# Fundamental Concepts of Mathematics 

## George Voutsadakis ${ }^{1}$

${ }^{1}$ Mathematics and Computer Science

Lake Superior State University

## LSSU Math 215

## (1) Definitions and Proofs

- Definition
- Theorem
- Proof
- Counterexample
- Boolean Algebra


## Subsection 1

## Definition

## Divisibility

- The set of integers is $\mathbb{Z}=\{\ldots,-3,-2,-1,0,1,2,3, \ldots\}$;


## Definition (Divisibility)

Let $a$ and $b$ be integers. We say that $a$ is divisible by $b$ provided there is an integer $c$ such that $b c=a$. We also say $b$ divides $a$, or $b$ is a factor of $a$, or $b$ is a divisor of $a$. The notation for this is $b \mid a$.

- Example: Is 12 divisible by 4 ? The definition says that $a=12$ is divisible by $b=4$ if we can find an integer $c$ so that $4 c=12$. There is such an integer, namely, $c=3$. Thus, 4 divides 12 or, equivalently, 4 is a factor or a divisor of 12 .
- Example: 12 is not divisible by 5 because there is no integer $x$ for which $5 x=12$.


## Even and Odd Integers

## Definition (Even)

An integer is called even provided it is divisible by two.

- Example: The number 12 is even because $2 \mid 12$, since $2 \cdot 6=12$. On the other hand, 13 is not even, because 13 is not divisible by 2 ; there is no integer $x$ for which $2 x=13$.


## Definition (Odd)

An integer $a$ is called odd provided there is an integer $x$ such that $a=2 x+1$.

- Example: 13 is odd because we can choose $x=6$ in the definition to give $13=2 \cdot 6+1$.


## Prime and Composite Integers

## Definition (Prime)

An integer $p$ is called prime provided that $p>1$ and the only positive divisors of $p$ are 1 and $p$.

- Example: 11 is prime because it satisfies both conditions in the definition: First, $11>1$, and second, the only positive divisors of 11 are 1 and 11 . Is 1 a prime? No, because $1 \ngtr 1$ !


## Definition (Composite)

A positive integer $a$ is called composite provided there is an integer $b$ such that $1<b<a$ and $b \mid a$.

- Example: The number 25 is composite because it satisfies the condition of the definition: There is a number $b$ with $1<b<25$ and $b \mid 25$; indeed, $b=5$ is the only such number.
Similarly, the number 360 is composite. In this case, there are several numbers $b$ that satisfy $1<b<360$ and $b \mid 360$.


## Subsection 2

## Theorem

## Statements and Theorems

- There are several kinds of statements:
- Questions, e.g., "Where is the newspaper?"
- Commands, e.g., "Come to a complete stop!"
- Declarative statements, a sentence that expresses an idea about how something is, such as: "It's going to rain tomorrow" or "The Yankees won last night".
- A theorem is a declarative statement about mathematics for which there is a proof.
- Mathematical statements fall into four categories:
- Statements we know to be true because we can prove them - we call these theorems.
- Statements whose truth we cannot ascertain - we call these conjectures.
- Statements that are false - we call these mistakes!
- Statements that do not make sense - we call these nonsense!

An example is "The square root of a triangle is a circle."

## If-then Statements

- In the statement "If $A$, then $B$," we might have condition $A$ true or false, and we might have condition $B$ true or false.
- If the statement "If $A$, then $B$ " is true, all that is promised is that whenever $A$ is true, $B$ must be true as well.
- If $A$ is not true, then no claim about $B$ is asserted by "If $A$, then $B$."
- There is an assortment of alternative ways to express "If $A$, then $B$.":
- " $A$ implies $B$." and, also, " $B$ is implied by $A$."
- "Whenever $A$, we have $B$." and, also, " $B$, whenever $A$."
- " $A$ is sufficient for $B$."
- "In order for $B$ to hold, it is enough that we have $A$."
- " $B$ is necessary for $A$."
- "A, only if $B$."
- " $A \Rightarrow B$."
- " $B \Leftarrow A$."


## If-then Statements: The Truth Table

- Since in the statement "If $A$, then $B$ ", we only want to ensure that $B$ is true whenever $A$ is true and we do not really care about the case when $A$ is false, we assign to "If $A$, then $B$ " the following truth table:

| $A$ | $B$ | $A \Rightarrow B$ |
| :---: | :---: | :---: |
| true | true | true |
| true | false | false |
| false | true | true |
| false | false | true |

## Vacuous Truth

- Consider an "if-then" statement in which the hypothesis is impossible:


## Vacuous Statement

If an integer is both a perfect square and prime, then it is negative.

- Is this statement true or false? We might be tempted to say that the statement is false because square numbers and prime numbers cannot be negative.
- However, a statement of the form "If $A$, then $B$ " is declared false only in the case when $A$ is true and $B$ is false.
- In the given statement, condition $A$ is impossible; there are no numbers that are both a perfect square and prime. So we cannot find an integer that renders condition $A$ true and condition $B$ false. Therefore, the statement is true!
- Statements of the form "If $A$, then $B$ " in which condition $A$ is impossible are called vacuous, and such statements are true because they have no exceptions (i.e., $A$ is false).


## And Statements

- The statement " $A$ and $B$ " means that both $A$ and $B$ are true.
- Example: "Every integer whose ones digit is 0 is divisible by 2 and is divisible by 5 ." This means that a number that ends in a zero, such as 230 , is divisible both by 2 and by 5 .
- For " $A$ and $B$ ", the following truth table applies:

| $A$ | $B$ | $A$ and $B$ |
| :---: | :---: | :---: |
| true | true | true |
| true | false | false |
| false | true | false |
| false | false | false |

## If-and-only-if Statements

- "If $A$ then $B$, and if $B$ then $A$ " is written as " $A$ if and only if $B$."
- Because both " $A$ implies $B$ " and " $B$ implies $A$ " have to be true for " $A$ if and only if $B$ " to be true, the following truth table applies:

| $A$ | $B$ | $A \Rightarrow B$ | $B \Rightarrow A$ | $A$ if and only if $B$ |
| :---: | :---: | :---: | :---: | :---: |
| true | true | true | true | true |
| true | false | false | true | false |
| false | true | true | false | false |
| false | false | true | true | true |

- There is also an assortment of alternative ways to express " $A$ if and only if $B$.":
- " $A$ iff $B$."
- " $A$ is necessary and sufficient for $B$."
- " $A$ is equivalent to $B$."
- " $A \Leftrightarrow B$."


## Example: Proving an If-and-Only-If Statement

- Prove that an integer $x$ is even if and only if $x+1$ is odd.

We must show that "if $x$ is even, then $x+1$ is odd" and "if $x+1$ is odd, then $x$ is even;
We show, first, that "if $x$ is even, then $x+1$ is odd":

- $x$ is even; (hypothesis)
- there exists an integer $c$, such that $2 c=x$; (by the definition)
- $2 c+1=x+1$; (by adding 1 to both sides)
- $x+1$ is odd; (by the definition)

We show, next, that "if $x+1$ is odd, then $x$ is even":

- $x+1$ is odd; (hypothesis)
- there exists an integer $c$, such that $2 c+1=x+1$; (by the definition)
- $2 c=x$; (by subtracting 1 from both sides)
- $x$ is even; (by the definition)


## Not Statements

- The statement "not $A$ " is true if and only if $A$ is false.
- Example: The statement "All primes are odd" is false. Thus, the statement "Not all primes are odd" is true.
- For "not $A$ ", the following truth table applies:

| $A$ | not $A$ |
| :---: | :---: |
| true | false |
| false | true |

## Or Statements

- The statement " $A$ or $B$ " means that $A$ is true, or $B$ is true, or both $A$ and $B$ are true.
- Example: Consider the statement: "Suppose $x$ and $y$ are integers with the property that $x \mid y$ and $y \mid x$. Then $x=y$ or $x=-y$." The conclusion says that we may have any one of the following:
- $x=y$ but not $x=-y$ (e.g., take $x=3$ and $y=3$ ).
- $x=-y$ but not $x=y$ (e.g., take $x=-5$ and $y=5$ ).
- $x=y$ and $x=-y$, which is possible only when $x=0$ and $y=0$.
- For " $A$ or $B$ ", the following truth table applies:

| $A$ | $B$ | $A$ or $B$ |
| :---: | :---: | :---: |
| true | true | true |
| true | false | true |
| false | true | true |
| false | false | false |

## Alternative Names for Theorems

- Often, alternative names are used in place of theorem.
- The word theorem carries the connotation of importance and generality.
- Result: A modest, generic word for a theorem. Both important and unimportant theorems can be called results.
- Fact: A very minor theorem. The statement " $6+3=9$ " is a fact.
- Proposition: A minor theorem. A proposition is more important or more general than a fact but not as prestigious as a theorem.
- Lemma: A theorem whose main purpose is to help prove another, more important theorem. Some theorems have complicated proofs that can be broken down into smaller parts. The lemmas are the parts used to build the more complicated proof.
- Corollary: A result with a short proof whose main step involves the use of another, previously proved theorem.
- Claim: Similar to lemma. A claim is a theorem whose statement usually appears inside the proof of a theorem to help organize key steps in a proof. Often, the statement of a claim involves terms that make sense only in the context of the proof.


## Subsection 3

## Proof

## Direct Proof of an If-then Statement

## Proposition

The sum of two even integers is even.
(1) We show that if $x$ and $y$ are even integers, then $x+y$ is an even integer.
(2) Let $x$ and $y$ be even integers.
(3) Since $x$ is even, $x$ is divisible by 2 .
(1) Likewise, since $y$ is even, $2 \mid y$.
(3) Since $2 \mid x$, there is an integer a such that $x=2$ a.
(0) Likewise, since $2 \mid y$, there is an integer $b$ such that $y=2 b$.
( Now $x+y=2 a+2 b=2(a+b)$.
(3) Therefore, there is an integer $c=a+b$ such that $x+y=2 c$.
(- Thus, $2 \mid(x+y)$.
(0) Therefore, $x+y$ is even.

## Another Direct Proof of an If-then Statement

## Proposition

Let $a, b$ and $c$ be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.
(1) Suppose $a, b$ and $c$ are integers with $a \mid b$ and $b \mid c$.
(2) Since $a \mid b$, there is an integer $x$ such that $b=a x$.
(3) Likewise, there is an integer $y$ such that $c=b y$.
( ( Then for $z=x y$,

$$
a z=a(x y)=(a x) y=b y=c
$$

(3) Thus, there is an integer $z=x y$, such that $c=a z$.
(0) Therefore, $a \mid c$.

## A Third Direct Proof of an If-then Statement

## Proposition

Let $x$ be an integer. If $x>1$, then $x^{3}+1$ is composite.
(1) Let $x$ be an integer and suppose $x>1$.
(2) We have $x^{3}+1=(x+1)\left(x^{2}-x+1\right)$.
© Since $x$ is an integer, both $x+1$ and $x^{2}-x+1$ are integers.
Therefore $(x+1) \mid\left(x^{3}+1\right)$.
(1) Since $x>1$, we have $x+1>1+1=2>1$.
(0) Also $x>1$ implies $x^{2}>x$, and since $x>1$, we have $x^{2}>1$. Multiplying both sides by $x$ again yields $x^{3}>x$. Adding 1 to both sides gives $x^{3}+1>x+1$.
(2) Thus $x+1$ is an integer with $1<x+1<x^{3}+1$.
(1) Since $x+1$ is a divisor of $x^{3}+1$ and $1<x+1<x^{3}+1$, we have that $x^{3}+1$ is composite.

## Direct Proof of an If-and-only-if Statement

## Proposition

Let $x$ be an integer. Then $x$ is odd if and only if $x+1$ is even.
(1) Let $x$ be an integer.
(2) First, show that if $x$ is odd, then $x+1$ is even.

- Suppose $x$ is odd.
- This means that there exists an integer $a$, such that $x=2 a+1$.
- Adding 1 to both sides, we get $x+1=2 a+2=2(a+1)$.
- Since $a+1$ is an integer, $2 \mid x+1$.
- Therefore, $x+1$ is even.
(3) Next, show that, if $x+1$ is even, then $x$ is odd.
- Suppose $x+1$ is even.
- Thus, $2 \mid(x+1)$.
- Hence, there is an integer $b$ such that $x+1=2 b$.
- Subtracting 1 from both sides gives $x=2 b-1=2(b-1)+1$.
- Since $b-1$ is an integer, this shows that $x$ is odd.


## Proving a Proposition Directly

## Proposition

Let $a, b, c$ and $d$ be integers. If $a|b, b| c$, and $c \mid d$, then $a \mid d$.
(1) Let $a, b, c$ and $d$ be integers with $a|b, b| c$, and $c \mid d$.
(2) Since $a \mid b$, there is an integer $x$ such that $a x=b$.
(3) Since $b \mid c$, there is an integer $y$ such that $b y=c$.
( - Since $c \mid d$, there is an integer $z$ such that $c z=d$.
(3) Now we get

$$
a(x y z)=(a x)(y z)=b(y z)=(b y) z=c z=d .
$$

(0) Thus, there is an integer $w=x y z$ such that $a w=d$.
( Therefore, $a \mid d$.

## Proving the same Proposition Using a Lemma

- Recall that we proved:


## Lemma

Let $a, b$ and $c$ be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

- Suppose, next, that we would like to prove the


## Proposition

Let $a, b, c$ and $d$ be integers. If $a|b, b| c$, and $c \mid d$, then $a \mid d$.
(1) Let $a, b, c$ and $d$ be integers with $a|b, b| c$, and $c \mid d$.
(2) Since $a \mid b$ and $b \mid c$, by the Lemma we have $a \mid c$.
(3) Now, since $a \mid c$ and $c \mid d$, again by the Lemma we have $a \mid d$.

## Proving an Easy Equality

## Proposition

Let $x$ be a real number. Then $x+x=2 x$.

$$
\begin{aligned}
x+x & =1 \cdot x+1 \cdot x \quad(1 \text { is identity of multiplication }) \\
& =(1+1) x \quad(\text { distributivity }) \\
& =2 x ; \quad(1+1=2)
\end{aligned}
$$

## Proving a More Complex Equality

## Proposition

Let $x$ and $y$ be real numbers. Then $(x-y)(x+y)=x^{2}-y^{2}$.

$$
\begin{aligned}
(x-y)(x+y) & =x(x+y)-y(x+y) \quad \text { (distributivity) } \\
& =x^{2}+x y-y x-y^{2} \quad \text { (distributivity) } \\
& =x^{2}+x y-x y-y^{2} \quad \text { (commutativity) } \\
& =x^{2}+1 x y-1 x y-y^{2} \quad \text { (identity of multiplication) } \\
& =x^{2}+(1-1) x y-y^{2} \quad \text { (distributivity) } \\
& =x^{2}+0 x y-y^{2} \quad(1-1=0) \\
& =x^{2}+0-y^{2} \quad(\text { absorption of } 0) \\
& =x^{2}-y^{2} \quad \text { (identity of addition) }
\end{aligned}
$$

## Proving an Inequality

## Proposition

If $x$ is a real number, with $x>2$, then $x^{2}>x+1$.
(1) We are given that $x>2$.
(2) Since $x$ is positive, multiplying both sides by $x$ gives $x^{2}>2 x$.
(3) So we have

$$
\begin{array}{rll}
x^{2} & >2 x \\
& =x+x & \\
& >x+2 \quad(\text { because } x>2) \\
& >x+1 \quad \text { (because } 2>1)
\end{array}
$$

(9) Therefore $x^{2}>x+1$.

## Subsection 4

## Counterexample

## Disproving by Providing a Counterexample

- We use proofs to show that a given statement is true.
- But not all statements about mathematics are true!
- Given a statement, how do we show that it is false?
- The typical way to disprove an if-then statement is to create a counterexample.
- A counterexample for the statement "If $A$, then $B$ " is an instance where $A$ is true but $B$ is false.
- Example: Consider the statement "If $x$ is a prime, then $x$ is odd." This statement is false. To prove that it is false, we just have to give an example of an integer that is prime but is not odd. The integer 2 has the requisite properties.


## Disproving a Statement

## A False Statement

Let $a$ and $b$ be integers. If $a \mid b$ and $b \mid a$, then $a=b$.

- Here is a counterexample:
- Take $a=5$ and $b=-5$.
- We have $5 \mid-5$ and $-5 \mid 5$.
- We also have $5 \neq-5$.
- So this is indeed a counterexample to the given if-then statement.


## Disproving Another Statement

## A False Statement

If $a$ and $b$ are nonnegative integers with $a \mid b$, then $a \leq b$.

- Here is a counterexample:
- Take $a=5$ and $b=0$.
- Since $5 \cdot 0=0$, we have that $5 \mid 0$.
- On the other hand, $5 \not \neq 0$.
- So this is indeed a counterexample to the given if-then statement.


## Disproving A Third Statement

## A False Statement

If $a, b$ and $c$ are positive integers with $a \mid(b c)$, then $a \mid b$ or $a \mid c$.

- Here is a counterexample:
- Take $a=6, b=2$ and $c=3$.
- We have that $6 \mid(2 \cdot 3)$.
- On the other hand, $6 \nmid 2$ and $6 \nmid 3$.
- So this is indeed a counterexample to the given if-then statement.


## Subsection 5

## Boolean Algebra

## Basics of Boolean Algbera

- Boolean algebra provides a framework for applying algebra to statements rather than to numbers.
- We begin with basic statements, such as "x is prime," and combine them using connectives such as if-then, and, or, not etc.
- Whereas in an ordinary algebraic expression, such as $3 x-4$, letters stand for numbers, and the operations are the familiar ones of addition, subtraction, multiplication etc., in Boolean algebra the letters (variables) stand for the values true $T$ and false $F$.
- There are several operations we can perform on the values $T$ and $F$, the most basic among which are and $(\wedge)$, or $(\vee)$, and not $(\neg)$.


## The Operation And $\wedge$

- The value of the expression $x \wedge y$ is $T$ when both $x$ and $y$ are $T$ and is $F$, otherwise.
- In truth table form:

| $x$ | $y$ | $x \wedge y$ |
| :---: | :---: | :---: |
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ |

## The Operation Or V

- The value of the expression $x \vee y$ is $T$ when at least one of $x$ and $y$ are $T$ and is $F$ only when both are $F$.
- In truth table form:

| $x$ | $y$ | $x \vee y$ |
| :---: | :---: | :---: |
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $F$ |

## The Operation Not $\neg$

- The value of the expression $\neg x$ is $T$ when $x$ is $F$ and is $F$ when $x$ is $T$.
- In truth table form:

| $x$ | $\neg x$ |
| :---: | :---: |
| $T$ | $F$ |
| $F$ | $T$ |

- Example: Calculate the value of $T \wedge(\neg F \vee F)$.

$$
\begin{aligned}
T \wedge(\neg F \vee F) & =T \wedge(T \vee F) \\
& =T \wedge T \\
& =T
\end{aligned}
$$

## Boolean Versus Ordinary Identities

- In algebra we learn how to manipulate formulas so we can derive identities such as $(x+y)^{2}=x^{2}+2 x y+y^{2}$.
- In Boolean algebra we are interested in deriving similar identities, such as $x \wedge y=y \wedge x$.
- The meaning of $(x+y)^{2}=x^{2}+2 x y+y^{2}$ being an identity is that, for any (numeric) values for $x$ and $y$, the two expressions $(x+y)^{2}$ and $x^{2}+2 x y+y^{2}$ must be equal.
- Similarly, the Boolean identity $x \wedge y=y \wedge x$ means that for all (truth) values for $x$ and $y$, the results $x \wedge y$ and $y \wedge x$ must be the same.
- Even though it would be ridiculous to try to prove $(x+y)^{2}=$ $x^{2}+2 x y+y^{2}$ by trying to substitute all possible values for $x$ and $y$ (there are infinitely many possibilities), it is not hard to try all the possibilities to prove a Boolean algebraic identity.
- In the case of $x \wedge y=y \wedge x$, there are only four possibilities, which can be easily summarized in the form of a truth table!


## Logical Equivalence

- Example: Show that $x \wedge y=y \wedge x$.

We use a truth table to show that for all assignments of truth values to $x$ and $y$, the expressions $x \wedge y$ and $y \wedge x$ are equal.

| $x$ | $y$ | $x \wedge y$ | $y \wedge x$ |
| :---: | :---: | :---: | :---: |
| $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $F$ |
| $F$ | $T$ | $F$ | $F$ |
| $F$ | $F$ | $F$ | $F$ |

- When two Boolean expressions, such as $x \wedge y$ and $y \wedge x$, are equal for all possible values of their variables, we call these expressions logically equivalent.


## Another Logical Equivalence

## Proposition

The Boolean expressions $\neg(x \wedge y)$ and $\neg x \vee \neg y$ are logically equivalent.

- We construct the truth table:

| $x$ | $y$ | $x \wedge y$ | $\neg(x \wedge y)$ | $\neg x$ | $\neg y$ | $\neg x \vee \neg y$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $T$ | $T$ | $T$ | $F$ | $F$ | $F$ | $F$ |
| $T$ | $F$ | $F$ | $T$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $F$ | $T$ | $T$ | $F$ | $T$ |
| $F$ | $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |

Since the columns for $\neg(x \wedge y)$ and $\neg x \vee \neg y$ are the same, the two expressions are logically equivalent!

## Summary of Some Logical Equivalences

## Theorem (Some Logical Equivalences)

- $x \wedge y=y \wedge x$ and $x \vee y=y \vee x$. (Commutative properties)
- $(x \wedge y) \wedge z=x \wedge(y \wedge z)$ and $(x \vee y) \vee z=x \vee(y \vee z)$. (Associative properties)
- $x \wedge T=x$ and $x \vee F=x$. (Identity elements)
- $\neg(\neg x)=x$. (Double Negation)
- $x \wedge x=x$ and $x \vee x=x$. (Idempotency)
- $x \wedge(y \vee z)=(x \wedge y) \vee(x \wedge z)$ and $x \vee(y \wedge z)=(x \vee y) \wedge(x \vee z)$.
(Distributive properties)
- $x \wedge(\neg x)=F$ and $x \vee(\neg x)=T$.
- $\neg(x \wedge y)=(\neg x) \vee(\neg y)$ and $\neg(x \vee y)=(\neg x) \wedge(\neg y)$.
(De Morgan's Laws)


## Some Additional Boolean Operations

- The operations $\wedge, \vee$ and $\neg$ were created to replicate the formal use of the words and, or, and not.
- We now introduce two more operations $\rightarrow$ and $\leftrightarrow$ designed to model statements of the form "If $A$, then $B$ " and " $A$ if and only if $B$ ", respectively.
- The simplest way to define these is through truth tables.

| $x$ | $y$ | $x \rightarrow y$ |
| :---: | :---: | :---: |
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ |


| $x$ | $y$ | $x \leftrightarrow y$ |
| :---: | :---: | :---: |
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $T$ |

## A Logical Equivalence Involving $\rightarrow$

## Proposition

The expressions $x \rightarrow y$ and $(\neg x) \vee y$ are logically equivalent.

| $x$ | $y$ | $x \rightarrow y$ | $\neg x$ | $y$ | $(\neg x) \vee y$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $T$ | $T$ | $T$ | $F$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| $F$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $F$ | $T$ |

