MOE H3 Math

Numbers and Proofs

Lecture 3

- Proving existential statements
  - Constructive Proof
  - Non-constructive Proof

Proving Existential Statements

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

$\forall x \in D, \exists y \in D, P(x, y)$

$\exists x \in D, \forall y \in D, P(x, y)$

Two approaches:

1. Constructive proof
2. Non-constructive proof

Constructive Proof

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

- Give specific example for x.

$\forall\, x \in D, \exists\, y \in D, P(x, y)$

- Construct example for y in terms of x.

$\exists\, x \in D, \forall\, y \in D, P(x, y)$

- Construct example for x independent of y.

❖ Justify that the given examples satisfy the stated condition P

Pythagorean Triples

Definition

(a, b, c) is called a Pythagorean Triple iff a, b and c are positive integers and satisfy $a^2 + b^2 = c^2$.

Example

(3, 4, 5), (5, 12, 13)

Example 1

Theorem
There is one and only one Pythagorean triple (a, b, c) such that a, b, c are consecutive integers.

Proof (There is one) Constructive proof

Take $(a, b, c) =$

(There is only one)

Suppose a, b, c are consecutive.

Then $b = a + 1$, $c = a + 2$. To show a must equal 3

$a^2 + (a+1)^2 = (a+2)^2 \Rightarrow a^2 - 2a - 3 = 0 \Rightarrow (a - 3)(a + 1) = 0$

So $a = 3$ or $a = -1$.

Since Pythagorean triple consists of positive integers, so a can only be 3. $\square$

Example 2

Theorem
There are infinitely many Pythagorean triples

Proof Constructive proof

Suppose (a, b, c) is a Pythagorean triple, say $(a, b, c) = (3, 4, 5)$

Then $a^2 + b^2 = c^2$.

Let k be any positive integer.

$$(ka)^2 + (kb)^2 = k^2a^2 + k^2b^2 = k^2(a^2 + b^2) = k^2c^2 = (kc)^2$$

So (ka, kb, kc) is also a Pythagorean triple.

Since there are infinitely many k,
we have infinitely many Pythagorean triple (ka, kb, kc). $\square$

Prime and composite numbers

Definition
An integer n is prime iff
$n > 1$ and for all positive integers r and s,
if $n = rs$, then either $r = n$ or $s = n$.

equiv: the only positive divisors of n are 1 and n

Definition
An integer n is composite iff
$n > 1$ and $n = rs$ for some positive integers r and s such that $1 < r < n$ and $1 < s < n$.

equiv: n has a divisor d such that $1 < d < n$.

Example 3

Theorem

We can find 100 consecutive positive integers which are all composite numbers.

Constructive proof

Find integers $n, n+1, n+2, \ldots, n+99$, all of which are composite.

Proof

Take $n = 101! + 2$

Then n has a factor 2 and hence is composite.

Similarly, $n + k = 101! + (k+2)$ has a factor $k+2$ and hence is composite for $k = 1, 2, \ldots, 99$.

Hence the existential statement is proven. $\square$

Example 4

Theorem

For all rational numbers p and q with $p < q$, there is a rational number x such that $p < x < q$.

Constructive proof

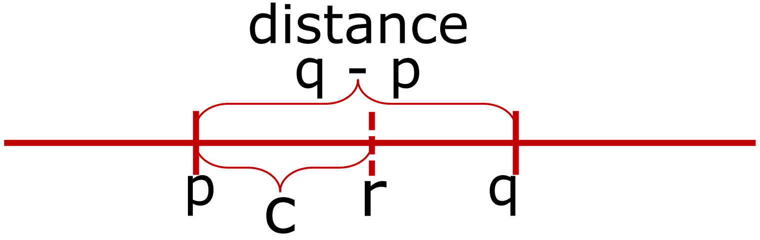
Find such a rational x in terms of p and q.

Proof Let $x = \dfrac{p+q}{2}$ which is a rational number.

Since $p < q$, $x = \dfrac{p+q}{2} < \dfrac{q+q}{2} = q$ So $x < q$

$x = \dfrac{p+q}{2} > \dfrac{p+p}{2} = p$ So $p < x$

Hence, we have shown the existence of rational number x such that $p < x < q$. $\square$



Example 5

Theorem

For all rational numbers p and q with $p < q$, there is an irrational number r such that $p < r < q$.

Idea of Proof

Construct r in terms of p and q.

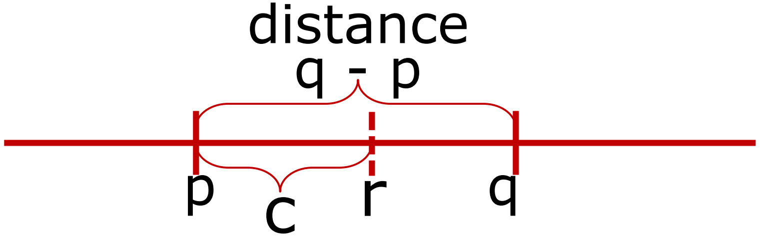
$r = p + c$

$0 < c < q - p$

Take

$$c = \frac{q - p}{\text{(a number greater than 1)}}$$

irrational



Example 5 (Cont.)

Theorem

For all rational numbers p and q with $p < q$, there is an irrational number r such that $p < r < q$.

Proof

Take $r = p + (q - p)/\sqrt{2}$.
We need to show r is irrational and $p < r < q$.

Since $q > p$, $r = p + (\text{positive number}) > p$
On the other hand, $(q - p)/\sqrt{2} < q - p$.
So $r < p + (q - p) = q$.

Suppose r is rational.
We have $\sqrt{2} = (q - p)/(r - p)$.
Since p, q, r are all rational, and $r - p \neq 0$,
this implies $\sqrt{2}$ is rational, which gives a contradiction.

□

Non-Constructive Proof

- Use when specific examples are not easy or not possible to find or construct.
- Make arguments why such objects have to exist.
- May need to use proof by contradiction.
- Use definition, axioms or results that involves existential statements.

Example 6

Theorem
Every integer greater than 1 is divisible by a prime.

Proof

If n is a prime, then we are done as $n \mid n$.

If n is not a prime, then n is a composite number.

So n has a divisor d_1 such that $1 < d_1 < n$.

If d_1 is a prime, then we are done as $d_1 \mid n$.

If d_1 is not a prime, then d_1 is composite and has a divisor d_2 such that $1 < d_2 < d_1$.

If d_2 is a prime, then we are done as $d_2 \mid d_1$ and $d_1 \mid n$ imply $d_2 \mid n$.

If d_2 is not a prime, then d_2 is composite and has a divisor d_3 such that $1 < d_3 < d_2$.

Example 6 (Cont.)

Theorem

Every integer greater than 1 is divisible by a prime.

Proof (cont.)

Continuing in this manner after k times, we will get

$$1 < d_k < d_{k-1} < \dots < d_2 < d_1 < n$$

where $d_i \mid n$ for all i.

This process must stop after finite steps,
as there can only be a finite number of d_i's between 1 and n.
On the other hand, the process will stop only if there is a d_i which is a prime.
So we conclude that there must be a divisor d_i of n which is a prime.

□

Example 7

Theorem

For any 5 distinct integers, there are (at least) 2 of them are congruence to each other modulo 4.

Proof Let the 5 integers be a_1, a_2, a_3, a_4, a_5.

By Quotient-Remainder Theorem, there are only 4 possible remainders (0, 1, 2, 3) when the a_i are divided by 4.

This means there are at least 2 integers a_i and a_j among the 5 having the same remainder r.

$$a_i = 4k + r \quad \text{and} \quad a_j = 4h + r$$

So we have $a_i - a_j = 4(k - h)$

This means $a_i \equiv a_j \pmod 4$ □

Pigeonhole Principle

In the above example, we have applied the Pigeonhole Principle:

If m pigeons go into r pigeonholes and $m > r$, then at least one pigeonhole has more than one pigeon.

A Hairy Problem

It is known that the maximum number of hairs on a human head is less than 200,000.
Prove that there are at least two people in Singapore with exactly the same number of hairs on their heads.

Example 8

Theorem

If 101 integers are chosen from 1 to 200 (inclusive), there must be at least two of them such that one is divisible by the other.

Idea of Proof

Group the 200 integers into 100 disjoint groups

A_1: 1 , 2, 4, 8, …
A_3: 3 , 2(3), 4(3), 8(3), …
A_5: 5 , 2(5), 4(5), 8(5), …
:
A_k: K , 2(k), 4(k), 8(k), …
:
A_{199} : 199

Example 8 (Cont.)

Theorem

If 101 integers are chosen from 1 to 200 (inclusive), there must be at least two of them such that one is divisible by the other.

Proof

There are 100 odd integers between 1 and 200.
Now we group the 200 integers into 100 disjoint groups as follow:
(i) Each group has exactly one odd integer. Denote the group with odd number k as A_k.
(ii) An even integer which can be expressed as $2^n k$ will be put in group A_k.
In other words, A_k contains all integers of the form k, 2k, 4k, 8k … which are smaller than 200. (Note that every even integer belongs to only one such group.)

Example 8 (Cont.)

Theorem

If 101 integers are chosen from 1 to 200 (inclusive), there must be at least two of them such that one is divisible by the other.

Proof (cont.)

Observe that if there are more than 1 number in a particular group A_k, then the smaller number always divides the larger number.

Now if we are to choose 101 integers, by pigeonhole principle, there will be at least one group A_k that we have to choose two numbers a and b, say $a < b$.

So we have $a \mid b$.

$\square$

Example 9

Theorem

There exist two irrational numbers a and b such that a^b is rational.

Idea of Proof

Try some simple irrational numbers for a and b:
say $\sqrt{2}^{\sqrt{2}}$
It is not easy to prove whether this is rational or irrational.
So we use an indirect argument instead.

Example 9 (Cont.)

Theorem

There exist two irrational numbers a and b such that a^b is rational.

Proof

Consider $\sqrt{2}^{\sqrt{2}}$. (This number is either rational or irrational)

Case 1: Suppose $\sqrt{2}^{\sqrt{2}}$ is rational.

Then we can take $a = b = \sqrt{2}$ which are irrational.

Then a^b is rational, and so we are done.

Case 2: Suppose $\sqrt{2}^{\sqrt{2}}$ is irrational.

Then we can take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ which are irrational.

Then $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$

which is rational, and we are done. $\square$

Negation

Example 10

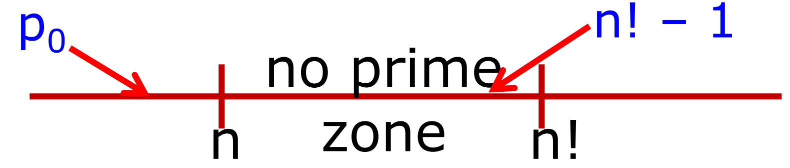
Theorem

For all integers $n > 1$, there is a prime number p such that $n \le p \le n!$.

Idea of Proof

Negation:
There is a positive integer $n > 1$ such that
for all prime p, either $p < n$ or $p > n!$.
Consider $n! - 1$ and one of its prime divisors p_0
Use this p_0 to derive a contradiction.

Negation



Example 10 (Cont.)

Theorem

For all integers $n > 1$, there is a prime number p such that $n \le p \le n!$.

Proof (By contradiction)

Suppose there is a positive integer $n > 1$ such that for all prime p, either $p < n$ or $p > n!$.
If $n = 2$, we have $n \le 2 \le n!$ (by taking 2 as the prime p).
This gives a contradiction.
Let $n > 2$. Hence $n! - 1 > 1$.
Take a prime divisor $p_0 \mid n! - 1$.
By our assumption, this $p_0 < n$ (since $p_0 \le n! - 1 < n!$).
This implies $p_0 \mid n!$ (any positive integer less than n is a factor of n!).
As it is not possible to have a same prime dividing two consecutive integers, we get a contradiction. $\square$

Example 11 (2018 paper)

Let x be any positive real numbers and n be any positive integer. Prove that there are integers a and b with $1 \le b \le n$, such that

$$\left|x - \frac{a}{b}\right| < \frac{1}{bn}$$

Hint: Use pigeonhole principle and the fractional parts of the (real) numbers x, 2x, .., nx.

Notation For any real number y, we write:

$$y = \underbrace{\lfloor y \rfloor}_{\text{integer part}} + \underbrace{\text{frac}(y)}_{\text{fractional part}}$$

integer part

fractional part
$0 < \text{frac}(y) < 1$

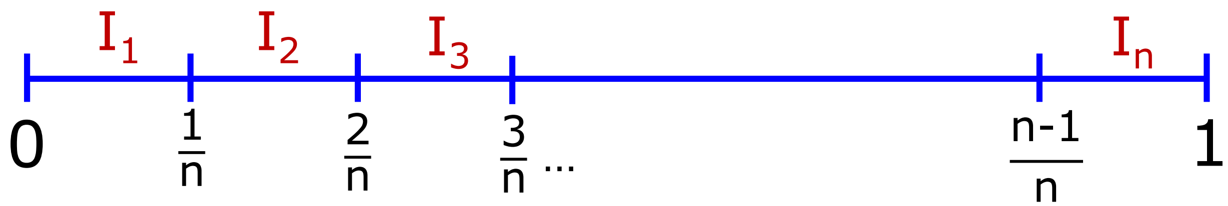
Example 11 (Cont.)

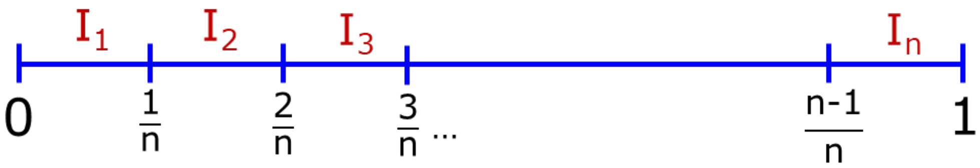
Let x be any positive real numbers and n be any positive integer. Prove that there are integers a and b with $1 \le b \le n$, such that

$$\left| x - \frac{a}{b} \right| < \frac{1}{bn}$$

Consider:

- frac(x), frac(2x), .., frac(nx)
- Subintervals of [0, 1) of length $\frac{1}{n}$





Example 11 (Cont.)

Let x be any positive real numbers and n be any positive integer. Prove that there are integers a and b with $1 \le b \le n$, such that

$$\left|x - \frac{a}{b}\right| < \frac{1}{bn}$$

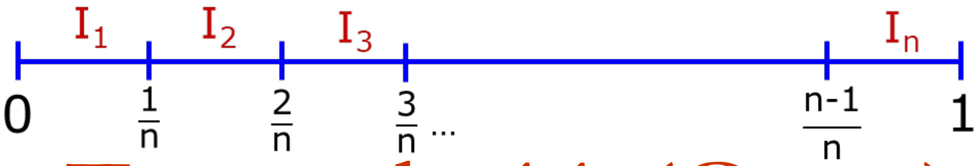
Case 1: Some frac(kx) falls in I_1

Then $kx - \lfloor kx \rfloor = \text{frac}(kx) < \frac{1}{n}$

Divide both sides by k

$$\left|x - \frac{\lfloor kx \rfloor}{k}\right| < \frac{1}{kn}$$

By taking $a = \lfloor kx \rfloor$ and $b = k$, we have the inequality.



integers a and b with $1 \le b \le n$

$$\left|x - \frac{a}{b}\right| < \frac{1}{bn}$$

Example 11 (Cont.)

Case 2: None of frac(kx) falls in I_1

All frac(kx) fall in I_2, I_3, …, I_n

Pigeonhole Principle: At least two frac(kx) fall in same I_i

Let $\frac{i-1}{n} \le \text{frac}(px) < \frac{i}{n}$ and $\frac{i-1}{n} \le \text{frac}(qx) < \frac{i}{n}$

Then $|\ \text{frac}(px) - \text{frac}(qx)\ | < \frac{1}{n}$

$$|\ (px - \lfloor px \rfloor) - (qx - \lfloor qx \rfloor)\ | < \frac{1}{n}$$

$$|\ (px - qx) - (\lfloor px \rfloor - \lfloor qx \rfloor)\ | < \frac{1}{n}$$

$$|\ (p - q)x - (\lfloor px \rfloor - \lfloor qx \rfloor)\ | < \frac{1}{n}$$

WLOG: assume $p > q$

Then $1 \le p - q < n$

By taking
$a = \lfloor px \rfloor - \lfloor qx \rfloor$, $b = p-q$,
we have the inequality.

Divide both sides by $p-q$

$$\left|x - \frac{(\lfloor px \rfloor - \lfloor qx \rfloor)}{p-q}\right| < \frac{1}{(p-q)n}$$

□

Example 12

Theorem

There are infinitely many prime numbers.

A variation of existential statement

Non-constructive proof

Rephrase:
It is not that
there are only finitely many prime numbers.

Assume negation is true

Suppose there are only finitely many primes.

Example 12 (Cont.)

Proof (by contradiction)

Suppose there are only finitely many primes.

Let $p_1, p_2, p_3, \ldots, p_m$ be all the primes.

Consider the integer $M = p_1p_2p_3\ldots p_m + 1$

Since $M > 1$, it has a divisor which is a prime

This prime divisor must be one of $p_1, p_2, p_3, \ldots, p_m$.

So $p_i \mid M$ for some prime p_i.

Also $M - 1 = p_1p_2p_3\ldots p_m \Rightarrow p_i \mid (M - 1)$

But there is no integer $a > 1$ such that $a \mid M$ and $a \mid (M - 1)$.

This gives a contradiction.

So we conclude that there are infinitely many prime numbers. $\square$