MOE H3 Math Numbers and Proofs

Lecture 1

Proving Techniques

- Direct proofs
- Proof by cases

Number Theory Concepts

 Parity, Divisibility, Congruence Modulo, GCD

Types of statements (Structure)

Conditional statement

Standard form: If P then Q

Symbolic form: $P \rightarrow Q$

P is called the hypothesis; Q is called the conclusion

Example: If n > 2, then n > 1

Biconditional statement

Standard form: P if and only if Q abbr: P iff Q

Symbolic form: $P \leftrightarrow Q$

Example: n is odd if and only if n + 1 is even.

Types of statements (Structure)

Existential statement

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

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

D is called the domain

Example: There exists real number x such that $x^2 = 2$

D is the set of real numbers P(x) is $x^2 = 2$

Other phrases

There is ..., For some ..., We can find ..., ... has ...

Types 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.

Examples

An integer a is even if and only if there exists an integer n such that a = 2n.

An integer a is odd if and only if there exists an integer n such that a = 2n+1.

Types 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 a proof.

Example: If x and y are integers, then x + y is an integer

More axioms are listed in Appendix A

Basic Properties of Numbers

The following properties of real numbers \boldsymbol{R} are regarded as axioms.

Properties	For all real numbers x, y and z
Closure	$x + y$ and $x \cdot y$ are real numbers
Identity	$x + 0 = x$ and $x \cdot 1 = x$
Inverse	$x + (-x) = 0$ and $x \cdot (1/x) = 1$ if $x \neq 0$
Commutative	$x + y = y + x$ and $x \cdot y = y \cdot x$
Associative	$x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Distributive	$x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$

These properties also hold for integers Z.

H3 Math

Lecture 1

Proof

```
Theorem conditional statement: P \rightarrow Q
For a \in Z, if a is odd, then a + 1 is even.

Proof Suppose a is odd. Starting from hypothesis
```

```
there exists an integer n definition of odd no. such that a = 2n + 1

So a + 1 = 2n + 2 = 2(n + 1) algebraic manipulation

Since n + 1 is an integer m, closure property of + so a + 1 = 2m for some integer m definition of even no. hence a + 1 is even. Ending with conclusion
```

H3 Math Lecture 1

Direct Proof

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

It is a series of valid argument that start with the hypothesis P and end with the conclusion Q.

Starting from hypothesis P

true statement true statement :

Conclusion Q

Definitions
Properties/axioms
Algebraic manipulation
Other known results

Existential Instantiation

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
So a + 1 = 2n + 2 = 2(n + 1)
Since n + 1 is an integer m,
so a + 1 = 2m for some integer m
hence a + 1 is even
```

Ask yourself what your "goal" is.

Existential Instantiation

- If you know something exists, you can give it a name.
- However, you cannot use the same name to refer to two different things, both of which are currently under discussion.

Example

Let a be an odd integer. Then there exists an integer n such that 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.

Theorem

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

"Proof"

Suppose m is even and n is odd.

If mn is even, then $\exists r \in \mathbb{Z}$ such that mn = 2r.

Also since m is even, $\exists p \in Z$ such that m = 2p,

and since n is odd, $\exists q \in Z$ such that n = 2q + 1.

Thus mn = (2p)(2q + 1) = 2r, where r is an integer.

Hence mn is even.



Notation d | n

Divisibility

negation d∤n

Definition

Let n and d be integers with $d \neq 0$.

We say n is divisible by d if and only if there exists an integer k such that n = dk.

Example

12 is divisible by 3 as $12 = 3 \times 4$ 3 | 12

21 is divisible by 7 as $21 = 7 \times 3$ 7 | 21

In general, when n is divisible by m, then n can be written in the form $m \times k$ where k is an integer

Theorem

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

```
Proof Since x is even, Starting from hypothesis there exist an integer n such that x = 2n. definition of even no. So, we obtain x^2 = (2n)^2 = 4n^2 algebraic manipulation Since n^2 is an integer q, closure property of x this means that x^2 = 4q for some integer q. definition of divisibility Hence, x^2 is divisible by 4. Conclusion
```

H3 Math Lecture 1 13

Exercise Prove the following theorem:

If a | b and a | c, then a | (b + c) and a | (b - c).

Example 4

```
Theorem Let a, b \in \mathbb{Z}.
If a and b > 0 and a \mid b, then a \le b.
```

Proof

Suppose a and b > 0 and a | b. Starting from hypothesis Then there exists an integer k so that b = ak.

definition of divisibility

So k > 0, as a and b are positive property T25 of App A It follows that $1 \le k$, as every positive integer ≥ 1

basic property of integer

14

Then $a \le ak$, as multiplying both sides of an inequality by a positive number preserves the inequality. property T20 of App A Hence $a \le b$. Conclusion

H3 Math Lecture 1

Counter-examples

To show that a conditional statement is false: Give counter-examples.

Example Let a, b, c be non-zero integers.

- (i) If $c \mid ab$, then $c \mid a$ or $c \mid b$. Counter-examples: a = 3, b = 2, c = 6
- (ii) If a | c and b | c, then ab | c. Counter-examples: a = 4, b = 6, c = 12

Note: your counter-examples must make the hypothesis a true statement, and the conclusion a false statement.

Congruence modulo

Definition

Let a, b and n be integers with n > 0.

Then $a \equiv b \pmod{n}$ if and only if $n \mid a - b$.

a = b + nk for some integer k

We say: a and b are congruence modulo n or a is congruent to b modulo n

```
Example 24 \equiv 3 \pmod{7}

n = 7 31 \equiv -11 \pmod{7}

25 \not\equiv 10 \pmod{7}
```

"≡" behaves like "="

Properties of Congruence

```
Theorem Let n be an integer with n > 1.
```

- (1) For every integer a, $a \equiv a \mod n$ reflexive property
- (2) For all integers a and b, symmetric property if $a \equiv b \mod n$, then $b \equiv a \mod n$
- (3) For all integers a, b and c, transitive property if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$

Exercise: Prove parts 1, 2, 3

Modular Arithmetic

"≡" behaves like "="

Theorem

For all integers a, b, c, d and n, with n > 1

If $a \equiv b \mod n$ and $c \equiv d \mod n$, then

1. $a + c \equiv b + d \mod n$

preserve addition

2. $ac \equiv bd \mod n$

- preserve multiplication
- 3. $a + k \equiv b + k \mod n$ for every $k \in \mathbb{Z}$
- 4. $ka \equiv kb \mod n$ for every $k \in \mathbb{Z}$
- 5. $a^m \equiv b^m \mod n$ for every $m \in \mathbb{Z}^+$ preserve power

```
Part 2 of Theorem
If a \equiv b \mod n and c \equiv d \mod n, then ac \equiv bd \mod n
Proof Given a \equiv b \mod n.
      So a = b + nk for some integer k (1)
      Given c \equiv d \mod n.
       So c = d + nh for some integer h (2)
     By multiplying (1) and (2),
   ac = (b+nk)(d+nh) = ... = bd + n(dk + bh + nkh)
       So ac = bd + nq for some integer q.
       So ac \equiv bd mod n.
```

Greatest common divisor

Definition

Let a, b be integers, not both 0.

The largest integer that divides both a and b is called the greatest common divisor of a and b.

Notation gcd(a, b)

Example gcd(48, 84) = 12

Divisors of 48:

 ± 1 , ± 2 , ± 3 , ± 4 , ± 6 , ± 8 , ± 12 , ± 16 , ± 24 , ± 48

Divisors of 84:

 ± 1 , ± 2 , ± 3 , ± 4 , ± 6 , ± 7 , ± 12 , ± 14 , ± 21 , ± 28 , ± 42 , ± 84

Basic properties of GCD

Let a and b be integers with a \neq 0.

$$2.\gcd(a, a) =$$

$$3.\gcd(a, 0) =$$

"Working" Definition of GCD

Rephrasing the definition

Let a, b be integers, not both 0, and $d \in \mathbb{Z}^+$.

```
d = gcd(a, b) iff
```

- d | a and d | band
- For all $k \in \mathbb{Z}^+$, if $k \mid a$ and $k \mid b$, then $k \leq d$

Theorem

Let a, b be integers, not both 0. Then $gcd(a + b, a - b) \le gcd(2a, 2b)$

Proof

```
Let e = gcd(a + b, a - b).

Then e \mid (a + b) and e \mid (a - b).

So e \mid (a + b) + (a - b) \Rightarrow e \mid 2a

and e \mid (a + b) - (a - b) \Rightarrow e \mid 2b

This implies e is a common divisor of 2a and 2b.

So e \leq gcd(2a, 2b).
```

Theorem

```
Let c and d be integers, not both 0.

If q and r are integers such that c = dq + r,

then gcd(c, d) = gcd(d, r).
```

Proof

```
Let m = gcd(c, d) and n = gcd(d, r)
To prove m = n:
we will show m \le n and n \le m.
```

Example 7 (cont.)

```
Proof Show n < m
  n = gcd(d, r) \Rightarrow n \mid d \text{ and } n \mid r
 There exists integers x and y: d = nx and r = ny
  From c = dq + r we have c = (nx)q + ny
                                     c = n(xq + y)
  Hence n | c
   n is a common divisor of c and d.
   n \leq gcd(c, d).
   So n \leq m.
 Show m \le n: Exercise
```

H3 Math Lecture 1 25

Relatively Prime

Definition

Let a and b be two nonzero integers.

Then a and b are relatively prime

if and only if gcd(a, b) = 1.

In other words, a and b have no common divisors > 1.

Alternative term: co-prime

Remark

The integers a and b need not be prime numbers in order to be relatively prime.

Linear combination

Theorem

Let a and b be integers, not both 0.

- (i) $gcd(a, b) = ax_0 + by_0$ for some integers x_0 and y_0 .
- (ii) If a and b are relatively prime, then $1 = ax_0 + by_0$ for some integers x_0 and y_0 .

Proof of (ii) follow from (i)

a and b relatively prime

- \Rightarrow gcd(a, b) = 1
- \Rightarrow 1 = $ax_0 + by_0$ for some integers x_0 and y_0 .

```
Theorem (Euclid's Lemma)
Let a, b, c be any integers.

If a | bc and gcd(a, b) = 1, then a | c.
```

```
Proof a \mid bc \Rightarrow bc = ak some k \in \mathbb{Z}

gcd(a, b) = 1 \Rightarrow ax + by = 1 some x, y \in \mathbb{Z}

\Rightarrow cax + cby = c

\Rightarrow acx + aky = c

\Rightarrow a(cx + ky) = c

\Rightarrow a \mid c
```

Also known as: Division Algorithm

Quotient Remainder Theorem

```
Let n, d \in \mathbb{Z}^+
d \mid n \text{ means } n = dq \text{ for some } q \in \mathbb{Z}
r = 0
d \nmid n \text{ means } n \neq dq \text{ for any } q \in \mathbb{Z}
n = dq + r
0 < r < d
```

Theorem

For all integers n and d with d > 0, there exist unique integers q and r such that

$$n = dq + r$$

$$0 \le r < d$$

H3 Math Lecture 1 29

Quotient Remainder Theorem

```
Let n, d \in \mathbb{Z} with d > 0
          n = dq + r
                         0 \le r < d
Example
n = 17, d = 5 Take q = 3 and r = 2
                  17 = 5 \times 3 + 2
                                         0 \le 2 < 5
n = 4, d = 5 Take q = 0 and r = 4
                 4 = 5 \times 0 + 4
n = -4, d = 5
```

Proof by Cases

Theorem

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

$$(n = 3k \text{ or } n = 3k + 1 \text{ or } n = 3k + 2)$$

We prove the three cases:

If n = 3k, then $3 | n^3 - n$.

AND

If n = 3k + 1, then $3 | n^3 - n$.

AND

If n = 3k + 2, then $3 | n^3 - n$.

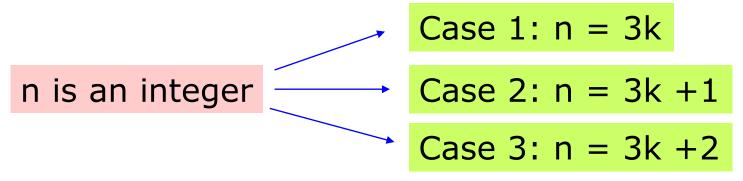
Theorem

```
If n is an integer, then 3 divides n^3 - n.
        Consider three cases:
Proof
Case 1: n = 3k for some integer k
       Then n^3 - n = (3k)^3 - (3k)
                    = 3[9k^3 - k]
       Since 9k^3 - k is an integer, so 3 \mid n^3 - n.
Case 2: n = 3k + 1 for some integer k
       Then n^3 - n = (3k+1)^3 - (3k+1)
                    = 3[9k^3 + 9k^2 + 2k]
       Since 9k^3 + 9k^2 + 2k is an integer, so 3 \mid n^3 - n.
Case 3: n = 3k + 2 for some integer k Exercise
```

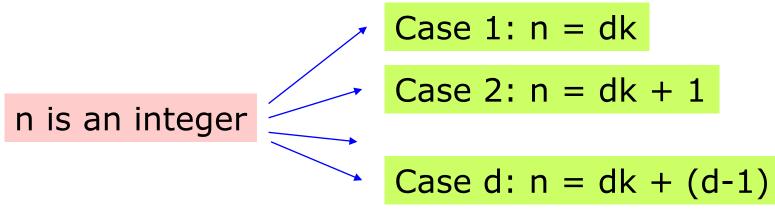
H3 Math Lecture 1 32

When using cases, they must cover all possibilities

Cases by Remainder



Usually when the statement involves divisibility by 3 or multiples of 3.



Usually when the statement involves divisibility by d or multiples of d.

H3 Math Lecture 1 33

When using cases, they must cover all possibilities

Cases by Parity

n is an integer

Case 1: n is even

Case 2: n is odd

Usually when the statement involves divisibility by an even integer or multiples of an even integer.

m and n are integers

Case 1: m and n even

Case 2: m and n odd

Case 3: m odd and n even

Case 4: m even and n odd

When using cases, they must cover all possibilities

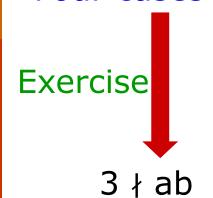
Example 10

Theorem

For all integers a and b, if $3 \nmid a$ and $3 \nmid b$, then $3 \nmid ab$.

$$a = 3k + 1$$
 $b = 3m + 1$
or $3k + 2$ or $3m + 2$

Four cases



Case 1:
$$a = 3k + 1$$
 and $b = 3m + 1$

Case 2:
$$a = 3k + 1$$
 and $b = 3m + 2$

Case 3:
$$a = 3k + 2$$
 and $b = 3m + 1$

Case 4:
$$a = 3k + 2$$
 and $b = 3m + 2$