Math 245: Discrete Mathematics

Elementary Number Theory and Methods of Proof

Direct Proof and Counterexample

Lecture #5

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 1.10 2006/09/26 22:44:59 blomgren Exp $

Introduction

We have spent quite some time and effort building up our toolbox of logic reasoning.

We are now ready to ***apply*** that toolbox to something — the properties of integers, rational, and real numbers.

We are going to try to establish the truth or falsity of mathematical statements.

Let the ***floor of*** $\mathbf{x}$, denoted $\lfloor x \rfloor$, be the integer part of x, *e.g.* $\lfloor \pi \rfloor = 3$. Consider the two statements:

1.	$\forall x \in \mathbb{R}$	$\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1.$
2.	$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$	$\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor.$

It turns out statement ***1.*** is true, and ***2.*** is false... We are going to look at methods for proving this.

Basic Building Blocks — Definitions

Mathematicians define terms very carefully and precisely, most of the time every word and symbol in a definition is there for a reason.

We are going to start from a few definitions, and use our logic toolbox to evaluate the truth or falsity of mathematical statements.

***Definition*: Even and Odd Integers —**

An integer n is **even** if, and only if, $n = 2k$ for some integer k.

An integer n is **odd** if, and only if, $n = 2k + 1$ for some integer k.

Symbolically, if $n \in \mathbb{Z}$, then

$$n \text{ is even} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \text{ such that } n = 2k$$

$$n \text{ is odd} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1.$$

Deductions

Now,

If we know...	**Then we can deduce...**
a particular integer n is even	n has the form $2k$
a particular integer n is odd	n has the form $2k+1$
a particular integer n has the form $2k$	n is even
a particular integer n has the form $2k+1$	n is odd

We can now answer the following questions:

Is 0 even?	Yes, $0 = 2 \cdot 0$
Is -301 odd?	Yes, $-301 = 2 \cdot [-151] + 1$
If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, is $6a^2b$ even?	Yes, $6a^2b = 2 \cdot 3a^2b$
If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, is $10a + 8b + 1$ odd?	Yes, $10a + 8b + 1 = 2(5a + 4b) + 1$

Here, we have also use the fact that ***sums and products of integers are integers***.

Prime Numbers

***Definition*: Prime / Composite Integers —**
An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$. An integer n is **composite** if, and only if $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Symbolically, if $n \in \mathbb{N} \setminus \{1\}$, then

n is prime $\Leftrightarrow$ $\forall r, s \in \mathbb{N}$ if $n = r \cdot s$, then $r = 1$ or $s = 1$

n is composite $\Leftrightarrow$ $\exists r, s \in \mathbb{N}$ such that $n = r \cdot s$ and $r \neq 1$ and $s \neq 1$

Notice that the definitions of prime and composite are negations of each other... Hence every integer (greater than 1) is either a prime or a composite.

Writing Proofs: Existential Statements

There are two ways of proving the statement

$$\exists x \in D \text{ such that } Q(x)$$

"There is an SDSU student interested in Mathematics"

1. Find an $x \in D$ such that $Q(x)$ is true. (Find an SDSU student interested in Mathematics).

2. Give a set of directions for finding such an $x \in D$. ***Important:*** — The directions must ***guarantee*** that we find $x \in D$.

Both these methods are called **constructive proofs of existence.** — They tell us something exists, ***and*** tell us how to find it.

Non-constructive Proofs of Existence

It is also possible to prove the existence of an $x \in D$ such that $Q(x)$ is true by: —

1. Showing that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem.

2. Showing that the assumption that there is no such x leads to a contradiction.

These proofs give us no information about ***how*** to find such a value, hence they are called **non-constructive**.

Clearly, if you ***are*** looking for a value making $Q(x)$ true, a non-constructive proof is a disadvantage. Such a proof is still useful, since it tells us there is indeed something to look for.

Proving Universal Statements Method of Exhaustion

The vast majority of mathematical statements to be proved are universal, basically on the form

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

The ***method of exhaustion*** can be used in two situations:

1. When D contains a finite number of elements

2. When there are only a finite number of elements in the truth set of $P(x)$

The method of exhaustion will make you exhausted quickly: you have to plug in every possible value of $x \in D$ (or from the truth set of $P(x)$) and then check $P(x) \rightarrow Q(x)$.

This is sometimes called a ***brute force method*** and quickly becomes infeasible!

Clearly, we would like a method of proving universal statements which works regardless of the size of the domain over which the statement is quantified.

The underlying idea of the **method of generalizing from the generic particular**:

> To show that every element of a domain satisfies a certain property, suppose x is a ***particular*** but ***arbitrarily chosen*** element of the domain and show that x satisfies the property.

We will use this tool in the **Method of Direct Proof**...

The Method of Direct Proof

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$."

2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. [Abbreviated: "suppose $x \in D$ and $P(x)$."]

3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Note: The point of selecting x arbitrarily is that everything you deduce about a generic element in D will be true for every other element in D.

Let's Try It...

Theorem: "If the sum of two integers is even, so is their difference."

Restatement: $\forall m, n \in \mathbb{Z}$, if $(m+n)$ is even, then $(m-n)$ is even.

1. $(m+n) = 2k$, for some $k \in \mathbb{Z}$. ***solve for*** m...

2. $m = 2k - n$. ***substitute into*** $(m-n)$***...***

3. $(m-n) = (2k-n) - n = 2k - 2n = 2(k-n)$.

We're done! (Sort of... Let's clean it up and make it more readable.)

Our First Theorem with Proof

Theorem: If the sum of any two integers is even, then so is their difference.

Proof: Suppose m and n are integers so that $m+n$ is even. By definition of even $m+n=2k$ for some integer k. Subtracting n from both side gives $m=2k-n$, then

$$\begin{aligned} m-n &= (2k-n)-n && \text{by substitution} \\ &= 2k-2n && \text{by combining terms / basic algebra} \\ &= 2(k-n) && \text{by factoring out a 2 / basic algebra} \end{aligned}$$

But $k-n$ is an integer because it is the difference between integers, Hence $m-n$ equals 2 times an integer, and so by the definition of even, $m-n$ is even. $\square$

How to Write a Proof

1. Write the theorem to be proved.

2. Clearly mark the beginning of the proof with the word ***proof*** .

3. Make your proof self-contained:

— In the body (text) of the proof, ***identify*** each variable used in the proof. The reader ***should not*** have to guess, or assume anything.

4. Write proofs in complete (English) sentences.

This ***does not*** mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate then into sentences.

Your proofs: It's better you are ***too*** detailed, but don't be ridiculous!

1. *Arguing from Examples*

Examples help understanding, but special cases do not prove general statements. — Think of the statement "All odd number integers greater than 1 are prime" and the examples 3, 5, 7...

2. *Using the same letter to mean two things*

For instance, if m and n are two even integers, don't say $m = 2r$ and $n = 2r$... Disaster! You're saying $m = n$!!! (Use, *e.g.* $m = 2r$ and $n = 2s$.)

3. *Jumping to a Conclusion*

To state that something is true without giving adequate reason. ***"cuz I say so!!!"*** is not sufficient logical argument!

4. Begging the Question

To assume what it to be proved. — Usually in a logically equivalent form that looks different...

5. Misuse of the Word "if"

Using the word "if" instead of "since" or "because". Consider

"Suppose p is a prime. If p is prime, then p cannot be written as a product of two smaller numbers."

and

"Suppose p is a prime. Since p is prime, p cannot be written as a product of two smaller numbers."

In the first formulation, the primeness of p seems to be in doubt in the second sentence... Such imprecise use of language can cascade through the proof and generate problems later.

Comic Relief — The Odd Prime Number Theory

An engineer, a mathematician, and a physicist are testing the theory that all odd numbers are prime: —

Physicist: "1 is prime, 3 is prime, 5 is prime, 7 is prime, 9 — must be experimental error, 11 is prime, 13 is prime. That's enough data points; the theory is true."

Mathematician: "By convention, 1 is not prime, but 3 is a prime, 5 is a prime, 7 is a prime, 9 is not a prime — counterexample — claim is false."

Engineer: "1 is prime, 3 is prime, 5 is prime, 7 is prime, 9 is prime, 11 is prime, 13 is prime, 15 is prime, 17 is prime, 19 is prime... Hmmm, theory appears to be true."

Second Engineer, who slept through some early math classes: "What do you mean, '1 is not prime?' "

Disproof By Counterexample

Disproving a statement of the form

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

amounts to proving that the negation of the statement is true

$$\exists x \in D \text{ such that } P(x) \text{ and } \sim Q(x)$$

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" find a value of x in D for which $P(x)$ is true and $Q(x)$ is false. Such an x is called a **counterexample**.

Examples: Disproofs

Bogus Theorem #1: "All odd integers greater than 1 are prime."

Disproof: Since $9 = 2 \cdot 4 + 1$ it is odd. Further, $9 = 3 \cdot 3$ which shows that 9 is a composite number, hence not a prime.

Bogus Theorem #2: $\forall a \in \mathbb{R}$, $b \in \mathbb{R}$, if $a^2 = b^2$, then $a = b$.

Disproof: Let $a = 1$, and $b = -1$, $a^2 = b^2 = 1$, but $a \neq b$.

Famous Proofs and Disproofs

Fermat's Last Theorem: If n is an integer greater than 2, then the equation $x^n + y^n = z^n$ has no solutions where x, y, and z are positive integers. (Pierre de Fermat lived 1601–1665)

Euler's Conjecture: $a^4 + b^4 + c^4 = d^4$ has no integer solutions. (Leonhard Euler lived 1707–1783)

Fermat's Last Theorem was finally proved by Andrew Wiles in September 1994.

Euler's Conjecture was disproved by Noam Elkie (Harvard University) in 1986. One counterexample is $95,800^4 + 217,519^4 + 414,560^4 = 422,481^4$ — found by Roger Frye of Thinking Machines Corporation.

Homework #4 — Due 10/6/2006, 12noon, GMCS-587 version $\frac{1}{3}$

3rd Edition	2nd Edition
Problems	
3.1: 27, 31, 37, 49	***3.1:*** 12, –, 24, 35

Please use the ***3rd Edition*** numbering when handing in your solutions.

Divisibility and Number Theory — Introduction

Epp*-§*3.2: skip.

Divisibility of the central concept of **number theory** — the study of properties of integers.

Important applications of number theory include keeping your credit card number safe when you hit *"buy now"* in your web browser.

We look at some more statements about integers, and prove a few of them...

Divisibility of an Integer

Definition: **Divisibility —**

If n and d are integers and $d \neq 0$, then

n is **divisible by** d if, and only if, $n = d \cdot k$ for some integer k

Alternatively, we say that

n **is a multiple of** d, or

d **is a factor of** n, or

d **is a divisor of** n, or

d **divides** n.

The notation $\mathbf{d|n}$ is read "d divides n." Symbolically if n and d are integers and $d \neq 0$,

$$d|n \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \ : \ n = d \cdot k$$

Divisibility: Examples

Example #1: Suppose a and b are positive integers, and $a|b$. Is $a \leq b$?

Solution: $a|b$ means that $b = k \cdot a$ for some positive integer k (since both a and b are positive). Therefore $k \geq 1$. This shows that $b = k \cdot a \geq a$ (by multiplying both sides of the inequality by the positive integer a). Hence we can conclude that $a \leq b$.

Divisibility: Examples

Example #2:

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution:

a. By basic algebra (the distributive law) we can write $3a + 3b = 3(a + b)$, and since $a + b$ is an integer (being a sum of integers), we have shown that $3|(3a + 3b)$.

b. By basic algebra (the associative law) we can write $10km = 5 \cdot 2km$, where $2km$ is an integer (being a product of integers). We have shown $5|10km$.

Divisibility — Primeness, and Transitivity

We can use the concept of divisibility to define primeness:

> ***Definition:*** **Prime Integer (Alternative) —**
> A positive integer $n > 1$ is **prime**, if and only if, its only divisors are 1 and n.

Divisibility is **transitive**: If one number a divides a second number b ($a|b$) and the second number divides a third number c ($b|c$), then the first number divides the third ($a|c$).

This is an important fact, lets prove it!

Proof: Divisibility is a Transitive Property

Theorem:
For all integers a, b and c, if $a|b$ and $b|c$, then $a|c$.

Proof: Suppose a, b and c are ***particular but arbitrarily chosen*** integers such that $a|b$ and $b|c$. By the definition of divisibility we know that

$$a|b \quad \Leftrightarrow \quad b = a \cdot r, \text{ for some integer } r, \text{ and}$$

$$b|c \quad \Leftrightarrow \quad c = b \cdot t, \text{ for some integer } t.$$

Combining these two, we have

$$c = b \cdot t = a \cdot r \cdot t, \quad \text{for some integers } r \text{ and } t.$$

Hence, we can write

$$c = a \cdot (r \cdot t), \text{ where } r \cdot t \text{ is an integer,}$$

which shows that $a|c$. $\square$

Does $a|b$ and $b|a$ imply $a = b$?

Question: Is it true that for all integers a and b, if $a|b$ and $b|a$ then $a = b$?

Solution: Suppose a and b are integers such that $a|b$ and $b|a$, then we must have

$$b = a \cdot r, \quad r \in \mathbb{Z}, \qquad a = b \cdot s, \quad s \in \mathbb{Z}.$$

By substitution

$$b = a \cdot r = b \cdot (s \cdot r)$$

which is true if and only if $(s \cdot r) = 1$, *i.e.* both r and s are divisors of 1.

The only divisors of 1 are 1 and -1. $r = s = -1$ gives us infinitely many counterexamples ($a = -b$), thus we conclude

$$a|b \quad \text{and} \quad b|a \quad \not\Rightarrow \quad a = b.$$

The Unique Factorization Theorem

Theorem: **The Unique Factorization Theorem —**
Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers p_1, p_2, ..., p_k, and positive integers e_1, e_2, ..., e_k, such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

and any other expression of n as a product of prime numbers is identical to this (except, possibly, for the order in which the factors are written).

The proof is beyond the scope of this class, but the theorem is important enough that you should know it!

If you write the factors such that $p_1 < p_2 < \cdots < p_k$, then the form is called the **standard factored form**.

Using the Unique Factorization Theorem

Question: Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10$$

Does $17|m$?

Solution: 17 is a prime number. Since it is a factor on the right side of the equation, it must also be a factor on the left side of the equation, by the Unique Factorization Theorem (UFT). But 17 cannot factor any of the numbers 8, 7, 6, 5, 4, 3, 2 — since it is too large. Hence it must factor m, so $17|m$.

The Quotient-Remainder Theorem

Theorem: **Quotient-Remainder —**
Given any integer n and a positive integer d, there exist unique integers q (the **quotient**) and r (the **remainder**) such that

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

Example: Say you have 10 cookies ($n = 10$), and you want to distribute as many of them as possible among 3 children ($d = 3$) (so that each child receives the same number of cookies, of course!)... After you have distributed 3 sets ($q = 3$) of 3 cookies, you have one ($r = 1$) remaining... By the quotient-remainder theorem you got it right — there is only one (unique) way of solving the problem.

We are going to need more tools before we can prove this theorem (we'll get to it in a couple of weeks), for now we take it as given.

Notation: div and mod

Definition:

Given a non-negative integer n and a positive integer d, we define

n div d	$= q$	the integer quotient
		obtained when n is divided by d
n mod d	$= r$	the integer remainder
		obtained when n is divided by d

The ***quotient-remainder theorem*** tells us that

$$n \bmod d \in \{0, 1, \ldots, d-1\}$$

and

$$n \bmod d = 0 \quad \Leftrightarrow \quad d|n$$

Using div and mod

Example: February 17, 2005 was a Thursday. What day was it one year earlier?

Solution: 366 days passed since February 17 2004, and each week has seven days. Since

$$366 \text{ div } 7 = 52, \quad \text{and} \quad 366 \bmod 7 = 2$$

it follows that exactly 52 weeks and 2 days passed between the two dates. Thus 2/17/2004 was a Tuesday.

The Parity of an Integer

The **parity property** is the fact that an integer is either even or odd (but not both).

We use the quotient-remainder theorem, and and our new operation mod to classify the integers:

For an integer n

If $n \bmod 2 = 0$ then n is even

If $n \bmod 2 = 1$ then n is odd

Proof by Dividing into Cases

Theorem: Any two consecutive integers have opposite parity.

Proof: Let* m and $m+1$ be two consecutive integers. By the parity property, m is even, or m is odd.

case 1: (m is even) In this case, $m = 2k$ for some $k \in \mathbb{Z}$, and so $m+1 = 2k+1$, which is odd by the definition of odd. In this case, m is even and $m+1$ is odd.

case 2: (m is odd) In this case, $m = 2k+1$ for some $k \in \mathbb{Z}$, and so $m+1 = 2k+2 = 2(k+1)$, which is even by the definition of even. In this case, m is odd and $m+1$ is even.

It follows that regardless of which case occurs for the particular choice of m and $m+1$, one of them is even and the other one is odd. Hence we have proved the theorem. $\square$

Homework #4 — Due 10/6/2006, 12noon, GMCS-587 version $\frac{2}{3}$

3rd Edition	2nd Edition
Problems	
3.1: 27, 31, 37, 49	***3.1:*** 12, –, 24, 35
3.3: 17, 25, 26, 36a, 36b	***3.3:*** 16, 24, 25, 35, –

Please use the ***3rd Edition*** numbering when handing in your solutions.

Checking the Road Map

Where are we? Are we lost?

In chapters 1 and 2 we talked about logic in its purest form; learning about logic operator and connectives; truth tables; compound statements; conditional statements; quantified statements; predicates. — Things were pretty good (some of y'all fell asleep since things were quite cozy and familiar).

Now, in chapter 3 we are talking about different **methods of proof**; where we must use our logic toolbox from chapters 1 and 2 to prove that certain mathematical statements are true.

We are working in the **context of number theory** — the study of the properties of integers.

We are introducing both proof-methodologies and number theory at the same time, maybe a source of confusion?!?

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$"

2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. [Abbreviated: "suppose $x \in D$ and $P(x)$."]

3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" find a value of x in D for which $P(x)$ is true and $Q(x)$ is false. Such an x is called a **counterexample**.

Example: Disproof of "$a^4 + b^4 + c^4 = d^4$ *does not have any positive integer solutions.*"

Review: Proof Techniques — Division into Cases

Proof by Division into Cases

Conjectures can often be simplified by dividing a proof into cases. When a conjecture is true in all cases, it is a theorem. If a conjecture is a theorem, a proof by cases may simplify the argument, since each case is a simpler form of the conjecture.

Also, if a conjecture is not a theorem, an attempted proof by cases may simplify the conjecture and make it easier to understand why the proof is not succeeding.

Example: The successful proof of *"Any two integers consecutive have opposite parity."*

Review: Number Theory — Divisibility

Definition: **Divisibility —**

If n and d are integers and $d \neq 0$, then

n is **divisible by** d if, and only if, $n = d \cdot k$ for some integer k

Alternatively, we say that

n **is a multiple of** d, or

d **is a factor of** n, or

d **is a divisor of** n, or

d **divides** n.

The notation $\mathbf{d|n}$ is read "d divides n." Symbolically if n and d are integers and $d \neq 0$,

$$d|n \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \ : \ n = d \cdot k$$

Review: Number Theory — Primeness, Two Definitions

***Definition*: Prime / Composite Integers —**

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$. An integer n is **composite** if, and only if $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Symbolically, if $n \in \mathbb{N} \setminus \{1\}$, then

n is prime $\Leftrightarrow$ $\forall r, s \in \mathbb{N}$ if $n = r \cdot s$, then $r = 1$ or $s = 1$

n is composite $\Leftrightarrow$ $\exists r, s \in \mathbb{N}$ such that $n = r \cdot s$ and $r \neq 1$ and $s \neq 1$

***Definition:* Prime (Alternative) —**

A positive integer $n > 1$ is **prime**, if and only if, its only divisors are 1 and n.

Review: Number Theory — Integer Division and Modulus

Definition: **Integer Division and Modulus —**

Given a non-negative integer n and a positive integer d, we define

n div d	$= q$	the integer quotient
		obtained when n is divided by d
n mod d	$= r$	the integer remainder
		obtained when n is divided by d

Review: Number Theory — Unique Factorization Theorem

Theorem: **The Unique Factorization Theorem —**
Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers p_1, p_2, ..., p_k, and positive integers e_1, e_2, ..., e_k, such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

and any other expression of n as a product of prime numbers is identical to this (except, possibly, for the order in which the factors are written).

The proof is beyond the scope of this class, but the theorem is important enough that you should know it! — Know the **statement**, and how to **use** it.

If you write the factors such that $p_1 < p_2 < \cdots < p_k$, then the form is called the **standard factored form**.

Review: Number Theory — Quotient-Remainder Theorem

Theorem: **Quotient-Remainder —**
Given any integer n and a positive integer d, there exist unique integers q (the **quotient**) and r (the **remainder**) such that

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

Those are our theoretical "toys" so far...

Now, lets move forward...

Exercise: Representation of Integers Modulo 4

Conjecture: All integers can be written in one of the forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3.$$

Solution: Let* n be an integer. We apply the quotient-remainder theorem with $d = 4$, this implies there exists a unique pair of quotient-remainder pair q and r such that

$$n = 4 \cdot q + r, \quad \text{where } r \in \{0, 1, 2, 3\}.$$

This shows that the conjecture is **true**.

This (seemingly simple) result will be useful in a few slides...

The Mathematical "Let"

The statement ***"Let n be an integer"*** means: ***"Suppose n is a particular but arbitrarily chosen integer."***

That is, we ***randomly*** select an integer from $\mathbb{Z}$.

The statement ***may look casual***, but it means something ***very specific*** in the language of mathematics.

You will see similar statements all over the math-literature:

- *"Let p be a prime such that $p = 2^n - 1$, for some $n \in \mathbb{Z}$."*
- *"Let r and s be two real numbers such that...."*

Conjecture: The square of any odd integer has the form $8m + 1$ for some integer m.

Solution: Let n be an odd integer. By the quotient-remainder theorem, n can be written in one of the forms (see previous exercise):

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3.$$

Now, since n is odd, this reduces the possibilities to the forms

$$n = 4q + 1 \quad \text{or} \quad n = 4q + 3.$$

case-1: We have that $n = 4q + 1$ for some integer q, therefore

$$n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8\underbrace{(2q^2 + q)}_{\text{integer}} + 1$$

Identifying $m = 2q^2 + q$ shows that $n^2 = 8m + 1$ for some integer m.
[end case-1].

case-2: We have that $n = 4q + 3$ for some integer q, therefore

$$n^2 = (4q+3)^2 = 16q^2 + 24q + 9 = 8\underbrace{(2q^2 + 3q + 1)}_{\text{integer}} + 1$$

Identifying $m = 2q^2 + 3q + 1$ shows that $n^2 = 8m + 1$ for some integer m. ***[end case-2]***.

case-1 and ***case-2*** shows that given *any* odd integer n, whether of the form $4q + 1$ or $4q + 3$, its square can be written on the form $n^2 = 8m + 1$ for some integer m. $\square$

Exercise: Making Change

The following algorithms gives makes change: it determines how many quarters (25¢) q, dimes (10¢) d, nickels (5¢), and pennies (1¢) p equals c (the total amount of change).

Given c	$c = 99$	$c = 69$	$c = 83$
$q = c \text{ div } 25$	3	2	3
$c_2 = c \bmod 25$	24	19	8
$d = c_2 \text{ div } 10$	2	1	0
$c_3 = c_2 \bmod 10$	4	9	8
$n = c_3 \text{ div } 5$	0	1	1
$p = c_3 \bmod 5$	4	4	3

Exercise: $(n \bmod 3) \in \{0, 1, 2\}$

Conjecture: Any integer n can be written in one of the three forms:

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2.$$

Solution: Let n be an integer. By the quotient-remainder theorem with $d = 3$ there exist unique integers q and r such that

$$n = 3 \cdot q + r, \quad \text{where } 0 \leq r < d$$

This shows that n can be written in one of the forms above. $\square$.

We are now going to use this result to show something a little more complicated...

Conjecture: The product of three consecutive integers is divisible by 3.

Solution: Let n, $n+1$ and $n+2$ be three consecutive integers. By the quotient-remainder theorem (see previous exercise), n can be written in one of the forms

$$n = 3q \quad \text{or} \quad n = 3q+1 \quad \text{or} \quad n = 3q+2$$

case-1: $n = 3q$ for some integer q, in this case the product

$$n(n+1)(n+2) = 3q(3q+1)(3q+2) = 3 \cdot \underbrace{(q(3q+1)(3q+2))}_{\text{integer}}$$

which shows that $3|n(n+1)(n+2)$.

case-2: $n = 3q + 1$ for some integer q, in this case the product

$$n(n+1)(n+2) = (3q+1)(3q+2)(3q+3) = 3 \cdot \underbrace{((3q+1)(3q+2)(q+1))}_{\text{integer}}$$

which shows that $3|n(n+1)(n+2)$.

case-3: $n = 3q + 2$ for some integer q, in this case the product

$$n(n+1)(n+2) = (3q+2)(3q+3)(3q+4) = 3 \cdot \underbrace{((3q+2)(q+1)(3q+4))}_{\text{integer}}$$

which shows that $3|n(n+1)(n+2)$.

In all three cases we have $3|n(n+1)(n+2)$, thus we have shown that the product of *any* three consecutive integers is divisible by 3. □

Homework #4 — Due 10/6/2006, 12noon, GMCS-587 Final Version

3rd Edition	2nd Edition
Problems	
3.1: 27, 31, 37, 49	***3.1:*** 12, –, 24, 35
3.3: 17, 25, 26, 36a, 36b	***3.3:*** 16, 24, 25, 35, –
3.4: 7, 8, 9, 10, 24, 29, 43	***3.4:*** 7, –, –, –, 18, –, 30

Please use the ***3rd Edition*** numbering when handing in your solutions.

Writing your name on, and ***stapling*** your homework is highly recommended.