Proofs (Chapter 4, 5 and 6)

Proofs

- A proof of a mathematical statement is logical argument which establishes the truth of a statement.
- We will cover a variety of methods of proofs.
- There are terms which we should know while proving things.

Terminology

- A <u>theorem</u> is a statement that can be shown to be true (via a proof).
- A <u>proof</u> is a sequence of statements that form an argument.
- <u>Axioms</u> or <u>postulates</u> are statements taken to be self evident or assumed to be true.
- A <u>lemma</u> (plural lemmas or lemmata) is a theorem useful within the proof of a theorem.
- A <u>corollary</u> is a theorem that can be established from theorem that has just been proven.
- A <u>proposition</u> that is true is usually a 'less' important theorem.
- A <u>conjecture</u> is a statement whose truth value is unknown.
- The <u>rules of inference</u> are the means used to draw conclusions from other assertions, and to derive an argument or a proof.

Theorems: Example

- Theorem (Divisor theorem)
  - Let a, b, and c be integers. Then
    - If $a|b$ and $a|c$ then $a|(b+c)$
    - If $a|b$ then $a|bc$ for all integers c
    - If $a|b$ and $b|c$, then $a|c$
- Corrollary:
  - If a, b, and c are integers such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers
  - By part 2 it follows that a|mb and a|nc.
  - By part 1 it follows that a|(mb+nc).
- What is the assumption? What is the conclusion?

Definitions

- An integer n is **even** if n=2a for some integer a $\in$ Z.
- A.n integer n is **odd** if n= 2a + 1 for some integer a $\in$ Z.
- Two integers have the **same parity** if they are both even or they are both odd. Otherwise, they have **opposite parity**.
- Other definitions…

Divisors

- Consider three integers a, b and c, $a \neq 0$, such that $b = ac$. In this case we say that a divides b.
- We write $a \mid b$.
- We also say that b is a multiple of a.

Divisors (Examples)

- Which of the following is true?
  - 12 | 12
  - 13 | 0
  - 0 |13
  - 121 | 11
  - 11 | 121

- **Accepted facts we will use as obvious (axioms):**
  - In algebra, a + b = b + a
  - Laws of algebra
  - Laws of set theory
  - Laws of inference

Euclidean Geometry

- Points and lines are our universe.
- Definition: Two angles are supplementary if the sum of the angles is 180 degrees.
- Axiom: Given two points, there is exactly one line.
- Theorem: If the two sides of a triangle are equal, the angles opposite them are equal.
- Corollary: If a triangle is equilateral, it is equiangular.

Multiples of an integer

- How many positive multiples of 12 are less than 100,000?
- The number of such multiples is $\lfloor 100{,}000/12 \rfloor$ which is 8333.
- In general, the number of t-multiples less than N is given by:

$$|\{m \in Z^+ \;\mid\; t \mid m \text{ and } m \le N\}| = \lfloor N/t \rfloor.$$

The Division Algorithm

Theorem: Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = qd + r$.

- **a is called dividend,**
- **d is called divisor,**
- **q is called the quotient, and**
- **r is called the remainder**

Prime numbers

Definition:

A number $n \geq 2$, is **prime** if it is only divisible by 1 and itself. A number $n \geq 2$ which is not a prime is called **composite**.

- Numbers 2,3,5,7,11, … are examples of prime numbers.

Greatest Common Divisor (gcd)

Definition:

The gcd of integers a and b, denoted gcd(a,b), is the largest integer that divides both a and b.

- gcd(18,24) = 6; gcd(10,9)=1; gcd(6,0) =6

Least Common Multiple (lcm)

Definition:

The lcm of non-zero integers a and b, denoted lcm(a,b), is the smallest positive integer that is multiple of both a and b.

- lcm(4,6) = 12; lcm(7,7)=7.

Comments

- Not all terms can be defined.
- We accept some ideas as being so intuitively clear that they require no definitions or verifications.
- We accept natural ordering of the elements of N, Z, Q and R. We also accept that for integers a and b,
  - $a + b \in Z$
  - $a - b \in Z$
  - $ab \in Z$.

Direct Proofs

- We are interested in proving an implication:

  $P \Rightarrow Q$, i.e. **if P, then Q**.

Direct Proofs

- We are interested in proving an implication:

  $P \Rightarrow Q$, i.e. **if P, then Q**.

- Consider the truth table of $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	**F**
F	T	T
F	F	T

- Our goal is to show that this conditional statement $P \Rightarrow Q$ is true.

Direct Proofs

- We are interested in proving an implication: $P \Longrightarrow Q$, i.e. **if P, then Q**.
- Consider the truth table of $P \Longrightarrow Q$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	**F**
F	T	T
F	F	T

- Our goal is to show that this conditional statement $P \Longrightarrow Q$ is true.
- Since $P \Longrightarrow Q$ is true, if P is false. Therefore, we need to show that $P \Longrightarrow Q$ is true when P is true.

Direct Proof of P $\Rightarrow$ Q

- Outline of direct proof

Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore Q. ■

- We use the rules of inference, axioms, definitions, and logical equivalences to prove Q.

Direct Proofs

- Direct proofs are used when we need to proof statements like

$$\forall x\, (P(x) \rightarrow Q(x))$$

- Main steps

Our goal is to prove that $P(a) \rightarrow Q(a)$ is a tautology for a generic value a.

1. Assume that $P(a)$ is true
2. Using axioms, previous theorems etc. prove that $Q(a)$ is true
3. Conclude that $P(a) \rightarrow Q(a)$ is true
4. Use the rule of universal generalization to infer

$$\forall x\, (P(x) \rightarrow Q(x))$$

Problem:

- Consider the following hypotheses (premises)
  - More I study, more I know
  - More I know, more I forget
  - More I forget, less I know.
- Conclusion: Everyone who studies more knows less.
  - s(x): x studies more; m(x): x knows more;
  - f(x) : x forgets more ; l(x): x knows less
- In symbols

$\forall x$, [(s(x) $\Rightarrow$ m(x)) $\wedge$ (m(x) $\Rightarrow$ f(x)) $\wedge$ (f(x) $\Rightarrow$ l(x)) $\Rightarrow$ (s(x) $\Rightarrow$ l(x)]

Problem (contd.):

- Conclusion: Everyone who studies more knows less.
  - s(x): x studies more; m(x): x knows more;
  - f(x) : x forgets more ; l(x): x knows less
  - In symbols

$$\forall x, [(s(x) \Rightarrow m(x)) \wedge (m(x) \Rightarrow f(x)) \wedge (f(x) \Rightarrow l(x)) \Rightarrow (s(x) \Rightarrow l(x)]$$

- Direct Proof: Let **c** be an arbitrary element of the universe
- (population). We need to show that **s(c) ⇒ l(c).**
  - s(c) is true.

Problem (contd.):

- Conclusion: Everyone who studies more knows less.
  - s(x): x studies more; m(x): x knows more;
  - f(x) : x forgets more ; l(x): x knows less
  - In symbols

$$\forall x, [(s(x) \Rightarrow m(x)) \wedge (m(x) \Rightarrow f(x)) \wedge (f(x) \Rightarrow l(x)) \Rightarrow (s(x) \Rightarrow l(x)]$$

- Direct Proof: Let **c** be an arbitrary element of the universe
- (population). We need to show that **$s(c) \Rightarrow l(c)$.**
  - s(c) is true.
  - $s(c) \Rightarrow m(c)$; $m(c) \Rightarrow f(c)$; $f(c) \Rightarrow l(c)$

Problem (contd.):

- Conclusion: Everyone who studies more knows less.
  - s(x): x studies more; m(x): x knows more;
  - f(x) : x forgets more ; l(x): x knows less
  - In symbols

$$\forall x, [(s(x) \Rightarrow m(x)) \wedge (m(x) \Rightarrow f(x)) \wedge (f(x) \Rightarrow l(x)) \Rightarrow (s(x) \Rightarrow l(x)]$$

- Direct Proof: Let **c** be an arbitrary element of the universe
- (population). We need to show that **s(c) ⇒ l(c).**
  - s(c) is true.
  - s(c) ⇒ m(c); m(c) ⇒ f(c); f(c) ⇒ l(c)
  - s(c) ⇒ l(c) by the transitivity

Problem (contd.):

- Conclusion: Everyone who studies more knows less.
  - s(x): x studies more; m(x): x knows more;
  - f(x) : x forgets more ; l(x): x knows less
  - In symbols

$$\forall x, [(s(x) \Rightarrow m(x)) \wedge (m(x) \Rightarrow f(x)) \wedge (f(x) \Rightarrow l(x)) \Rightarrow (s(x) \Rightarrow l(x))]$$

- Direct Proof: Let **c** be an arbitrary element of the universe
- (population). We need to show that **s(c) ⇒ l(c).**
  - s(c) is true.
  - s(c) ⇒ m(c); m(c) ⇒ f(c); f(c) ⇒ l(c)
  - s(c) ⇒ l(c) by the transitivity
  - **∀x (s(x) ⇒ l(x))** Universal generalization

Proposition: $\forall x$, if x is odd, x^2 is odd.

Proposition: ∀x, if x is odd, x^2 is odd.

- We have the starting structure for an arbitrary element x of the universe:

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Therefore x^2 is odd. ■

indicates the end of the proof

Proposition: $\forall x$, if x is odd, x^2 is odd.

- Using the definition of odd numbers we get

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a+1$ *for some* $a \in \mathbb{Z}$, *by definition of an odd number.*

Therefore x^2 is odd. ■

Proposition: $\forall x$, if x is odd, x^2 is odd.

- We are almost there:

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.
Thus $x^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.
So $x^2 = 2b + 1$ *where* b *is the integer* $b = 2a^2 + 2a$.
Thus $x^2 = 2b + 1$ for an integer b.
Therefore x^2 is odd, by definition of an odd number. ■

Proposition: $\forall x$, if x is odd, x^2 is odd.

- The above proof can also be written as follows (x is an arbitrary element of the universe):
  - P(x): x is odd $\Rightarrow$ (x=2a+1)
  - (x=2a+1) $\Rightarrow$ (x^2 =2($2a^2$+2a+1) +1)
  - (x^2=2b +1) $\Rightarrow$ Q(x^2): x^2 is odd
- Thus P(x) $\Rightarrow$ Q(x^2) is true for an arbitrary x.

Show that 1+2+3+ …+ n =n(n+1)/2

- We assume that $n \in N$.
- We write
  - $x = 1 + 2 + \ldots + n.$

Show that 1+2+3+ …+ n =n(n+1)/2

- We assume that $n \in N$.
- We write
  - $x = 1 + 2 + \dots + n.$
  - $\Rightarrow x = n + (n-1) + \dots + 1.$ (Commutative property)

Show that 1+2+3+ …+ n =n(n+1)/2

- We assume that $n \in N$.
- We write
  - $x = 1 + 2 + \ldots + n.$
  - $\Rightarrow x = n + (n-1) + \ldots + 1.$ (Commutative property)
  - $\Rightarrow 2x = n(n+1)$ (adding both the rows)
  - $\Rightarrow x = n(n+1)/2$

Q. 4(4):

- Suppose x, y are integers. If x and y are odd, xy is odd.
  - Assume x and y are odd integers.
  - Then $x=2a + 1$, and $y=2b+1$ for some integers a and b.

Q. 4(4):

- Suppose x, y are integers. If x and y are odd, xy is odd.
  - Assume x and y are odd integers.
  - Then $x=2a + 1$, and $y=2b+1$ for some integers a and b.
  - As a result $xy = (2a+1).(2b+1)=4ab + 2a +2b +1 = 2(2ab+a+b) +1 =2t+1$ where t is an integer.
  - Therefore, if x and y are odd integers, xy is odd.
  - This completes the proof.

Q. 4(6):

- Suppose a,b,c are integers. If a|b and a|c, the a|(b+c).
  - by definitions, a|b implies b=ad for some integer d.
  - Similarly a|c imples c= af for some integer f.

Q. 4(6):

- Suppose a,b,c are integers. If a|b and a|c, the a|(b+c).
  - by definitions, a|b implies b=ad for some integer d.
  - Similarly a|c imples c= af for some integer f.
  - We can now write b + c =a(f+d) = a.t, for some integer t. Therefore, by definition, a | (b+c).

Q. 4(12):

- **If x ∈ R, and 0 < x < 4,** $\frac{4}{x(4-x)} \geq 1.$

Q. 4(12):

- **If $x \in R$, and $0 < x < 4$,** $\frac{4}{x(4-x)} \geq 1.$
  - We can rewrite the above equation as $4 \geq x(4-x)$. This is only possible if $x(4-x) > 0$. This is true since $0 < x < 4$.

Q. 4(12):

- **If x ∈ R, and 0 < x < 4,** $\frac{4}{x(4-x)} \geq 1$.
  - We can rewrite the above equation as $4 \geq x(4-x)$. This is only possible if $x(4-x) > 0$. This is true since $0 < x < 4$.
  - Upon further simplification we get $(x-2)^2 \geq 0$.
  - Thus the above statement is true.

Proof by cases

- Sometimes it is easier to prove a theorem by
  - breaking it down into cases and
  - proving each case separately.
- It is a direct method of proving statements like **$p_1 \vee p_2 \vee \ldots. \vee p_n \Rightarrow q$** is equivalent to proving **$(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q) \wedge \ldots. \wedge (p_n \Rightarrow q)$.**

Example

- **For any two reals x and y, show that $|x+y| \leq |x| + |y|$.**
- Proof by cases:

Example

- **For any two reals x and y, show that $|x+y| \leq |x| + |y|$.**
- Proof by cases:
  - (Case 1) $x \geq 0, y \geq 0$
    - Theorem is true since $(x+y) = x + y$.

Example

- **For any two reals x and y, show that $|x+y| \le |x| + |y|$.**
- Proof by cases:
  - (Case 1) $x \ge 0$, $y \ge 0$
    - Theorem is true since $(x+y) = x + y$.
  - (Case 2) $x < 0$, $y \ge 0$
    - Theorem is true since $|x+y| < \max\{|x|,|y|\} < |x| + |y|$

Example

- **For any two reals x and y, show that $|x+y| \leq |x| + |y|$.**
- Proof by cases:
  - (Case 1) $x \geq 0, y \geq 0$
    - Theorem is true since $(x+y) = x + y$.
  - (Case 2) $x < 0, y \geq 0$
    - Theorem is true since $|x+y| < |y| < |x| + |y|$
  - (Case 3) $x \geq 0, y < 0$
    - Very similar to the second case
  - (Case 4) $x < 0, y < 0$
    - In this case $|x+y| = |x| + |y|$.

Example

Problem: Let n $\in$ *Z*. Prove that $9n^2+3n-2$ is even.

Example

Problem: Let n $\in \mathbb{Z}$. Prove that $9n^2+3n-2$ is even.

- Observe that $9n^2+3n-2=(3n+2)(3n-1)$
- n is an integer $\rightarrow (3n+2)(3n-1)$ is the product of two integers
- **Case 1**: Assume 3n+2 is even

  $\rightarrow 9n^2+3n-2$ is trivially even because it is the product of two integers, one of which is even
- **Case 2**: Assume 3n+2 is odd

  $\rightarrow$ 3n+2-3 is even $\rightarrow$ 3n-1 is even $\rightarrow 9n^2+3n-2$ is even because one of its factors is even

Proof by cases

- In proving a statement is true, we sometimes have to examine multiple case before showing the statement is true in all possible scenarios.

Proposition If $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1+(-1)^n(2n-1) = 1+(1)(2\cdot 2k-1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1+(-1)^n(2n-1) = 1-(2(2k+1)-1) = -4k$, which is a multiple of 4.

These cases show that $1+(-1)^n(2n-1)$ is always a multiple of 4. ■

Practice problems from the text:

- Chapter 4
  - 3,5, 7, 9, 14, 18, 19, 20, 21, 22, 26

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 $a \equiv b \pmod{n}$
  - $9 \equiv 1 \pmod{4}$
  - $109 \equiv 4 \pmod{3}$
  - $14 \neq 8 \pmod{4}$

Problem

- Proposition: Given integers a and b and an $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.
- Direct Proof: Suppose $a \equiv b \pmod{n}$.
  - By definition, $n|(a-b)$.
  - This means $(a-b) = nc$ for some integer c.
  - Multiplying both sides by $(a+b)$ we get $a^2 - b^2 = nc(a+b)$.
  - Since $c(a+b)$ is an integer, the above equation tells us that $n|(a^2 - b^2)$.
  - From the definition it follows that $a^2 \equiv b^2 \pmod{n}$.

Example

Show that $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \Rightarrow k^3 \equiv 1 \pmod 9$

Example

Show that $\forall k \in \mathbf{Z}\ k \equiv 1 (\text{mod } 3) \Rightarrow k^3 \equiv 1 (\text{mod } 9)$

1. $k \equiv 1(\text{mod } 3)$
2. $\exists n \ \ k\text{-}1 = 3n$

Example

Show that $\forall k \in \mathbf{Z}\ k \equiv 1 (\text{mod } 3) \Rightarrow k^3 \equiv 1 (\text{mod } 9)$

1. $k \equiv 1(\text{mod } 3)$
2. $\exists n\ \ k\text{-}1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$
5. $\exists n\ \ k^3 = 27n^3 + 27n^2 + 9n + 1$
6. $\exists n\ \ k^3\text{-}1 = 27n^3 + 27n^2 + 9n$
7. $\exists n\ \ k^3\text{-}1 = (3n^3 + 3n^2 + n)\cdot 9$

Example

Show that $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \Rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$
5. $\exists n\ \ k^3 = 27n^3 + 27n^2 + 9n + 1$
6. $\exists n\ \ k^3-1 = 27n^3 + 27n^2 + 9n$
7. $\exists n\ \ k^3-1 = (3n^3 + 3n^2 + n)\cdot 9$
8. $\exists m\ \ k^3-1 = m\cdot 9$
9. $k^3 \equiv 1 \pmod 9$

Discussion

- The first strategy you should try to prove an assertion is the direct proof method.
- Don’t try to do too much at once. Be patient: take small steps using the appropriate definitions and previously proven facts.

Contrapositive Proof (Chapter 5)

- We use the fact that $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are logically equivalent.
- The expression $\neg Q \Rightarrow \neg P$ is called the **contrapositive** form of $P \Rightarrow Q$.

Contrapositive Proof (Chapter 5)

- We use the fact that $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are logically equivalent.
- The expression $\neg Q \Rightarrow \neg P$ is called the **contrapositive** form of $P \Rightarrow Q$.
- In order to prove $P \Rightarrow Q$ is true, it suffices to instead prove that $\neg Q \Rightarrow \neg P$ is true.
- In order to use direct proof to show $\neg Q \Rightarrow \neg P$ is true, we would assume that $\neg Q$ is true, and use this to deduce that $\neg P$ is true.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$$\vdots$$

Therefore $\sim P$. ■

Example

- Prove that for any sets A, B and C that if A-C $\not\subseteq$ A-B, then B $\not\subseteq$ C
- Proof: The contrapositive statement of the above is

Example

- Prove that for any sets A, B and C that if $A-C \not\subseteq A-B$, then $B \not\subseteq C$
- Proof: The contrapositive statement of the above is if $B \subseteq C$, $A-C \subseteq A-B$.
- To conclude that $A-C \subseteq A-B$, we must show that if $x \in A-C$, then $x \in A-B$.

Example

- Prove that for any sets A, B and C that if $A-C \not\subseteq A-B$, then $B \not\subseteq C$
- Proof: The contrapositive statement of the above is if $B \subseteq C$, $A-C \subseteq A-B$.
- To conclude that $A-C \subseteq A-B$, we must show that if $x \in A-C$, then $x \in A - B$.
  - Suppose $x \in A - C$. This means that $x \in A$ and $x \notin C$
  - However, we are given that $B \subseteq C$.
  - Because $x \notin C$, we deduce that $x \notin B$ either.
  - Thus we have $x \in A$ and $x \notin B$.
  - This implies that $x \in A-B$.

Example

- Prove that for any sets A, B and C that if $A-C \not\subseteq A-B$, then $B \not\subseteq C$
- Proof: The contrapositive statement of the above is if $B \subseteq C$, $A-C \subseteq A-B$.
- To conclude that $A-C \subseteq A-B$, we must show that if $x \in A-C$, then $x \in A - B$.
  - Suppose $x \in A - C$. This means that $x \in A$ and $x \notin C$
  - However, we are given that $B \subseteq C$.
  - Because $x \notin C$, we deduce that $x \notin B$ either.
  - Thus we have $x \in A$ and $x \notin B$.
  - This implies that $x \in A-B$.
- Contrapositive statement is true.
- Original statement is also true

Example

Proposition Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$.
By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$.
Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.
Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ay)$, and that means $5 \mid xy$.
Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ax)$, and that means $5 \mid xy$.
The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ∎

Example 5(11)

- Suppose x, y are integers. If $x^2(y+3)$ is even, the x is even or y is odd.
- The equivalent contrapositive statement is:
  - if x is odd and y is even, $x^2(y+3)$ is odd.

Practice Problems of Chapter 5

- 4, 5, 12, 13, 17, 24, 25, 27, 28

Proof by Contradiction (Chapter 6)

- This method is not just limited to conditional statements.
  - Show that the number $\sqrt{2}$ is irrational. (Note: A number is irrational if it cannot be expressed as $\frac{a}{b}$ where a and b are integers, and b is non-zero.)

Proof by Contradiction (Chapter 6)

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

- C is some statement.

Proof by Contradiction (Chapter 6)

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

$\neg P \Rightarrow (C \wedge \neg C)$

- C is some statement.

Show that the number $\sqrt{2}$ is irrational.

- Suppose ¬P : $\sqrt{2}$ is rational.

Show that the number $\sqrt{2}$ is irrational.

- Suppose ¬ P : $\sqrt{2}$ is rational.
  - Then by definition $\sqrt{2}$ = $\frac{a}{b}$ where a and b are integers and a and non-zero b have no common factors, i.e. gcd(a,b) = 1.

Show that the number $\sqrt{2}$ is irrational.

- Suppose ¬ P : $\sqrt{2}$ is rational.
  - Then by definition $\sqrt{2} = \frac{a}{b}$ where a and b are integers and a and non-zero b have no common factors, i.e. gcd(a,b) = 1.
  - Squaring we get $2b^2 = a^2$. This implies that a is even. Therefore, a=2k, for some k.

Show that the number $\sqrt{2}$ is irrational.

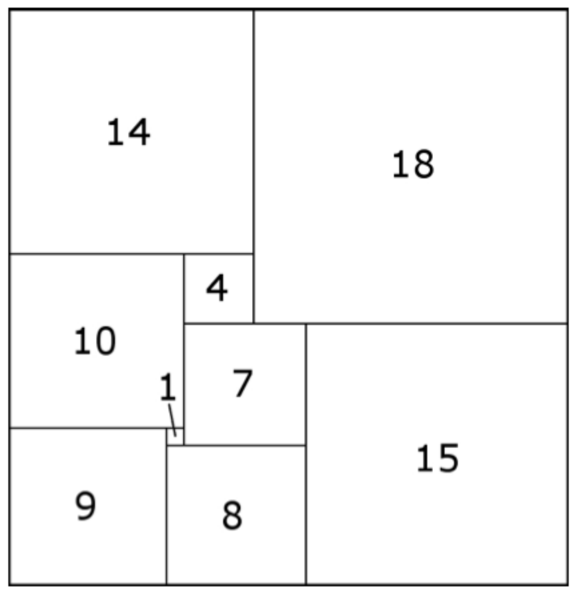
- Suppose ¬ P : $\sqrt{2}$ is rational.
  - Then by definition $\sqrt{2} = \frac{a}{b}$ where a and b are integers and a and non-zero b have no common factors, i.e. gcd(a,b) = 1.
  - Squaring we get $2b^2 = a^2$. This implies that a is even. Therefore, a=2k, for some k.
  - We can write $2b^2 = 4k^2$, i.e. $b^2 = 2k^2$.
  - Hence b is also even.

Show that the number $\sqrt{2}$ is irrational.

- Suppose ¬ P : $\sqrt{2}$ is rational.
  - Then by definition $\sqrt{2} = \frac{a}{b}$ where a and b are integers and a and non-zero b have no common factors, i.e. gcd(a,b) = 1.
  - Squaring we get $2b^2 = a^2$. This implies that a is even. Therefore, a=2k, for some k.
  - We can write $2b^2 = 4k^2$, i.e. $b^2 = 2k^2$.
  - Hence b is also even.
  - This means that a and b have 2 as a common factor.
  - We arrive at a contradiction.
  - ¬ P $\Rightarrow$ F
  - P is true.

Arrangement of squares

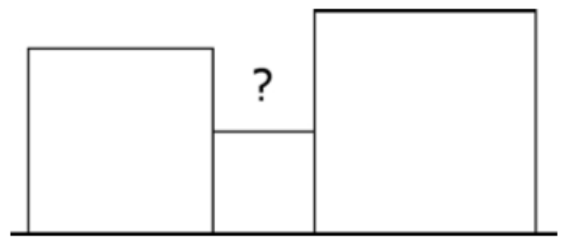
- Consider a 32 x 33 rectangle partitioned into nine squares:



- Claim: Smallest square in the partition must always lie in the middle.

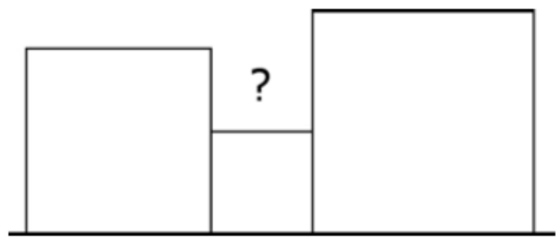
Proof by Contradiction.

- Suppose it is possible to place the smallest square on the boundary.



Proof by Contradiction.

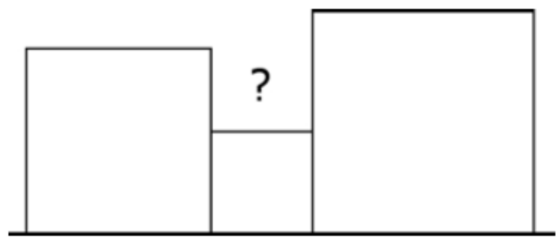
- Suppose it is possible to place the smallest square on the boundary.



- Observe that the squares immediately adjacent to the smallest square are larger.

Proof by Contradiction.

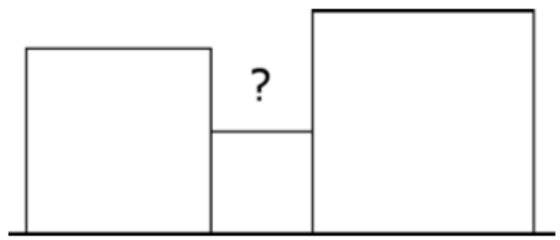
- Suppose it is possible to place the smallest square on the boundary.



- Observe that the squares immediately adjacent to the smallest square are larger.
- The area marked ? cannot be covered by larger size squares.

Proof by Contradiction.

- Suppose it is possible to place the smallest square on the boundary.



- Observe that the squares immediately adjacent to the smallest square are larger.
- The area marked ? cannot be covered by larger size squares.
- The starting assumption leads to a contradiction.
- The starting assumption is wrong.
- Therefore, the smallest square must appear in the middle of the configuration of squares.

There are infinitely many primes.

There are infinitely many primes.

- Suppose there are finite number of primes, and they are, say, p_1, p_2, ….., p_n.
- Let p_n is the largest prime number in the list.

There are infinitely many primes.

- Suppose there are finite number of primes, and they are, say, p_1, p_2, ….., p_n.
- Let p_n is the largest prime number in the list.
- Consider the number $a = p_1 x\ p_2 x\ \ldots\ldots x\ p_n + 1$.

There are infinitely many primes.

- Suppose there are finite number of primes, and they are, say, p_1, p_2, ….., p_n.
- Let p_n is the largest prime number in the list.
- Consider the number $a = p_1 x\ p_2 x\ .....x\ p_n + 1$.
- Since a is not divisible by p_i for any i, a is also a prime number.

There are infinitely many primes.

- Suppose there are finite number of primes, and they are, say, p_1, p_2, ….., p_n.
- Let p_n is the largest prime number in the list.
- Consider the number $a = p_1 x\ p_2 x \ldots.. x\ p_n + 1$.
- Since a is not divisible by a_i for any i, a is also a prime number.
- Thus a is a prime number larger that p_n.
- The starting assumption leads to a contradiction.
- This proves that there are infinitely many prime.

Proving conditional statements by contradiction

Outline for Proving a Conditional Statement with Contradiction

Proposition If P, then Q.

Proof. Suppose P and $\sim Q$.

$\vdots$

Therefore $C \wedge \sim C$. ■

Proving conditional statements by contradiction

Outline for Proving a Conditional Statement with Contradiction

Proposition If P, then Q.

Proof. Suppose P and $\sim Q$.

$\vdots$

Therefore $C \wedge \sim C$. ■

$P \wedge \neg Q \Rightarrow F$

Example

- Let x and y be real numbers. If $5x+25y = 1723$, then x or y is not an integer.

Example

- Let x and y be real numbers. If 5x+25y = 1723, then x or y is not an integer.
- Here P(x,y): 5x + 25 y =1723;
- Q(x,y): (x is not an integer) $\vee$ (y is not an integer)

Example

- Let x and y be real numbers. If $5x+25y = 1723$, then x or y is not an integer.
- Here $P(x,y)$: $5x + 25y = 1723$;
- $Q(x,y)$: (x is not an integer) $\vee$ (y is not an integer)
- Suppose $\forall x,y\ (P(x,y) \wedge \neg Q(x,y))$
- $\neg Q(x,y)$: x and y are integers.

Example

- Let x and y be real numbers. If $5x+25y = 1723$, then x or y is not an integer.
- Here $P(x,y)$: $5x + 25y = 1723$;
- $Q(x,y)$: (x is not an integer) $\vee$ (y is not an integer)
- Suppose $\forall x,y\ (P(x,y) \wedge \neg Q(x,y))$
- $\neg Q(x,y)$: x and y are integers.
- Note that $5x + 25y = 1723$ is $5(x+5y) = 1723$.
- Since $x+5y$ is an integer, therefore 5 divides 1723, a contradiction.

Example

- Consider the statement: For all nonnegative real numbers a, b, and c, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
  - Solve in the class.

Fill in the blanks

If we are proving the implication $p \rightarrow q$ we assume...

(1) p for a direct proof.
(2) ______ for a proof by contrapositive
(3) ______ for a proof by contradiction.

We are then allowed to use the truth of the assumption in 1, 2, or 3 in the proof.

After the initial assumption, we prove $p \rightarrow q$ by showing

(4) q must follow from the assumptions for a direct proof.
(5) ______ must follow the assumptions for a proof by contrapositive.
(6) ______ must follow the assumptions for a proof by contradiction.

Practice problems from Chapter 6.

- 3, 4, 5, 8, 14, 19, 21.

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 $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then
  - $(a + c) \equiv b + d \pmod{n}$

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)
  - $a - c \equiv b - d \pmod{n}$

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 $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then
  - ○ $(a + c) \equiv b + d \pmod{n}$ (easy)
  - ○ $a - c \equiv b - d \pmod{n}$
    - (Easy) since $(a - c) - (b - d) = (a - b) + (d - c)$
  - ○ $ac \equiv bd \pmod{n}$
    - Given $a\text{-}b = t.n$ 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.
    - $ac \equiv bd \pmod{n}$