COMP 233 Discrete Mathematics

Elementary Number Theory and Methods of Proof

4.4 Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Quotient-Remainder Theorem (warm up)

Suppose 14 objects are divided into groups of 3?

x x x   x x x   x x x   x x x   x x

The result is 4 groups of 3 each with 2 left over.

We write

$$\begin{array}{rl} & 4 \leftarrow \textit{quotient} \\ \cline{2-2} 3 \,\big| & 14 \\ & \underline{12} \\ & 2 \leftarrow \textit{remainder} \end{array}$$

or, $\frac{14}{3} = 4 + \frac{2}{3}$

or, **better**, $14 = 4 \cdot 3 + 2.$

Note: The number left over has to be less than the size of the groups.

Quotient-Remainder Theorem (warm up)

Notice that:

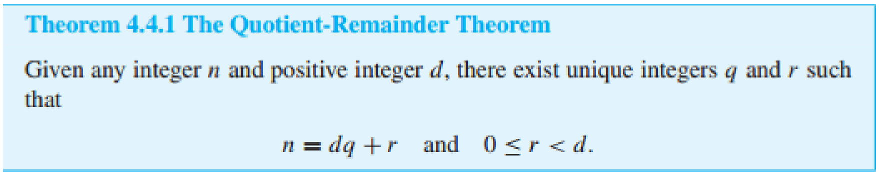
$$\begin{array}{rl} & 2 \leftarrow \text{quotient} \\ \cline{2-2} 4 \,\big| & 11 \\ & \underline{8} \\ & 3 \leftarrow \text{remainder} \end{array}$$

$$11 = \underset{\substack{\uparrow \\ \text{2 groups of 4}}}{2 \cdot 4} + \underset{\substack{\uparrow \\ \text{3 left over}}}{3}.$$

Examples:

$54 = 4 \cdot 13 + 2$	$q = 13$	$r = 2$
$-54 = 4 \cdot (-14) + 2$	$q = -14$	$r = 2$
$54 = 70 \cdot 0 + 54$	$q = 0$	$r = 54$

Quotient-Remainder Theorem



Theorem 4.4.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

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

The quotient-remainder theorem says that when any integer **n** is divided by any positive integer **d** (group size), the result is a quotient **q** and a nonnegative remainder **r** that is smaller than **d**

The proof that there exist integers q and r with the given properties is in Section 5.4.

The proof that q and r are **unique** is outlined in exercise 18 in Section 4.7.

Consequences

1. Apply the quotient-remainder theorem with ***d* = 2**. The result is that there exist unique integers *q* and *r* such that

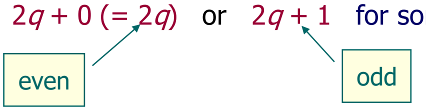
$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

What are possible values for *r*?

Answer: ***r* = 0 or *r* = 1**

Consequence: No matter what integer you start with, it either equals

$2q + 0\ (= 2q)$ or $2q + 1$ for some integer q.



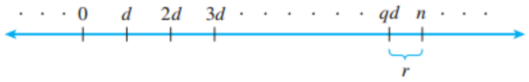
So: Every integer is either even or odd.

Exercises

Ex: Find q and r if $n = 23$ and $d = 6$.

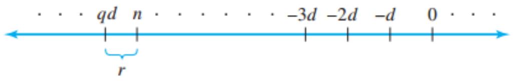
Answer: $q = 3$ and $r = 5$

If n is positive, the quotient-remainder theorem can be illustrated on the number line as follows:



Ex: Find q and r **if** $n = -23$ and $d = 6$.

Answer: $q = -4$ and $r = 1$



Exercises (**)

2. *Similarly*: Given any integer n, apply the quotient-remainder theorem with $d = 3$. The result is that there exist unique integers q and r such that

$$n = 3q + r \quad \text{and} \quad 0 \leq r < 3.$$

What are possible values for r?

Answer: $\boldsymbol{r = 0}$ **or** $\boldsymbol{r = 1}$ **or** $\boldsymbol{r = 2}$

Consequence: Given any integer n, there is an integer q so that n can be written in one of the following three forms:

$$\mathbf{n = 3q, \quad n = 3q + 1, \quad n = 3q + 2.}$$

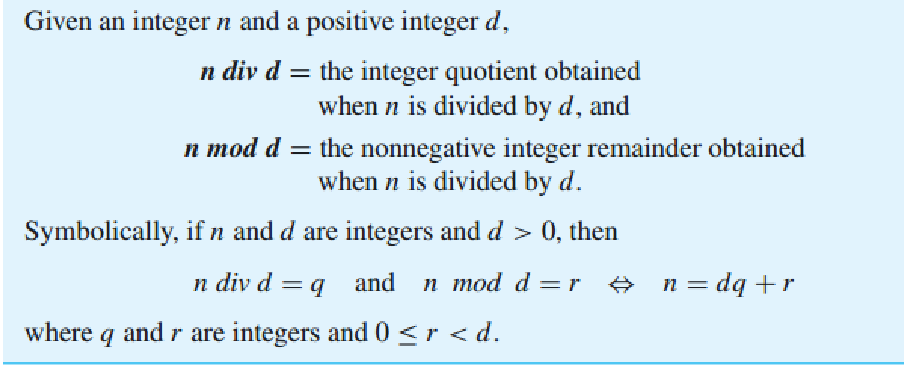
3. Similarly for other values of *d*.

More later… (**)

- Quotient-remainder theorem
  - Powerful tool for method of proof by division into cases
  - Ex. Prove that: given any integer n, there is an integer k so that $n^2 = 3k$ or $n^2 = 3k + 1$.
    - Any integer can be written as
      - n=4q or n=4q+1 or n=4q+2 or n=4q+3
  - Ex. Prove that the square of any odd integer has the form 8m+1 for some integer m
    - Any odd integer can be
      - 4q+1 or 4q+3.

div and mod

div and mod



Given an integer n and a positive integer d,

n ***div*** d = the integer quotient obtained when n is divided by d, and

n ***mod*** d = the nonnegative integer remainder obtained when n is divided by d.

Symbolically, if n and d are integers and $d > 0$, then

$$n \; div \; d = q \quad \text{and} \quad n \;\; mod \;\; d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \le r < d$.

$$n = d \cdot (n \text{ div } d) + n \text{ mod } d$$

Examples:

32 div 9 = 3
32 mod 9 = 5

Recall: 2k-1 example!

- Proof: if k is integer then 2k-1 is odd
- (2k-1) mod 2=r and (2k-1) div 2 =q

Iff 2k-1=2q+r

r =2k-2q-1

=2(k-q)-1

Definition. if n and d are integers and $d > 0$, then $n \; div \; d = q$ and $n \; mod \; d = r \Leftrightarrow n = dq + r$, where q and r are integers and $0 \le r < d$.

- 0≤r <2.

r=0 or r=1

- If r=0 then k-q=1/2 which is impossible

Then r=1

Application1

Given the following code, prove that when the first condition is satisfied, the code will always print “Lucky”.

```
int a,b,c;
if((b%a==0)&&(c%a==0))
   if((b+c)%a  == 0)
         printf(“Lucky”);
   else printf(“Not lucky”);
```

b%a==0 --> b = aq
c%a==0 -- > c = ap
b + c = a(q+p) + 0
--- > (b + c) % a == 0

Note: rewrite the code as a conditional statement:

“For all integers a, b, and c, if b|a & c|a then (b+c)|a

Application2

Computing the Day of the Week

If today is Wednesday and it is 2/11/2016, which day it will be the valentine's day in 2017?

Valentine’s day = 14/2/2017

The number of days from today to 14/2/2017 = 28 in November + 31 in December + 31 in January + 14 in February = **104 days**

104 div 7 = 14 104 mod 7 =6

That is, after 14 weeks the day will be Wednesday, and 6 days after, it will be Tuesday

Application3

Solving a Problem about mod

Suppose m is an integer.
If m mod 11 = 6, what is $4m$ mod 11 ?

$$m = 11q + 6.$$

$$4m = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2.$$

$$4m \bmod 11 = 2.$$

Representing Integers using the quotient-remainder theorem

Parity Property

We represent any number as:

$$n = 2q + r \quad \text{and} \quad 0 \le r < 2$$

Because we have only r = 0 and r =1, then:

$n = 2q + 0$ or $n = 2q + 1$

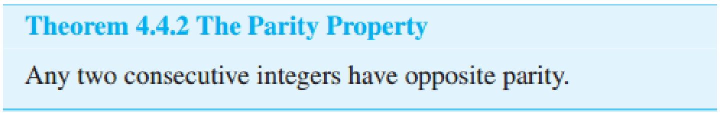
Even Odd

Therefore, n is either even or odd (parity)

The ***parity*** of an integer refers to whether the integer is even or odd

Representing Integers using the quotient-remainder theorem

Parity Property



Theorem 4.4.2 The Parity Property

Any two consecutive integers have opposite parity.

Proof:

Given m and $m+1$ are consecutive integers

Then, one is odd and the other is even (by parity property)

Case1 (m is even): $m = 2k$, so $m+1 = 2k+1$, which is odd

Case2 (m is odd): $m = 2k + 1$ and so

$m+1 = (2k+1) + 1 = 2k + 2 = 2(k+1)$.

thus $m + 1$ is even.

Method of Proof by Division into Cases

Method of Proof by Division into Cases

How do you prove? If *A* **or** *B* is true then *C* is also true.

Technique: Prove

If *A* is true then *C* is true **and** if *B* is true then *C* is true.

Method of Proof by Division into Cases

To prove a statement of the form

"If *A1* or *A2* or ... or *An*, then *C*"

prove all of the following:

If A_1, then C,
If A_2, then C,
.
If A_n, then C.

This process shows that *C* is true regardless of which of A_1, A_2, . . . , A_n happens to be the case.

Example: Representations of Integers Modulo 4

Show that any integer can be written in one of the four forms:

$n=4q$ or $n=4q+1$ or $n=4q+2$ or $n=4q+3$

for some integer q.

Solution: apply the quotient-remainder theorem to n with $d = 4$

There exist an integer quotient q and a remainder r such that

$n = 4q + r$ and $0 \leq r < 4$.

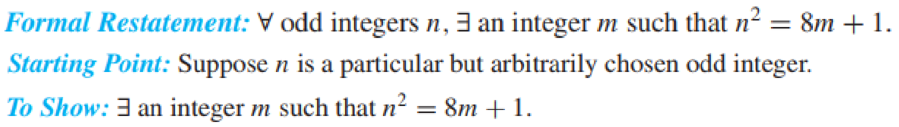
But the only nonnegative remainders that are less than 4 are 0, 1, 2, and 3.

Thus, any integer can be represented as:

$n=4q$ or $n=4q+1$ or $n=4q+2$ or $n=4q+3$

Example: The Square of an Odd Integer

Proof: The **square** of any **odd** integer has the form **8m+1** for some integer m



Formal Restatement: ∀ odd integers n, ∃ an integer m such that $n^2 = 8m + 1$.

Starting Point: Suppose n is a particular but arbitrarily chosen odd integer.

To Show: ∃ an integer m such that $n^2 = 8m + 1$.

Hint: any odd integer can be 4q+1 or 4q+3.

Case 1 (n=4q+1):

$n^2 = (4q+1)^2 = 16q^2 + 8q +1 = 8(\underline{2q^2 + q}) +1$

Let $(2q^2 + q)$ be an integer m, thus $n^2 = 8m + 1$

Case 2 (n=4q+3):

$n^2 = (4q+3)^2 = 16q^2 + 24q +8 +1$

$= 8(\underline{2q^2 + 3q+1}) +1$

Let $(2q^2 + 3q+1)$ be an integer m, thus $n^2 = 8m + 1$

In details on page 186 - Theorem 4.4.3

Example

Theorem: Prove that given any integer n, there is an integer k s.t. $n^2 = 3k$ or $n^2 = 3k + 1$.

Outline of Proof: Suppose n is ***any*** integer. By the quotient-remainder theorem with $d = 3$, there is an integer q so that

$$n = 3q, \quad n = 3q + 1, \quad n = 3q + 2.$$

We will show that regardless of which of these happens to be the case, the conclusion of the theorem follows.

Case 1, $n = 3q$ for some integer q: (*fill in*)

Case 2, $n = 3q$ + 1 for some integer q: (*fill in*)

Case 3, $n = 3q$ + 2 for some integer q: (*fill in*)

Hence, in every case there exists an integer k so that $n^2 = 3k$ or $n^2 = 3k + 1$, as was to be shown.

How would we fill in Case 2, for example?

Case 2, $n = 3q + 1$ for some integer q: In this case,

$$\begin{aligned} n^2 &= (3q + 1)^2 && \text{by substitution} \\ &= (3q + 1)(3q + 1) \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1 && \text{by algebra.} \end{aligned}$$

Let $k = 3q^2 + 2q$.

Then k is an integer because it is a sum of products of integers.

Thus there is an integer k such that $n^2 = 3k + 1$.

Method of Proof by Contradiction

Method of Proof by Contradiction

Definition: A **contradiction** is a form of statement that is "always" false.

Ex: $p \wedge {\sim}p$

Claim: Suppose **c** is a contradiction. Then the following is a valid form of argument:

$$\boxed{\begin{array}{l} {\sim}p \to \mathbf{c} \\ \therefore\ p \end{array}}$$

Proof:

			premise	conclusion
p	**c**	${\sim}p$	${\sim}p \to \mathbf{c}$	p
T	F	F	T	T
F	F	T	F	F

In the only case where the premise is true, the conclusion is also true. So this form of argument is valid.

Method of Proof by Contradiction

To prove a statement by contradiction,

Suppose the statement is not true.

Show that this supposition leads logically to a contradiction.

*[**Conclude**: The supposition is false. That is, conclude that the given statement is true.]*

Recall: 2k-1 example!

- Proof: if k is integer then 2k-1 is odd
- Suppose it is even,
  - i.e., 2k-1=2k′, k′ is integer
  - 2k=2k′+1,   k=k′+1/2
- But k is integer by hypothesis
  - contradiction

Prove that $\sqrt{2}$ is not rational. (A rational number is one which can be written in the form p/q where $q \neq 0$ and p and q are integers.)

Proof

The proof of this theorem is a well known example of proof by contradiction. We assume that $\sqrt{2}$ *is* rational and show that this leads to a contradiction.

Suppose that $\sqrt{2}$ is rational, i.e. $\sqrt{2} = m/n$ where m and n are integers and $n \neq 0$. We may assume that the fraction m/n is in its 'lowest terms', i.e. that m and n have no common factors. If they do have common factors we simply cancel them.

Prove that $\sqrt{2}$ is not rational. (A rational number is one which can be written in the form p/q where $q \neq 0$ and p and q are integers.)

Now

$$\begin{array}{ll}
 & \sqrt{2} = m/n \\
\Rightarrow & 2 = m^2/n^2 \\
\Rightarrow & 2n^2 = m^2 \\
\Rightarrow & m^2 \text{ is even} \\
\Rightarrow & m \text{ is even} \quad \text{(see example 2.3.1)} \\
\Rightarrow & m = 2p \quad \text{for some integer } p \\
\Rightarrow & m^2 = 4p^2.
\end{array}$$

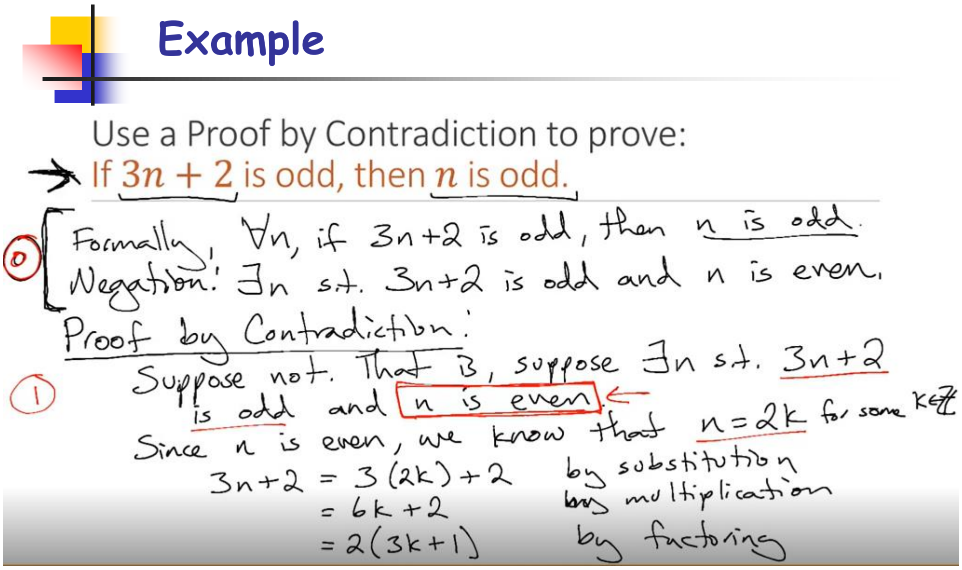
Substituting this result into the equation $2n^2 = m^2$ gives

$$\begin{array}{ll}
 & 2n^2 = 4p^2 \\
\Rightarrow & n^2 = 2p^2 \\
\Rightarrow & n^2 \text{ is even} \\
\Rightarrow & n \text{ is even.}
\end{array}$$

We have now shown that both m and n are even, i.e. that they have a common factor 2. But m and n have no common factors because any such factors were cancelled at the beginning. Hence we have deduced the conjunction of a proposition and its negation, i.e. a contradiction, and this proves the theorem. □

Example

Use a Proof by Contradiction to prove:
If $3n + 2$ is odd, then n is odd.



Example

Use a Proof by Contradiction to prove:
→ If $\underbrace{3n + 2}$ is odd, then $\underbrace{n}$ is odd.

⓪ Formally, $\forall n$, if $3n+2$ is odd, then n is odd.
Negation: $\exists n$ s.t. $3n+2$ is odd and n is even.

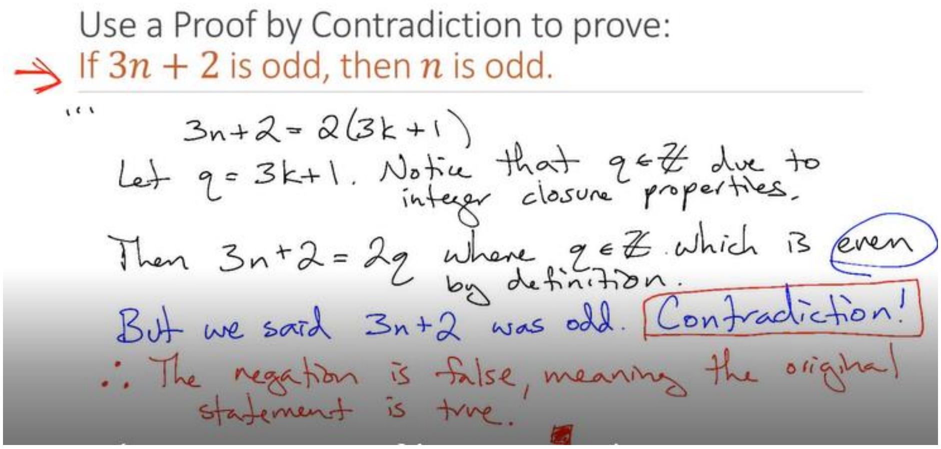
Proof by Contradiction:

① Suppose not. That is, suppose $\exists n$ s.t. $3n+2$ is odd and n is even ←

Since n is even, we know that $n = 2k$ for some $k \in \mathbb{Z}$

$$\begin{aligned} 3n+2 &= 3(2k)+2 && \text{by substitution} \\ &= 6k+2 && \text{by multiplication} \\ &= 2(3k+1) && \text{by factoring} \end{aligned}$$

Example



Use a Proof by Contradiction to prove:

→ If $3n + 2$ is odd, then n is odd.

...

$3n+2 = 2(3k+1)$

Let $q = 3k+1$. Notice that $q \in \mathbb{Z}$ due to integer closure properties.

Then $3n+2 = 2q$ where $q \in \mathbb{Z}$ which is even by definition.

But we said $3n+2$ was odd. Contradiction!

∴ The negation is false, meaning the original statement is true.

A "Lemma"

A lemma is a statement whose main use is to help prove another, more important, statement, called a theorem.

Lemma: If the square of an integer is even, then the integer is even.

Formal restatement:

∀ integers n, if n^2 is even then n is even.

Negation:

∃ an integer n such that n^2 is even and n is not even.

Think the negation to get a proof by contradiction started.

Proof of Lemma

Lemma: If the square of an integer is even, then the integer is even.

Proof by contradiction: Suppose not. That is, suppose there exists an integer n such that n^2 is even and n is not even. Then n is odd (why?) and so, by definition of odd, $n = 2s + 1$ for some integer s.

quotient-remainder theorem

Then $n^2 = (2s + 1)^2$ by substitution

$= 4s^2 + 4s + 1$

$= 2(2s^2 + 2s) + 1$ by algebra.

But $2s^2 + 2s$ is an integer b/c it is a sum of products of integers. Hence n^2 equals twice an integer plus 1 and thus is odd by definition of odd. But this contradicts the fact that n^2 is even. *[Hence the supposition is false and the lemma is true.]*

Exercises

Task: Solve the equation $2(x - 7) + 5(3 - x) = 3(2 - x)$.

Solution: ***Suppose*** x is a number for which the equation is true:

$$2(x - 7) + 5(3 - x) = 3(2 - x)$$

Then

$2x - 14 + 15 - 5x = 6 - 3x$ by multiplying out.

So $-3x + 1 = 6 - 3x$ by combining like terms

and thus $1 = 6$ by adding $3x$ to both sides

But 1 is not equal to 6. Therefore the supposition that there is a solution for the equation is false, and this equation has no solution.

summary

Complete the following sentences:

An integer **n is even** if, and only if *n* is equal to twice some integer.

An integer **n is odd** if, and only if *n* is equal to twice some integer plus 1.

An integer **n is prime** if, and only if,

$n > 1$ and the only positive integer divisors of *n* are 1 and *n*.

A real number **r is rational** if, and only if

it is equal to a quotient of integers with a nonzero denominator.

Given integers *n* and *d*, **d divides n** if, and only if,

n equals *d* times some integer.

NOTE: There are a number of other correct versions of these definitions.

Summary.

What is the **quotient-remainder** theorem?

For all integers *n* and positive integers *d*, there exist unique integers *q* and *r* such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

What is the **"transitivity of divisibility"** theorem?

∀ integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

What does it mean for an integer >1 to **not be prime**?

n is a product of positive integers, neither of which is 1.

What is the **unique factorization** theorem?

Given any integer $n > 1$, either *n* is prime or *n* can be written as a product of prime numbers in a way that is unique, except, possibly, for the order in which the numbers are written.

Absolute Value and the Triangle Inequality

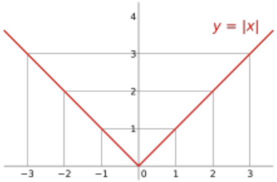
- **Definition**

For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

Example:

$|2| = 2$
$|-2| = 2$



Absolute Value

Lemma 4.4.4

For all real numbers r, $-|r| \leq r \leq |r|$.

Proof:

Suppose r is any real number. We divide into cases according to whether $r \geq 0$ or $r < 0$.

Case 1 ($r \geq 0$): In this case, by definition of absolute value, $|r| = r$. Also, since r is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that

$$-|r| \leq r \leq |r|.$$

Case 2 ($r < 0$): In this case, by definition of absolute value, $|r| = -r$. Multiplying both sides by -1 gives that $-|r| = r$. Also, since r is negative and $|r|$ is positive, $r < |r|$. Thus it is also true in this case that

$$-|r| \leq r \leq |r|.$$

Hence, in either case,

$$-|r| \leq r \leq |r|$$

[as was to be shown].

Absolute Value

Lemma 4.4.5

For all real numbers r, $|-r| = |r|$

Proof:

Suppose r is any real number. By Theorem T23 in Appendix A, if $r > 0$, then $-r < 0$, and if $r < 0$, then $-r > 0$. Thus

$$|-r| = \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases}$$

by definition of absolute value

$$= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } -r < 0 \end{cases}$$

because $-(-r) = r$ by Theorem T4 in Appendix A

$$= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } r > 0 \end{cases}$$

because, by Theorem T24 in Appendix A, when $-r > 0$, then $r < 0$, when $-r < 0$, then $r > 0$, and when $-r = 0$, then $r = 0$

$$= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases}$$

by reformatting the previous result

$$= |r|$$

by definition of absolute value.

Absolute Value and Triangle Inequality

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof:

Suppose x and y, are any real numbers.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

***Case 1* ($x + y \geq 0$):** In this case, $|x + y| = x + y$, and so, by Lemma 4.4.4,

$$x \leq |x| \quad \text{and} \quad y \leq |y|.$$

Hence, by Theorem T26 of Appendix A,

$$|x + y| = x + y \leq |x| + |y|.$$

***Case 2* ($x + y < 0$):** In this case, $|x + y| = -(x + y) = (-x) + (-y)$, and so, by Lemmas 4.4.4 and 4.4.5,

$$-x \leq |-x| = |x| \quad \text{and} \quad -y \leq |-y| = |y|.$$

It follows, by Theorem T26 of Appendix A, that

$$|x + y| = (-x) + (-y) \leq |x| + |y|.$$

Hence in both cases $|x + y| \leq |x| + |y|$ *[as was to be shown]*.