

$\sim (P \text{ or } Q) \equiv \sim P \text{ and } \sim Q$

$\sim (P \text{ and } Q) \equiv \sim P \text{ or } \sim Q$

Universal statement

Example

If N is an even square, then N is divisible by 4.

If the N here refers to a general integer, then it is known as a universal statement.

For every even integer N which is a square,
N is divisible by 4.

Standard form: For all x in D, P(x)

Symbolic form: $\forall x \in D, P(x)$

Other phrases

for each …, for every …, for any …

Negation of universal statement

$\forall\, x \in D, P(x)$ Negation: $\sim(\forall\, x \in D, P(x))$

$\exists\, x \in D, \sim P(x)$

Example (daily life)

S: All students hand in homework

~S: Not all students hand in homework

~S: Some students do not hand in homework

T: All even numbers are divisible by 4

~T: Not all even numbers are divisible by 4

~T: Some even numbers are not divisible by 4

Negation of existential statement

$\exists\ x \in D, P(x)$ Negation: $\sim(\exists\ x \in D, P(x))$

$\forall\ x \in D, \sim P(x)$

Example (daily life)

S: Some students hand in homework

~S: No students hand in homework
~S: All students do not hand in homework

T: Some even numbers are divisible by 4

~T: No even numbers are divisible by 4

~T: All even numbers are not divisible by 4

Proof by Contrapositive

If P then Q

Contrapositive: If ~Q then ~P

same meaning

For every integer a, if $3a^2 + 1$ is even, then a is odd.

same as

For every integer a, if a is even, then $3a^2 + 1$ is odd.

When the hypothesis involves a more complicated expression of the variable

Example 1

Theorem

For every integer a, if $3a^2 + 1$ is even, then a is odd.

Proof We prove this by contrapositive:

Suppose a is not odd. We shall prove $3a^2 + 1$ is not even.

So $a = 2k$ for some integer k.

Then $3a^2 + 1 = 3(2k)^2 + 1$

$= 3(4k^2) + 1$

$= 2(6k^2) + 1$

Since $3a^2 + 1 = 2q + 1$ for some integer q

So $3a^2 + 1$ is odd. □

When the hypothesis or conclusion involves the 'negation' of concepts

Example 2

Theorem

For m, n $\in \mathbb{Z}$, if $3 \nmid mn$, then $3 \nmid m$.

Contrapositive

For m, n $\in \mathbb{Z}$, if $3 \mid m$, then $3 \mid mn$.

Proof We prove this by contrapositive:

Suppose $3 \mid m$. We shall prove $3 \mid mn$.

Exercise (complete the proof)

Rational and irrational numbers

Definition

A real number r is a rational number iff
r can be written as a quotient m/n
where m and n are integers, with $n \neq 0$.

Definition

An irrational number
is a real number that is not a rational number.

Remark

Every integer <u>is</u> a rational number.

When the hypothesis or conclusion involves the 'negation' of concepts

Example 3

Theorem

If r is an irrational number, then $\sqrt{r}$ is also an irrational number.

Contrapositive

If $\sqrt{r}$ is a rational number, then r is also a rational number.

Proof We prove this by contrapositive:

Suppose $\sqrt{r}$ is rational. We shall prove r is rational.

Exercise (complete the proof)

Direct VS Contrapositive

Theorem

For $m \in \mathbb{Z}$, if $3 \mid m^2$, then $3 \mid m$.

Which proving method shall we use?

Direct proof

Start from $3 \mid m^2$; end with $3 \mid m$.

Contrapositive

Start from $3 \nmid m$; end with $3 \nmid m^2$.

Consider cases: $m = 3k+1$ and $m = 3k+2$

Example 4

Theorem

For $m \in \mathbb{Z}$, if $3 \mid m^2$, then $3 \mid m$.

Proof We prove this by contrapositive:

Suppose $3 \nmid m$. We shall prove $3 \nmid m^2$.

Consider the two cases:

Case (i) $m = 3k+1$

Then $m^2 = (3k + 1)^2 = \ldots = 3(3k^2 + 2k) + 1$

So m^2 has remainder 1 when divided by 3.

We conclude that $3 \nmid m^2$.

Case (ii) $m = 3k+2$ Exercise $\square$

Proving Biconditionals

Theorem
For m, n $\in \mathbb{Z}$, mn is odd if and only if m and n are odd.

Need to break down into two parts:

($\Leftarrow$) The "If" part: Direct proof

For m, n $\in \mathbb{Z}$, if m and n are odd, then mn is odd.

($\Rightarrow$) The "only if" part: Proof by contrapositive

For m, n $\in \mathbb{Z}$, if mn is odd, then m and n are odd.

For m, n $\in \mathbb{Z}$, if m or n is even, then mn is even.

For m, n $\in \mathbb{Z}$, if m and n are odd, then mn is odd.

Example 5 (Biconditionals)

Theorem

For m, n $\in \mathbb{Z}$, mn is odd if and only if m and n are odd.

Proof ($\Leftarrow$)

Since m and n are odd,

there exist integers p, q such that $m = 2p+1, n = 2q+1$.

So, we obtain $mn = (2p+1)(2q+1) = 4pq + 2p + 2q + 1$

$= 2(2pq + p + q) + 1$

So $mn = 2k + 1$ for some integer k.

Hence, mn is odd.

For $m, n \in \mathbb{Z}$, if mn is odd, then m and n are odd.

Example 5 (cont.)

Theorem
For $m, n \in \mathbb{Z}$, mn is odd if and only if m and n are odd.

Proof $(\Rightarrow)$ We prove this by contrapositive:

Assume m or n are even. We shall prove mn is even.

Consider two cases: (i) m is even; (ii) n is even

Case (i) m is even
There exists an integer p such that $m = 2p$

So, we obtain $mn = (2p)n = 2(pn)$

So $mn = 2k$ for some integer k. Hence, mn is even.

Case (ii) n is even Similar to case (i) $\square$

Proof by Contradiction

To prove statement R is true

Assume ~R is true

Try to get a contradiction

Conclude that R must be true

When R is a universal statement, R : $(\forall x)\ P(x)$

then ~R : $(\exists x)\ {\sim}P(x)$.

By assuming ~R is true,
we can start the proof with:
There is some x such that ~P(x).
From there we try to get a contradiction.

Using Contradiction

When do we use?

- When there's no direct proof
- When it's easy to work with $\sim R$

Advantage

For conditional statement $P \to Q$,
we have more assumption to work with:

P is true and $\sim Q$ is true

Disadvantage

No clear goal to work toward.

Example 6

Theorem

Let a, b, c be integers such that $a^2 + b^2 = c^2$.
Then a, b cannot be both odd.

Negation

For some integers a, b, c, we have $a^2 + b^2 = c^2$ and a, b are both odd.

Contradiction: odd = even

Example 6 (cont.)

Proof (by contradiction)

Suppose $a^2 + b^2 = c^2$ and a, b are both odd.

Since a, b are odd, then a^2, b^2 are also odd.

So $c^2 = a^2 + b^2$ is even and hence c is even.

Write: $a = 2k + 1$, $b = 2h + 1$, $c = 2t$ for $k, h, t \in \mathbb{Z}$

$$\begin{aligned} a^2 + b^2 = c^2 &\Rightarrow (2k+1)^2 + (2h+1)^2 = (2t)^2 \\ &\Rightarrow (4k^2 + 4k + 1) + (4h^2 + 4h + 1) = 4t^2 \\ &\Rightarrow (4k^2 + 4k + 4h^2 + 4h) + 2 = 4t^2 \\ &\Rightarrow 2(k^2 + k + h^2 + h) + 1 = 2t^2 \end{aligned}$$

divide both sides by 2

Since LHS is odd and RHS is even, we get a contradiction.

So when $a^2 + b^2 = c^2$, a and b cannot be both odd. $\square$

Example 7

Theorem
For any integer n, there is no integer a > 1 such that a | n and a | (n+1).

Negation

There is an integer n and there is an integer a > 1 such that a | n and a | (n+1).

Contradiction: $a > 1$ and $a = \pm 1$

Example 7 (cont.)

Proof (by contradiction)

Suppose there is an integer n and integer $a > 1$ such that $a \mid n$ and $a \mid (n+1)$.

Then $n = ak$ and $n + 1 = ah$ for some integers k, h

Then $ak + 1 = ah$

$\Rightarrow 1 = ah - ak = a(h-k)$

$\Rightarrow a \mid 1 \Rightarrow a = \pm 1$

This contradictions that $a > 1$.

We conclude that, for any n, there is no integer $a > 1$ such that $a \mid n$ and $a \mid (n+1)$. □

Rational Numbers in Lowest Term

Every rational number can be written as quotient in more than one way.

Example

lowest term $\boxed{\frac{2}{3},}\ \frac{4}{6},\ \frac{6}{9},\ \cdots$

all represent the same rational number.

numerator and denominator have no common factor > 1

We say a rational number m/n (with n > 0) is in lowest term if m and n are relatively prime.

Contradiction: m/n in lowest term and m, n have common factor 2

Example 8

Theorem

$\sqrt{2}$ is an irrational number.

Proof (by contradiction): Assume $\sqrt{2}$ is rational

Write $\sqrt{2}$ as quotient in lowest term $\sqrt{2} = \dfrac{m}{n}$

m and n relatively prime

$$\frac{m^2}{n^2} = 2$$

$\Rightarrow m^2 = 2n^2$

$\Rightarrow m^2$ is even

$\Rightarrow m$ is even

$\Rightarrow m = 2k$ for some integer k

$\Rightarrow 4k^2 = 2n^2$

$\Rightarrow 2k^2 = n^2$

$\Rightarrow n^2$ is even

$\Rightarrow n$ is even

$\Rightarrow$ m, n have common factor 2

This contradicts m and n relatively prime

We conclude that $\sqrt{2}$ is irrational. $\square$

Euclidean Algorithm

Procedure to find gcd(a, b): (for $a \neq 0$)

$b = a \times q_1 + r_1$	$\gcd(a, r_1)$
$a = r_1 \times q_2 + r_2$	$= \gcd(r_1, r_2)$
$r_1 = r_2 \times q_3 + r_3$	$= \gcd(r_2, r_3)$
$\vdots$	$=$
$r_{n-3} = r_{n-2} \times q_{n-1} + r_{n-1}$	$\gcd(r_{n-2}, r_{n-1})$
$r_{n-2} = r_{n-1} \times q_n + r_n$	$= \gcd(r_{n-1}, r_n)$
$r_{n-1} = r_n \times q_{n+1} + r_{n+1}$	$= \gcd(r_n, 0)$

Example 9 (2017 paper)

Theorem

There is no integer solution x, y with x prime such that $1591x + 3913y = 9331$

Proof (by contradiction):

First we find gcd(1591, 3913)

Euclidean Algorithm

$3913 = 1591 \times 2 + 731$

$1591 = 731 \times 2 + 129$

$731 = 129 \times 5 + 86$

$129 = 86 \times 1 + 43$

$86 = 43 \times 2 + 0$

So gcd(1591, 3913) = 43

So there are integer solutions for $1591x + 3913y = 43$

We check: $43 \mid 9331$

So there are also integer solutions for

$1591x + 3913y = 9331$

Example 9 (cont.)

Theorem

There is no integer solution x, y with x prime such that $1591x + 3913y = 9331$

Proof (by contradiction):

Assume x is prime with some integer y such that

$1591x + 3913y = 9331$ Divide both sides by d = 43

$37x + 91y = 217$ (*)

Observe that $7 \mid 91$ and $7 \mid 217$. So $7 \mid 37x$

Since gcd(7, 37) = 1, so $7 \mid x$.

By our assumption, x is a prime, so $x = 7$.

Substitute in (*): $91y = 217 - 37\times7 = -42$

This contradicts y is an integer. We conclude that x cannot be a prime. $\square$