Elementary Number Theory and Methods of Proof

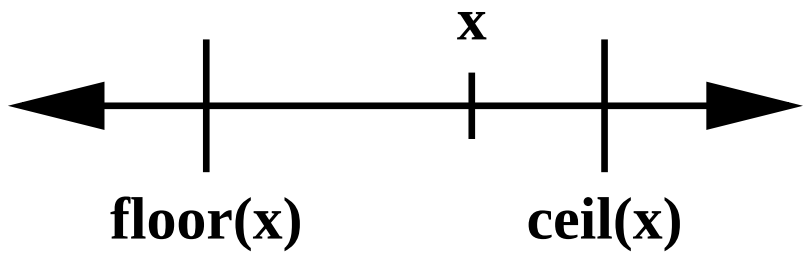
Floor and Ceiling; Proofs by Contradiction and Contraposition

Lecture Notes #6

Peter Blomgren
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
blomgren@terminus.SDSU.EDU
http://terminus.SDSU.EDU

$Id: lecture.tex,v 1.4 2006/09/27 20:47:10 blomgren Exp $

The floor and ceiling of a Real Number



Imagine a real number $x \in \mathbb{R}$ sitting on the number line...

The ***floor*** of x is the integer $\underline{n} \in \mathbb{Z}$ which is to the left of x (*i.e.* the largest integer, which is smaller than or equal to x).

The ***ceiling*** of x is the integer $\overline{n} \in \mathbb{Z}$ which is to the right of x (*i.e.* the smallest integer, which is larger than or equal to x).

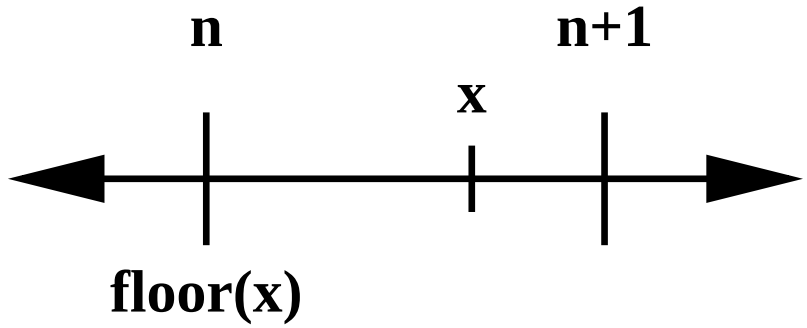
We have,

$$\underline{n} \leq x \leq \overline{n}$$

where equality holds if and only if x is an integer:

$$\underline{n} = x = \overline{n}, \quad \Leftrightarrow \quad x \in \mathbb{Z}$$

Floor — Formal Definition and Notation



Definition: ***The floor of*** $\mathbf{x}$ **—**

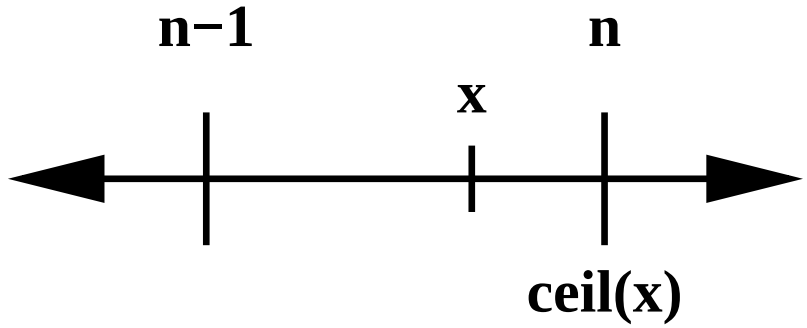
Given any real number x, the **floor of** x, denoted $\lfloor x \rfloor$, is defined as follows:

$$\lfloor x \rfloor = \text{the unique integer } n \text{ such that } n \leq x < n+1.$$

Symbolically, if x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n+1$$

Ceiling — Formal Definition and Notation



Definition: ***The ceiling of*** **x** **—**

Given any real number x, the **ceiling of** x, denoted $\lceil x \rceil$, is defined as follows:

$$\lceil x \rceil = \text{the unique integer } n \text{ such that } n - 1 < x \leq n.$$

Symbolically, if x is a real number and n is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n$$

Examples

#1 — Loading students into Buses: 1370 students are going to the zoo. Due to budget constraints the principal will only allow full buses to leave. Each bus holds at most 40 students. How many buses can leave?

Solution: $\lfloor 1370/40 \rfloor = \lfloor 34.25 \rfloor = 34.$

Comment: This example may seem a little silly — since we are dealing with integer quantities we could have used $1370 \operatorname{div} 40 = 34$.

Examples

#2 — Tax Refund: Due to a sudden miracle, the state controller has found a surplus of \$4,168,325,218.32 in the budget. This money is to be distributed among 24,123,451 taxpayers. However, each check must be in whole dollars only (no pennies). How large will the tax refund be?

Solution:

$$\lfloor 4,168,325,218.32/24,123,451 \rfloor = \lfloor 172.791414392576 \rfloor = \$172.$$

Examples

#3 — Hot Dogs on the Grill: You are expecting 12 friends to come over for a BBQ. An average person eats 3.2 hot-dogs. Hot-dogs are packaged 12/pack and buns 10/pack. How many packs of hot-dogs and buns do you have to buy?

Solution:

Hot-dogs:

$$\lceil 13 \cdot 3.2/12 \rceil = \lceil 3.4667 \rceil = 4$$

Buns:

$$\lceil 13 \cdot 3.2/10 \rceil = \lceil 4.1600 \rceil = 5$$

Why 13??? — You're eating too, right?!?

Examples

#4 — Disproving an alleged property of the floor function.

Statement: For all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.

Disproof by Counter-example:

Consider the case $x = y = \frac{1}{2}$. Then

$$\lfloor x \rfloor + \lfloor y \rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = 0 + 0 = 0$$

But

$$\lfloor x + y \rfloor = \left\lfloor \frac{1}{2} + \frac{1}{2} \right\rfloor = \lfloor 1 \rfloor = 1$$

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof:

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Let* x be real number and m be an integer.

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Let* x be real number and m be an integer. Let $n = \lfloor x \rfloor$.

By the definition of floor, n is an integer and $n \leq x < n + 1$.

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Let* x be real number and m be an integer. Let $n = \lfloor x \rfloor$. By the definition of floor, n is an integer and $n \leq x < n + 1$. Add m to all three entries in the inequality to get

$$(n + m) \leq (x + m) < (n + m) + 1$$

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Let* x be real number and m be an integer. Let $n = \lfloor x \rfloor$. By the definition of floor, n is an integer and $n \leq x < n + 1$. Add m to all three entries in the inequality to get

$$(n + m) \leq (x + m) < (n + m) + 1$$

Since $n + m$ is an integer, by the definition of floor

$$\lfloor x + m \rfloor = n + m$$

A Theorem...

Theorem:

$\forall x \in \mathbb{R}$ and $m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof: Let* x be real number and m be an integer. Let $n = \lfloor x \rfloor$. By the definition of floor, n is an integer and $n \leq x < n + 1$. Add m to all three entries in the inequality to get

$$(n + m) \leq (x + m) < (n + m) + 1$$

Since $n + m$ is an integer, by the definition of floor

$$\lfloor x + m \rfloor = n + m$$

Now we recall that $n = \lfloor x \rfloor$, and by substitution we have

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m. \quad \square$$

Theorem: The Floor of $n/2$

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof:

Theorem: The Floor of $n/2$

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let n be an integer.

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let n be an integer. By the quotient-remainder theorem, n is odd or n is even.

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let n be an integer. By the quotient-remainder theorem, n is odd or n is even.

case 1: When n is odd, then $n = 2k + 1$ for some integer k.

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let n be an integer. By the quotient-remainder theorem, n is odd or n is even.

case 1: When n is odd, then $n = 2k + 1$ for some integer k. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because k is an integer and $k \leq k + 1/2 < k + 1$.

Theorem: For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let n be an integer. By the quotient-remainder theorem, n is odd or n is even.

case 1: When n is odd, then $n = 2k + 1$ for some integer k. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because k is an integer and $k \leq k + 1/2 < k + 1$. Now since $n = 2k + 1$ it follows that $k = \frac{n-1}{2}$, and we have shown that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ when n is odd.

case 2: When n is even, then $n = 2k$ for some integer k.

case 2: When n is even, then $n = 2k$ for some integer k. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k$$

because k is an integer and $k \leq k < k + 1$.

case 2: When n is even, then $n = 2k$ for some integer k. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k$$

because k is an integer and $k \leq k < k + 1$. Now since $n = 2k$ it follows that $k = \frac{n}{2}$, and we have shown that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ when n is even.

case 2: When n is even, then $n = 2k$ for some integer k. By substitution,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k$$

because k is an integer and $k \leq k < k + 1$. Now since $n = 2k$ it follows that $k = \frac{n}{2}$, and we have shown that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ when n is even.

Together, case 1 (n odd) and case 2 (n even) shows that the statement is true. □

Theorem: Floor and the Quotient-Remainder Theorem

Theorem:

If n is a non-negative integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d.$$

Proof:

Theorem: Floor and the Quotient-Remainder Theorem

Theorem:

If n is a non-negative integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d.$$

Proof: Let n be a non-negative integer, d a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d \cdot \lfloor n/d \rfloor$. **You can get this far without having any idea of how to prove the theorem... The beginning of the proof is just restating the assumptions of the theorem!**

Theorem: Floor and the Quotient-Remainder Theorem

Theorem:

If n is a non-negative integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d.$$

Proof: Let n be a non-negative integer, d a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d \cdot \lfloor n/d \rfloor$. By substitution

$$dq + r = d \cdot \left\lfloor \frac{n}{d} \right\rfloor + \left(n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor \right) = n.$$

So it remains to show that $0 \leq r < d$.

Theorem: Floor and the Quotient-Remainder Theorem

Theorem:

If n is a non-negative integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

$$n = d \cdot q + r, \quad \text{and} \quad 0 \leq r < d.$$

Proof: Let n be a non-negative integer, d a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d \cdot \lfloor n/d \rfloor$. By substitution

$$dq + r = d \cdot \left\lfloor \frac{n}{d} \right\rfloor + \left(n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor \right) = n.$$

So it remains to show that $0 \leq r < d$. But $q = \lfloor n/d \rfloor$. Thus by the definition of floor,

$$q \leq \frac{n}{d} < q + 1$$

Proof, continued

Then

$$dq \leq n < dq + d$$

and so

$$0 \leq n - dq < d$$

But

$$r = n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor = n - dq$$

Hence, we have shown

$$0 \leq r < d$$

Both parts of the theorem have been proved. $\square$.

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x + 1 \rceil = \lceil x \rceil + 1$?

Solution:

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x+1 \rceil = \lceil x \rceil + 1$?

Solution: Let x be a real number.

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x+1 \rceil = \lceil x \rceil + 1$?

Solution: Let x be a real number. Then $n = \lceil x+1 \rceil$ is an integer. By the definition of ceiling

$$n - 1 < (x+1) \leq n$$

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x+1 \rceil = \lceil x \rceil + 1$?

Solution: Let x be a real number. Then $n = \lceil x+1 \rceil$ is an integer. By the definition of ceiling

$$n - 1 < (x+1) \leq n$$

Subtracting 1 from all parts of the inequality gives

$$n - 2 < x \leq n - 1$$

and by the definition of ceiling, $\lceil x \rceil = (n-1)$.

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x+1 \rceil = \lceil x \rceil + 1$?

Solution: Let x be a real number. Then $n = \lceil x+1 \rceil$ is an integer. By the definition of ceiling

$$n - 1 < (x+1) \leq n$$

Subtracting 1 from all parts of the inequality gives

$$n - 2 < x \leq n - 1$$

and by the definition of ceiling, $\lceil x \rceil = (n-1)$. Solving this expression for n gives $n = \lceil x \rceil + 1$.

Examples:

Epp-3.5.19: Is the following statement true or false — For all real numbers x, $\lceil x+1 \rceil = \lceil x \rceil + 1$?

Solution: Let x be a real number. Then $n = \lceil x+1 \rceil$ is an integer. By the definition of ceiling

$$n - 1 < (x+1) \leq n$$

Subtracting 1 from all parts of the inequality gives

$$n - 2 < x \leq n - 1$$

and by the definition of ceiling, $\lceil x \rceil = (n-1)$. Solving this expression for n gives $n = \lceil x \rceil + 1$.

Putting the two expressions for n together shows

$\lceil x+1 \rceil = \lceil x \rceil + 1$. Hence, the statement is ***true***

Homework #5 — Due 10/13/2006, 12noon, GMCS-587 Version $\frac{1}{3}$

Know this by the midterm; turn in problems on 10/13/2006.

Epp, 2nd/3rd edition:

Understand the following theorems with proofs: Theorem-3.5.1, Theorem-3.5.2, Theorem-3.5.3; Problems 3.5.13, 3.5.17

Next: New methods of proof — Proof by Contradiction, Proof by Contraposition.

Indirect Arguments: Introduction Contradiction

In **Direct proof** we start with the hypothesis of a statement and make a series of deductions (using known theorems, definition, and some algebraic manipulations) until we reach the conclusion.

Indirect proofs are a little more complicated... In ***arguments by contradiction*** we use the fact that a well formed argument is either ***true*** or ***false***, but ***not both***.

If you can show that a given assumption is ***not true*** leads to a contradiction, impossibility, or absurdity, then that assumption must be false; hence the given statement must be ***true***.

> If $\sim P(x) \Rightarrow Q(x)$, and $Q(x)$ clearly is wrong, then $P(x)$

$Q(x)$ could be something like "all integers are negative," or "all real numbers equal to 4."

In ***arguments by contraposition*** we rely on the fact that a statement is logically equivalent to its contrapositive.

To prove something by contraposition, we write down the contrapositive of the statement, prove that this form is true by direct proof. Then we can conclude that the original statement is true, by the logical equivalence of the two statements.

Recall: ***Definition***

The **contrapositive** of a conditional statement of the form "if p then q" is,

$$\text{If } (\sim q) \text{ then } (\sim p)$$

Symbolically, the contrapositive of $(p \rightarrow q)$ is $((\sim q) \rightarrow (\sim p))$.

Method of Proof by Contradiction

Method of Proof by Contradiction

1. Suppose the statement to be proved is ***false***.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Keep in mind that supposing that a statement is ***false*** is the same thing as supposing that the negation of the statement it ***true***. Hence, step 1 means we must write down the negation of the statement.

Here, we are using quite a few of our tools from chapters 1–2.

When to Use Method of Proof by Contradiction???

Unfortunately, there are no clear "rules" for when a proof by contradiction is better (or easier to execute) than a direct proof.

Proofs by contradiction tends to come in handy when you want to show that there is ***no*** object with a certain property, or if you want to show that a certain object ***does not*** have a certain property.

As you see more proofs throughout you mathematical career, you will get a better gut-feeling for when proofs by contradiction are the preferred method.

The next few examples is a starting point...

Example: Proof by Contradiction

Theorem:

There is no greatest integer.

Proof:

Example: Proof by Contradiction

Theorem:

There is no greatest integer.

Proof: Suppose the statement is false.

Example: Proof by Contradiction

Theorem:
There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N.

Example: Proof by Contradiction

Theorem:
There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N. Since N is the greatest integer, $N \geq n \; \forall n \in \mathbb{Z}$.

Example: Proof by Contradiction

Theorem:

There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N. Since N is the greatest integer, $N \geq n \; \forall n \in \mathbb{Z}$. Now, let $M = N + 1$. M being a sum of integers, must be an integer.

Example: Proof by Contradiction

Theorem:

There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N. Since N is the greatest integer, $N \geq n \; \forall n \in \mathbb{Z}$. Now, let $M = N + 1$. M being a sum of integers, must be an integer. Further, $M > N$ since $M = N + 1$.

Example: Proof by Contradiction

Theorem:
There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N. Since N is the greatest integer, $N \geq n \; \forall n \in \mathbb{Z}$. Now, let $M = N + 1$. M being a sum of integers, must be an integer. Further, $M > N$ since $M = N + 1$.

Thus M is an integer greater than the greatest integer, which is a ***contradiction***. *The contradiction shows that* ***the supposition is false*** *and, therefore the theorem is true.* $\square$

Example: Proof by Contradiction

Theorem:
There is no greatest integer.

Proof: Suppose the statement is false. That is, suppose there is a greatest integer N. Since N is the greatest integer, $N \geq n \; \forall n \in \mathbb{Z}$. Now, let $M = N+1$. M being a sum of integers, must be an integer. Further, $M > N$ since $M = N + 1$.

Thus M is an integer greater than the greatest integer, which is a ***contradiction***. *The contradiction shows that* ***the supposition is false*** *and, therefore the theorem is true.* $\square$

Note: After a contradiction has been reached, the argument is always the same — *This is a contradiction. Hence the supposition is false and the theorem is true.* Most mathematical texts end proofs by contradiction once the contradiction has been reached.

Example#2: Proof by Contradiction

> ***Theorem:*** The sum of any rational number and any irrational number is irrational.

The theorem talks about the sum of a rational and irrational number not having the property of being rational... Suggesting a proof by contradiction.

Proof:

Example#2: Proof by Contradiction

Theorem: The sum of any rational number and any irrational number is irrational.

The theorem talks about the sum of a rational and irrational number not having the property of being rational... Suggesting a proof by contradiction.

Proof: Suppose the theorem is false.

Example#2: Proof by Contradiction

Theorem: The sum of any rational number and any irrational number is irrational.

The theorem talks about the sum of a rational and irrational number not having the property of being rational... Suggesting a proof by contradiction.

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational.

Example#2: Proof by Contradiction

Theorem: The sum of any rational number and any irrational number is irrational.

The theorem talks about the sum of a rational and irrational number not having the property of being rational... Suggesting a proof by contradiction.

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d. [continued...]

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d.

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d. By substitution,

$$\frac{a}{b} + s = \frac{c}{d}$$

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d. By substitution,

$$\frac{a}{b} + s = \frac{c}{d}$$

Hence, a little bit of algebra shows:

$$s = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d. By substitution,

$$\frac{a}{b} + s = \frac{c}{d}$$

Hence, a little bit of algebra shows:

$$s = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

Now, $(bc - ad)$ and bd are both integers, and $bd \neq 0$ (since both $b \neq 0$ and $d \neq 0$). Hence s is a quotient of two integers. By the definition of a rational number s is rational.

Proof: Suppose the theorem is false. That is, suppose there is a rational number r and an irrational number s so that the sum $r + s$ is rational. By the definition of rational, we must have

$$r = \frac{a}{b}, \quad r + s = \frac{c}{d}$$

for some integers a, b, c, d. By substitution,

$$\frac{a}{b} + s = \frac{c}{d}$$

Hence, a little bit of algebra shows:

$$s = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

Now, $(bc - ad)$ and bd are both integers, and $bd \neq 0$ (since both $b \neq 0$ and $d \neq 0$). Hence s is a quotient of two integers. By the definition of a rational number s is rational. This contradicts the supposition that s is irrational. $\square$

Method of Proof by Contraposition

Method of Proof by Contraposition

1. Express the statement to be proved in the form

$$\forall x \in D, \text{ if } P(x), \text{ then } Q(x).$$

2. Rewrite this statement in the contrapositive form

$$\forall x \in D, \text{ if } (\sim Q(x)), \text{ then } (\sim P(x)).$$

3. Prove the contrapositive by a direct proof.

a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is ***false***.

b. Show that $P(x)$ is ***false***.

Example#3: Proof by Contraposition

Theorem:

Given any integer n, if n^2 is even, then n is even.

Proof:

Example#3: Proof by Contraposition

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose n is odd (and show n^2 is odd).

Example#3: Proof by Contraposition

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose n is odd (and show n^2 is odd). Since n is odd, $n = 2k + 1$ by the quotient-remainder theorem (with $d = 2$) [or by the definition of odd].

Example#3: Proof by Contraposition

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose n is odd (and show n^2 is odd). Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or by the definition of odd]. Now,

$$n \cdot n = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{\text{integer}} + 1$$

Example#3: Proof by Contraposition

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose n is odd (and show n^2 is odd). Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or by the definition of odd]. Now,

$$n \cdot n = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{\text{integer}} + 1$$

Hence $n^2 = 2 \cdot (\text{integer}) + 1$, which by the definition of odd shows that n^2 is odd. $\square$

Some Notes...

Proof by contraposition ***only*** works for statements that are universal and conditional, *i.e.* of the form

$$\textbf{(S)} \qquad \forall x \in D, \text{ if } P(x), \text{ then } Q(x)$$

It turns out that any statement that can be proved by contraposition can also be proved by contradiction (but not the other way around).

The contrapositive of the statement ***(S)*** (above) is

$$\textbf{(C)} \qquad \forall x \in D, \text{ if } (\sim Q(x)), \text{ then } (\sim P(x))$$

Some Notes... Contrapositive vs. Contradiction

In a ***proof by contraposition*** we

1. Suppose x is an arbitrary element of D such that $(\sim Q(x))$.

2. Execute a sequence of steps to show $(\sim P(x))$.

We can use the ***same(!)*** sequence of steps to show the result by contradiction.

In a ***proof by contradiction*** we

1. Suppose x is an arbitrary element of D such that $P(x)$ and $(\sim Q(x))$.

2. Execute a sequence of steps to show *a contradiction*, $(\sim P(x)) \wedge P(x)$.

Example#4: Proof by Contradiction

Theorem:

Given any integer n, if n^2 is even, then n is even.

Proof:

Example#4: Proof by Contradiction

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose there exists an integer n such that $\mathbf{n^2}$ **is even** and n is odd.

Example#4: Proof by Contradiction

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose there exists an integer n such that $\mathbf{n^2}$ **is even** and n is odd. Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or the definition of odd].

Example#4: Proof by Contradiction

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose there exists an integer n such that $\mathbf{n^2}$ **is even** and n is odd. Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or the definition of odd]. Now,

$$n \cdot n = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{\text{integer}} + 1$$

Example#4: Proof by Contradiction

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose there exists an integer n such that $\mathbf{n^2}$ **is even** and n is odd. Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or the definition of odd]. Now,

$$n \cdot n = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{\text{integer}} + 1$$

Hence $n^2 = 2 \cdot (\text{integer}) + 1$, which by the definition of odd shows that $\mathbf{n^2}$ **is odd**.

Example#4: Proof by Contradiction

Theorem:
Given any integer n, if n^2 is even, then n is even.

Proof: Suppose there exists an integer n such that $\mathbf{n^2}$ **is even** and n is odd. Since n is odd, $n = 2k+1$ by the quotient-remainder theorem (with $d = 2$) [or the definition of odd]. Now,

$$n \cdot n = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{\text{integer}} + 1$$

Hence $n^2 = 2 \cdot (\text{integer}) + 1$, which by the definition of odd shows that $\mathbf{n^2}$ **is odd**. Now, n^2 is odd and n^2 is even, ***a contradiction.*** $\square$

Note: The steps of the proof are exactly the same as in the proof by contraposition.

Contradiction vs. Contraposition

In a sense, we don't need proofs by contraposition (since they can always be converted to proofs by contradiction).

The advantage of the proof by contraposition is that ***you know exactly*** what conclusion you need to show — *i.e.* the negation of the hypothesis.

In a proof by contradiction it may be difficult to see where the contradiction will appear.

Further, in a proof by contradiction you have to negate the full statement (of the theorem), which may be complicated.

We like contraposition since it seems easier to argue "forward" toward a known goal. However, these proofs only work for universal conditional statements.

The Irrationality of $\sqrt{2}$

Theorem:
$\sqrt{2}$ is irrational.

Proof:

The Irrationality of $\sqrt{2}$

Theorem:
$\sqrt{2}$ is irrational.

Proof: Suppose not ***(proof by contradiction).***

The Irrationality of $\sqrt{2}$

Theorem:
$\sqrt{2}$ is irrational.

Proof: Suppose not ***(proof by contradiction).*** Then there are two integers m and n with *no common factors*, so that

$$\sqrt{2} = \frac{m}{n}.$$

The Irrationality of $\sqrt{2}$

Theorem:
$\sqrt{2}$ is irrational.

Proof: Suppose not ***(proof by contradiction).*** Then there are two integers m and n with *no common factors*, so that

$$\sqrt{2} = \frac{m}{n}.$$

Squaring both sides gives

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

or equivalently, $m^2 = 2n^2$.

The Irrationality of $\sqrt{2}$

Theorem:
$\sqrt{2}$ is irrational.

Proof: Suppose not ***(proof by contradiction).*** Then there are two integers m and n with *no common factors*, so that

$$\sqrt{2} = \frac{m}{n}.$$

Squaring both sides gives

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

or equivalently, $m^2 = 2n^2$. This shows that m^2 is even by the definition of even. We have previously [slide #24] shown that this implies that m is even. [continued...]

Now, since m is even, we can write $m = 2k$ for some integer k.

Now, since m is even, we can write $m = 2k$ for some integer k.

Substituting this into $m^2 = 2n^2$ gives

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Now, since m is even, we can write $m = 2k$ for some integer k.

Substituting this into $m^2 = 2n^2$ gives

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Dividing both sides (of $4k^2 = 2n^2$) by 2 gives

$$n^2 = 2k^2$$

which shows that n^2, is even; therefore n is even.

Now, since m is even, we can write $m = 2k$ for some integer k.

Substituting this into $m^2 = 2n^2$ gives

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Dividing both sides (of $4k^2 = 2n^2$) by 2 gives

$$n^2 = 2k^2$$

which shows that n^2, is even; therefore n is even. Now, both m and n are even; hence they have a common factor of 2. This ***contradicts*** the supposition that m and n does not have any common factors. □

Something to think about: is $\sqrt{3}$ irrational? How would you prove it?

There are infinitely many prime numbers; *i.e.* there is no largest prime.

In order the show this we first need to prove the following result:

> ***Theorem***:
> For any integer a and prime number p, if $p|a$, then $p \not| (a+1)$.

Proof:

There are infinitely many prime numbers; *i.e.* there is no largest prime.

In order the show this we first need to prove the following result:

> ***Theorem***:
> For any integer a and prime number p, if $p|a$, then $p \not| (a+1)$.

Proof: Suppose the statement is false, then there is an integer a and a prime number p such that $p|a$ and $p|(a+1)$.

There are infinitely many prime numbers; *i.e.* there is no largest prime.

In order the show this we first need to prove the following result:

> ***Theorem***:
> For any integer a and prime number p, if $p|a$, then $p \not| (a+1)$.

Proof: Suppose the statement is false, then there is an integer a and a prime number p such that $p|a$ and $p|(a+1)$. By definition we can find integers r and s such that $a = pr$ and $(a+1) = ps$.

There are infinitely many prime numbers; *i.e.* there is no largest prime.

In order the show this we first need to prove the following result:

> ***Theorem***:
> For any integer a and prime number p, if $p|a$, then $p \not| (a+1)$.

Proof: Suppose the statement is false, then there is an integer a and a prime number p such that $p|a$ and $p|(a+1)$. By definition we can find integers r and s such that $a = pr$ and $(a+1) = ps$. It follows that $1 = (a+1) - a = ps - pr = p(s-r)$.

There are infinitely many prime numbers; *i.e.* there is no largest prime.

In order the show this we first need to prove the following result:

> ***Theorem***:
> For any integer a and prime number p, if $p|a$, then $p \not| (a+1)$.

Proof: Suppose the statement is false, then there is an integer a and a prime number p such that $p|a$ and $p|(a+1)$. By definition we can find integers r and s such that $a = pr$ and $(a+1) = ps$. It follows that $1 = (a+1) - a = ps - pr = p(s-r)$. Since $(s-r)$ is an integer, it follows that $p|1$, but ± 1 are the only divisors of 1. Since p is a prime, we must have $p > 1$, a contradiction. $\square$.

Theorem:

The set of prime numbers is infinite.

Proof:

Theorem:

The set of prime numbers is infinite.

Proof: Suppose not — suppose the set of prime numbers if finite.

Theorem:
The set of prime numbers is infinite.

Proof: Suppose not — suppose the set of prime numbers if finite. Then all prime numbers can be listed in ascending order

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n = ?$$

Theorem:
The set of prime numbers is infinite.

Proof: Suppose not — suppose the set of prime numbers if finite. Then all prime numbers can be listed in ascending order

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n = ?$$

Now consider the integer

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Then $N > 1$, so by theorem-3.3.2 (see Epp), N is divisible by some prime number p, $(p|N)$.

Theorem:
The set of prime numbers is infinite.

Proof: Suppose not — suppose the set of prime numbers if finite. Then all prime numbers can be listed in ascending order

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n = ?$$

Now consider the integer

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Then $N > 1$, so by theorem-3.3.2 (see Epp), N is divisible by some prime number p, $(p|N)$. Also, since p is prime it must equal one of the primes p_i $(1 < i < n)$. Thus $p|(p_1 \cdot p_2 \cdot p_3 \cdots p_n)$. By the previous theorem [slide 31] $p \not| (p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1)$. This contradicts $p|N$. $\square$

Know this by the midterm; turn in problems on 10/13/2006.

Epp, 2nd/3rd edition:

Understand the following theorems with proofs: Theorem-3.5.1, Theorem-3.5.2, Theorem-3.5.3; Problems ***Epp-3.5.13, Epp-3.5.17***.

Epp, 3rd edition:

Epp-3.6.5, Epp-3.6.8a, Epp-3.6.8b, Epp-3.6.30

Epp, 2nd edition:

Epp-3.6.2, –, Epp-3.6.6, –

If you do not have the 3rd edition, it is your responsibility to seek out the "missing" questions. — Phone-a-Friend, or come to office hours!