What is a proof?

**Definition**

- **Proof** is a method for establishing the truth of a statement.

<table>
<thead>
<tr>
<th>Rigor</th>
<th>Truth type</th>
<th>Field</th>
<th>Truth teller</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Word of God</td>
<td>Religion</td>
<td>God/Priests</td>
</tr>
<tr>
<td>1</td>
<td>Authoritative truth</td>
<td>Business/School</td>
<td>Boss/Teacher</td>
</tr>
<tr>
<td>2</td>
<td>Legal truth</td>
<td>Judiciary</td>
<td>Law/Judge/Law makers</td>
</tr>
<tr>
<td>3</td>
<td>Philosophical truth</td>
<td>Philosophy</td>
<td>Plausible argument</td>
</tr>
<tr>
<td>4</td>
<td>Scientific truth</td>
<td>Physical sciences</td>
<td>Experiments/Observations</td>
</tr>
<tr>
<td>5</td>
<td>Statistical truth</td>
<td>Statistics</td>
<td>Data sampling</td>
</tr>
<tr>
<td>6</td>
<td>Mathematical truth</td>
<td>Mathematics</td>
<td>Logical deduction</td>
</tr>
</tbody>
</table>
### Definition

- **A mathematical proof** is a verification for establishing the truth of a proposition by a chain of logical deductions from a set of axioms.

### Concepts

1. **Proposition**
   - Covered in sufficient depth in logic
2. **Axiom**
   - An axiom is a proposition that is assumed to be true
   - Example: For mathematical quantities $a$ and $b$, if $a = b$, then $b = a$
3. **Logical deduction**
   - We call this process – the axiomatic method
   - We will cover several proof techniques in this chapter
Why care for mathematical proofs?

- The current world ceases to function without math proofs
- (My belief) **Reduction tree** showing subjects that possibly could be expressed or understood in terms of other subjects

```
   Humanities
    ↓        ↓
Psychology  Biology
  ↓        ↓
Chemistry  Physics
  ↓
Mathematics
```

```
   CS
```

## Methods of mathematical proof

<table>
<thead>
<tr>
<th>Statements</th>
<th>Method of proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proving existential statements</td>
<td>Constructive proof</td>
</tr>
<tr>
<td>(Disproving universal statements)</td>
<td>Non-constructive proof</td>
</tr>
<tr>
<td>Proving universal statements</td>
<td>Direct proof</td>
</tr>
<tr>
<td>(Disproving existential statements)</td>
<td>Proof by mathematical induction</td>
</tr>
<tr>
<td></td>
<td>Well-ordering principle</td>
</tr>
<tr>
<td></td>
<td>Proof by exhaustion</td>
</tr>
<tr>
<td></td>
<td>Proof by cases</td>
</tr>
<tr>
<td></td>
<td>Proof by contradiction</td>
</tr>
<tr>
<td></td>
<td>Proof by contraposition</td>
</tr>
<tr>
<td></td>
<td>Computer-aided proofs</td>
</tr>
</tbody>
</table>
**Definition**

- Number theory is the branch of mathematics that deals with the study of integers

<table>
<thead>
<tr>
<th>Numbers</th>
<th>Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural numbers ((\mathbb{N}))</td>
<td>{1, 2, 3, \ldots}</td>
</tr>
<tr>
<td>Whole numbers ((\mathbb{W}))</td>
<td>{0, 1, 2, \ldots}</td>
</tr>
<tr>
<td>Integers ((\mathbb{Z}))</td>
<td>{0, \pm 1, \pm 2, \pm 3, \ldots}</td>
</tr>
<tr>
<td>Even numbers ((\mathbb{E}))</td>
<td>{0, \pm 2, \pm 4, \pm 6, \ldots}</td>
</tr>
<tr>
<td>Odd numbers ((\mathbb{O}))</td>
<td>{\pm 1, \pm 3, \pm 5, \pm 7, \ldots}</td>
</tr>
<tr>
<td>Prime numbers ((\mathbb{P}))</td>
<td>{2, 3, 5, 7, 11, \ldots}</td>
</tr>
<tr>
<td>Composite numbers ((\mathbb{C}))</td>
<td>{Natural numbers (&gt; 1) that are not prime}</td>
</tr>
<tr>
<td>Rational numbers ((\mathbb{Q}))</td>
<td>{Ratio of integers with non-zero denominator}</td>
</tr>
<tr>
<td>Real numbers ((\mathbb{R}))</td>
<td>{Numbers with infinite decimal representation}</td>
</tr>
<tr>
<td>Irrational numbers ((\mathbb{I}))</td>
<td>{Real numbers that are not rational}</td>
</tr>
<tr>
<td>Complex numbers ((\mathbb{S}))</td>
<td>{real + (i) \cdot real}</td>
</tr>
</tbody>
</table>
Even and odd numbers

Definitions

- An integer $n$ is even iff $n$ equals twice some integer; Formally, for any integer $n$,

  $$n \text{ is even } \iff n = 2k \text{ for some integer } k$$

- An integer $n$ is odd iff $n$ equals twice some integer plus 1; Formally, for any integer $n$,

  $$n \text{ is odd } \iff n = 2k + 1 \text{ for some integer } k$$

Examples

- Even numbers:
  $$0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, \ldots$$

- Odd numbers:
  $$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, \ldots$$
Rational and irrational numbers

**Definitions**

- A real number $r$ is **rational** iff it can be expressed as a ratio of two integers with a nonzero denominator; Formally, if $r$ is a real number, then

  $$ r \text{ is rational} \iff \exists \text{ integers } a, b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0 $$

- A real number $r$ is **irrational** iff it is not rational

**Examples**

- **Rational numbers:**
  10, −56.47, 10/13, 0, −17/9, 0.121212..., −91, ...

- **Irrational numbers:**
  $\sqrt{2}, \sqrt{3}, \sqrt{2^{\sqrt{2}}}, \pi, \phi, e, \pi^2, e^2, 2^{1/3}, \log_2 3, ...$

- **Open problems:**
  It’s not known if $\pi + e, \pi e, \pi/e, \pi e, \pi^{\sqrt{2}}$, and $\ln \pi$ are irrational.
Divisibility

Definitions

- If \( n \) and \( d \) are integers, then \( n \) is divisible by \( d \), denoted by \( d | n \), iff \( n \) equals \( d \) times some integer and \( d \neq 0 \);
  
  Formally, if \( n \) and \( d \) are integers

  \[
  d | n \iff \exists \text{ integer } k \text{ such that } n = dk \text{ and } d \neq 0
  \]

- Instead of “\( n \) is divisible by \( d \),” we can say:
  \( n \) is a multiple of \( d \), or
  \( d \) is a factor of \( n \), or
  \( d \) is a divisor of \( n \), or
  \( d \) divides \( n \) (denoted by \( d | n \))

- Note: \( d | n \) is different from \( d/n \)

Examples

- Divides: \( 1 | 1, 10 | 10, 2 | 4, 3 | 24, 7 | -14, \ldots \)
- Does not divide: \( 2 \nmid 1, 10 \nmid 1, 10 \nmid 2, 7 \nmid 10, 10 \nmid 7, 10 \nmid -7, \ldots \)
Quotient-Remainder theorem

**Theorem**

- Given any integer $n$ and a positive integer $d$, there exists an integer $q$ and a whole number $r$ such that

$$n = qd + r \text{ and } r \in [0, d - 1]$$

**Examples**

- Let $n = 6$ and $d \in [1, 7]$

<table>
<thead>
<tr>
<th>Num. ($n$)</th>
<th>Divisor ($d$)</th>
<th>Theorem</th>
<th>Quotient ($q$)</th>
<th>Rem. ($r$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>$6 = 6 \times 1 + 0$</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$6 = 3 \times 2 + 0$</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>$6 = 2 \times 3 + 0$</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>$6 = 1 \times 4 + 2$</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>$6 = 1 \times 5 + 1$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>$6 = 1 \times 6 + 0$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>$6 = 0 \times 7 + 6$</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Num.</td>
<td>Factorization</td>
<td>Prime?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$2 = 1 \times 2 = 2 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$3 = 1 \times 3 = 3 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$4 = 1 \times 4 = 4 \times 1 = 2 \times 2$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>$5 = 1 \times 5 = 5 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$6 = 1 \times 6 = 6 \times 1 = 2 \times 3 = 3 \times 2$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>$7 = 1 \times 7 = 7 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$8 = 1 \times 8 = 8 \times 1 = 2 \times 4 = 4 \times 2$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>$9 = 1 \times 9 = 9 \times 1 = 3 \times 3$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$10 = 1 \times 10 = 10 \times 1 = 2 \times 5 = 5 \times 2$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>$11 = 1 \times 11 = 11 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>$12 = 1 \times 12 = 12 \times 1 = 2 \times 6 = 6 \times 2 = 3 \times 4 = 4 \times 3$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>$13 = 1 \times 13 = 13 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$14 = 1 \times 14 = 14 \times 1 = 2 \times 7 = 7 \times 2$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>$15 = 1 \times 15 = 15 \times 1 = 3 \times 5 = 5 \times 3$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>$16 = 1 \times 16 = 16 \times 1 = 2 \times 8 = 8 \times 2 = 4 \times 4$</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>$17 = 1 \times 17 = 17 \times 1$</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prime numbers

Definitions

- A natural number $n$ is **prime** iff $n > 1$ and it has exactly two positive divisors: 1 and $n$
- A natural number $n$ is **composite** iff $n > 1$ and it has at least three positive divisors, two of which are 1 and $n$
- A natural number $n$ is a **perfect square** iff it has an odd number of divisors
- A natural number $n$ is **not a perfect square** iff it has an even number of divisors

Examples

- Perfect squares: 1, 4, 9, 16, 25, ...  
- Not perfect squares: 2, 3, 5, 6, 7, 8, 10, ...
**Definitions**

- A natural number $n$ is **prime** iff $n > 1$ and for all natural numbers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$; Formally, for each natural number $n$ with $n > 1$,

  $n$ is prime $\iff \forall$ natural numbers $r$ and $s$, if $n = rs$ then $n = r$ or $n = s$

- A natural number $n$ is **composite** iff $n > 1$ and $n = rs$ for some natural numbers $r$ and $s$ with $1 < r < n$ and $1 < s < n$; Formally, for each natural number $n$ with $n > 1$,

  $n$ is composite $\iff \exists$ natural numbers $r$ and $s$, if $n = rs$ and $1 < r < n$ and $1 < s < n$
## Unique prime factorization of natural numbers

<table>
<thead>
<tr>
<th>$n$</th>
<th>Unique prime factorization</th>
<th>$n$</th>
<th>Unique prime factorization</th>
<th>$n$</th>
<th>Unique prime factorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>16</td>
<td>$2^4$</td>
<td>30</td>
<td>$2 \times 3 \times 5$</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>17</td>
<td>17</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>4</td>
<td>$2^2$</td>
<td>18</td>
<td>$2 \times 3^2$</td>
<td>32</td>
<td>$2^5$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>19</td>
<td>19</td>
<td>33</td>
<td>$3 \times 11$</td>
</tr>
<tr>
<td>6</td>
<td>$2 \times 3$</td>
<td>20</td>
<td>$2^2 \times 5$</td>
<td>34</td>
<td>$2 \times 17$</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>21</td>
<td>$3 \times 7$</td>
<td>35</td>
<td>$5 \times 7$</td>
</tr>
<tr>
<td>8</td>
<td>$2^3$</td>
<td>22</td>
<td>$2 \times 11$</td>
<td>36</td>
<td>$2^2 \times 3^2$</td>
</tr>
<tr>
<td>9</td>
<td>$3^2$</td>
<td>23</td>
<td>23</td>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>10</td>
<td>$2 \times 5$</td>
<td>24</td>
<td>$2^3 \times 3$</td>
<td>38</td>
<td>$2 \times 19$</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>25</td>
<td>$5^2$</td>
<td>39</td>
<td>$3 \times 13$</td>
</tr>
<tr>
<td>12</td>
<td>$2^2 \times 3$</td>
<td>26</td>
<td>$2 \times 13$</td>
<td>40</td>
<td>$2^3 \times 5$</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>27</td>
<td>$3^3$</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>14</td>
<td>$2 \times 7$</td>
<td>28</td>
<td>$2^2 \times 7$</td>
<td>42</td>
<td>$2 \times 3 \times 7$</td>
</tr>
<tr>
<td>15</td>
<td>$3 \times 5$</td>
<td>29</td>
<td>29</td>
<td>43</td>
<td>43</td>
</tr>
</tbody>
</table>

- **What is the pattern?**
### Definition

- Any natural number $n > 1$ can be uniquely represented as a product of as follows:

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

such that $p_1 < p_2 < \cdots < p_k$ are primes in $[2, n]$, $e_1, e_2, \ldots, e_k$ are whole number exponents, and $k$ is a natural number.

- The theorem is also called **fundamental theorem of arithmetic**
- The form is called **standard factored form**
### Definitions

- **Absolute value** of real number $x$, denoted by $|x|$ is
  
  $$|x| = \begin{cases} 
  x & \text{if } x \geq 0 \\
  -x & \text{if } x < 0 
  \end{cases}$$

- **Triangle inequality.** For all real numbers $x$ and $y$,
  
  $$|x + y| \leq |x| + |y|$$

- **Floor** of a real number $x$, denoted by $\lfloor x \rfloor$ is
  
  $$\lfloor x \rfloor = \text{unique integer } n \text{ such that } n \leq x < n + 1$$

  $$\lfloor x \rfloor = n \iff n \leq x < n + 1$$

- **Ceiling** of a real number $x$, denoted by $\lceil x \rceil$ is
  
  $$\lceil x \rceil = \text{unique integer } n \text{ such that } n - 1 < x \leq n$$

  $$\lceil x \rceil = n \iff n - 1 < x \leq n$$
Given an integer $n$ and a natural number $d$, 
$n \text{ div } d = \text{ integer quotient obtained when } n \text{ is divided by } d$, 
$n \text{ mod } d = \text{ whole number remainder obtained when } n \text{ is divided by } d$.

Symbolically, 
$n \text{ div } d = q \text{ and } n \text{ mod } d = r \iff n = dq + r$
where $q$ and $r$ are integers and $0 \leq r < d$. 
Properties of a proof

Properties

- Concise  (not unnecessarily long)
- Clear    (not ambiguous)
- Complete  (no missing intermediate steps)
- Logical  (every statement logically follows)
- Rigorous (uses mathematical expressions)
- Convincing (does not raise questions)
- The way a proof is presented might be different from the way the proof is discovered.
Direct Proof
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sum of an even integer and an odd integer is odd.</td>
</tr>
<tr>
<td>Proposition</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Sum of an even integer and an odd integer is odd.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Suppose $a$ is even and $b$ is odd. Then</td>
</tr>
<tr>
<td>$a + b$</td>
</tr>
<tr>
<td>$= (2m) + b$</td>
</tr>
<tr>
<td>(defn. of even, $a = 2m$ for integer $m$)</td>
</tr>
<tr>
<td>$= (2m) + (2n + 1)$</td>
</tr>
<tr>
<td>(defn. of odd, $b = 2n + 1$ for integer $n$)</td>
</tr>
<tr>
<td>$= 2(m + n) + 1$</td>
</tr>
<tr>
<td>(taking 2 as common factor)</td>
</tr>
<tr>
<td>$= 2p + 1$</td>
</tr>
<tr>
<td>($p = m + n$ and addition is closed on integers)</td>
</tr>
<tr>
<td>$= \text{odd}$</td>
</tr>
<tr>
<td>(defn. of odd)</td>
</tr>
</tbody>
</table>
Prove the following propositions:

- Even + even = even
- Even + odd = odd
- Odd + odd = even
- Even × integer = even
- Odd × odd = odd
Proposition

- The square of an odd integer is odd.
The square of an odd integer is odd.

Proof

Prove: If \( n \) is odd, then \( n^2 \) is odd.

\[
\begin{align*}
n & \text{ is odd} \\
\implies n &= (2k + 1) \quad \text{(defn. of odd, } k \text{ is an integer)} \\
\implies n^2 &= (2k + 1)^2 \quad \text{(squaring on both sides)} \\
\implies n^2 &= 4k^2 + 4k + 1 \quad \text{(expanding the binomial)} \\
\implies n^2 &= 2(2k^2 + 2k) + 1 \quad \text{(factoring 2 from first two terms)} \\
\implies n^2 &= 2j + 1 \quad \text{(let } j = 2k^2 + 2k) \\
\quad j & \text{ is an integer as mult. and add. are closed on integers} \\
\implies n^2 & \text{ is odd} \quad \text{(defn. of odd)}
\end{align*}
\]
### Proposition

- Every odd integer is equal to the difference between the squares of two integers.
### Proposition

- Every odd integer is equal to the difference between the squares of two integers

### Workout

- Write a formal statement.
  \[ \forall \text{ integer } k, \exists \text{ integers } m, n \text{ such that } (2k + 1) = m^2 - n^2. \]
- Try out a few examples.
  - \[ 1 = 1^2 - 0^2 \]
  - \[ -1 = 0^2 - (-1)^2 \]
  - \[ 3 = 2^2 - 1^2 \]
  - \[ -3 = (-1)^2 - (-2)^2 \]
  - \[ 5 = 3^2 - 2^2 \]
  - \[ -5 = (-2)^2 - (-3)^2 \]
  - \[ 7 = 4^2 - 3^2 \]
  - \[ -7 = (-3)^2 - (-4)^2 \]
- Find a pattern.
  \[ (k + 1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 = \text{odd} \]
Odd = difference of squares

**Proposition**

- Every odd integer is equal to the difference between the squares of two integers.

**Proof**

- Any odd integer can be written as $(2k + 1)$ for some integer $k$.
- We rewrite the expression as follows.
  
  $$
  2k + 1 = (k^2 + 2k + 1) - k^2 \quad \text{(adding and subtracting $k^2$)}
  $$
  
  $$
  = (k + 1)^2 - k^2 \quad \text{(write the first term as sum)}
  $$
  
  $$
  = m^2 - n^2 \quad \text{(set $m = k + 1$ and $n = k$)}
  $$

  The term $m$ is an integer as addition is closed on integers.
- So, every odd integer can be written as the difference between two squares.
Odd = difference of squares

\(k^2\) cells

\((k + 1)^2\) cells
If \( a \mid b \) and \( b \mid c \), then \( a \mid c \)

**Proposition**

- (Transitivity) For integers \( a, b, c \), if \( a \mid b \) and \( b \mid c \), then \( a \mid c \).
If \(a \mid b\) and \(b \mid c\), then \(a \mid c\)

### Proposition

- (Transitivity) For integers \(a, b, c\), if \(a \mid b\) and \(b \mid c\), then \(a \mid c\).

### Proof

- **Formal statement.**
  \[\forall\text{ integers } a, b, c, \text{ if } a \mid b \text{ and } b \mid c, \text{ then } a \mid c.\]
- \(c\)
  
  \[
  = bn \quad (b \mid c \text{ and definition of divisibility}) \\
  = (am)n \quad (a \mid b \text{ and definition of divisibility}) \\
  = a(mn) \quad \text{(multiplication is associative)} \\
  = ak \quad \text{(let } k = mn \text{ and multiplication is closed on integers)} \\
  \implies a \mid c \quad \text{(definition of divisibility and } k \text{ is an integer)}
  \]
Summation

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 + 2 + 3 + \cdots + n = n(n + 1)/2.$</td>
</tr>
</tbody>
</table>
Proposition

- $1 + 2 + 3 + \cdots + n = n(n + 1)/2$.

Proof

- **Formal statement.** $\forall$ natural number $n$, prove that $1 + 2 + 3 + \cdots + n = n(n + 1)/2$.
- $S = 1 + 2 + 3 + \cdots + n$
  $\implies S = n + (n - 1) + (n - 2) + \cdots + 1$
  (addition on integers is commutative)
  $\implies 2S = (n + 1) + (n + 1) + (n + 1) + \cdots + (n + 1)$
  \hspace{3cm} n \text{ terms}
  (adding the previous two equations)
  $\implies 2S = n(n + 1)$
  (simplifying)
  $\implies S = n(n + 1)/2$
  (divide both sides by 2)
Proof by Negation
Proposition

- $2^{999} + 1$ is prime.
$$2^{999} + 1$$

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $2^{999} + 1$ is prime.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workout</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trying out a few examples is not possible here.</td>
</tr>
<tr>
<td>• When is a number prime?</td>
</tr>
<tr>
<td>A number that is not composite is prime.</td>
</tr>
<tr>
<td>• When is a number composite?</td>
</tr>
<tr>
<td>A number is composite if we can factorize it.</td>
</tr>
<tr>
<td>• How do you check if a number can be factorized?</td>
</tr>
<tr>
<td>Check whether the number satisfies an algebraic formula that can be factorized.</td>
</tr>
<tr>
<td>It seems like the given number can be represented as $a^3 + b^3$.</td>
</tr>
</tbody>
</table>
\[ 2^{999} + 1 \]

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2^{999} + 1) is prime.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>False!</strong> (2^{999} + 1) is composite.</td>
</tr>
</tbody>
</table>
| \(2^{999} + 1\)  
  \(= (2^{333})^3 + 1^3\)  
  \(= a^3 + b^3\)  
  \(= (a + b)(a^2 - ab + b^2)\)  
  \(= (2^{333} + 1)(2^{666} - 2^{333} + 1)\)  
  \(= \text{composite}\) |

(terms represented as cubes)  
(set \(a = 2^{333}, b = 1\))  
(factorize \(a^3 + b^3\))  
(substituting \(a\) and \(b\) values)
### Proposition

- There is a natural number $n$ such that $n^2 + 3n + 2$ is prime.
Proposition

- There is a natural number $n$ such that $n^2 + 3n + 2$ is prime.

Workout

- Write a formal statement.
  \[ \exists \text{ natural number } n \text{ such that } n^2 + 3n + 2 \text{ is prime.} \]

- Try out a few examples.
  \[
  \begin{align*}
  1^2 + 3(1) + 2 &= 6 &\text{composite} \\
  2^2 + 3(2) + 2 &= 12 &\text{composite} \\
  3^2 + 3(3) + 2 &= 20 &\text{composite} \\
  4^2 + 3(4) + 2 &= 30 &\text{composite} \\
  5^2 + 3(5) + 2 &= 42 &\text{composite}
  \end{align*}
  \]

- Find a pattern.
  It seems like $n^2 + 3n + 2$ is always composite.
### Proposition

- There is a natural number \( n \) such that \( n^2 + 3n + 2 \) is prime.

### Solution

- **False!**
- Proving that the given statement is false is equivalent to proving that its negation is true.

**Negation.** \( \forall \) natural number \( n \), \( n^2 + 3n + 2 \) is composite.

- \( n^2 + 3n + 2 \)
  
  \[
  \begin{align*}
  &= n^2 + n + 2n + 2 \\
  &= n(n + 1) + 2(n + 1) \\
  &= (n + 1)(n + 2) \\
  &= \text{composite} \\
  \end{align*}
  \]

  (split 3n) (taking common factors) (distributive law) \((n + 1 > 1 \text{ and } n + 2 > 1)\)
Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$. 

Proof

Substitute $x = 7$ in the expression to get $7^3 - 7(7^2) + 7 - 7 = 0$. As $x$ satisfies the equation, $x = 7$. Incorrect! What's wrong?
Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof

- Substitute $x = 7$ in the expression to get $7^3 - 7(7^2) + 7 - 7 = 0$. As $x$ satisfies the equation, $x = 7$. 
**Polynomial root**

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Substitute $x = 7$ in the expression to get $7^3 - 7(7^2) + 7 - 7 = 0$. As $x$ satisfies the equation, $x = 7$.</td>
</tr>
</tbody>
</table>

• Incorrect! What's wrong?
## Proposition

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If</strong> $x^3 - 7x^2 + x - 7 = 0$, <strong>then</strong> $x = 7$.</td>
<td></td>
</tr>
</tbody>
</table>
### Proposition

- If \( x^3 - 7x^2 + x - 7 = 0 \), then \( x = 7 \).

### Proof

- **False!**
- A polynomial equation of degree \( n \) has \( n \) roots. So, the polynomial equation \( x^3 - 7x^2 + x - 7 = 0 \) has 3 roots.
- We factorize the expression.
  \[
  x^3 - 7x^2 + x - 7 = x^2(x - 7) + (x - 7) \quad \text{(taking } x^2 \text{ factor from first two terms)}
  \]
  \[
  = (x - 7)(x^2 + 1) \quad \text{(taking } (x - 7) \text{ factor)}
  \]
  \[
  = (x - 7)(x + i)(x - i) \quad \text{(factorizing } (x^2 + 1)\text{)}
  \]
  (this is because \((x + i)(x - i) = (x^2 - i^2) = (x^2 + 1)\))

So, the three roots to the equation \( x^3 - 7x^2 + x - 7 = 0 \) are \( x = 7, x = -\sqrt{-1}, \) and \( x = \sqrt{-1} \).
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Exactly one of the three roots is $x = 7$. Hence, we have</td>
</tr>
<tr>
<td>$x = 7 \implies x^3 - 7x^2 + x - 7 = 0$</td>
</tr>
<tr>
<td>$x^3 - 7x^2 + x - 7 = 0 \iff x = 7$</td>
</tr>
</tbody>
</table>
Proposition

• If $x$ is a real number and $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$. 
Proposition

- If \( x \) is a real number and \( x^3 - 7x^2 + x - 7 = 0 \), then \( x = 7 \).

Proof

- We factorize the expression.
  \[
  x^3 - 7x^2 + x - 7 = x^2(x - 7) + (x - 7) \quad \text{(taking } x^2 \text{ factor from first two terms)}
  = (x - 7)(x^2 + 1) \quad \text{(taking } (x - 7) \text{ factor)}
  = (x - 7)(x + i)(x - i) \quad \text{(factorizing } (x^2 + 1)\text{)}
  \]
  (this is because \((x + i)(x - i) = (x^2 - i^2) = (x^2 + 1)\))

So, the three roots to the equation \( x^3 - 7x^2 + x - 7 = 0 \) are \( x = 7, x = -\sqrt{-1}, \) and \( x = \sqrt{-1} \).

As \( x \) has to be a real number, \( x = 7 \).
Proof by Counterexample
Proposition

- For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$. 

Solution

False! Counterexample: $a = 1$ and $b = -1$.

In this example, $a^2 = b^2$ but $a \neq b$. 
Proposition

- For all real numbers \( a \) and \( b \), if \( a^2 = b^2 \), then \( a = b \).

Solution

- False! Counterexample: \( a = 1 \) and \( b = -1 \).
  In this example, \( a^2 = b^2 \) but \( a \neq b \).
<table>
<thead>
<tr>
<th>Proposition</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.</td>
<td>• False! Counterexample: $a = 1$ and $b = -1$. In this example, $a^2 = b^2$ but $a \neq b$.</td>
</tr>
<tr>
<td>Proposition</td>
<td></td>
</tr>
<tr>
<td>• For all nonzero integers $a$ and $b$, if $a</td>
<td>b$ and $b</td>
</tr>
<tr>
<td>Proposition</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>• For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False! Counterexample: $a = 1$ and $b = -1$. In this example, $a^2 = b^2$ but $a \neq b$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For all nonzero integers $a$ and $b$, if $a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False! Counterexample: $a = 1$ and $b = -1$. In this example, $a</td>
</tr>
<tr>
<td>Proposition</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>$2^n + 1$ is prime for any natural number $n$.</td>
</tr>
</tbody>
</table>
## Proposition

- $2^n + 1$ is prime for any natural number $n$.

## Workout

- **Write a formal statement.**
  \[ \forall \text{ natural number } n, \ 2^n + 1 \text{ is prime.} \]
- **Try out a few examples.**
  \[
  \begin{align*}
  2^1 + 1 &= 3 & \text{prime} \\
  2^2 + 1 &= 5 & \text{prime} \\
  2^3 + 1 &= 9 = 3^2 & \text{composite}
  \end{align*}
  \]
- **Find a pattern.**
  $2^n + 1$ can be either prime or composite.
**Proposition**

- $2^n + 1$ is prime for any natural number $n$.

**Workout**

- **Write a formal statement.**
  \[ \forall \text{ natural number } n, \ 2^n + 1 \text{ is prime.} \]

- **Try out a few examples.**
  \[
  \begin{align*}
  2^1 + 1 &= 3 & \text{prime} \\
  2^2 + 1 &= 5 & \text{prime} \\
  2^3 + 1 &= 9 = 3^2 & \text{composite}
  \end{align*}
  \]

- **Find a pattern.**
  $2^n + 1$ can be either prime or composite.

**Solution**

- **False!** Counterexample: $n = 3$
  When $n = 3$, then $2^n + 1 = 2^3 + 1 = 9 = 3^2$ is composite.
\[ n^2 + n + 41 \]

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ( n^2 + n + 41 ) is prime for any whole number ( n ).</td>
</tr>
</tbody>
</table>
### Proposition

- \( n^2 + n + 41 \) is prime for any whole number \( n \).

### Workout

- **Write a formal statement.**
  \[ \forall \text{ whole number } n, \ n^2 + n + 41 \text{ is prime.} \]
- **Try out a few examples.**
  
  \[
  \begin{align*}
  0^2 + 0 + 41 & = 41 & \text{prime} \\
  1^2 + 1 + 41 & = 43 & \text{prime} \\
  2^2 + 2 + 41 & = 47 & \text{prime} \\
  3^2 + 3 + 41 & = 53 & \text{prime} \\
  4^2 + 4 + 41 & = 61 & \text{prime} \\
  5^2 + 5 + 41 & = 71 & \text{prime}
  \end{align*}
  \]
- **Find a pattern.**
  It seems like \( n^2 + n + 41 \) is always prime.
Proposition

- $n^2 + n + 41$ is prime for any whole number $n$. 

Solution: False!

Formal statement: $\forall$ whole numbers $n$, $n^2 + n + 41$ is prime.

Counterexample: 41.

$(41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \times 43)$

Another counterexample: 40.

$(40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41(40 + 1) = 41 \times 41)$
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $n^2 + n + 41$ is prime for any whole number $n$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False!</td>
</tr>
<tr>
<td>• Formal statement. $\forall$ whole numbers $n$, $n^2 + n + 41$ is prime.</td>
</tr>
<tr>
<td>• Counterexample: 41.</td>
</tr>
<tr>
<td>$$(41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \times 43)$$</td>
</tr>
<tr>
<td>• Another counterexample: 40.</td>
</tr>
<tr>
<td>$$(40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41(40 + 1) = 41 \times 41)$$</td>
</tr>
</tbody>
</table>
\[ \frac{x}{y + z} + \frac{y}{x + z} + \frac{z}{x + y} \]

**Proposition**

\[ \frac{x}{y + z} + \frac{y}{x + z} + \frac{z}{x + y} = 4 \] has no positive integer solutions.
Proposition

\[
\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4 \text{ has no positive integer solutions.}
\]

Workout

- **Write a formal statement.**
  \[
  \forall \ x, y, z \in \mathbb{N}, \ x/(y + z) + y/(x + z) + z/(x + y) \neq 4.
  \]

- **Try out a few examples.**
  
  \[
  (x, y, z) \quad x/(y + z) + y/(x + z) + z/(x + y) = 4 \ ?
  \]

  \[
  (1, 1, 1) \quad 1/2 + 1/2 + 1/2 = 1.5 \neq 4
  \]

  \[
  (1, 2, 1) \quad 1/3 + 2/2 + 1/3 = 1.666\cdots \neq 4
  \]

  \[
  (1, 2, 3) \quad 1/5 + 2/4 + 3/3 = 1.7 \neq 4
  \]

  \[
  (1, 10, 100) \quad 1/110 + 10/101 + 100/11 = 9.199\cdots \neq 4
  \]

- **Find a pattern.**

  It seems like there are no \(+ve\) integers satisfying the property.
\[ \frac{x}{y + z} + \frac{y}{x + z} + \frac{z}{x + y} = 4 \]

**Proposition**

- \( \frac{x}{y + z} + \frac{y}{x + z} + \frac{z}{x + y} = 4 \) has no positive integer solutions.

**Solution**

- **False!**
- **Counterexample:**

\[
\begin{align*}
x &= 15447680210874616644195131501991983748566432566 \\
&\quad 9565431700026634898253202035277999 \\
y &= 36875131794129999827197811565225474825492979968 \\
&\quad 971970996283137471637224634055579 \\
z &= 37361267792869725786125260237139015281653755816 \\
&\quad 1613618621437993378423467772036
\end{align*}
\]
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For whole numbers $n$, $1211 \cdots 1$ is composite.</td>
</tr>
</tbody>
</table>

$\underbrace{n \text{ terms}}$
### Proposition

- For whole numbers $n$, $1211 \cdots 1$ is composite.

### Workout

- **Try out a few examples.**

<table>
<thead>
<tr>
<th>$(n, \text{Number})$</th>
<th>Factorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0,12)$</td>
<td>$3 \times 4$</td>
</tr>
<tr>
<td>$(1,121)$</td>
<td>$11 \times 11$</td>
</tr>
<tr>
<td>$(2,1211)$</td>
<td>$7 \times 173$</td>
</tr>
<tr>
<td>$(3,12111)$</td>
<td>$33 \times 367$</td>
</tr>
<tr>
<td>$(4,121111)$</td>
<td>$281 \times 431$</td>
</tr>
<tr>
<td>$(5,1211111)$</td>
<td>$253 \times 4787$</td>
</tr>
</tbody>
</table>

- **Find a pattern.**
  
  It seems like the sequence of numbers is composite.
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For whole numbers $n \geq 0$, $1211 \cdot \ldots \cdot 1$ is composite.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False!</td>
</tr>
<tr>
<td>• Smallest counterexample: $n = 136$.</td>
</tr>
</tbody>
</table>

$$12,111111111, 1111111111, 11111111111, 111111111111, 1111111111111, 11111111111111, 111111111111111, 1111111111111111 \text{ is prime.}$$
Proof by Contraposition
Proposition

- If $n^2$ is odd, then $n$ is odd.
$n^2$ is odd $\implies n$ is odd

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If $n^2$ is odd, then $n$ is odd.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • Seems very difficult to prove directly.  
  Contraposition: If $n$ is even, then $n^2$ is even.  
  
  $n$ is even  
  $\implies n = 2k$ (defn. of even, $k$ is an integer)  
  $\implies n^2 = (2k)^2$ (squaring on both sides)  
  $\implies n^2 = 4k^2$ (simplifying)  
  $\implies n^2 = 2(2k^2)$ (factoring 2)  
  $\implies n^2 = 2j$ (let $j = 2k^2$)  
  $\implies n^2$ is even ($j$ is an integer as mult. is closed on integers) (defn. of even)  
  $\implies n^2$ is even |
Proposition

- The square of an integer is odd if and only if the integer itself is odd.
**Proposition**

- The square of an integer is odd if and only if the integer itself is odd.

<table>
<thead>
<tr>
<th>Odd numbers</th>
<th>Even numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 1)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(3, 9)</td>
<td>(2, 4)</td>
</tr>
<tr>
<td>(5, 25)</td>
<td>(4, 16)</td>
</tr>
<tr>
<td>(7, 49)</td>
<td>(6, 36)</td>
</tr>
</tbody>
</table>

**Workout**

- Write a formal statement.
  \( \forall \text{ integer } n, \ n^2 \text{ is odd } \iff \ n \text{ is odd.} \)
- Try out a few examples.
  - Pattern. It seems that the proposition is true.
### Proposition

- The square of an integer is odd if and only if the integer itself is odd.

### Proof

There are two parts in the proof.

1. Prove that if \( n \) is odd, then \( n^2 \) is odd.
   - Direct proof

2. Prove that if \( n^2 \) is odd, then \( n \) is odd.
   - Proof by contraposition
Corollary

- Prove that the fourth power of an integer is odd if and only if the integer itself is odd.
### Corollary

- Prove that the fourth power of an integer is odd if and only if the integer itself is odd.

### Proof

- We have
  
  \[
  n \text{ is odd } \iff n^2 \text{ is odd} \quad \text{(previous theorem)}
  \]
  
  \[
  \implies n^2 \text{ is odd } \iff n^4 \text{ is odd} \quad \text{(previous theorem used on } n^2) 
  \]
  
  \[
  \implies n \text{ is odd } \iff n^4 \text{ is odd} \quad \text{(transitivity of biconditional)}
  \]
<table>
<thead>
<tr>
<th>Corollary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove that the fourth power of an integer is odd if and only if the integer itself is odd.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• We have</td>
</tr>
</tbody>
</table>
| \[
\begin{align*}
\text{n is odd } & \iff \text{n}^2 \text{ is odd} & \text{(previous theorem)} \\
\implies & \text{n}^2 \text{ is odd } \iff \text{n}^4 \text{ is odd} & \text{(previous theorem used on n}^2) \\
\implies & \text{n is odd } \iff \text{n}^4 \text{ is odd} & \text{(transitivity of biconditional)}
\end{align*}
\] |

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Suppose (k) is a whole number. Prove that an integer (n) is odd if and only if (n^{2^k}) is odd.</td>
</tr>
</tbody>
</table>
Proposition

- For all integers \( n \), if \( n^2 \) is even, then \( n \) is even.
Proposition

For all integers $n$, if $n^2$ is even, then $n$ is even.

Proof

- **Contrapositive.** For all integers, if $n$ is odd, then $n^2$ is odd.

  - $n = 2k + 1$ (definition of odd number)
  
    \[ n^2 = (2k + 1)^2 \]  
    
    (squaring both sides)
  
    \[ n^2 = 4k^2 + 4k + 1 \]  
    
    (expand)
  
    \[ n^2 = 2(2k^2 + 2k) + 1 \]  
    
    (taking 2 out from two terms)
  
    \[ n^2 = 2m + 1 \]  
    
    (set $m = 2k^2 + 2k$)
  
    (m is an integer as multiplication is closed on integers)
  
    \[ n^2 = \text{odd} \]  
    
    (definition of odd number)

- Hence, the proposition is true.
Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x \neq 10$. 

Proof

Contrapositive. If $x = 10$, then $x^3 - 7x^2 + x - 7 \neq 0$.

Substitute $x = 10$ in the expression.

We get $10^3 - 7(10^2) + 10 - 7 = 1000 - 700 + 10 - 7 = 303 \neq 0$.

That is, $x = 10$ does not satisfy $x^3 - 7x^2 + x - 7 = 0$ equation.

Hence, the contraposition is correct which implies that the original statement is correct.
# Polynomial root

## Proposition

- If \( x^3 - 7x^2 + x - 7 = 0 \), then \( x \neq 10 \).

## Proof

- **Contrapositive.** If \( x = 10 \), then \( x^3 - 7x^2 + x - 7 \neq 0 \)
  
  Substitute \( x = 10 \) in the expression.
  
  We get \( 10^3 - 7(10^2) + 10 - 7 = 1000 - 700 + 10 - 7 = 303 \neq 0 \).
  
  That is, \( x = 10 \) does not satisfy \( x^3 - 7x^2 + x - 7 = 0 \) equation.

  Hence, the contraposition is correct which implies that the original statement is correct.
Proposition

Let $a, b, n \in \mathbb{Z}$. If $n \nmid ab$, then $n \nmid a$ and $n \nmid b$. 

\begin{align*}
\text{Proof} \quad & \text{Contrapositive. Let } a, b, n \in \mathbb{Z}. \text{ If } n \mid a \text{ or } n \mid b, \text{ then } n \mid ab. \\
& n \mid a \iff a = nc \text{ (for some } c \in \mathbb{Z}) \\
& \Rightarrow ab = (nc)b = n(cb) \text{ (multiply by } b) \\
& \Rightarrow n \mid ab \text{ (definition of divisibility)} \\
& n \mid b \iff b = nd \text{ (for some } d \in \mathbb{Z}) \\
& \Rightarrow ab = a(nd) = n(ad) \text{ (multiply by } a) \\
& \Rightarrow n \mid ab \text{ (definition of divisibility)} \\
\end{align*} 

Hence, the proposition is true.
Proposition

Let $a, b, n \in \mathbb{Z}$. If $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.

Proof

- **Contrapositive.** Let $a, b, n \in \mathbb{Z}$. If $n \mid a$ or $n \mid b$, then $n \mid ab$.
  
  - $n \mid a$
    
    $\implies a = nc$  
    
    $\implies ab = (nc)b = n(cb)$  
    
    $\implies n \mid ab$  
    
    (for some $c \in \mathbb{Z}$)
    
    (multiply by $b$)
    
    (definition of divisibility)
  
  - $n \mid b$
    
    $\implies b = nd$  
    
    $\implies ab = a(nd) = n(ad)$  
    
    $\implies n \mid ab$  
    
    (for some $d \in \mathbb{Z}$)
    
    (multiply by $a$)
    
    (definition of divisibility)

- Hence, the proposition is true.
Proposition

- Let $n \in \mathbb{Z}$. If $n^2 - 6n + 5$ is even, then $n$ is odd.
\[ n^2 - 6n + 5 \text{ is even} \iff n \text{ is odd} \]

**Proposition**

- Let \( n \in \mathbb{Z} \). If \( n^2 - 6n + 5 \) is even, then \( n \) is odd.

**Proof**

- **Contrapositive.** If \( n \) is even, then \( n^2 - 6n + 5 \) is odd.
- \( n \) is even
  
  \[ \implies n = 2a \text{ for some integer } a \]  
  \[ \text{(defn. of even)} \]
  
  \[ \implies n^2 - 6n + 5 = (2a)^2 - 6(2a) + 5 \]  
  \[ \text{(substitute } n = 2a) \]
  
  \[ \implies n^2 - 6n + 5 = 2(2a^2) - 2(6a) + 2(2) + 1 \]  
  \[ \text{(simplify)} \]
  
  \[ \implies n^2 - 6n + 5 = 2(2a^2 - 6a + 2) + 1 \]  
  \[ \text{(take 2 common)} \]
  
  \[ \implies n^2 - 6n + 5 \text{ is odd} \]  
  \[ \text{(defn. of odd)} \]

- Hence, the proposition is true.
For reals $x$ and $y$, if $xy > 9$, then either $x > 3$ or $y > 3$. 

Incorrect! Why?
Proposition

- For reals $x$ and $y$, if $xy > 9$, then either $x > 3$ or $y > 3$.

Proof

- **Contrapositive.** If $x \leq 3$ and $y \leq 3$, then $xy \leq 9$.
- Suppose $x \leq 3$ and $y \leq 3$.
  \[ \Rightarrow xy \leq 9 \]  (multiply the two inequalities)
- Hence, the proposition is true.
Proposition

- For reals $x$ and $y$, if $xy > 9$, then either $x > 3$ or $y > 3$.

Proof

- **Contrapositive.** If $x \leq 3$ and $y \leq 3$, then $xy \leq 9$.
- Suppose $x \leq 3$ and $y \leq 3$.
  \[
  \implies xy \leq 9
  \]
  (multiply the two inequalities)
- Hence, the proposition is true.

- Incorrect! Why?
Nonconstructive Proof
An irrational raised to an irrational power may be rational.
Proposition

- An irrational raised to an irrational power may be rational.

Proof

- We make use of the fact that $\sqrt{2}$ is irrational.

  Let $x = \sqrt{2}^{\sqrt{2}}$. Number $x$ is either rational or irrational.

  Case 1. If $x$ is rational, then the proposition is true.

<table>
<thead>
<tr>
<th>Irrational</th>
<th>Irrational</th>
<th>Rational</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sqrt{2}$</td>
<td>$\sqrt{2}$</td>
<td>$\sqrt{2}^{\sqrt{2}} = x = \text{rational}$</td>
</tr>
</tbody>
</table>

  Case 2. If $x$ is irrational, then the proposition is true.

<table>
<thead>
<tr>
<th>Irrational</th>
<th>Irrational</th>
<th>Rational</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$\sqrt{2}$</td>
<td>$x^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2^2} = 2$</td>
</tr>
</tbody>
</table>
Proof by Contradiction
Proposition

- For all integers $n$, if $n^2$ is even, then $n$ is even.
Proposition

- For all integers $n$, if $n^2$ is even, then $n$ is even.

Proof

- Negation. Suppose there is an integer $n$ such that $n^2$ is even but $n$ is odd.
- $n = 2k + 1$  
  \[\Rightarrow n^2 = (2k + 1)^2\]  
  \[\Rightarrow n^2 = 4k^2 + 4k + 1\]  
  \[\Rightarrow n^2 = 2(2k^2 + 2k) + 1\]  
  \[\Rightarrow n^2 = 2m + 1\]  
  (setting $m = 2k^2 + 2k$)  
  ($m$ is an integer as multiplication is closed on integers)  
  \[\Rightarrow n^2 = \text{odd}\]  
  (definition of odd number)

- Contradiction! Hence, the proposition is true.
Proposition

- There is no greatest integer.
## Greatest integer

### Proposition
- There is no greatest integer.

### Proof
- **Negation.** Suppose there is a greatest integer \( N \).
  
  Then \( N \geq n \) for every integer \( n \).
  
  Let \( M = N + 1 \).
  
  \( M \) is an integer since addition is closed on integers.
  
  \( M > N \) since \( M = N + 1 \).
  
  \( M \) is an integer that is greater than \( N \).
  
  So, \( N \) is not the greatest integer.
  
  Contradiction! Hence, the proposition is true.
\( \sqrt{2} \) is irrational

**Proposition**

- \( \sqrt{2} \) is irrational.
\( \sqrt{2} \) is irrational

### Proposition

- \( \sqrt{2} \) is irrational.

### Proof

- Suppose \( \sqrt{2} \) is the simplest rational.
  - \( \implies \sqrt{2} = m/n \) \( (m, n \text{ have no common factors, } n \neq 0) \)
  - \( \implies m^2 = 2n^2 \) \( \text{(squaring and simplifying)} \)
  - \( \implies m^2 = \text{even} \) \( \text{(definition of even)} \)
  - \( \implies m = \text{even} \) \( \text{(why?)} \)
  - \( \implies m = 2k \) for some integer \( k \) \( \text{(definition of even)} \)
  - \( \implies (2k)^2 = 2n^2 \) \( \text{(substitute } m) \)
  - \( \implies n^2 = 2k^2 \) \( \text{(simplify)} \)
  - \( \implies n^2 = \text{even} \) \( \text{(definition of even)} \)
  - \( \implies n = \text{even} \) \( \text{(why?)} \)
  - \( \implies m, n \text{ are even} \) \( \text{(previous results)} \)
  - \( \implies m, n \text{ have a common factor of 2} \) \( \text{(definition of even)} \)
- Contradiction! Hence, the proposition is true.
If \( p | n \), then \( p \nmid (n + 1) \).

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For any integer ( n ) and any prime ( p ), if ( p</td>
</tr>
</tbody>
</table>
### Proposition

- For any integer \( n \) and any prime \( p \), if \( p \mid n \), then \( p \nmid (n + 1) \).

### Proof

- **Negation.** Suppose there exists integer \( n \) and prime \( p \) such that \( p \mid n \) and \( p \mid (n + 1) \).
  - \( p \mid n \) implies \( pr = n \) for some integer \( r \)
  - \( p \mid (n + 1) \) implies \( ps = n + 1 \) for some integer \( s \)

Eliminate \( n \) to get:

\[
1 = (n + 1) - n = ps - pr = p(s - r)
\]

Hence, \( p \mid 1 \), from the definition of divisibility.

As \( p \mid 1 \), we have \( p \leq 1 \). \((\text{why?})\)

As \( p \) is prime, \( p > 1 \).

Contradiction! Hence, the proposition is true.
#Primes is infinite

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The set of prime numbers is infinite.</td>
</tr>
</tbody>
</table>
### Proposition

- The set of prime numbers is infinite.

### Proof

- **Negation.** Assume that there are only finite number of primes.
  Let the set of primes be \( \{p_1, p_2, \ldots, p_n\} \)
  such that \( p_1 = 2 \) \(<\) \( p_2 = 3 \) \(<\cdots\)< \( p_n \).
  Consider the number \( N = p_1 p_2 p_3 \cdots p_n + 1 \). Clearly, \( N > 1 \).
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The set of prime numbers is infinite.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • **Negation.** Assume that there are only finite number of primes. Let the set of primes be \( \{p_1, p_2, \ldots, p_n\} \) such that \( p_1 = 2 < p_2 = 3 < \cdots < p_n \). Consider the number \( N = p_1p_2p_3 \ldots p_n + 1 \). Clearly, \( N > 1 \).  
  (i) There is a prime that divides \( N \).  
Use **unique prime factorization theorem**.
Proposition

- The set of prime numbers is infinite.

Proof

- **Negation.** Assume that there are only finite number of primes. Let the set of primes be \( \{p_1, p_2, \ldots, p_n\} \) such that \((p_1 = 2) < (p_2 = 3) < \cdots < p_n\).

Consider the number \( N = p_1p_2p_3\ldots p_n + 1 \). Clearly, \( N > 1 \).

(i) There is a prime that divides \( N \).

Use **unique prime factorization theorem**.

(ii) No prime divides \( N \).

For all \( i \in [1, n] \), \( p_i \) does not divide \( N \) as it leaves a remainder of 1 when it divides \( N \).

So, \( p_1 \nmid N, p_2 \nmid N, \ldots, p_n \nmid N \).

Contradiction! Hence, the proposition is true.
**Proposition**

- If $a_1, a_2, \ldots, a_n$ are $n$ real numbers for natural number $n$, then at least one of these $n$ numbers is greater than or equal to the average of those $n$ numbers.
**Proposition**

- If $a_1, a_2, \ldots, a_n$ are $n$ real numbers for natural number $n$, then at least one of these $n$ numbers is greater than or equal to the average of those $n$ numbers.

**Proof**

- Average $A = (a_1 + a_2 + \cdots + a_n)/n$
- **Negation.** $\forall i \in \{1, 2, \ldots, n\}$ $a_i < A$. That is
- We have $a_1 < A$, $a_2 < A$, $\ldots$, $a_n < A$
### Proposition

- If $a_1, a_2, \ldots, a_n$ are $n$ real numbers for natural number $n$, then at least one of these $n$ numbers is greater than or equal to the average of those $n$ numbers.

### Proof

- Average $A = (a_1 + a_2 + \cdots + a_n)/n$
- **Negation.** $\forall i \in \{1, 2, \ldots, n\}$ $a_i < A$. That is $a_1 < A$, $a_2 < A$, $\ldots$, $a_n < A$
- We have $a_1 < A$, $a_2 < A$, $\ldots$, $a_n < A$
  - Now add all these inequalities to get $(a_1 + a_2 + \cdots + a_n) < n \times A$
  - $\Rightarrow A > (a_1 + a_2 + \cdots + a_n)/n$ on simplification
  - How is it possible that $A$ is both equal to and greater than $(a_1 + a_2 + \cdots + a_n)/n$
- **Contradiction!** Hence, the proposition is true.
If $a_1, a_2, \ldots, a_n$ are $n$ real numbers for natural number $n$, then at least one of these $n$ numbers is greater than or equal to the average of those $n$ numbers.
### Average

#### Proposition

- If \( a_1, a_2, \ldots, a_n \) are \( n \) real numbers for natural number \( n \), then at least one of these \( n \) numbers is greater than or equal to the average of those \( n \) numbers.

#### Proof

- Let \( a_{\text{max}} \) represent the maximum among the \( n \) real numbers.
- Let average \( A = (a_1 + a_2 + \cdots + a_n)/n \). Then
## Proposition

- If \( a_1, a_2, \ldots, a_n \) are \( n \) real numbers for natural number \( n \), then at least one of these \( n \) numbers is greater than or equal to the average of those \( n \) numbers.

## Proof

- Let \( a_{\text{max}} \) represent the maximum among the \( n \) real numbers.
- Let average \( A = \frac{(a_1 + a_2 + \cdots + a_n)}{n} \). Then
- \( a_1 = a_{\text{max}} - b_1 \) such that \( b_1 \geq 0 \)
  \[ a_2 = a_{\text{max}} - b_2 \] such that \( b_2 \geq 0 \)
  \[ \vdots \]
  \[ a_n = a_{\text{max}} - b_n \] such that \( b_n \geq 0 \)
### Average

#### Proposition

- If \( a_1, a_2, \ldots, a_n \) are \( n \) real numbers for natural number \( n \), then at least one of these \( n \) numbers is greater than or equal to the average of those \( n \) numbers.

#### Proof

- Let \( a_{\text{max}} \) represent the maximum among the \( n \) real numbers.
- Let average \( A = (a_1 + a_2 + \cdots + a_n)/n \). Then
- \( a_1 = a_{\text{max}} - b_1 \) such that \( b_1 \geq 0 \)
- \( a_2 = a_{\text{max}} - b_2 \) such that \( b_2 \geq 0 \)
- \( \ldots \)
- \( a_n = a_{\text{max}} - b_n \) such that \( b_n \geq 0 \)

Adding the above equations, we get

\[
(a_1 + a_2 + \cdots + a_n) = n \times a_{\text{max}} - (b_1 + b_2 + \cdots + b_n)
\]

\[
\implies a_{\text{max}} = [(a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n)]/n
\]

\[
= ((a_1 + a_2 + \cdots + a_n)/n) + ((b_1 + b_2 + \cdots + b_n)/n)
\]

\[
= A + ((b_1 + b_2 + \cdots + b_n)/n)
\]

\[
\geq A \quad (\forall i, b_i \geq 0)
\]
$2^p - 1$ is prime $\iff p$ is prime

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then $p$ is prime.</td>
</tr>
</tbody>
</table>
### Proposition

- Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then $p$ is prime.

### Proof

- **Negation.** Suppose $p$ is an integer at least 2 such that $2^p - 1$ is prime and $p$ is composite.
Proposition

Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then $p$ is prime.

Proof

• **Negation.** Suppose $p$ is an integer at least 2 such that $2^p - 1$ is prime and $p$ is composite.

  • $p$ is composite

    $\implies p = rs$ such that both $r, s$ are in the range $[2, p - 1]$

    Then, $2^p - 1$

    $= 2^{rs} - 1$ (substitute for $p$)

    $= (2^r)^s - 1$ ($a^{bc} = (a^b)^c$)

    $= (2^r - 1) \left( \frac{(2^r)^s - 1}{2^r - 1} \right)$ (multiply and divide by $(2^r - 1) > 0$)

    $= (2^r - 1) \left( 1 + (2^r)^1 + (2^r)^2 + \cdots + (2^r)^{s-1} \right)$

    $= m \times n$ ($m \geq 2$ and $n \geq 2$)

• Contradiction! Hence, the proposition is true.
Proposition

- For integers \(a, b, c\), if \(a^2 + b^2 = c^2\), then \(a\) is even or \(b\) is even.
Pythagorean triplets

**Proposition**

For integers $a, b, c$, if $a^2 + b^2 = c^2$, then $a$ is even or $b$ is even.

**Proof**

- **Negation.** $a$ and $b$ are odd and $a^2 + b^2 = c^2$.

Consider $a^2 + b^2 = (2m + 1)^2 + (2n + 1)^2 = 4m^2 + 4n^2 + 4m + 4n + 2$ (expand)

$\equiv 2 \mod 4$ (remainder is 2 when divided by 4)

$c^2 = 4k^2$ or $4(k^2 + k) + 1$ (squaring)

$\not\equiv 2 \mod 4$ (remainder is never 2 when divided by 4)

Contradiction! Hence, the proposition is true.
### Pythagorean triplets

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For integers $a, b, c$, if $a^2 + b^2 = c^2$, then $a$ is even or $b$ is even.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • **Negation.** $a$ and $b$ are odd and $a^2 + b^2 = c^2$.  
• $a = 2m + 1; b = 2n + 1$ (definition of odd)  
  Consider $a^2 + b^2$  
  $= (2m + 1)^2 + (2n + 1)^2$  
  $= 4m^2 + 4n^2 + 4m + 4n + 2$ (expand)  
  $= 4 \times (m^2 + n^2 + m + n) + 2$ (take common factor)  
  $\equiv 2 \mod 4$ (remainder is 2 when divided by 4) |
Pythagorean triplets

**Proposition**
- For integers \( a, b, c \), if \( a^2 + b^2 = c^2 \), then \( a \) is even or \( b \) is even.

**Proof**
- **Negation.** \( a \) and \( b \) are odd and \( a^2 + b^2 = c^2 \).
- \( a = 2m + 1; \ b = 2n + 1 \) (definition of odd)
  - Consider \( a^2 + b^2 \)
    \[ = (2m + 1)^2 + (2n + 1)^2 \]
    \[ = 4m^2 + 4n^2 + 4m + 4n + 2 \]
    \[ = 4 \times (m^2 + n^2 + m + n) + 2 \] (expand)
    \[ \equiv 2 \mod 4 \] (remainder is 2 when divided by 4)
- \( c = 2k \) or \( c = 2k + 1 \) (quotient-remainder theorem)
  - Consider \( c^2 \)
    \[ = 4k^2 \) or \( 4(k^2 + k) + 1 \) (squaring)
    \[ \not\equiv 2 \mod 4 \] (remainder is never 2 when divided by 4)
- **Contradiction!** Hence, the proposition is true.
Proof by Division into Cases
Proposition

- There is a natural number $n$ such that $n^2 + 3n + 2$ is prime.

Proof 2

- False!
- Negation. $\forall$ natural number $n$, $n^2 + 3n + 2$ is composite.
  We prove the negation in two cases:
  1. $n$ is even
  2. $n$ is odd
Proof 2 (continued)

1. **Prove that** $n$ **is even** $\implies n^2 + 3n + 2$ **is composite.**
   - $n$ **is even**
   - $\implies n^2$ **is even** and $3n$ **is even** (even $\times$ integer $=$ even)
   - $\implies n^2 + 3n + 2$ **is even** (even $+$ even $=$ even)
   - $\implies n^2 + 3n + 2$ **is composite** (2 is a factor)

2. **Prove that** $n$ **is odd** $\implies n^2 + 3n + 2$ **is composite.**
   - $n$ **is odd**
   - $\implies n^2$ **is odd** and $3n$ **is odd** (odd $\times$ odd $=$ odd)
   - $\implies n^2 + 3n$ **is even** (odd $+$ odd $=$ even)
   - $\implies n^2 + 3n + 2$ **is even** (even $+$ even $=$ even)
   - $\implies n^2 + 3n + 2$ **is composite** (2 is a factor)
Proof 2 (continued)

1. Prove that $n$ is even $\implies n^2 + 3n + 2$ is composite.

   - $n$ is even
     $\implies n^2$ is even and $3n$ is even \hspace{1cm} (even $\times$ integer $=$ even)
     $\implies n^2 + 3n + 2$ is even \hspace{1cm} (even + even $=$ even)
     $\implies n^2 + 3n + 2$ is composite \hspace{1cm} (2 is a factor)

2. Prove that $n$ is odd $\implies n^2 + 3n + 2$ is composite.

   - $n$ is odd
     $\implies n^2$ is odd and $3n$ is odd \hspace{1cm} (odd $\times$ odd $=$ odd)
     $\implies n^2 + 3n$ is even \hspace{1cm} (odd + odd $=$ even)
     $\implies n^2 + 3n + 2$ is even \hspace{1cm} (even + even $=$ even)
     $\implies n^2 + 3n + 2$ is composite \hspace{1cm} (2 is a factor)

Proposition

- Use this approach to prove that for all natural number $n$,
  
  $9n^4 - 7n^3 + 5n^2 - 3n + 10$ is composite.
Proposition

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

$\text{Odd}^2 = 8m + 1$
### Proposition

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

### Proof

- $n$ is odd
  
  $\implies n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$
  
  ($n$ can be written in one of the four forms using the quotient-remainder theorem)

  But, $n \neq 4q$ and $n \neq 4q + 2$ (as $4q$ and $4q + 2$ are even)

  Hence, $n = 4q + 1$ or $n = 4q + 3$.

- **Case 1.** $n = 4q + 1$.
  
  $\implies n^2 = (4q + 1)^2 = 8(2q^2 + q) + 1 = 8m + 1$, where $m = 2q^2 + q = \text{integer}$.

- **Case 2.** $n = 4q + 3$.
  
  $\implies n^2 = (4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8m + 1$, where $m = 2q^2 + 3q + 1 = \text{integer}$.
Proposition

- There is no solution in integers to: $(x^2 - y^2) \mod 4 \neq 2$. 
Proposition

- There is no solution in integers to: \((x^2 - y^2) \mod 4 = 2\).

Proof

- **Case 1.** \(x\) is even and \(y\) is even.
  \[\implies x^2 = 4m \quad \text{and} \quad y^2 = 4n\]
  \[\implies x^2 - y^2 = 4(m - n).\]

- **Case 2.** \(x\) is even and \(y\) is odd.
  \[\implies x^2 = 4m \quad \text{and} \quad y^2 = 4n + 1\]
  \[\implies x^2 - y^2 = 4(m - n) - 1.\]

- **Case 3.** \(x\) is odd and \(y\) is even.
  \[\implies x^2 = 4m + 1 \quad \text{and} \quad y^2 = 4n\]
  \[\implies x^2 - y^2 = 4(m - n) + 1.\]

- **Case 4.** \(x\) is odd and \(y\) is odd.
  \[\implies x^2 = 4m + 1 \quad \text{and} \quad y^2 = 4n + 1\]
  \[\implies x^2 - y^2 = 4(m - n).\]

- In all these four cases, \((x^2 - y^2) \mod 4 \neq 2\).
Prove or disprove the following propositions:

- If more than \( n \) pigeons fly into \( n \) pigeon holes for natural number \( n \), then at least one pigeon hole will contain at least two pigeons. [Hint: Contradiction.]
- \( \frac{1}{\sqrt{2}} \) is irrational. [Hint: Contradiction.]
- \( \sqrt{3} \) is irrational. [Hint: Contradiction.]
- \( \sqrt{6} \) is irrational. [Hint: Contradiction.]
- \( \log_2 3 \) is irrational. [Hint: Contradiction.]
- \( \log_2 7 \) is irrational. [Hint: Contradiction.]
- For all integers \( a \) and \( b \), if \( ab \) is a multiple of 6, then \( a \) is even and \( b \) is a multiple of 3. [Hint: Counterexample.]
- There are no integers \( a \) and \( b \) such that \( 752b = 4183 - 326a \). [Hint: Contradiction.]
- \( a^n + b^n = c^n \) has no integral solutions for all natural numbers \( n \geq 1 \). [Hint: Counterexample.]
- Suppose \( p \in \mathbb{N} \) and \( p \geq 2 \). If \( 2^p - 1 \) is prime, then \( p \) is prime. [Hint: Contraposition.]
Prove or disprove the following propositions:

• For integers $a, b, c$, if $a^2 + b^2 = c^2$, then $a$ is even or $b$ is even. [Hint: Contraposition + division into cases.]
• There are 1000 consecutive natural numbers that are not perfect squares. [Hint: Direct proof.]
• Consider any ten prime numbers that are greater than or equal to 15. Then the sum of these prime numbers can never be $(1 \text{ trillion } + 1)$. [Hint: Direct proof, contradiction.]
• Let $n$ be a positive integer. Prove that the closed interval $[n, 2n]$ contains a power of 2. [Hint: Division into cases (power of 2 and not a power of 2).]
Prove or disprove the following propositions:

- **Rational + rational = rational.** [Hint: Direct proof.]
- **Rational + irrational = irrational.** [Hint: Contradiction.]
- **Irrational + irrational = rational or irrational.** [Hint: Examples. \(\sqrt{2} + (-\sqrt{2}) = 0\) and \(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \sqrt{2}\).]
- **Rational \times rational = rational.** [Hint: Direct proof.]
- **Rational \times irrational = rational or irrational.** [Hint: Examples. \(0 \times \sqrt{2} = 0\) and \(1 \times \sqrt{2} = \sqrt{2}\).]
- **Nonzero rational \times irrational = irrational.** [Hint: Contradiction.]
- **Irrational \times irrational = rational or irrational.** [Hint: Examples. \(\sqrt{2} \times \sqrt{2} = 2\) and \(\sqrt{2} \times \sqrt{2} = \sqrt{6}\).]
- **Rational^{rational} = rational or irrational.** [Hint: Examples \(1^1 = 1\) and \(2^{1/2} = \sqrt{2}\).]
Bogus Proofs
Prove 1 = 2 using basic algebra

Proof
- $a > 0, b > 0$  ▶️ Given
- $a = b$  ▶️ Given
- $ab = b^2$  ▶️ Multiply both sides by $b$
- $ab - a^2 = b^2 - a^2$  ▶️ Subtract $a^2$ from both sides
- $a(b - a) = (b + a)(b - a)$  ▶️ Factoring
- $a = b + a$  ▶️ Divide both sides by $(b - a)$
- $0 = b$  ▶️ Subtract $a$ from both sides
- $b = 2b$  ▶️ Add $b$ to both sides
- $1 = 2$  ▶️ Divide both sides by $b$

What is the problem with this proof?

Error
- Cannot divide by 0 in mathematics
- Cannot divide by $(b - a)$ as $a = b$
Prove 1 = 2 using basic algebra

Proof

• $a > 0, b > 0$ ▷ Given
• $a = b$ ▷ Given
• $ab = b^2$ ▷ Multiply both sides by $b$
• $ab - a^2 = b^2 - a^2$ ▷ Subtract $a^2$ from both sides
• $a(b - a) = (b + a)(b - a)$ ▷ Factoring
• $a = b + a$ ▷ Divide both sides by $(b - a)$
• $0 = b$ ▷ Subtract $a$ from both sides
• $b = 2b$ ▷ Add $b$ to both sides
• $1 = 2$ ▷ Divide both sides by $b$

What is the problem with this proof?

Error

• Cannot divide by 0 in mathematics
• Cannot divide by $(b - a)$ as $a = b$
Prove \(1 = 2\) using basic algebra

**Proof**

- \(n^2 + 2n + 1 = (n + 1)^2\)  \(\triangleright \) Expand
- \(n^2 = (n + 1)^2 - (2n + 1)\)  \(\triangleright \) Subtract
- \(n^2 - n(2n + 1) = (n + 1)^2 - (2n + 1) - n(2n + 1)\)  \(\triangleright \) Subtract
- \(n^2 - n(2n + 1) = (n + 1)^2 - (n + 1)(2n + 1)\)  \(\triangleright \) Factoring
- \(n^2 - n(2n + 1) + (2n + 1)^2/4 = (n + 1)^2 - (n + 1)(2n + 1) + (2n + 1)^2/4\)  \(\triangleright \) Add
- \((n - (2n + 1)/2)^2 = ((n + 1) - (2n + 1)/2)^2\)  \(\triangleright \) Simplify
- \(n - (2n + 1)/2 = (n + 1) - (2n + 1)/2\)  \(\triangleright \) Square roots
- \(n = n + 1\)  \(\triangleright \) Add
- \(1 = 2\)  \(\triangleright \) Subtract

**What is the problem with this proof?**
Prove 1 = 2 using basic algebra

Proof

- \( n^2 + 2n + 1 = (n + 1)^2 \)
- \( n^2 = (n + 1)^2 - (2n + 1) \)
- \( n^2 - n(2n + 1) = (n + 1)^2 - (2n + 1) - n(2n + 1) \) ▶ Subtract
- \( n^2 - n(2n + 1) = (n + 1)^2 - (n + 1)(2n + 1) \) ▶ Factoring
- \( n^2 - n(2n + 1) + (2n + 1)^2/4 = (n + 1)^2 - (n + 1)(2n + 1) + (2n + 1)^2/4 \) ▶ Add
- \( (n - (2n + 1)/2)^2 = ((n + 1) - (2n + 1)/2)^2 \) ▶ Simplify
- \( n - (2n + 1)/2 = (n + 1) - (2n + 1)/2 \) ▶ Square roots
- \( n = n + 1 \)
- \( 1 = 2 \)
- What is the problem with this proof?

Error

- Cannot take square roots directly
- \( a^2 = b^2 \) does not imply \( a = b \)
- E.g.: \( 1^2 = (-1)^2 \) does not imply \( 1 = -1 \)
### Prove 1 = 2 using calculus

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $\int u dv = uv - \int v du$ &gt; Product rule</td>
</tr>
<tr>
<td>• Set $u = \frac{1}{x}$ and $v = x$; We get $du = -\frac{1}{x^2} dx$ and $dv = dx$</td>
</tr>
<tr>
<td>• $\int \frac{1}{x} dx = x \cdot \frac{1}{x} - \int x \cdot \left(-\frac{1}{x^2}\right) dx$ &gt; Substitute</td>
</tr>
<tr>
<td>• $\int \frac{1}{x} dx = 1 + \int \frac{1}{x} dx$ &gt; Simplify</td>
</tr>
<tr>
<td>• $0 = 1$ &gt; Subtract</td>
</tr>
<tr>
<td>• $1 = 2$ &gt; Add</td>
</tr>
<tr>
<td>• What is the problem with this proof?</td>
</tr>
</tbody>
</table>

Error

Cannot subtract integrals from both sides

$\int dx = x + \text{const.}$ \> const. depends on conditions

E.g.: $\int \left(\frac{1}{x^2} + 1\right) dx = \int \left(\frac{1}{x^2} + 2\right) dx$ does not imply

$\int \frac{1}{x} dx = 1 + \int \frac{1}{x} dx$
### Proof

- \( \int u \, dv = uv - \int v \, du \) \hspace{1cm} \( \triangleright \) Product rule
- Set \( u = \frac{1}{x} \) and \( v = x \); We get \( du = -\frac{1}{x^2} \, dx \) and \( dv = dx \)
- \( \int \frac{1}{x} \, dx = x \cdot \frac{1}{x} - \int x \cdot \left( -\frac{1}{x^2} \right) \, dx \) \hspace{1cm} \( \triangleright \) Substitute
- \( \int \frac{1}{x} \, dx = 1 + \int \frac{1}{x} \, dx \) \hspace{1cm} \( \triangleright \) Simplify
- \( 0 = 1 \) \hspace{1cm} \( \triangleright \) Subtract
- \( 1 = 2 \) \hspace{1cm} \( \triangleright \) Add
- What is the problem with this proof?

### Error

- Cannot subtract integrals from both sides
- \( \int dx = x + \text{const.} \) \hspace{1cm} \( \triangleright \) const. depends on conditions
  - E.g.: \( \frac{d}{dx} (x + 1) = \frac{d}{dx} (x + 2) \) does not imply
  - \( \int \frac{d}{dx} (x + 1) = \int \frac{d}{dx} (x + 2) \)
Prove 1 = 2 using algebra and calculus

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $x \neq 0$</td>
</tr>
<tr>
<td>• $x = x$</td>
</tr>
<tr>
<td>• $x + x = 2x$</td>
</tr>
<tr>
<td>• $x + x + \cdots + x = x^2$ $\quad \uparrow$ Repeatedly add $x$ times</td>
</tr>
<tr>
<td>• $1 + 1 + \cdots + 1 = 2x$ $\quad \uparrow$ Differentiate</td>
</tr>
<tr>
<td>• $x = 2x$ $\quad \uparrow$ Simplify</td>
</tr>
<tr>
<td>• $1 = 2$ $\quad \uparrow$ Divide</td>
</tr>
</tbody>
</table>

• What is the problem with this proof?
Prove 1 = 2 using algebra and calculus

**Proof**
- \( x \neq 0 \)  
- \( x = x \)  
- \( x + x = 2x \)  
- \( x + x + \cdots + x = x^2 \) \( x \) times  
- \( 1 + 1 + \cdots + 1 = 2x \) \( x \) times  
- \( x = 2x \)  
- \( 1 = 2 \)  
- **What is the problem with this proof?**

**Error**
- Cannot write \( x + x + \cdots + x = x^2 \) for non-integers \( x \) times  
- E.g.: Cannot write \( 1.5 + 1.5 + \cdots + 1.5 = 1.5^2 \) \( 1.5 \) times
Prove 1 = 2 using continued fractions

Proof

1 = \frac{2}{3-1} = \frac{2}{3-\frac{2}{3-1}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-1}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-1}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\ldots}}}}}

2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-2}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-2}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\ldots}}}}}

1 = 2 \quad \triangleright \quad \text{Continued fractions are the same}

What is the problem with this proof?
### Prove 1 = 2 using continued fractions

#### Proof

<table>
<thead>
<tr>
<th>1 = \frac{2}{3-1} = \frac{2}{3-\frac{2}{3-1}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-1}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-1}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-1}}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-...}}}}}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-2}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-2}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-2}}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-...}}}}}}</td>
</tr>
</tbody>
</table>

- 1 = 2

▶ Continued fractions are the same

- What is the problem with this proof?

#### Error

- Cannot equate the values of the continued fractions
- The given continued fraction is \(x = \frac{2}{3-x}\)
  Solving for \(x\), we have \(x = 1\) or \(x = 2\)
- Beware of infinity!
Prove 1 = 2 using infinite series

Proof

- Consider Grandi’s series $S = 1 - 1 + 1 - 1 + \cdots$
- $S = (1 - 1) + (1 - 1) + \cdots = 0 + 0 + \cdots = 0$
- $S = 1 + (-1 + 1) + (-1 + 1) + \cdots = 1 + 0 + 0 + \cdots = 1$
- $0 = 1$ \(\triangleright S = 0\) and $S' = 1$
- $1 = 2$ \(\triangleright\) Add
- What is the problem with this proof?

Error

- Cannot use several algebraic methods on a divergent series
- Grandi’s series is divergent
- Beware of infinity!
Prove 1 = 2 using infinite series

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • Consider Grandi’s series $S = 1 - 1 + 1 - 1 + \cdots$
| • $S = (1 - 1) + (1 - 1) + \cdots = 0 + 0 + \cdots = 0$
| • $S = 1 + (-1 + 1) + (-1 + 1) + \cdots = 1 + 0 + 0 + \cdots = 1$
| • $0 = 1$ \hspace{1cm} △ $S = 0$ and $S' = 1$
| • $1 = 2$ \hspace{1cm} △ Add
| • What is the problem with this proof? |

<table>
<thead>
<tr>
<th>Error</th>
</tr>
</thead>
</table>
| • Cannot use several algebraic methods on a divergent series
| • Grandi’s series is divergent
| • Beware of infinity! |
Proof

- Using Georg Cantor’s set theory and his idea of one-to-one correspondence, we can show that the number of points on the number line segment $[0, 1]$ is same as the number of points on the number line segment $[0, 2]$
- $1 = 2$
- What is the problem with this proof?
Proof

- Using Georg Cantor’s set theory and his idea of one-to-one correspondence, we can show that the number of points on the number line segment \([0, 1]\) is same as the number of points on the number line segment \([0, 2]\)
- \(1 = 2\)
- What is the problem with this proof?

Error

- Solution is out of scope
- The problem is because the principles that apply in the world of finite quantities do not apply in the world of infinite quantities
- Beware of infinity!
Prove $1 = 2$ using geometry

Proof

- Banach-Tarski paradox states that a solid ball can be split into a finite number of disjoint subsets, which can then be assembled to create two identical copies of the original solid ball.

$$
\begin{array}{c}
\text{blue ball} \\
\rightarrow \\
\text{red ball} + \\
\text{red ball}
\end{array}
$$

- $1 = 2$
- What is the problem with this proof?
**Prove $1 = 2$ using geometry**

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banach-Tarski paradox states that a solid ball can be split into a finite number of disjoint subsets, which can then be assembled to create two identical copies of the original solid ball.</td>
</tr>
<tr>
<td><img src="image" alt="Banach-Tarski diagram" /></td>
</tr>
<tr>
<td>$1 = 2$</td>
</tr>
<tr>
<td><strong>What is the problem with this proof?</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solution is out of scope</strong></td>
</tr>
<tr>
<td>The problem is because the principles that apply in the world of finite quantities do not apply in the world of infinite quantities.</td>
</tr>
<tr>
<td><strong>Beware of infinity!</strong></td>
</tr>
</tbody>
</table>
• **History.** The theorem first appeared in a Babylonian tablet dated 1900-1600 B.C.

• **Incorrect proofs.** Alexander Bogomolny’s website [Cut-The-Knot](https://www.cut-the-knot.org/pythagoras/FalseProofs.shtml) presents 9 incorrect proofs of the theorem.

• **Correct proofs.** Elisha Scott Loomis’ book “The Pythagorean Proposition” presents 367 correct proofs of the theorem (algebraic proofs + geometric proofs + trigonometric proofs).

• **More Proofs.** An infinite number of algebraic and geometric proofs exist for the theorem (Proof?)