Math 300–03

Wolmer V. Vasconcelos

Set 1

Fall 2008

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

General Orientation

- Pre-requisites: Calc 2
- web:www.math.rutgers.edu/(tilde)vasconce
- Meetings: TF3 12:00-1:20 SEC-212
- email: vasconce at math.rutgers.edu
- Office Hours [Hill 228]: M 2:00-4:00, or by arrangement
- Textbook: **A Transition to Advanced Mathematics**, 6th Ed., by D. Smith, M. Eggen & R. St. Andre
- All this detailed in General Info page: Look it over

Scoring Info

- Weekly Homework Total: 100
- 2 Midterms Total: 2 x 100 = 200
- Final: 200
- Total: 500 pts

Some Goals

- Reading and Writing Mathematics
- What are Theorems and what are Proofs: How to go About?
- Understand Statements such as

$$\ln 2 = \int_1^2 \frac{1}{x} dx$$

$$\ln 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$$

Outline

1. General Orientation
2. **Numbers**
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Language of Math

Before we start, we ponder the following:

- The language of mathematics is set theory: All mathematical objects can be regarded as sets, and relations between them can be reduced to expressions that use only the belongs to relation: $\in$.
- For instance, integers are certain finite sets, rational numbers are pairs of integers, real numbers are identified to some sets called Dedekind cuts of rational numbers,functions are some sets of pairs.
- We are not going to begin at the beginning... Means what?

Numbers

We are not start at the very beginning, but will visit it occasionally. At the outset of our journey are the **natural** numbers

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

Its 'modern' construction [e.g. Peano's] is a paradigm of beauty. It is enlarged by the **integers**

$$\mathbb{N} \subset \mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

and the **rational** numbers

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} = \left\{ \frac{m}{n}, \quad m, n \in \mathbb{Z}, n \neq 0 \right\}$$

We will also meet $\mathbb{R}$, **real** numbers: $\mathbb{Q} \subset \mathbb{R}$

Propositions

One of our goals is to determine which *mathematical statements* are *true* and which are *false*. A statement that is either true or false is called a **proposition**.

Definition

A **proposition** is a sentence that is either true or false.

Examples from book:

1. 5(8)-42 is a positive number.
2. 1+1 = 5.
3. The elephant will become extinct by the year 2525.
4. Julius Caesar had two eggs for breakfast on his tenth birthday.
5. What did you say?
6. $x^2 = 25$.
7. She has your car keys.
8. This sentence is false.

Examples: Which statements are Propositions?

- RU will be the football champs this season.
- RU will be the football champs this season!
- Will RU be the football champs this season?
- RU has a 10% chance to be the football champs this season.
- Half the class will ace the course.
- Half the class will ace the course, one third will get a B, one quarter will get a C.

Grand Examples

Theorem

If $\mathbf{f}$ *is continuous on* $[a, b]$ *then* $\int_a^b \mathbf{f}(x)dx$ *exists.*

Theorem (FTC)

Let $\mathbf{f} : [a, b] \to \mathbb{R}$ *be a function such that* $\int_a^b \mathbf{f}$ *exists. If* $\mathbf{F}$ *is a function such that* $\mathbf{F}'(c) = \mathbf{f}(c)$ *for all* $c \in [a, b]$*, then*

$$\int_a^b \mathbf{f}(x)dx = \mathbf{F}(b) - \mathbf{F}(a).$$

Representing Propositions

While not absolutely necessary, it is convenient to represent statements by Letters or Abbreviations.

- $P =$"RU will be the football champs this season."
- $Q =$ "RU will be the football champs this season!"
- $R =$ "There will be assigned HW every week [collected the following week for grading]"
- $S =$ "John has classes on Tuesdays"
- $T5 =$ "John has classes on Thursdays"
- $U2 =$ "Mary enjoyed the **The Dark Knight**"

Logical Connectives

A compound proposition is a proposition formed from simpler propositions by the use of connectives such as AND, OR and NOT.

Definition

Given propositions P and Q,

- The **conjunction** of P and Q, denoted by $P \wedge Q$, is the proposition "P and Q." $P \wedge Q$ is true exactly when *both* P and Q are true.
- The **disjunction** of P and Q, denoted by $P \vee Q$, is the proposition "P or Q." $P \vee Q$ is true when *at least one* of P or Q is true.
- The **negation** of P, denoted by $\sim P$, is the proposition "not P." $\sim P$ is true exactly when P is false.

Comment: Noticed how the usage of "OR" may differ from the usual?

Examples: Still from book

If P is "$1 \neq 3$" and Q is "7 is odd"

1. $P \wedge Q$ is "$1 \neq 3$ and 7 is odd"
2. $P \vee Q$ is "$1 \neq 3$ or 7 is odd"
3. $\sim Q$ is "It is not the case that 7 is odd"

Note that $P \wedge Q$ is true, $P \vee Q$ is true, but $\sim Q$ is false.
The following are examples of true propositions:

1. "It is not true that $\sqrt{10} > 4$"
2. " $\sqrt{2} < \sqrt{3}$ or chickens have lips."
3. " Venus is smaller than Earth or $1 + 4 = 5$."
4. "$6 < 7$ and $7 < 8$"

XOR: The Exclusive OR

Given propositions P and Q,

- The **inclusive OR** of P and Q, denoted by $P \vee Q$, is the proposition "P or Q." $P \vee Q$ is true when at least one of P or Q are true.
- The **exclusive OR** of P and Q, denoted by $P \text{ XOR } Q$, is the proposition "P or Q but not both." $P \text{ XOR } Q$ is true when P or Q are true but not both.

Propositional Forms

Definition

A **propositional variable** is a (usually capital) letter representing a proposition. A **propositional form** is an expression of propositional variables involving connectives, formed according to the following rules:

1. If P is a propositional form then $\sim P$ is a proposition form.
2. If P, Q are propositional forms then $P \vee Q$, $P \wedge Q$ are propositional forms.

Predicates: From CTW

Some statements are not **propositions** because they contain unknowns. For instance, *she loves that kind of ice-cream*: both *she* and *kind* are unknown.
A collection of possible values of a variable is called an *universe*. What are some of the universes for *she* and *kind* above?
A statement containing variables that becomes a proposition after a substitute for each variable is a **predicate**. For example, the statement $P(x)$ given by $x^2 = 4$ is a predicate. If we substitute $x = 2$, $P(x)$ becomes a proposition which happens to be true. If we substitute $x = 3$, $P(x)$ becomes another proposition which happens to be false.

Truth Tables

Let P, Q be propositions and $\mathbf{f}(P, Q)$ a proposition obtained by using the rules above. To determine when $\mathbf{f}(P, Q)$ is true or false, we build its truth table:

P	Q	$\mathbf{f}(P, Q)$
T	T	$\mathbf{f}(T, T)$
T	F	$\mathbf{f}(T, F)$
F	T	$\mathbf{f}(F, T)$
F	F	$\mathbf{f}(F, F)$

Examples

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$	P XOR Q
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

Long Tables

True tables can be very large if there are many variables:

P	Q	R	$\mathbf{f}(P, Q, R)$
T	T	T	$\mathbf{f}(T, T, T)$
T	T	F	$\mathbf{f}(T, T, F)$
T	F	T	$\mathbf{f}(T, F, T)$
T	F	F	$\mathbf{f}(T, F, F)$
F	T	T	$\mathbf{f}(F, T, T)$
F	T	F	$\mathbf{f}(F, T, F)$
F	F	T	$\mathbf{f}(F, F, T)$
F	F	F	$\mathbf{f}(F, F, F)$

If there are 4 variables, the table has 16 rows.

Comparing Propositional Forms

P	Q	$\mathbf{f}(P, Q)$	$\mathbf{h}(P, Q)$
T	T	$\mathbf{f}(T, T)$	$\mathbf{h}(T, T)$
T	F	$\mathbf{f}(T, F)$	$\mathbf{h}(T, F)$
F	T	$\mathbf{f}(F, T)$	$\mathbf{h}(F, T)$
F	F	$\mathbf{f}(F, F)$	$\mathbf{h}(F, F)$

Example

P	$\sim P$	$\sim (\sim P)$
T	F	T
F	T	F

Look: "P is equivalent to $\sim (\sim P)$" [have the same truth tables]

Truth Tables of some well-defined Forms

P	Q	$P \wedge Q$	$P \vee Q$	$\sim P$	$\sim (\sim P)$
T	T	T	T	F	T
T	F	F	T	F	T
F	T	F	T	T	F
F	F	F	F	T	F

Equivalent Forms

Definition

Two propositional forms are **equivalent** if and only if they have the same truth tables.

For example, the forms P and $\sim(\sim P)$ are equivalent:

P	$\sim P$	$\sim(\sim P)$
T	F	T
F	T	F

Examples

P	Q	$\sim (P \vee Q)$	$\sim P \wedge \sim Q$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

P	Q	$\sim (P \wedge Q)$	$\sim P \vee \sim Q$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	T	T

Outline

1. General Orientation
2. Numbers
3. **Last Class...**
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Last Class...

Last time we introduced the notions:

- **Proposition**
- **The logical connectives:** $\vee$, $\wedge$, $\sim$, XOR **disjunction, conjunction, negation, exclusive OR**
- **Propositional form**
- **Predicate**
- **Truth table**

P	$\sim P$	$\sim(\sim P)$
T	F	T
F	T	F

- **Equivalence of propositional forms**
- Today we begin by mentioning some special propositional forms

Tautology

Definition

A **tautology** is a propositional form that is true for every assignment of truth values to its components.

Example: Law of Excluded Middle, $P \vee \sim P$

P	$\sim P$	$P \vee \sim P$
T	F	T
F	T	T

Contradiction and Denial

Definition

A **contradiction** is a propositional form that is false for every assignment of truth values to its components.

$P \wedge \sim P$ is an example of a contradiction.

Definition

A **denial** of a proposition P is any proposition equivalent to $\sim P$.

Example: The proposition "$\sqrt{2}$ is irrational" has numerous denials:
"It is not the case that $\sqrt{2}$ is irrational"
"$\sqrt{2}$ is the quotient of two integers"
"The decimal expansion of $\sqrt{2}$ is repeating or terminating"
"It is not the case that it is not the case that $\sqrt{2}$ is rational"

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. **Conditionals and Biconditionals**
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Conditionals and Biconditionals

Definition

For propositions P and Q, the **conditional sentence** $P \Rightarrow Q$ is the proposition "If P then Q". Proposition P is called the **antecedent** and Q is the **consequent**.The conditional sequence $P \Rightarrow Q$ is *true* if and only if P is false or Q is true.

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

The truth table for $P \Rightarrow Q$ only gives the value F when P is true and Q is false, so agrees with the common usage "if ..., then ... ".

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

Suppose A tells her friend B: “If $1 + 1 = 2$, then I will give you a dollar.” Since $1 + 1 = 2$ is true, we must find the value of the statement in lines 1 or 3. If A does not give B one dollar (line 3) the promise is broken and the statement is false.To keep the promise and thus make the sentence true, A must give B one dollar (line 1).
When the antecedent is false, the promise is always true: If A said to B: “If $1 + 1 = 5$, then I will give you a dollar,” she would keep her promise.According to lines 2 and 4, this sentence is true whether A gives B a dollar or not.

Converse and Contrapositive

Two propositions closely related to $P \Rightarrow Q$ are its converse and contrapositive.

Definition

Let P and Q be propositions.

- The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$.
- The **contrapositive** of $P \Rightarrow Q$ is $(\sim Q) \Rightarrow (\sim P)$.

- **Conditional sentence:** "If $\mathbf{f}(x)$ is differentiable at x_0, then $\mathbf{f}$ is continuous at x_0.
- **Contrapositive:** "If $\mathbf{f}$ is not continuous at x_0, then $\mathbf{f}$ is not differentiable at x_0" also true.
- **Converse:** "If $\mathbf{f}$ is continuous at x_0, then $\mathbf{f}$ is differentiable at x_0" which is false for $\mathbf{f}(x) = |x|$ and x_0 is 0.

Remarks on $\Rightarrow$

P	Q	$P \Rightarrow Q$	$\sim P \vee Q$
T	T	T	T
F	T	T	T
T	F	F	F
F	F	T	T

- The truth table of says that $P \Rightarrow Q$ is true whenever the antecedent is true or the consequent is false.
- The first row of the table is the only line where both P ND $P \Rightarrow Q$ are true. Note that Q is also true. In other words, if P and $P \Rightarrow Q$ are true, then Q is also true. This rule is known as **modus ponens**.

Theorem

1. *A conditional proposition and its contrapositive are equivalent.*
2. *A conditional proposition and its converse are not equivalent.*

Proof. We will compare the truth tables of the forms $P \Rightarrow Q$, $(\sim Q) \Rightarrow (\sim P)$ and $Q \Rightarrow P$.

P	Q	$P \Rightarrow Q$	$\sim P$	$\sim Q$	$(\sim Q) \Rightarrow (\sim P)$	$Q \Rightarrow P$
T	T	T	F	F	T	T
F	T	T	T	F	T	F
T	F	F	F	T	F	T
F	F	T	T	T	T	T

Note that the tables for $P \Rightarrow Q$ and $(\sim Q) \Rightarrow (\sim P)$ identical.

Biconditionals

Definition

For propositions P and Q, the **biconditional sentence** $P \Leftrightarrow Q$ is the proposition "P if and only if Q". $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth values.

P	Q	$P \Leftrightarrow Q$
T	T	T
F	T	F
T	F	F
F	F	T

A long theorem...

Theorem

1. $P \Rightarrow Q$ *is equivalent to* $(\sim P) \vee Q$.
2. $P \Leftrightarrow Q$ *is equivalent to* $(P \Rightarrow Q) \vee (Q \Rightarrow P)$.
3. $\sim (P \wedge Q)$ *is equivalent to* $(\sim P) \vee (\sim Q)$.
4. $\sim (P \vee Q)$ *is equivalent to* $(\sim P) \wedge (\sim Q)$.
5. $\sim (P \Rightarrow Q)$ *is equivalent to* $P \Rightarrow \wedge \sim Q$.
6. $\sim (P \wedge Q)$ *is equivalent to* $P \Rightarrow \sim Q$.
7. $P \wedge (Q \vee R)$ *is equivalent to* $(P \wedge Q) \vee (P \wedge R)$.
8. $P \vee (Q \wedge R)$ *is equivalent to* $(P \vee Q) \wedge (P \vee R)$.

HowTo Prove?

Consider the first statement: $P \Rightarrow Q$ is equivalent to $(\sim P) \vee Q$. To prove it we build and compare their truth tables:

P	Q	$P \Rightarrow Q$	$(\sim P) \vee Q$
T	T	?	?
F	T	?	?
T	F	?	?
F	F	?	?

The last two columns must be identical.

Exercise

The **inverse**, or **opposite** of the conditional sentence $P \Rightarrow Q$ is $\sim P \Rightarrow \sim Q$. Show that $P \Rightarrow Q$ and its inverse are not equivalent: Compare their truth tables

P	Q	$P \Rightarrow Q$	$\sim P \Rightarrow \sim Q$
T	T	T	T
F	T	T	F
T	F	F	T
F	F	T	T

Exercise

Which is equivalent to the converse of a conditional sentence, the contrapositive of its inverse, or the inverse of its contrapositive? Suggest write them out:

1. **conditional sentence:** $P \Rightarrow Q$
2. **its inverse:** $\sim P \Rightarrow \sim Q$
3. **its converse:** $Q \Rightarrow P$
4. **its contrapositive:** $\sim Q \Rightarrow \sim P$
5. **contrapositive of its inverse:** $\sim (\sim Q) \Rightarrow \sim (\sim P)$
6. **inverse of its contrapositive:** $\sim (\sim Q) \Rightarrow \sim (\sim P)$

Note that $(3) = (5) = (6)$

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. **Quantifiers**
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Quantifiers

- **open sentence or predicate:** a sentence $P(x), P(x_1, \ldots, x_n)$ which depends on one or more variables. For instance the sentence "$s \geq 3$" is not a proposition, but becomes one once the value of x is assigned. Thus if x is given the value 5, "$5 > 3$" is a true proposition.

  Another example of an open sentence: the sentence P given by $x + y = z$ written $P(x, y, z)$. Thus $P(2, 4, 6)$ is true but $P(1, 2, 4)$ is false.
- **truth set of a sentence:** the collection of objects that make an open sentence a true proposition.
- **universe of discourse:** the set of objects which are available for consideration
- **typical universes:** $\mathbb{N} = \{1, 2, 3, \ldots\}$; $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$; $\mathbb{Q}$ rational numbers; $\mathbb{R}$ real numbers.

Definition

With a specified universe, two open sentences $P(x)$ and $Q(x)$ are **equivalent** iff they have the same truth set.

Examples: "$3x + 2 = 20$" and "$x = 6$" are equivalent open sentences. "$x^2 = 4$" and "$x = 2$" are not equivalent when the universe is $\mathbb{R}$, but are equivalent when the universe is $\mathbb{N}$.

Existential and Universal Quantifier

Definition

For an open sentence $P(x)$, the sentence $(\exists x)P(x)$ is read " **there is** x **such that** $P(x)$", or "**for some** x**,** $P(x)$" and is true if the truth set of $P(x)$ is *nonempty*. The symbol $\exists$ is called the **existential qualifier**.

Definition

For an open sentence $P(x)$, the sentence $(\forall x)P(x)$ is read "**for all** x**,** $P(x)$" and is true if the truth set of $P(x)$ is the *entire* universe. The symbol $\forall$ is called the **universal qualifier**.

technical name	meaning	notation	other meanings
universal	for all	$\forall$	for every
existential	there exists	$\exists$	there is, there are some

Example

Universe: All living things, and let H be the set of all people.

- Some people are tall:

$$(\exists x)(x \in H \wedge x \text{ is tall})$$

- Everyone has some faults:

$$(\forall x)(x \in H \Rightarrow x \text{ has some faults})$$

$$(\forall x)(x \in H)(x \text{ has some faults})$$

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. **Homework #1**
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

About Proofs

1. Most theorems are of the form $P \Rightarrow Q$.
2. Scan the statements and assure yourself that you understand all the definitions.
3. Since there are various methods of proof...look up in notes.
4. Write very clearly, you will not just trying to convince yourself [this for sure] but maybe a machine intelligence as well...

Homework #1

1. Section 1.1 problems 2 (b,e,h,k) 3 (d,f,i) 4 (a,d,g,i,k) 5 (a,b,d) 8 (a,c).
2. Section 1.2 4 (a,b,d,h,i) 5 (a,b,d,k) 6 (a,d) 9 (a,e,f) 10 (b,c) 13 (b,d,f).

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. **Last Class...**
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Last Class...

We last discussed several types of propositional forms, conditional sentences, transformations of conditional propositions:

- **Tautoloty, contradiction, denial**
- **Conditional and Biconditional**
- **Converse, contrapositive**
- **Equivalence of propositions**
- **Inverse or opposite**
- **Universe of discourse**
- **Quantifiers, existencial quantifier, universal quantifier**

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. **Quantified Sentences**
9. Proof Methods I
10. Proof Methods II
11. Homework #2

Equivalence of Quantified Sentences

Definition

Two quantified sentences are **equivalent in a given universe** iff they have the same truth value in that universe. Two quantified sentences are **equivalent** iff they have the same truth value in every universe.

Example: $(\forall x)(x > 3)$ and $(\forall x)(x \geq 4)$ are equivalent in the universe of the integers (they are both false), the universe of integers greater than 10 (when they are both true), but in the universe of real numbers larger than 3.4 they are not equivalent.

Theorem

If $A(x)$ is an open sentence with variable x, then

1. $\sim (\forall x)A(x)$ *is equivalent to* $(\exists x) \sim A(x)$.
2. $\sim (\exists x)A(x)$ *is equivalent to* $(\forall x) \sim A(x)$.

Proof.

- Let U be any universe.
- The sentence $\sim (\forall x)(A(x))$ is true in U
- iff $(\forall x)A(x)$ is false in U
- iff the truth set of $A(x)$ is not the universe.
- iff the truth set of $\sim A(x)$ is nonempty.
- iff $(\exists x) \sim A(x)$ is true in U.

Proof. of $\sim (\exists x)A(x)$ is equivalent to $(\forall x) \sim A(x)$.

- Let U be any universe.
- The sentence $\sim (\exists x)A(x)$ is true in U
- iff $(\exists x)A(x)$ is false in U.
- iff the truth set of $A(x)$ is the universe.
- iff the truth set of $\sim A(x)$ is empty.
- iff $(\forall x) \sim A(x)$ is true in U.

$\exists!$

Definition

For an open sentence $P(x)$, the proposition $(\exists! x)P(x)$ is read " **there exists a unique** x **such that** $P(x)$", or "**for some** x**,** $P(x)$" and is true iff the truth set of $P(x)$ has *exactly one element*. The symbol $\exists!$ is called the **unique existential qualifier**.

Key points: Truth set of $(\exists x)P(x)$ has at least one element, while the truth set of $(\exists! x)P(x)$ has exactly one element.

Theorem

If $A(x)$ is an open sentence with variable x, then

1. $(\exists! x)A(x) \Rightarrow (\exists x)A(x)$.
2. $(\exists! x)A(x)$ *is equivalent to* $(\exists x)A(x) \wedge (\forall y)(\forall z)A(y) \wedge A(z) \Rightarrow y = z$.

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. **Proof Methods I**
10. Proof Methods II
11. Homework #2

Proof Methods I

A **theorem** is a sentence involving mathematical objects and constructions.Typically one seeks to ascertain that it is a **proposition**. A **proof** is the justification of its truth value.

Theorem

Suppose $a, b,$ and c are integers. If a divides b and a divides c, then a divides $b - c$.

Proof.

1. First we parse the keywords integers and *divides* for their meanings [these are assumptions]
2. Then $b = am$ and $c = an$.
3. Thus, $b - c = am - an = a(m - n)$.
4. Since $m - n$ is an integer, a divides $b - c$.

Rewording

The **universe of discourse** is $\mathbb{N}$: the natural numbers.
Consider the sentence $P(x, y)$: " $\exists z$ such that $y = xz$"

Theorem

$P(a, b) \wedge P(a, c) \Rightarrow P(a, b - c)$.

Another way:

Theorem

If a, b and c are integers, then

$$(a|b) \wedge (a|c) \Rightarrow a|(b - c).$$

Theorem

If a, b and c are integers, then

$$a|b \wedge a|c \Rightarrow a|(b - c).$$

Proof of a Conditional Proposition

DIRECT PROOF OF $P \Rightarrow Q$

Proof.

Assume P.

$\vdots$

Therefore, Q.

Thus, $P \Rightarrow Q$.

1. Determine precisely the hypotheses (if any) and the antecedent and consequent.
2. Replace (if necessary) the antecedent with a more usable equivalent.
3. Replace (if necessary) the consequent by something equivalent or more readily shown.
4. Develop a chain of statements, each deducible from its predecessors or other known results, that leads from the antecedent to the consequent.

Example

Theorem

If $x < -4$ and $y > 2$, then the distance from (x, y) to $(1, -2)$ is at least 6.

Proof. Assume that $x < -4$ and $y > 2$. Then $x - 1 < -5$, so $(x-1)^2 > 25$. Also $y + 2 > 4$, so $(y+2)^2 > 16$. Therefore

$$\sqrt{(x-1)^2 + (y+2)^2} > \sqrt{25 + 16} > \sqrt{36},$$

so the distance from (x, y) to $(1, -2)$ is at least 6. □

Proposition

If x, y are positive real numbers then

$$\frac{x+y}{2} \geq \sqrt{xy}.$$

Proof. We work backward, start with the consequent, decide what statement could be used to prove, another statement that could be used to prove that one, and so forth. Continue until you reach the hypothesis, the antecedent, or a known fact.

1. Squaring the consequent,

$$(\frac{x+y}{2})^2 = \frac{x^2+y^2+2xy}{4} \geq xy.$$

2. Thus, $(x^2+y^2) \geq 2xy$.
3. Hence, $x^2+y^2-2xy \geq 0$.
4. Therefore, $(x-y)^2 \geq 0$.
5. A direct proof is obtained by reversing the steps.

Example

Theorem

If n is a natural number then $n^2 + n + 3$ is odd.

Proof. $P(n)$ "n is a natural number" can be seen as

$$P(n) = Q(n) \vee R(n),$$

with $Q(n)$ "n is even" and $R(n)$: "n is odd".
We will make use of the tautology

$$[(P \vee Q) \Rightarrow R] \Leftrightarrow [(P \Rightarrow R) \vee (Q \Rightarrow R)].$$

Case 1: If n is even, $n = 2m$ and therefore

$$n^2 + n + 3 = (2m)^2 + 2m + 3 = 4m^2 + 2m + 2 + 1 = 2(2m^2 + m + 1) + 1,$$

an odd integer.

Case 2: If n is odd, $n = 2m + 1$ and therefore

$$\begin{aligned} n^2 + n + 3 &= (2m+1)^2 + (2m+1) + 3 \\ &= (4m^2 + 4m + 1) + (2m+1) + 3 \\ &= 2(2m^2 + 3m) + 1 + 1 + 3 \\ &= 2(2m^2 + 3m + 2) + 1, \end{aligned}$$

which is also an odd integer. □

Theorem

$\forall n \in \mathbb{N}$, $n^2 + n + 3$ *is an odd integer.*

Proof. (Direct) Write

$$n^2 + n + 3 = n(n+1) + 3.$$

In the product $n(n+1)$ one of the factors is even, so the product is even.
Thus $n(n+1) + 3$ is a sum of an even integer and an odd integer, therefore it is odd. □

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. **Proof Methods II**
11. Homework #2

More Proof Techniques

PROOF BY CONTRAPOSITION OF $P \Rightarrow Q$

Proof.

Assume $\sim Q$.

$\vdots$

Therefore, $\sim P$.

Thus, $\sim Q \Rightarrow \sim P$.

Thus, $P \Rightarrow Q$.

This is helpful when we have more direct access to the denials of P and Q.

Examples

Proposition

Let m be an integer. If m^2 is odd, then m is odd.

P means "m^2 is odd", and Q means "m is odd."

Proof.

1. Let m be an integer. Suppose m is not odd. (Suppose $\sim Q$, where Q is "m is odd.")
2. Then $m = 2k$ for some integer k.
3. Then $m^2 = (2k)^2 = 2(2k^2)$ is even.
4. Thus m^2 is not odd. (We have proved $\sim P$.)
5. Therefore if m is not odd, then m^2 is not odd.
6. By contraposition, if m^2 is odd, then m is odd.

Proof by Contradiction

PROOF OF P BY CONTRADICTION

Proof.

Suppose $\sim P$.

$\vdots$

Therefore, Q.

$\vdots$

Therefore, $\sim Q$.

Hence, $Q \wedge \sim Q$, a contradiction.

Thus, P.

If a statement cannot be false, then it must be true.

Example

Proposition

(P) The graphs of $y = x^2 + x + 2$ and $y = x - 2$ do not intersect.

Proof.

1. $(\sim P)$: Suppose the graphs do intersect at some point (a, b).
2. Thus $b = a - 2$ and $b = a^2 + a + 2$.
3. Therefore, $b = (a - 2) = a^2 + a + 2$.
4. Therefore, $a^2 + 4 = 0$,
5. Hence, $a^2 = -4$. But a is a real number so $a^2 \geq 0$.
6. This is a contradiction. ($(a^2 < 0 \wedge a^2 > 0$ is a contradiction).
7. Therefore, the graphs do not intersect.

Two Beautiful Examples

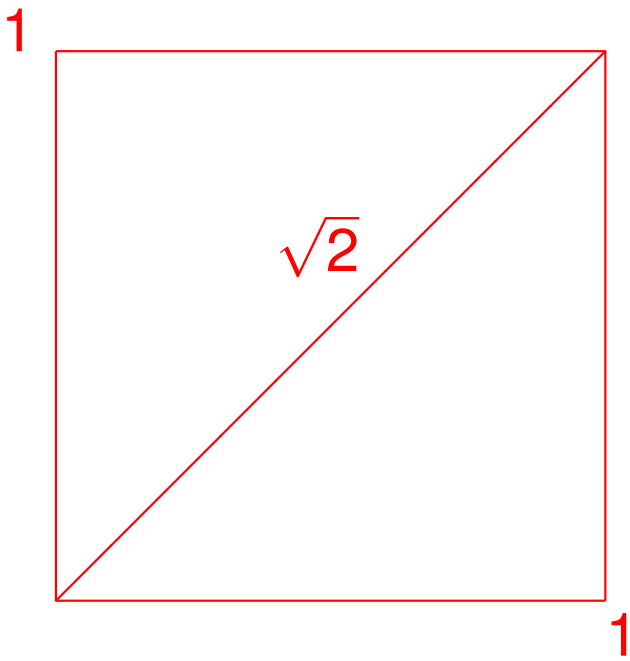
Theorem

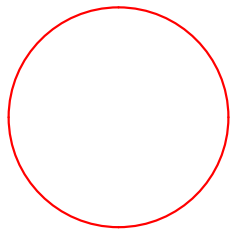
$\sqrt{2}$ is an irrational number.

1. P : **irrational** means "not a fraction", that is $\sqrt{2} \neq s/t$, for any choices of the integers s, t, $t \neq 0$.
2. Assume $\sim P$: $\sqrt{2} = s/t$, $s, t \in \mathbb{N}$.
3. We may assume that s and t have no common factor, since $s = as'$ and $t = at'$ gives $s/t = s'/t'$. (Q: "s, t have no common factor)
4. Thus $2 = s^2/t^2$, $2t^2 = s^2$.
5. Since s^2 is even, s must be even since a square of an odd integer is odd (previous proposition!)
6. Thus, $s = 2p$ and therefore $2t^2 = s^2 = 4p^2$.
7. Hence, $t^2 = 2p^2$.
8. Therefore, t is even, $t = 2q$ for some integer.
9. Hence t and s have a common factor (which is a contradiction).

Irrationality of $\sqrt{2}$

The arrival of new numbers:





The construction of an irrational number

Example

Theorem

$\sqrt{2} \notin \mathbb{Q}$.

Proof.

- We are going to argue by contradiction: Suppose

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

- We may assume that m and n have no common factor.
- Squaring both sides of the equality, we obtain $m^2 = 2n^2$
- This implies that m is even, as the square of an odd number, say $m = 2p + 1$, is odd

$$(2p + 1)^2 = 4p^2 + 4p + 1 = 4(p^2 + p) + 1$$

- We may then assume that m is even. In $m^2 = 2n^2$, set $m = 2p$ to get

$$4p^2 = 2n^2$$

  and therefore
- $n^2 = 2p^2$, which implies that n is also even.
- This contradicts our assumption that m and n have no common factors. □

This will also work with $\sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{8}$ and many other cases. Obviously, these **numbers** need a **home**.

Euclid's Theorem

Theorem (Euclid)

The set of primes is infinite.

Proof.

1. We assume $\sim P$, that the set of primes is finite, that is made up of $\{p_1, p_2, \ldots, p_k\}$.
2. Let $n = p_1 \cdot p_2 \cdots p_k + 1$.
3. If n is prime, we have a contradiction already since n is different from all p_i.
4. If n is not prime, then it must be divisible by some prime p.
5. Thus, p divides n and the product $p_1 \cdot p_2 \cdots p_k$ (being one of the p_i).
6. Therefore p divides the difference which is 1.
7. Hence p is not prime.
8. Therefore, the set of primes is infinite.

TWO-PART PROOF OF $P \Leftrightarrow Q$

Proof.

Show $P \Rightarrow Q$ by any method.

Show $Q \Rightarrow P$ by any method.

Therefore, $P \Leftrightarrow Q$.

Example: Multiple Proofs

Proposition

$$(x \text{ is odd} \wedge y \text{ is odd}) \Rightarrow xy \text{ is odd}.$$

Direct Proof: Assume x and y are odd. Then there are integers m, n such that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1.$$

Thus, xy is an odd integer. □

Proof by Contraposition: The contraposite of the sentence is

$$(xy \text{ is even}) \Rightarrow \sim [x \text{ is odd} \wedge y \text{ is odd}] = [y \text{ is even}) \vee x \text{ is even}].$$

Assume xy is even.Then 2 divides xy.Since 2 is prime, it divides x or y. Therefore either x or y is even. Thus, if $x \vee y$ are odd, then xy is odd.

Proof by Contradiction: Suppose x and y are odd and xy is even. (This is $\sim P$.) Then there are integers m, n such that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1.$$

Thus xy is the next integer to the even integer $2(mn + m + n)$. Thus xy is odd.

Proofs involving Quantifiers

Existence Propositions are statements of the form

$$\boxed{\exists x P(x)}$$

A constructive proof we name the object that makes $P(a)$ true, which directly shows that the truth set of $P(x)$ is nonempty.

- Prove that $(\exists x)(x$ is prime and even): **Proof.** 2 is both prime and even.
- Prove that exists a natural number whose fourth power is the sum of three other (nonzero) fourth powers: **Proof.**

$$20615673^4 = 2682440^4 + 15365639^4 + 18796760^4.$$

PROOF OF $(\exists x)P(x)$ BY CONTRADICTION

Proof.

Suppose $\sim (\exists x)P(x)$.

Then $(\forall x) \sim P(x)$

$\vdots$

Therefore, $\sim Q \wedge Q$, a contradiction

Thus, $(\forall x) \sim P(x)$ is false

Therefore, $(\exists x)P(x)$ is true.

Euclid's Algorithm

Definition

Let a, b and c be positive integers.

1. c is a **common divisor** of a and b iff c divides both a and b.
2. If d is a common divisor of a and b and every common divisor c of a and b is less than or equal to d, then we say that d is the **greatest common divisor** of a and b. We write $d = \gcd(a, b)$.

Example: The common divisors of 18 and 45 are: $1, 3, 9$. Thus $\gcd(18, 45) = 9$.

Question: What are the properties of the *function* gcd? They are based on a remarkable method to determine $\gcd(a, b)$.

Lemmata

Proposition (Long Division Algorithm)

If a and b are natural numbers and $a \geq b$, then there exists a natural number q (the quotient) and a nonnegative integer r (the remainder), such that

$$a = bq + r,$$

where $0 \leq r < b$.

Note: We will borrow a proof from the past [middle school], or from the future [Chapter 2]. Practice with one example!

Lemma

Let a, b and c be integers. If c divides a and c divides b, then c divides any combination $an + bm$, where n and m are integers.

Proof. Let n and m be integers. Suppose that c divides a and c divides b. Then there are integers h and k such that $a = ch$ and $b = ck$. Then

$$an + bm = chn + ckm = c(hn + km).$$

Thus c divides $an + bm$. □

Lemma (The heart of the proof)

Let a and b be natural numbers and $a \geq b$. Suppose $a = bq + r$, where $0 \leq r < b$.

1. *If $r = 0$, then $\gcd(a, b) = b$.*
2. *If $r \neq 0$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. (1) is clear since b divides a.
(2) Since a can be written as $a = bq + r$, by the previous lemma, any divisor c of b and r will divide the combination $bq + r$. Thus, $\gcd(b, r) \leq \gcd(a, b)$.
Conversely, the equation $a = bq + r$ can also be written as $r = a - bq$. Thus every divisor d of a and b, will also divide r. Thus $\gcd(a, b) \leq \gcd(b, r)$.

Euclid's Algorithm

Theorem (Euclid)

Let a and b be two positive integers with $a \geq b$. Let $d = \gcd(a, b)$. Then there two lists of positive integers q_i and r_i such that

$$
\begin{aligned}
b &> r_1 > r_2 > r_3 > \cdots > r_{k-1} > r_k > r_{k+1} = 0 \\
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k \\
r_{k-1} &= r_k q_{k+1}
\end{aligned}
$$

and $r_k = \gcd(a, b)$.

Corollary

The GCD of a and b may be written as a combination of a and b; that is,

$$d = \gcd(a, b) = ax + by,$$

for some integers x and y.

Proof. To show that $d = ax + by$, we start with the equation $r_{k-2} = r_{k-1}q_k + r_k$, where $d = r_k$.

$$d = r_{k-2} - r_{k-1}q_k.$$

Now we use the previous equation, $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$, to write

$$\begin{aligned} d &= r_{k-2} - r_{k-1}q_k = r_{k-2} - (r_{k-3} - r_{k-2}q_k - 1)q_k \\ &= r_{k-2}(1 + q_{k-1}q_k) + r_{k-3}(-q_k). \end{aligned}$$

Continuing is this manner, d may eventually be written as a combination $ax + by$.

Example

Find $\gcd(44, 144)$, and write it as a combination of 144 and 44.

$$\begin{aligned} 144 &= 44(2) + 16 \\ 44 &= 16(2) + 12 \\ 16 &= 12(1) + 4 \\ 12 &= 4(3) \end{aligned}$$

$4 = \gcd(144, 44)$.

$$\begin{aligned} 4 &= 16 - 12 \\ &= 16 - (44 - 16(2)) = 16(3) - 44 \\ &= (144 - 44(2))(3) - 44 \\ &= 144(3) + 44(-7). \end{aligned}$$

Example

Theorem

The only triple a, b, c of consecutive odd prime numbers is $3, 5, 7$.

Proof.

1. We begin by writing the assumption in a convenient form: $a = x$, $b = x + 2$, and $c = x + 4$. We must prove that $x = 3$.
2. We are going to use the remainders of these numbers mod 3: We are going to write all the possible remainders.

a	b	c
0	2	1
1	0	2
2	1	0

3. The table shows that in each possible case, one of a, b or c is divisible by 3.

Outline

1. General Orientation
2. Numbers
3. Last Class...
4. Conditionals and Biconditionals
5. Quantifiers
6. Homework #1
7. Last Class...
8. Quantified Sentences
9. Proof Methods I
10. Proof Methods II
11. **Homework #2**

Homework #2

1. Section 1.3: 1 (a,c,j), 5 (a,b,i), 6 (b,d,g), 8 (d), 11
2. Section 1.4: 2, 8, 9(e), 11