Specialized vocabulary
- Specialized vocabulary
- More world-building: divisibility
■ Specialized vocabulary
■ More world-building: divisibility
■ Then we prove stuff!!!
Theorems

Definition

A statement that is true and has been proved to be true can be a \textbf{theorem}, a \textbf{proposition}, a \textbf{lemma}, or a \textbf{corollary}. 

- \textbf{Theorem}: most significant.
- \textbf{Proposition}: slightly less significant, or perhaps quite basic.
- \textbf{Lemma}: only use is to prove a theorem or proposition.
- \textbf{Corollary}: follows directly from a theorem. (If you know a theorem, then its corollary should be extremely easy to prove.) Can also be significant.

- **Pythagorean Theorem**: If a right triangle has hypotenuse of length \(c\), and other sides of length \(a\) and \(b\) respectively, then \(a^2 + b^2 = c^2\).
- **Fundamental Theorem of Algebra**: If \(P(x)\) is a polynomial, with real coefficients, in the single variable \(x\), then \(P(x)\) can be factored into the product of linear and quadratic functions.
- **Fundamental Theorem of Calculus, Part 1**: If \(f\) is continuous on \([a, b]\), then the function \(g(x)\), defined by \(g(x) = \int_a^x f(t) \, dt\), with domain \(a \leq x \leq b\), is continuous on \([a, b]\), differentiable on \((a, b)\), and \(g'(x) = f(x)\).
Theorems

Definition

A statement that is true and has been proved to be true can be a theorem, a proposition, a lemma, or a corollary.

Theorem: most significant.
A statement that is true and has been proved to be true can be a theorem, a proposition, a lemma, or a corollary.

**Theorem:** most significant.

**Proposition:** slightly less significant, or perhaps quite basic.
A statement that is true and has been proved to be true can be a theorem, a proposition, a lemma, or a corollary.

Theorem: most significant.
Proposition: slightly less significant, or perhaps quite basic.
Lemma: only use is to prove a theorem or proposition.
Definition

A statement that is true and has been proved to be true can be a theorem, a proposition, a lemma, or a corollary.

Theorem: most significant.
Proposition: slightly less significant, or perhaps quite basic.
Lemma: only use is to prove a theorem or proposition.
Corollary: follows directly from a theorem. (If you know a theorem, then its corollary should be extremely easy to prove.) Can also be significant.
Theorems

Definition

A a statement that is true and has been proved to be true can be a theorem, a proposition, a lemma, or a corollary.

Theorem: most significant.

Proposition: slightly less significant, or perhaps quite basic.

Lemma: only use is to prove a theorem or proposition.

Corollary: follows directly from a theorem. (If you know a theorem, then its corollary should be extremely easy to prove.) Can also be significant.

Pythagorean Theorem: If a right triangle has hypotenuse of length $c$, and other sides of length $a$ and $b$ respectively, then $a^2 + b^2 = c^2$.

Fundamental Theorem of Algebra: If $P(x)$ is a polynomial, with real coefficients, in the single variable $x$, then $P(x)$ can be factored into the product of linear and quadratic functions.

Fundamental Theorem of Calculus, Part 1: If $f$ is continuous on $[a, b]$, then the function $g(x)$, defined by $g(x) = \int_a^x f(t)dt$, with domain $a \leq x \leq b$, is continuous on $[a, b]$, differentiable on $(a, b)$, and $g'(x) = f(x)$.

Theorem: There are infinitely many prime numbers.
Statements that Aren’t Theorems

A conjecture is a statement that someone thinks is true, but that has not been proven to be true or false.
A conjecture is a statement that someone thinks is true, but that has not been proven to be true or false.

**Goldbach Conjecture:** Every even integer greater than 2 can be written as the sum of two primes.
A conjecture is a statement that someone thinks is true, but that has not been proven to be true or false.

**Goldbach Conjecture:** Every even integer greater than 2 can be written as the sum of two primes.

**Conjecture:** $P \neq NP$
A conjecture is a statement that someone thinks is true, but that has not been proven to be true or false.

**Goldbach Conjecture:** Every even integer greater than 2 can be written as the sum of two primes.

**Conjecture:** $P \neq NP$

**Conjecture:** $P = NP$
A conjecture is a statement that someone thinks is true, but that has not been proven to be true or false.

**Goldbach Conjecture:** Every even integer greater than 2 can be written as the sum of two primes.

**Conjecture:** $P \neq NP$

**Conjecture:** $P = NP$

**Collatz Conjecture:** Given any positive integer $n$, the series of operations:

- if $n$ is even, replace it with $\frac{n}{2}$
- if $n$ is odd, replace it with $3n + 1$

will eventually result in $n = 1$. 
A **definition** is an unambiguous explanation of the meaning of a mathematical word or phrase.
Definitions

A definition is an unambiguous explanation of the meaning of a mathematical word or phrase.

A definition isn’t true or false: it’s simply agreed on.
A **definition** is an unambiguous explanation of the meaning of a mathematical word or phrase.

A definition isn’t true or false: it’s simply agreed on.

**Definition:** Let $\mathbb{N}$ be the set of natural numbers, $\{1, 2, 3, \ldots\}$
A **definition** is an unambiguous explanation of the meaning of a mathematical word or phrase.

A definition isn’t true or false: it’s simply agreed on.

**Definition:** Let $\mathbb{N}$ be the set of natural numbers, \{1, 2, 3, \ldots\}

**Definition:** Let $a$ be the largest element in the set \{a_1, a_2, a_3\}. 

**Definition:** Let $\mathbb{N}$ be the set of natural numbers, \{1, 2, 3, \ldots\}
Definition

A **definition** is an unambiguous explanation of the meaning of a mathematical word or phrase.

A definition isn’t true or false: it’s simply agreed on.

**Definition:** Let \( \mathbb{N} \) be the set of natural numbers, \( \{1, 2, 3, \ldots\} \)

**Definition:** Let \( a \) be the largest element in the set \( \{a_1, a_2, a_3\} \).

**Definition:** A set is a collection of objects.

**Bad definition:** Is the set of all sets a set?
Parity

Definition

An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.
Parity

Definition

An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

True or False: 0 is both odd and even.
Parity

Definition

An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

True or False: 0 is both odd and even.

**False.** There is no integer $a$ so that $0 = 2a + 1$, so 0 is not odd.
Parity

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>An integer $n$ is <strong>even</strong> if $n = 2a$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
<tr>
<td>An integer $n$ is <strong>odd</strong> if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
</tbody>
</table>

True or False: 0 is both odd and even.
False. There is no integer $a$ so that $0 = 2a + 1$, so 0 is not odd.

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two integers have the <strong>same parity</strong> if they are both even or both odd. If one integer is even and another integer is odd, they have <strong>opposite parity</strong>.</td>
</tr>
</tbody>
</table>
Parity

### Definition

An integer \( n \) is **even** if \( n = 2a \) for some integer \( a \in \mathbb{Z} \).

An integer \( n \) is **odd** if \( n = 2a + 1 \) for some integer \( a \in \mathbb{Z} \).

True or False: 0 is both odd and even.

False. There is no integer \( a \) so that \( 0 = 2a + 1 \), so 0 is not odd.

### Definition

Two integers have the **same parity** if they are both even or both odd. If one integer is even and another integer is odd, they have **opposite parity**.

Show that the sum of two numbers of opposite parity is odd.
Parity

Definition

An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

True or False: 0 is both odd and even.
False. There is no integer $a$ so that $0 = 2a + 1$, so 0 is not odd.

Definition

Two integers have the **same parity** if they are both even or both odd.
If one integer is even and another integer is odd, they have **opposite parity**.

Show that the sum of two numbers of opposite parity is odd.
Let $n$ be an even number and $m$ be an odd number.
By the definitions of even and odd, there exist integers $a$ and $b$ such that $n = 2a$ and $m = 2b + 1$.
Then $n + m = (2a) + (2b + 1) = 2(a + b) + 1$.
Since $a + b$ is an integer, by the definition of odd, $n + m$ is odd.
A Note on Definitions

We use a special convention with definitions.

We use a special convention with definitions.
A Note on Definitions

We use a special convention with definitions.

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>An integer $n$ is <strong>even</strong> if $n = 2a$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
<tr>
<td>An integer $n$ is <strong>odd</strong> if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
</tbody>
</table>
A Note on Definitions

We use a special convention with definitions.

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>An integer $n$ is <strong>even</strong> if $n = 2a$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
<tr>
<td>An integer $n$ is <strong>odd</strong> if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.</td>
</tr>
</tbody>
</table>

Written:

$n = 2a \implies n$ even
We use a special convention with definitions.

**Definition**

An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

**Written:**

$n = 2a \implies n$ even

**Intended Meaning:**

$n = 2a \iff n$ even
A Note on Definitions

We use a special convention with definitions.

**Definition**

An integer \( n \) is **even** if and only if \( n = 2a \) for some integer \( a \in \mathbb{Z} \).

An integer \( n \) is **odd** if and only if \( n = 2a + 1 \) for some integer \( a \in \mathbb{Z} \).

**Written:**

\[ n = 2a \implies n \text{ even} \]

**Intended Meaning:**

\[ n = 2a \iff n \text{ even} \]
A Note on Definitions

We use a special convention with definitions.

**Definition**

An integer \( n \) is **even** if and only if \( n = 2a \) for some integer \( a \in \mathbb{Z} \).

An integer \( n \) is **odd** if and only if \( n = 2a + 1 \) for some integer \( a \in \mathbb{Z} \).

**Written:**

\[ n = 2a \implies n \text{ even} \]

**Intended Meaning:**

\[ n = 2a \iff n \text{ even} \]

This is how people write definitions. (Convention.)
More Definitions

Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a | b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$. 

Example: $10 = 2 \cdot 5$

$2$ is a divisor of $10$

$10$ is a multiple of $2$
More Definitions

Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
- $2$ is a divisor of $10$
More Definitions

Definition

Suppose \( a \) and \( b \) are integers. We say \( a \) divides \( b \), written \( a \mid b \), if \( b = ac \) for some \( c \in \mathbb{Z} \). In this case we also say that \( a \) is a divisor of \( b \), and \( b \) is a multiple of \( a \).

Example: \( 10 = 2 \cdot 5 \)

- \( 2 \mid 10, \ 5 \mid 10 \)
- \( 2 \) is a divisor of \( 10 \)
- \( 10 \) is a multiple of \( 2 \)
More Definitions

Definition

Suppose \( a \) and \( b \) are integers. We say \( a \) divides \( b \), written \( a \mid b \), if \( b = ac \) for some \( c \in \mathbb{Z} \). In this case we also say that \( a \) is a divisor of \( b \), and \( b \) is a multiple of \( a \).

Example: \( 10 = 2 \cdot 5 \)

- \( 2 \mid 10 \), \( 5 \mid 10 \)
- \( 2 \) is a divisor of \( 10 \)
- \( 10 \) is a multiple of \( 2 \)
- Is \( 0 \) a divisor of \( 10 \)?
More Definitions

Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? No. There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \nmid 10$
Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? **No.** There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \not| 10$
- Is $-1$ a divisor of $10$?
Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a | b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2 | 10$, $5 | 10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? No. There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \nmid 10$
- Is $-1$ a divisor of $10$? Yes, $-10 \in \mathbb{Z}$ and $(-1)(-10) = 10$. 
More Definitions

Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? No. There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \nmid 10$
- Is $-1$ a divisor of $10$? Yes, $-10 \in \mathbb{Z}$ and $(-1)(-10) = 10$.

$\{a \in \mathbb{Z} : a|10\} = \{a \in \mathbb{Z} : a|0\} =$
Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written $a | b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2 | 10$, $5 | 10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? No. There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \nmid 10$
- Is $-1$ a divisor of $10$? Yes, $-10 \in \mathbb{Z}$ and $(-1)(-10) = 10$.

$\{a \in \mathbb{Z} : a | 10\} = \{-10, -5, -2, -1, 1, 2, 5, 10\}$
$\{a \in \mathbb{Z} : a | 0\} =$
Definition

Suppose $a$ and $b$ are integers. We say $a$ divides $b$, written

$$a|b$$

if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a divisor of $b$, and $b$ is a multiple of $a$.

Example: $10 = 2 \cdot 5$

- $2|10$, $5|10$
- $2$ is a divisor of $10$
- $10$ is a multiple of $2$
- Is $0$ a divisor of $10$? No. There is no $a \in \mathbb{Z}$ with $0a = 10$. We write $0 \not| 10$
- Is $-1$ a divisor of $10$? Yes, $-10 \in \mathbb{Z}$ and $(-1)(-10) = 10$

$$\{a \in \mathbb{Z} : a|10\} = \{-10, -5, -2, -1, 1, 2, 5, 10\}$$
$$\{a \in \mathbb{Z} : a|0\} = \mathbb{Z}$$
Definition

A number $n \in \mathbb{N}$ is \textbf{prime} if it has exactly two positive divisors, 1 and $n$. 
More Definitions

Definition

A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

Is 1 prime?
A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

Is 1 prime? **No:** it only has one positive divisor.
Definition

A number \( n \in \mathbb{N} \) is \textbf{prime} if it has exactly two positive divisors, 1 and \( n \).

Is 1 prime? \textbf{No}: it only has one positive divisor.

Can a negative number be prime?
Definition

A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and $n$.

Is 1 prime? **No**: it only has one positive divisor.

Can a negative number be prime? **No**: it is not in $\mathbb{N}$. 
A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and $n$.

An integer $n$ is **composite** if $n = ab$ for two integers $a, b$ with $a > 1$ and $b > 1$.

Is 1 prime? **No**: it only has one positive divisor.

Can a negative number be prime? **No**: it is not in $\mathbb{N}$. 
Definition

A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

An integer \( n \) is **composite** if \( n = ab \) for two integers \( a, b \) with \( a > 1 \) and \( b > 1 \).

Is 1 prime? **No:** it only has one positive divisor.

Can a negative number be prime? **No:** it is not in \( \mathbb{N} \).

What is the smallest composite number?
More Definitions

Definition

A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and $n$.

An integer $n$ is **composite** if $n = ab$ for two integers $a, b$ with $a > 1$ and $b > 1$.

Is 1 prime? **No**: it only has one positive divisor.

Can a negative number be prime? **No**: it is not in $\mathbb{N}$.

What is the smallest composite number? 4
4. Direct Proof

4.1 Theorems and their Friends

4.2 Definitions

4.3 Direct Proof

4.4 Using Cases

4.5 Treating Similar Cases

**More Definitions**

**Definition**

A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

An integer \( n \) is **composite** if \( n = ab \) for two integers \( a, b \) with \( a > 1 \) and \( b > 1 \).

**Definition**

The **greatest common divisor** of integers \( a \) and \( b \), which are not both zero, denoted \( \text{gcd}(a, b) \), is the largest integer that divides both \( a \) and \( b \).

The **least common multiple** of non-zero integers \( a \) and \( b \), denoted \( \text{lcm}(a, b) \), is the smallest positive integer that is a multiple of both \( a \) and \( b \).

\[
\text{gcd}(0, -18) = \]
Definition

A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and $n$.

An integer $n$ is **composite** if $n = ab$ for two integers $a, b$ with $a > 1$ and $b > 1$.

Definition

The **greatest common divisor** of integers $a$ and $b$, which are not both zero, denoted $\gcd(a, b)$, is the largest integer that divides both $a$ and $b$.

The **least common multiple** of non-zero integers $a$ and $b$, denoted $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both $a$ and $b$.

$\gcd(0, -18) = 18$
More Definitions

Definition

A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

An integer \( n \) is **composite** if \( n = ab \) for two integers \( a, b \) with \( a > 1 \) and \( b > 1 \).

Definition

The **greatest common divisor** of integers \( a \) and \( b \), which are not both zero, denoted \( \gcd(a, b) \), is the largest integer that divides both \( a \) and \( b \).

The **least common multiple** of non-zero integers \( a \) and \( b \), denoted \( \text{lcm}(a, b) \), is the smallest positive integer that is a multiple of both \( a \) and \( b \).

\[
\gcd(0, -18) = 18 \\
\text{lcm}(-2, 5) = 10
\]
More Definitions

Definition

A number \( n \in \mathbb{N} \) is **prime** if it has exactly two positive divisors, 1 and \( n \).

An integer \( n \) is **composite** if \( n = ab \) for two integers \( a, b \) with \( a > 1 \) and \( b > 1 \).

Definition

The **greatest common divisor** of integers \( a \) and \( b \), which are not both zero, denoted \( \gcd(a, b) \), is the largest integer that divides both \( a \) and \( b \).

The **least common multiple** of non-zero integers \( a \) and \( b \), denoted \( \text{lcm}(a, b) \), is the smallest positive integer that is a multiple of both \( a \) and \( b \).

\[
\gcd(0, -18) = 18 \quad \text{lcm}(-2, 5) = 10
\]
We can't define everything!
We can't define everything!

We accept the following facts:

- When we add, subtract, or multiply two integers, the result is an integer.
Generally Accepted

We can't define everything!

We accept the following facts:

- When we add, subtract, or multiply two integers, the result is an integer.
- It’s possible to divide any two non-zero numbers and end up with a quotient and remainder.
We can’t define everything!

We accept the following facts:

- When we add, subtract, or multiply two integers, the result is an integer.
- It’s possible to divide any two non-zero numbers and end up with a quotient and remainder.
- We can do algebra. For example, $\frac{4x}{2} = 2x$, and we can solve equations.
Generally Accepted

We can’t define everything!

We accept the following facts:

- When we add, subtract, or multiply two integers, the result is an integer.
- It’s possible to divide any two non-zero numbers and end up with a quotient and remainder.
- We can do algebra. For example, $\frac{4x}{2} = 2x$, and we can solve equations.
- Every natural number greater than 1 has a unique factorization into powers of primes.
Direct Proof of Conditional Statements

How to prove $P \Rightarrow Q$
How to prove $P \Rightarrow Q$

**Proposition:** If $P$, then $Q$.

**Proof:** Suppose $P$.

\[ \begin{array}{c}
\vdots \\
\therefore \\
\therefore Q.
\end{array} \]

Every step should be completely justified.
How to prove $P \Rightarrow Q$

**Proposition:** If $P$, then $Q$.

**Proof:** Suppose $P$.

\[ \therefore \]

Therefore $Q$.

Every step should be completely justified.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \Rightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
Direct Proof

Prove the following:

If $4 | x$, then $\frac{x}{2}$ is even.
Prove the following:

If $4 | x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4 | x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4 | x$.

Therefore, $\frac{x}{2}$ is even.
Direct Proof

Prove the following:
If $4 \mid x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4 \mid x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4 \mid x$.

Therefore, $\frac{x}{2} = 2a$ for some $a \in \mathbb{Z}$.

Therefore, $\frac{x}{2}$ is even by the definition of “even”. □
Prove the following:
If $4 \mid x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4 \mid x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4 \mid x$.
Then by the definition of “divides,” there exists some $b \in \mathbb{Z}$ such that $4b = x$.

Therefore, $\frac{x}{2} = 2a$ for some $a \in \mathbb{Z}$.

Therefore, $\frac{x}{2}$ is even by the definition of “even”. □
Proposition: If $4|x$, then $\frac{x}{2}$ is even.

Proof: Suppose $4|x$.
Then by the definition of “divides,” there exists some $b \in \mathbb{Z}$ such that $4b = x$.
Then $\frac{x}{2} = \frac{4b}{2} = 2b$

Therefore, $\frac{x}{2} = 2a$ for some $a \in \mathbb{Z}$.
Therefore, $\frac{x}{2}$ is even by the definition of “even”. □
Direct Proof

Prove the following:

If $4|\, \! x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4|\, \! x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4|\, \! x$.

Then by the definition of “divides,” there exists some $b \in \mathbb{Z}$ such that $4b = x$.

Then $\frac{x}{2} = \frac{4b}{2} = 2b$

Therefore, $\frac{x}{2} = 2b$ for some $b \in \mathbb{Z}$.

Therefore, $\frac{x}{2}$ is even by the definition of “even”. □
Prove the following:
If $4|\ x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4|\ x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4|\ x$.
Then by the definition of “divides,” there exists some $b \in \mathbb{Z}$ such that $4b = x$.
Then $\frac{x}{2} = \frac{4b}{2} = 2b$

Therefore, $\frac{x}{2} = 2b$ for some $b \in \mathbb{Z}$.
Therefore, $\frac{x}{2}$ is even by the definition of “even”.

Prove the following:

If $4|\ x$, then $\frac{x}{2}$ is even.

**Proposition:** If $4|\ x$, then $\frac{x}{2}$ is even.

**Proof:** Suppose $4|\ x$.

Then there exists some $a \in \mathbb{Z}$ such that $4a = x$. Then $\frac{x}{2} = 2a$, so $\frac{x}{2}$ is even.
Prove the following:

If $x$ is odd, then $x^2 + 1$ is even.
Prove the following: 
*If x is odd, then $x^2 + 1$ is even.*

**Proposition:** If $x$ is odd, then $x^2 + 1$ is even.

**Proof:** Suppose $x$ is odd.

Therefore, $x^2 + 1$ is even.
Direct Proof

Prove the following:

*If* $x$ *is odd, then* $x^2 + 1$ *is even.*

**Proposition:** If $x$ is odd, then $x^2 + 1$ is even.

**Proof:** Suppose $x$ is odd.
Then $x = 2a + 1$ for some integer $a$.
Then $x^2 + 1 = (2a + 1)^2 + 1 = 4a^2 + 4a + 1 + 1 = 2(2a^2 + 2a + 1)$.
If we define $b = 2a^2 + 2a + 1$, then $b \in \mathbb{Z}$ and $x = 2b$.
Therefore, $x^2 + 1$ is even.
4. Direct Proof

Prove the following:
*If* $x$ *is even, then for any* $n \in \mathbb{N}$, $x^n$ *is even as well.*

**Proposition:** If $x$ is even and $n \in \mathbb{N}$, then $x^n$ is even.

**Proof:** Suppose $x$ is even and $n \in \mathbb{N}$.

Therefore, $x^n$ is even.
Prove the following:

*If* $x$ *is even, then for any* $n \in \mathbb{N}$, *$x^n$ is even as well.*

---

**Proposition:** If $x$ is even and $n \in \mathbb{N}$, then $x^n$ is even.

**Proof:** Suppose $x$ is even and $n \in \mathbb{N}$.

Then $x = 2a$ for some integer $a$ and $n \geq 1$.

Since $n \geq 1$, $n - 1 \geq 0$, so $x^{n-1} \in \mathbb{Z}$.

Then $x^n = x \left( x^{n-1} \right) = 2a \left( x^{n-1} \right)$.

Let $b = a \left( x^{n-1} \right)$. Then $b \in \mathbb{Z}$ and $x^n = 2b$.

Therefore, $x^n$ is even.
Prove the following:
\textit{If }a \mid b, \textit{ then } a \mid (b^2 + 5a).

\begin{proof}
Suppose \(a \mid b\).

Then there exists some integer \(x\) such that \(b = ax\).

Then \(b^2 + 5a = (ax)^2 + 5a = a(ax^2 + 5)\).

If we let \(y = ax^2 + 5\), then \(y \in \mathbb{Z}\) and \(b = ay\).

Therefore, \(a \mid (b^2 + 5a)\).
\end{proof}
Prove the following:
*If* $a|b$, *then* $a|(b^2 + 5a)$.

**Proposition:** If $a|b$, then $a|(b^2 + 5a)$.

**Proof:** Suppose $a|b$.

Then there exists some integer $x$ such that $b = ax$.

Then $b^2 + 5a = (ax)^2 + 5a = a(ax^2 + 5)$.

If we let $y = ax^2 + 5$, then $y \in \mathbb{Z}$ and $b = ay$.

Therefore, $a|(b^2 + 5a)$. 

□
Prove the following:

For any two positive real numbers $z$ and $y$, if $x \leq y$ then $\sqrt{x} \leq \sqrt{y}$.

Hint: Factor $\sqrt{x^2} - \sqrt{y^2}$. You may assume that dividing both sides of an inequality by a positive number does not change the direction of the inequality.

**Proposition:**

*Proof:* Suppose $x, y \in \mathbb{R}$ and $0 < x \leq y$.

Therefore, $\sqrt{x} \leq \sqrt{y}$.  \qed
Prove the following:

For any two positive real numbers \( z \) and \( y \), if \( x \leq y \) then \( \sqrt{x} \leq \sqrt{y} \).

Hint: Factor \( \sqrt{x^2} - \sqrt{y^2} \). You may assume that dividing both sides of an inequality by a positive number does not change the direction of the inequality.

**Proposition:**

**Proof:** Suppose \( x, y \in \mathbb{R} \) and \( 0 < x \leq y \).

Since \( x \leq y \), \( x - y \leq 0 \).

Since \( x \) and \( y \) are nonnegative, \( \sqrt{x^2} = x \) and \( \sqrt{y^2} = y \).

Therefore, \( x - y \leq 0 \) tells us \( \sqrt{x^2} - \sqrt{y^2} \leq 0 \).

Factoring, we see \( (\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) \leq 0 \). Since \( \sqrt{x} + \sqrt{y} > 0 \), dividing both sides of this inequality by it yields \( \sqrt{x} - \sqrt{y} \leq 0 \).

Therefore, \( \sqrt{x} \leq \sqrt{y} \). \( \Box \)
Prove the following:

*For any two positive real numbers \( z \) and \( y \), if \( x \leq y \) then \( \sqrt{x} \leq \sqrt{y} \).

Hint: Factor \( \sqrt{x^2} - \sqrt{y^2} \). You may assume that dividing both sides of an inequality by a positive number does not change the direction of the inequality.

**Proposition:**

*Proof:* Suppose \( x, y \in \mathbb{R} \) and \( 0 < x \leq y \).

Since \( x \leq y \), \( x - y \leq 0 \).

Since \( x \) and \( y \) are nonnegative, \( \sqrt{x^2} = x \) and \( \sqrt{y^2} = y \).

Therefore, \( x - y \leq 0 \) tells us \( \sqrt{x^2} - \sqrt{y^2} \leq 0 \).

Factoring, we see \( (\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) \leq 0 \). Since \( \sqrt{x} + \sqrt{y} > 0 \), dividing both sides of this inequality by it yields \( \sqrt{x} - \sqrt{y} \leq 0 \).

Therefore, \( \sqrt{x} \leq \sqrt{y} \).

Corollary: for all nonnegative real \( x \) and \( y \), if \( x \leq y \), then \( \sqrt{x} \leq \sqrt{y} \).
4. Direct Proof

Prove the following:

*For any two nonnegative integers* \( z \) and \( y \), \( \sqrt{xy} \leq \frac{x + y}{2} \). (That is, the geometric mean is no greater than the arithmetic mean.)

Hint: use the result from the previous slide, \( x \leq y \Rightarrow \sqrt{x} \leq \sqrt{y} \) for all nonnegative real \( x, y \).

**Proposition:** For any two nonnegative integers \( z \) and \( y \), \( \sqrt{xy} \leq \frac{x + y}{2} \).

**Proof:** Suppose \( x \) and \( y \) are nonnegative integers.

Therefore, \( \sqrt{xy} \leq \frac{x + y}{2} \). \( \square \)
Direct Proof

Prove the following:

For any two nonnegative integers \( z \) and \( y \), \( \sqrt{xy} \leq \frac{x + y}{2} \). (That is, the geometric mean is no greater than the arithmetic mean.)

Hint: use the result from the previous slide, \( x \leq y \Rightarrow \sqrt{x} \leq \sqrt{y} \) for all nonnegative real \( x, y \).

**Proposition:** For any two nonnegative integers \( z \) and \( y \), \( \sqrt{xy} \leq \frac{x + y}{2} \).

**Proof:** Suppose \( x \) and \( y \) are nonnegative integers.

Note \( 0 \leq (x - y)^2 \).

Then \( 0 \leq x^2 - 2xy + y^2 \), so if we add \( 4xy \) to both sides, \( 4xy \leq x^2 + 2xy + y^2 = (x + y)^2 \).

Then (using the result from the last slide) \( 2\sqrt{xy} \leq x + y \).

Therefore, \( \sqrt{xy} \leq \frac{x + y}{2} \). \([\blacksquare]\)
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$. 
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$1 + (-1)^n(2n - 1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>-4</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>-8</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>-12</td>
</tr>
</tbody>
</table>
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

**Proposition:** For every $n \in \mathbb{Z}$, $1 + (-1)^n(2n - 1)$ is divisible by 4.
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

**Proposition:** For every $n \in \mathbb{Z}$, $1 + (-1)^n(2n - 1)$ is divisible by 4.

**Proof:**
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

**Proposition:** For every $n \in \mathbb{Z}$, $1 + (-1)^n(2n - 1)$ is divisible by 4.

**Proof:**
Let $n$ be an integer. Then $n$ is either even or odd.

**Suppose $n$ is even.**

**Suppose $n$ is odd.**
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

**Proposition:** For every $n \in \mathbb{Z}$, $1 + (-1)^n(2n - 1)$ is divisible by 4.

**Proof:**
Let $n$ be an integer. Then $n$ is either even or odd.

**Suppose $n$ is even.** Then $n = 2a$ for some integer $a$, and $(-1)^n = 1$.
So,

$$1 + (-1)^n(2n - 1) = 1 + 2(2a) - 1 = 4a$$

and thus the expression is divisible by 4.

**Suppose $n$ is odd.**
Prove that $1 + (-1)^n(2n - 1)$ is divisible by 4 for every $n \in \mathbb{Z}$.

**Proposition:** For every $n \in \mathbb{Z}$, $1 + (-1)^n(2n - 1)$ is divisible by 4.

**Proof:**
Let $n$ be an integer. Then $n$ is either even or odd.

**Suppose $n$ is even.** Then $n = 2a$ for some integer $a$, and $(-1)^n = 1$.
So,

$$1 + (-1)^n(2n - 1) = 1 + 2(2a) - 1 = 4a$$

and thus the expression is divisible by 4.

**Suppose $n$ is odd.** Then $n = 2a + 1$ for some integer $a$, and $(-1)^n = -1$.
So,

$$1 + (-1)^n(2n - 1) = 1 - 2(2a + 1) + 1 = -4a = 4(-a)$$

and thus the expression is divisible by 4. ∎
Cases

**Proposition:** If \( a \in \mathbb{Z} \) is a multiple of 4, then \( a = 1 + (-1)^n(2n - 1) \) for some \( n \in \mathbb{N} \).
Proposition: If \( a \in \mathbb{Z} \) is a multiple of 4, then \( a = 1 + (-1)^n(2n - 1) \) for some \( n \in \mathbb{N} \).
Cases

**Proposition:** If $a \in \mathbb{Z}$ is a multiple of 4, then $a = 1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

**Proof:** Suppose $a \in \mathbb{Z}$ is a multiple of 4. Then $a = 4b$ for some integer $b$.

**Suppose** $b \geq 0$. In this case, let $n = 2b$. Then

$$1 + (-1)^n(2n - 1) = 1 + (2(2b)) - 1) = 4b = a.$$  

Suppose $b < 0$. In this case, let $n = 1 - 2b$. Note $1 - 2b > 0$, since $b < 0$, so $n \in \mathbb{N}$. Also, $n$ is odd, so:

$$1 + (-1)^n(2n - 1) = 1 + (-1)(2(1 - 2b)) - 1) = 1 - (2 - 4b - 1) = 4b = a.$$  

$\square$
“Without Loss of Generality”

**Proposition:** Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.
Proposition: Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.

Example: given 1, 1, 7.8:
“Without Loss of Generality”

**Proposition:** Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.

**Example:** given 1, 1, 7.8: 1 < 1 + 7.8
“Without Loss of Generality”

**Proposition:** Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.

Example: given 1, 1, 7.8: \[ 1 < 1 + 7.8 \]
Example: given 5, 3, 8:
Proposition: Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.

Example: given 1, 1, 7.8: 1 < 1 + 7.8
Example: given 5, 3, 8: 3 < 5 + 8, and also 5 < 3 + 8
Proposition: Given any three (not necessarily distinct) positive numbers, it is possible to choose two so that their sum is strictly greater than the third.

Example: given 1, 1, 7.8: \(1 < 1 + 7.8\)
Example: given 5, 3, 8: \(3 < 5 + 8\), and also \(5 < 3 + 8\)

Proof: Let \(a, b, \) and \(c\) be positive numbers, and WLOG ("without loss of generality") let \(a \leq b\).
Then \(b + c \geq a + c > a\) (since \(c > 0\)).
Triangle Inequality

**Proposition:** \( \forall x, y \in \mathbb{Z}, |x + y| \leq |x| + |y| \)
Triangle Inequality

**Proposition:** \( \forall x, y \in \mathbb{Z}, |x + y| \leq |x| + |y| \)

**Example:** \( |1 + 1| \leq 1 + 1 \)
Triangle Inequality

**Proposition:** $\forall x, y \in \mathbb{Z}, |x + y| \leq |x| + |y|$

**Example:** $|1 + 1| \leq 1 + 1$
**Example:** $|2 - 1| \leq 2 + 1$
Proposition: \( \forall x, y \in \mathbb{Z}, |x + y| \leq |x| + |y| \)

Example: \( |1 + 1| \leq 1 + 1 \)
Example: \( |2 - 1| \leq 2 + 1 \)

Proof:
Suppose \( x, y \geq 0 \).

Suppose \( x, y < 0 \).

Suppose \( x \geq 0, y < 0 \).
Triangle Inequality

**Proposition:** $\forall x, y \in \mathbb{Z}, |x + y| \leq |x| + |y|$

**Example:** $|1 + 1| \leq 1 + 1$

**Example:** $|2 - 1| \leq 2 + 1$

**Proof:**

**Suppose** $x, y \geq 0$.

**Suppose** $x, y < 0$.

**Suppose** $x \geq 0, y < 0$. **Then** $|x| \geq |y|$ or $|x| < |y|$.
More Examples

**Proposition:** \( \forall n \in \mathbb{N}, n^2 - 3n + 9 \) is odd.

**Proposition:** Suppose \( \gcd(a, b) > 1 \) and \( b \) is prime. Then \( b = \gcd(a, b) \).

**Proposition:** For every \( a \in \mathbb{Z} \), if \( a^2 \) | \( a \), then \( a^2 = |a| \).

**Proposition:** Every odd integer is the difference of two squares.