Proofs (Chapters 7, 8 and 9)

Proof Techniques of $P \Rightarrow Q$

Proof Techniques of P $\Rightarrow$ Q

- Direct proof:

Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore Q. $\blacksquare$

Proof Techniques of $P \Rightarrow Q$

- Proof by cases:

- It is a direct method of proving statements like

$$P_1 \vee P_2 \vee \ldots. \vee P_n \Rightarrow Q$$

which is equivalent to proving

$$(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q) \wedge (P_3 \Rightarrow Q) \wedge \ldots. \wedge (P_n \Rightarrow Q).$$

Proof Techniques of P $\Rightarrow$ Q (contd.)

- Contrapositive proof (Indirect proof)
- Proving $\neg Q \Rightarrow \neg P$

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. ■

Proof Techniques of P $\Rightarrow$ Q (contd.)

- Contradiction proof.

Outline for Proving a Conditional Statement with Contradiction

Proposition If P, then Q.
Proof. Suppose P and $\sim Q$.
$\vdots$
Therefore $C \wedge \sim C$. ■

If-and-Only-If-Proof: P $\Leftrightarrow$ Q

If-and-Only-If-Proof: $P \Leftrightarrow Q$

- It is equivalent to proving $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

If-and-Only-If-Proof: $P \Leftrightarrow Q$

- It is equivalent to proving $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

Outline for If-and-Only-If Proof

Proposition P if and only if Q.

Proof.
[Prove $P \Rightarrow Q$ using direct, contrapositive or contradiction proof.]
[Prove $Q \Rightarrow P$ using direct, contrapositive or contradiction proof.] ■

Example

- Suppose a and b are integers. Prove that

  $(a \equiv b \pmod 6) \Leftrightarrow (a \equiv b \pmod 2) \land (a \equiv b \pmod 3)$

Example

- Suppose a and b are integers. Prove that

  $(a \equiv b \pmod{6}) \Leftrightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

- We first prove that
  - $a \equiv b \pmod{6} \Rightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

Example

- Suppose a and b are integers. Prove that

  $(a \equiv b \pmod{6}) \Leftrightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

- We first prove that
  - $a \equiv b \pmod{6} \Rightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

  This follows from the fact that if (a-b) is divisible by 6, (a-b) is also divisible by 2 and 3.

Example

- Suppose a and b are integers. Prove that

  $(a \equiv b \pmod{6}) \Leftrightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

- We first prove that
  - $a \equiv b \pmod{6} \Rightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

  This follows from the fact that if (a-b) is divisible by 6, (a-b) is divisible by 2 and 3.

- **Next we prove that**
  - $(a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3}) \Rightarrow a \equiv b \pmod{6}$.

Example

- Suppose a and b are integers. Prove that

  $(a \equiv b \pmod{6}) \Leftrightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

- We first prove that
  - $a \equiv b \pmod{6} \Rightarrow (a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3})$

  This follows from the fact that if (a-b) is divisible by 6, (a-b) is divisible by 2 and 3.

- **Next we prove that**
  - $(a \equiv b \pmod{2}) \wedge (a \equiv b \pmod{3}) \Rightarrow a \equiv b \pmod{6}$.

  This again follows from the fact that if (a-b) is divisible by 2 and 3, (a-b) is divisible by 6.

Example

- For any integer n, n is odd if and only if n^2 is odd.

Example

- For any integer n, n is odd if and only if n^2 is odd.
- In order to prove this statement we must prove two implications:
  - if n is odd, n^2 is odd.
  - if n^2 is odd, n is odd.
- Direct proof is easy to design.

Equivalent Statements

- Prove that the following statements are equivalent.
  1) $n - 5$ is odd.
  2) $3n+2$ is even.
  3) $n^2 - 1$ is odd.

Equivalent Statements

- Prove that the following statements are equivalent.
  1) $n - 5$ is odd.
  2) $3n+2$ is even.
  3) $n^2 - 1$ is odd.
- The above asserts that either the statements are all true or the statements are all false.

Equivalent Statements

- Prove that the following statements are equivalent.
  1) $n - 5$ is odd.
  2) $3n+2$ is even.
  3) $n^2 - 1$ is odd.
- The above asserts that either the statements are all true or the statements are all false.
- The above theorem is equivalent to proving the following implications:
  a) $(1) \Rightarrow$ **(2)**
  b) (2) $\Rightarrow$ **(3)**
  c) (3) $\Rightarrow$ **(1)**

Equivalent Statements

- Prove that the following statements are equivalent.
  1) n – 5 is odd.
  2) 3n+2 is even.
  3) $n^2 - 1$ is odd.
- The above asserts that either the statements are all true or the statements are all false.
- The above theorem is equivalent to proving the following implications:
  a) $(1) \Rightarrow$ **(2)**
  b) (2) $\Rightarrow$ **(3)**
  c) (3) $\Rightarrow$ **(1)**

The above statements are all true. Direct proof technique can be used to prove the implications.

Proving ∃x R(x)

- An **existence proof** is a proof of a statement of the form ∃x R(x).

Proving ∃x R(x)

- An **existence proof** is a proof of a statement of the form ∃x R(x).
- Constructive proof:
  - Establish R(c) for some c in the universe of x.

Proving ∃x R(x)

- An **existence proof** is a proof of a statement of the form ∃x R(x).
- Constructive proof:
  - Establish R(c) for some c in the universe of x.
- Nonconstructive proof
  - Assume no c exists that makes R(c) true, and derive a contradiction. In other words use a proof by contradiction.

Proving $\exists x\ R(x)$

- Example: Prove that if $f(x) = x^3 + x - 5$, there exists a positive real number c such that $f'(c) = 7$.
- In symbols: $\exists x \in \mathbf{R}, f'(x) = 7.$

Proving ∃x R(x)

- Example: Prove that if $f(x) = x^3 + x - 5$, there exists a positive real number c such that $f'(c) = 7$.
- In symbols: **$\exists x \in R$, $f'(x) = 7$.**
  - $f'(x) = 3x^2 + 1$.
  - Now $f'(x) = 7$ implies $x = \pm\sqrt{2}$
  - $c = \sqrt{2}$
  - $f'(\sqrt{2}) = 7$.

Example

- Prove

$$a, b \in \mathbb{N} \implies \exists\, k, \ell \in \mathbb{Z},\ \gcd(a,b) = ak + b\ell.$$

Example

- Prove

$$a, b \in \mathbb{N} \implies \exists k, \ell \in \mathbb{Z},\ \gcd(a,b) = ak + b\ell.$$

- Direct proof:
  - Given a and b, as stated, let A = { ax + by : x, y ∈ Z }.
  - This set has both positive and negative integers, as well as zero.
  - Let d be the smallest positive number of A.
  - Since d ∈ A, d is in the form d = ak +bl for some specific k, l ∈ Z.
  - d divides a and b. (why?)
  - We can now show that d = gcd(a,b). (see the text, page 126)

Practice Problems from Chapter 7

- 3, 4, 6, 7, 10, 13, 14, 17, 20, 22, 25, 28

Proofs Involving Sets (Chapter 8)

- Generally, a set **A** will be expressed in set-builder notation **A = {x:P(x)}** where **P(x)** is some statement about **x**.
  - {x: x is an odd integer}
  - $\{n \in Z$: n is odd$\}$
  - $\{(a,b) \in Z \times Z: b=a+5\}$
  - $\{X \in PowerSet(Z) : |X|=1\}$

- How to show $a \in \{x : P(x)\}$?

- How to show $a \in \{x: P(x)\}$?
  - Show that P(a) is true.

- How to show $a \in \{x: P(x)\}$?
  - Show that $P(a)$ is true.
- How to show that $a \in \{x \in S: P(x)\}$?
  - Verify that $a \in S$
  - Show that $P(a)$ is true.

- How to show $a \in \{x: P(x)\}$?
  - Show that $P(a)$ is true.
- How to show that $a \in \{x \in S: P(x)\}$?
  - Verify that $a \in S$
  - Show that $P(a)$ is true.
- Example: Suppose $A = \{x: x \in N \wedge 7 \mid x\}$.
  - Show that $14 \in A$.
  - Show that $-14 \notin A$.

How to prove A ⊆ B

- Direct approach: if a ∈ A, a ∈ B.

Proof. Suppose $a \in A$.

$\vdots$

Therefore $a \in B$.

Thus $a \in A$ implies $a \in B$,

so it follows that $A \subseteq B$. ■

How to prove A $\subseteq$ B

- Contrapositive approach: if a $\notin$ B, a $\notin$ A.

Proof. Suppose $a \notin B$.

$\vdots$

Therefore $a \notin A$.

Thus $a \notin B$ implies $a \notin A$,

so it follows that $A \subseteq B$. ■

Example

Prove that $\{x \in \mathbb{Z} : 18 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$.

Proof. Suppose $a \in \{x \in \mathbb{Z} : 18 | x\}$.
This means that $a \in \mathbb{Z}$ and $18 | a$.
By definition of divisibility, there is an integer c for which $a = 18c$.
Consequently $a = 6(3c)$, and from this we deduce that $6 | a$.
Therefore a is one of the integers that 6 divides, so $a \in \{x \in \mathbb{Z} : 6 | x\}$.

We've shown $a \in \{x \in \mathbb{Z} : 18 | x\}$ implies $a \in \{n \in \mathbb{Z} : 6 | x\}$, so it follows that $\{x \in \mathbb{Z} : 18 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$. ■

Example

Prove that if A and B are sets, then $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

- **Will be shown in the class.**

Example 8.9

Example 8.9 Suppose A and B are sets. If $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, then $A \subseteq B$.

- Solved in the text.

How to prove A = B

Proof.

[Prove that $A \subseteq B$.]

[Prove that $B \subseteq A$.]

Therefore, since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$. ■

Example

- Given sets A, B and C, prove that A x (B ∩ C) = (A x B) ∩ (A x C).
- We should be able to show that
  - A x (B ∩ C) ⊆ (A x B) ∩ (A x C), and
  - (A x B) ∩ (A x C) ⊆ A x (B ∩ C) .

An alternate solution

- Given sets A, B and C, prove that

  $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

- $A \times (B \cap C) =$

  $= \{(x,y): (x \in A) \wedge (y \in B \cap C)\}$ (def. of x)

  $= \{(x,y): (x \in A) \wedge ((y \in B) \wedge (y \in C))\}$ (def. of $\cap$)

  $= \{(x,y): ((x \in A) \wedge (y \in B)) \wedge ((x \in A) \wedge (y \in C))\}$ (rearranging)

  $= (A \times B) \cap (A \times C)$

- The proof is complete

Perfect Numbers

- Very old number theory topic.
- The problem involves adding up the positive divisors of natural numbers.

Perfect Numbers

- Very old number theory topic.
- The problem involves adding up the positive divisors of natural numbers.
- Positive divisors of 12 that are less than 12:
  - 1,2,3,4,6
  - They add up to 16 which is greater than 12.
- Positive divisors of 15 are
  - 1,3,5
  - They add up to 9 which is less than 15.
- Positive divisors of 6 are
  - 1, 2, 3
  - They add up to 6!

Perfect Numbers

- Very old number theory topic.
- The problem involves adding up the positive divisors of natural numbers.
- Positive divisors of 12 that are less than 12:
  - 1,2,3,4,6
  - They add up to 16 which is greater than 12.
- Positive divisors of 15 are
  - 1,3,5
  - They add up to 9 which is less than 15.
- Positive divisors of 6 are
  - 1, 2, 3
  - They add up to 6!

6 is called a perfect number.

Definition of Perfect Numbers

- A number p ∈ N is **perfect** if it equals the sum of the positive divisors less than it self.
- 6 is perfect since 6 = 1 + 2 + 3.
- 28 is perfect since28 = 1 + 2 + 4 +7 + 14.
- 496 is perfect since 496 = 1+2+4+8+16+31+62+124+248
- What is the next number?
  - 8128, then ?
- Euclid (323–283 BC) looked at this problem first.

Perfect Numbers

- Let P be the set containing the perfect numbers.
  - P= {p ∈ N: p is perfect}.
- Let A = $\{2^{n-1}(2^n-1)$: n ∈ N, and 2^n-1 is a prime number$\}$

First few entries of A

n	2^{n-1}	$2^n - 1$	$2^{n-1}(2^n - 1)$
1	1	1	*
2	2	3	6
3	4	7	28
4	8	15	*
5	16	31	496
6	32	63	*
7	64	127	8128
8	128	255	*
9	256	511	*
10	512	1023	*
11	1024	2047	*
12	2048	4095	*
13	4096	8191	33,550,336

A Theorem on Perfect Numbers

- **Theorem 8.1**: If
  - A = $\{2^{n-1}(2^n-1): n \in N$, and 2^n-1 is a prime number$\}$ and
  - P= $\{p \in N$: p is perfect $\}$,
  - then $A \subseteq P$.
- Set theory was invented over 2000 years after Euclid died.

Practice problems from Chapter 8

- 1, 2, 6, 7, 13, 15, 19, 20, 27, 29

Disproof

- We considered so far: given statement, prove that it is true.
- How do you prove that a statement is false?
- There is a very simple procedure that proves a statement is false.
- The procedure is called **disproof.**

There are three types of statements.

Known to be true (Theorems & propositions)	**Truth unknown** (Conjectures)	**Known to be false**
Examples: • Pythagorean theorem • Fermat's last theorem (Section 2.1) • The square of an odd number is odd. • The series $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges.	Examples: • All perfect numbers are even. • Any even number greater than 2 is the sum of two primes. (Goldbach's conjecture, Section 2.1) • There are infinitely many prime numbers of form $2^n - 1$, with $n \in \mathbb{N}$.	Examples: • All prime numbers are odd. • Some quadratic equations have three solutions. • $0 = 1$ • There exist natural numbers a, b and c for which $a^3 + b^3 = c^3$.

How to disprove P?

How to disprove P?

- Prove **¬P**.
- Now we can use the standard proof methods: direct proof, contrapositive proof, proof by contradiction.

Disproving Universal Statements: Counterexamples

- Universally quantified statement **$\forall x \in S, P(x)$**
- Its negation is **$\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$.**

Disproving Universal Statements: Counterexamples

- Universally quantified statement **$\forall x \in S, P(x)$**
- Its negation is **$\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$.**
- We just need an element **$x \in S$** that makes **$\neg P(x)$** true.
- i.e. an **x** that makes **P(x)** false.

Disproving Universal Statements: Counterexamples

- Universally quantified statement **$\forall x \in S, P(x)$**
- Its negation is **$\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$.**
- We just need an element **$x \in S$** that makes **$\neg P(x)$** true.
- i.e. an **x** that makes **P(x)** false.
- The outline of proof:

How to disprove $\forall x \in S, P(x)$.
Produce an example of an $x \in S$ that makes $P(x)$ false.

Disproving Universal Statements: Counterexamples

- The outline of proof:

> **How to disprove** $\forall x \in S, P(x)$.
>
> Produce an example of an $x \in S$ that makes $P(x)$ false.

> **How to disprove** $P(x) \Rightarrow Q(x)$.
>
> Produce an example of an x that makes $P(x)$ true and $Q(x)$ false.

Disproving Universal Statements: Counterexamples

- In both the outlines, the statement is disproved simply by citing an example that shows that the statement is not true.
- The special name for this example is called a **counterexample.**

Example:

- Conjecture: **For every n ∈, the integer $f(n) = n^2 - n + 11$ is prime.**

n	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
$f(n)$	23	17	13	11	11	13	17	23	31	41	53	67	83	101

Example:

- Conjecture: **For every n ∈, the integer f(n) = n^2-n+11 is prime.**

n	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
$f(n)$	23	17	13	11	11	13	17	23	31	41	53	67	83	101

- **Disproof:** The statement "For every n ∈, the integer f(n) = n^2-n+11 is prime" is false since f(11) = 121 = 11.11 is not a prime.

Disproving Existence Statements

- Disproving an existence statement: $\exists x \in S, P(x)$

Disproving Existence Statements

- Disproving an existence statement: **$\exists x \in S, P(x)$**
- To disprove it, we have to prove its negation.
- The negation is **$\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$.**

Disproving Existence Statements

- Disproving an existence statement: $\exists x \in S, P(x)$
- To disprove it, we have to prove its negation.
- The negation is $\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$.
- This negation is universally quantified. An example does not suffice.
- We must use direct, contrapositive or contradiction proof to prove the conditional statement

$$\text{If } \forall x \in S, \text{ then } \neg P(x)$$

Disproof by Contradiction

- To disprove **P**, we must prove **¬P.**
- To prove **¬P** with contradiction, we assume that **¬¬P ≡ P** is true and deduce a contradiction.

Example

- Disprove the conjecture:
  - (Example 9.5): There is a real number x for which $x^4 < x < x^2$.
  - (9(11)): If a, b $\in$ N, then a+b < ab.
- True or false:
  - (9(12)) If a, b, c $\in$ N and ab, bc and ac all have the same parity, then a, b and c all have the same parity.

Practice problems of Chapter 9

- 1, 2, 3, 18, 19, 22, 23, 29, 34.

Congruence of Integers

- Definition: Given integers a and b and an $n \in N$, we say that a and b are **congruent modulo n** if a and b have the same remainders when a and b are divided by n.
  - In other words, $n \mid (a-b)$.
  - We express $a \equiv b \pmod{n}$
  - $9 \equiv 1 \pmod{4}$
  - $109 \equiv 4 \pmod{3}$
  - $14 \neq 8 \pmod{4}$

Some properties of congruent modulo n

- For all integers a, $a \equiv a \pmod{n}$.

Some properties of congruent modulo n

- For all integers a, a ≡ a (mod n).
  - Follows easily since a – a = 0 = n x 0.
- If a and b are integers such that a ≡ b (mod n), b ≡ a (mod n).

Some properties of congruent modulo n

- For all integers a, a ≡ a (mod n).
  - Follows easily since a – a = 0 = n x 0.
- If a and b are integers such that a ≡ b (mod n), b ≡ a (mod n).
  - If n|(b-a), n|(a-b), vice versa.
- If a, b and c are integers such that a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (nod n).

Some properties of congruent modulo n

- For all integers a, a ≡ a (mod n).
  - Follows easily since a – a = 0 = n x 0.
- If a and b are integers such that a ≡ b (mod n), b ≡ a (mod n).
  - If n|(b-a), n|(a-b), vice versa.
- If a, b and c are integers such that a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (nod n).
  - Given n|(a-b) and n|(b-c). Now (a-c) = (a-b) + (b-c). Therefore, n|(a-c).

Modular arithmetic

- **(5(24))**Suppose that a, b and c, d are integers such that a ≡ b (mod n) and c ≡ d (mod n). Then
  - ○ (a + c) ≡ b + d (mod n)

Modular arithmetic

- **(5(24))**Suppose that a, b and c, d are integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then
  - $(a + c) \equiv b + d \pmod{n}$ (easy)
  - $a - c \equiv b - d \pmod{n}$

Modular arithmetic

- **(5(24))** Suppose that a, b and c, d are integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then
  - $(a + c) \equiv b + d \pmod{n}$ (easy)
  - $a - c \equiv b - d \pmod{n}$
    - (Easy) since $(a - c) - (b - d) = (a - b) + (d - c)$
  - $ac \equiv bd \pmod{n}$

Modular arithmetic

- **(5(24))**Suppose that a, b and c, d are integers such that a ≡ b (mod n) and c ≡ d (mod n). Then
  - ○ (a + c) ≡ b + d (mod n) (easy)
  - ○ a – c ≡ b – d (mod n)
    - (Easy) since (a – c) - (b – d) = (a– b) + (d – c)
  - ○ ac ≡ bd (mod n)
    - Given a-b = t.n and c – d = t'.n
    - Therefore, a = b+ t.n, and c = d + t'n
    - Hence ac = bd + n(bt' + dt + tt'n).
    - This implies that (ac –bd) is divisible by n.
    - ac ≡ bd (mod n)