CSE 215: Foundations of Computer Science
(Proof Techniques)

Pramod Ganapathithi
Department of Computer Science
State University of New York at Stony Brook

August 26, 2020
# What is a proof?

- **Definition**

A **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>
What is a mathematical proof?

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A <strong>mathematical proof</strong> is a verification for establishing the truth of a proposition by a chain of logical deductions from a set of axioms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concepts</th>
</tr>
</thead>
</table>
| 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:**
  - $10$, $-56.47$, $10/13$, $0$, $-17/9$, $0.121212\ldots$, $-91\ldots$
- **Irrational numbers:**
  - $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2^2}$, $\pi$, $\phi$, $e$, $\pi^2$, $e^2$, $2^{1/3}$, $\log_2 3$, $\ldots$
- **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
  \[
  n = qd + r \quad \text{and} \quad r \in [0, d - 1]
  \]

**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>
</tbody>
</table>
# Prime numbers

<table>
<thead>
<tr>
<th>Num.</th>
<th>Factorization</th>
<th>Prime?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2 = 1 \times 2 = 2 \times 1$</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>$3 = 1 \times 3 = 3 \times 1$</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>$4 = 1 \times 4 = 4 \times 1 = 2 \times 2$</td>
<td>✗</td>
</tr>
<tr>
<td>5</td>
<td>$5 = 1 \times 5 = 5 \times 1$</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>
</tr>
<tr>
<td>7</td>
<td>$7 = 1 \times 7 = 7 \times 1$</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>
</tr>
<tr>
<td>9</td>
<td>$9 = 1 \times 9 = 9 \times 1 = 3 \times 3$</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>
</tr>
<tr>
<td>11</td>
<td>$11 = 1 \times 11 = 11 \times 1$</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>
</tr>
<tr>
<td>13</td>
<td>$13 = 1 \times 13 = 13 \times 1$</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>
</tr>
<tr>
<td>15</td>
<td>$15 = 1 \times 15 = 15 \times 1 = 3 \times 5 = 5 \times 3$</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>
</tr>
<tr>
<td>17</td>
<td>$17 = 1 \times 17 = 17 \times 1$</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, …
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 \( n > 1 \),

\[
\text{n is prime } \iff \forall \text{ natural numbers } r \text{ and } s, \text{ if } n = rs \text{ then } n = r \text{ or } n = s
\]

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 \( n > 1 \),

\[
\text{n is composite } \iff \exists \text{ natural numbers } r \text{ and } s, \text{ if } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n
\]
## Unique prime factorization of natural numbers

<table>
<thead>
<tr>
<th>$n$</th>
<th>Unique prime factorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>$2^2$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>$2 \times 3$</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>$2^3$</td>
</tr>
<tr>
<td>9</td>
<td>$3^2$</td>
</tr>
<tr>
<td>10</td>
<td>$2 \times 5$</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>$2^2 \times 3$</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>14</td>
<td>$2 \times 7$</td>
</tr>
<tr>
<td>15</td>
<td>$3 \times 5$</td>
</tr>
<tr>
<td>16</td>
<td>$2^4$</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>18</td>
<td>$2 \times 3^2$</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>20</td>
<td>$2^2 \times 5$</td>
</tr>
<tr>
<td>21</td>
<td>$3 \times 7$</td>
</tr>
<tr>
<td>22</td>
<td>$2 \times 11$</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>24</td>
<td>$2^3 \times 3$</td>
</tr>
<tr>
<td>25</td>
<td>$5^2$</td>
</tr>
<tr>
<td>26</td>
<td>$2 \times 13$</td>
</tr>
<tr>
<td>27</td>
<td>$3^3$</td>
</tr>
<tr>
<td>28</td>
<td>$2^2 \times 7$</td>
</tr>
<tr>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>30</td>
<td>$2 \times 3 \times 5$</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>32</td>
<td>$2^5$</td>
</tr>
<tr>
<td>33</td>
<td>$3 \times 11$</td>
</tr>
<tr>
<td>34</td>
<td>$2 \times 17$</td>
</tr>
<tr>
<td>35</td>
<td>$5 \times 7$</td>
</tr>
<tr>
<td>36</td>
<td>$6^2$</td>
</tr>
<tr>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>38</td>
<td>$2 \times 19$</td>
</tr>
<tr>
<td>39</td>
<td>$3 \times 13$</td>
</tr>
<tr>
<td>40</td>
<td>$2^3 \times 5$</td>
</tr>
<tr>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>42</td>
<td>$2 \times 3 \times 7$</td>
</tr>
<tr>
<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 primes 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
  
  $$ \lceil x \rceil = \text{unique integer } n \text{ such that } n - 1 < x \leq n $$
  
  $$ \lceil x \rceil = n \iff n - 1 < x \leq n $$
Some terms

Definitions

- Given an integer \( n \) and a natural number \( d \),
  \( n \text{ div } d = \) integer quotient obtained when \( n \) is divided by \( d \),
  \( n \text{ mod } d = \) whole number remainder obtained when \( n \) is divided by \( d \).
- Symbolically,
  \( n \text{ div } d = q \) and \( n \text{ mod } d = r \iff n = dq + r \)
  where \( q \) and \( r \) are integers and \( 0 \leq r < d \).
Problems, Problems, Problems
Even + odd = odd

**Proposition**

- Sum of an even integer and an odd integer is odd.

Proof:

Suppose $a$ is even and $b$ is odd. Then

$$a + b = (2m) + b (\text{defn. of even, } a = 2m \text{ for integer } m)$$

$$= (2m) + (2n + 1) (\text{defn. of odd, } b = 2n + 1 \text{ for integer } n)$$

$$= 2(m + n) + 1 (\text{taking } 2 \text{ as common factor})$$

$$= 2p + 1 (p = m + n \text{ and addition is closed on integers})$$

$$= \text{odd (defn. of odd)}$$
Proposition

- Sum of an even integer and an odd integer is odd.

Proof

- Suppose $a$ is even and $b$ is odd. Then
  
  \[
  a + b \\
  = (2m) + b \quad \text{(defn. of even, } a = 2m \text{ for integer } m) \\
  = (2m) + (2n + 1) \quad \text{(defn. of odd, } b = 2n + 1 \text{ for integer } n) \\
  = 2(m + n) + 1 \quad \text{(taking 2 as common factor)} \\
  = 2p + 1 \quad (p = m + n \text{ and addition is closed on integers}) \\
  = \text{odd} \quad \text{(defn. of odd)}
  \]
### Propositions

Prove the following propositions:
- Sum of two even integers is even
- Sum of two odd integers is even
- Product of two even integers is even
- Product of an even integer and an odd integer is even
- Product of two odd integers is odd
Proposition

- For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$. 
\begin{itemize}
\item For all real numbers \(a\) and \(b\), if \(a^2 = b^2\), then \(a = b\).
\end{itemize}

\begin{itemize}
\item False!
\item Let \(a = 1\) and \(b = -1\).
\item Then, \(a^2 = b^2\). However, \(a \neq b\).
\item This proof style is called the \textbf{proof by counterexample}.
\end{itemize}
Proposition

• For all real numbers $a$ and $b$, if $a|b$ and $b|a$, then $a = b$. 
For all real numbers $a$ and $b$, if $a | b$ and $b | a$, then $a = b$.

Proof

- **False!**
  
  Let $a = 1$ and $b = -1$.
  
  Then, $a | b$ and $b | a$. However, $a \neq b$. 
Proposition

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

\[ \frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4 \]

has no positive integer solutions.

Workout

• Write a formal statement.
  \[ \forall \text{ integers } x, y, z, \frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} \neq 4. \]
• Try out a few examples.
  \begin{align*}
  (x, y, z) & \quad x/(y + z) + y/(x + z) + z/(x + y) = 4 ? \\
  (0, 1, 1) & \quad 0/2 + 1/1 + 1/1 = 2 \neq 4 \\
  (0, 2, 3) & \quad 0/5 + 2/3 + 3/2 = 13/6 \neq 4 \\
  (1, 1, 1) & \quad 1/2 + 1/2 + 1/2 = 3/2 \neq 4 \\
  (1, 2, 1) & \quad 1/3 + 2/2 + 1/3 = 5/3 \neq 4 \\
  \end{align*}
• Find a pattern.
  It seems like there are no +ve integers satisfying the property.
\[
x/(y+z) + y/(x+z) + z/(x+y)
\]

**Proposition**

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

**Proof**

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

  \[
  x = 15447680210874616644195131501991983748566432566 \\
  9565431700026634898253202035277999 \\
  y = 36875131794129999827197811565225474825492979968 \\
  971970996283137471637224634055579 \\
  z = 37361267792869725786125260237139015281653755816 \\
  1613618621437993378423467772036
  \]
### Proposition

- For whole numbers $n \geq 0$, $1211 \cdots 1$ is composite.  

\[ \text{\{ } n \text{ terms } \]
### Proposition

- For whole numbers $n \geq 0$, $\underbrace{1211 \cdots 1}_{n \text{ terms}}$ 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.
Proposition

• For whole numbers $n \geq 0$, $12\underbrace{11\ldots 1}_{n \text{ terms}}$ is composite.

Proof

• False!
• Smallest counterexample: $n = 136$.

$12,1111111111,1111111111,1111111111,1111111111,$
$1111111111,1111111111,1111111111,1111111111,$
$1111111111,1111111111,1111111111,1111111111,$
$1111111111,1111111111$ is prime.
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Every odd integer is equal to the difference between the squares of two integers</td>
</tr>
<tr>
<td>Proposition</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>• Every odd integer is equal to the difference between the squares of two integers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workout</th>
</tr>
</thead>
</table>
| • 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.  
   \[
   \begin{align*}
   1 &= 1^2 - 0^2 & -1 &= 0^2 - (-1)^2 \\
   3 &= 2^2 - 1^2 & -3 &= (-1)^2 - (-2)^2 \\
   5 &= 3^2 - 2^2 & -5 &= (-2)^2 - (-3)^2 \\
   7 &= 4^2 - 3^2 & -7 &= (-3)^2 - (-4)^2 \\
   \end{align*}
   \]
| • 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.
  \[
  2k + 1 = (k^2 + 2k + 1) - k^2
  \]
  \[
  = (k + 1)^2 - k^2
  \]
  \[
  = m^2 - n^2
  \]
  (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

\[ k^2 \text{ cells} \]

\[ \downarrow \]

\[ k \]

\[ (k + 1)^2 \text{ cells} \]
## Properties of a proof

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise</td>
<td>(not unnecessarily long)</td>
</tr>
<tr>
<td>Clear</td>
<td>(not ambiguous)</td>
</tr>
<tr>
<td>Complete</td>
<td>(no missing intermediate steps)</td>
</tr>
<tr>
<td>Logical</td>
<td>(every statement logically follows)</td>
</tr>
<tr>
<td>Rigorous</td>
<td>(uses mathematical expressions)</td>
</tr>
<tr>
<td>Convincing</td>
<td>(does not raise questions)</td>
</tr>
<tr>
<td>The way a proof is</td>
<td>presented might be different from the way</td>
</tr>
<tr>
<td>the proof is</td>
<td>discovered.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Proposition

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

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

### Proof

- Substitute \( x = 10 \) in the expression.
  We get \( 10^3 - 7(10^2) + 10 - 7 = 1000 - 700 + 10 - 7 = 303 \neq 0 \).
  As \( x = 10 \) does not satisfy \( x^3 - 7x^2 + x - 7 = 0 \) equation, we have \( x \neq 10 \).
## Proposition

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

---

In the proof, we substitute \( x = 7 \) into the equation to get:

\[
x^3 - 7x^2 + x - 7 = 7^3 - 7(7^2) + 7 - 7 = 0.
\]

As \( x \) satisfies the equation, we conclude that \( x = 7 \).

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, $x = 7$. 

Incorrect! What's wrong?
### 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

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.

\[ x^3 - 7x^2 + x - 7 = x^2(x - 7) + (x - 7) \text{ (taking } x^2 \text{ factor from first two terms)} \]

\[ = (x - 7)(x^2 + 1) \text{ (taking } (x - 7) \text{ factor)} \]

\[ = (x - 7)(x + i)(x - i) \text{ (factorizing } (x^2 + 1) \text{)} \]

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 $x = \sqrt{-1}$. 
Polynomial root

**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>
</tbody>
</table>
| \[
\begin{align*}
  x &= 7 &\implies& x^3 - 7x^2 + x - 7 &= 0 \\
  x^3 - 7x^2 + x - 7 &= 0 &\iff& x &= 7
\end{align*}
\] |
Proposition

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

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If ( x ) is a real number and ( x^3 - 7x^2 + x - 7 = 0 ), then ( x = 7 ).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • We factorize the expression.  
\[
x^3 - 7x^2 + x - 7 = x^2(x - 7) + (x - 7) \quad \text{(taking \( x^2 \) factor from first two terms)}
\]
\[
= (x - 7)(x^2 + 1) \quad \text{(taking \( (x - 7) \) 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, \( x = 7 \).
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.

Workout

• Write a formal statement.
  \( \forall \text{ integer } n, \ n^2 \text{ is odd } \iff n \text{ is odd.} \)

• Try out a few examples.

<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>

• Pattern. It seems that the proposition is true.
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>The square 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>There are two parts in the proof.</td>
</tr>
<tr>
<td>1. Prove that if $n$ is odd, then $n^2$ is odd.</td>
</tr>
<tr>
<td>2. Prove that if $n^2$ is odd, then $n$ is odd.</td>
</tr>
</tbody>
</table>
\[ n \text{ is odd } \iff n^2 \text{ is odd} \]

**Proof (continued)**

1. **Prove that if \( n \) is odd, then \( n^2 \) is odd.**

   \( n \) is odd

   \[ \implies n = (2k + 1) \quad \text{(defn. of odd, } k \text{ is an integer)} \]

   \[ \implies n^2 = (2k + 1)^2 \quad \text{(squaring on both sides)} \]

   \[ \implies n^2 = 4k^2 + 4k + 1 \quad \text{(expanding the binomial)} \]

   \[ \implies n^2 = 2(2k^2 + 2k) + 1 \quad \text{(factoring 2 from first two terms)} \]

   \[ \implies n^2 = 2j + 1 \quad \text{(let } j = 2k^2 + 2k) \]

   \[ (j \text{ is an integer as mult. and add. are closed on integers)} \]

   \[ \implies n^2 \text{ is odd} \quad \text{(defn. of odd)} \]
2. Prove that if \( n^2 \) is odd, then \( n \) is odd.

Seems very difficult to prove directly.

Contraposition: If \( n \) is even, then \( n^2 \) is even.

\[
\begin{align*}
n & \text{ is even} \\
\implies n & = 2k & \text{(defn. of even, } k \text{ is an integer)} \\
\implies n^2 & = (2k)^2 & \text{(squaring on both sides)} \\
\implies n^2 & = 4k^2 & \text{(simplifying)} \\
\implies n^2 & = 2(2k^2) & \text{(factoring 2)} \\
\implies n^2 & = 2j & \text{(let } j = 2k^2) \\
\end{align*}
\]

\((j \text{ is an integer as mult. is closed on integers})\)

\[
\implies n^2 \text{ is even} & \quad \text{(defn. of even)}
\]

This proof is called the 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
  
  \[ n \text{ is odd } \iff n^2 \text{ is odd} \]  
  (previous theorem)

  \[ \implies n^2 \text{ is odd } \iff n^4 \text{ is odd} \]  
  (previous theorem used on \( n^2 \))

  \[ \implies n \text{ is odd } \iff n^4 \text{ is odd} \]  
  (transitivity of biconditional)
### Corollary

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

### Proof

- We have:
  
  $n$ is odd $\iff n^2$ is odd $\iff n^4$ is odd (previous theorem)

  $\implies n^2$ is odd $\iff n^4$ is odd (previous theorem used on $n^2$)

  $\implies n$ is odd $\iff n^4$ is odd (transitivity of biconditional)

### Problem

- Suppose $k$ is a whole number. Prove that an integer $n$ is odd if and only if $n^{2k}$ is odd.
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<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.
  \[
  2^1 + 1 = 3 \quad \text{prime} \\
  2^2 + 1 = 5 \quad \text{prime} \\
  2^3 + 1 = 9 = 3^2 \quad \text{composite}
  \]
- Find a pattern.
  $2^n + 1$ can be either prime or composite.
<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $2^n + 1$ is prime for any natural number $n$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • False!  
When $n = 3$, $2^n + 1 = 2^3 + 1 = 9 = 3^2$ is composite.  
• This proof style is called the proof by counterexample. |
Proposition

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

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

---

**Workout**

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

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False! $2^{999} + 1$ is composite.</td>
</tr>
<tr>
<td>• $2^{999} + 1$</td>
</tr>
<tr>
<td>= $(2^{333})^3 + 1^3$ (terms represented as cubes)</td>
</tr>
<tr>
<td>= $a^3 + b^3$ (set $a = 2^{333}$, $b = 1$)</td>
</tr>
<tr>
<td>= $(a + b)(a^2 - ab + b^2)$ (factorize $a^3 + b^3$)</td>
</tr>
<tr>
<td>= $(2^{333} + 1)(2^{666} - 2^{333} + 1)$ (substituting $a$ and $b$ values)</td>
</tr>
<tr>
<td>= composite</td>
</tr>
</tbody>
</table>
**Proposition**

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

**Workout**

Write a formal statement.

$\forall$ whole number $n$, $n^2 + n + 41$ is prime.

Try out a few examples.

- $0^2 + 0 + 41 = 41$ prime
- $1^2 + 1 + 41 = 43$ prime
- $2^2 + 2 + 41 = 47$ prime
- $3^2 + 3 + 41 = 53$ prime
- $4^2 + 4 + 41 = 61$ prime

Find a pattern.

It seems like $n^2 + n + 41$ is always prime.
<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>Workout</th>
</tr>
</thead>
</table>
| • Write a formal statement.  
  $\forall$ whole number $n$, $n^2 + n + 41$ is prime. |
| • Try out a few examples. |
| 0$^2 + 0 + 41 = 41$ | prime |
| 1$^2 + 1 + 41 = 43$ | prime |
| 2$^2 + 2 + 41 = 47$ | prime |
| 3$^2 + 3 + 41 = 53$ | prime |
| 4$^2 + 4 + 41 = 61$ | prime |
| 5$^2 + 5 + 41 = 71$ | prime |
| • Find a pattern.  
  It seems like $n^2 + n + 41$ is always prime. |
Proposition

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

Proof

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.

($40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41(40 + 1)$)
$n^2 + n + 41$

<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>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • **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.  
  $(40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41(40 + 1) = 41 \times 41)$ |
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.
  \[
  \begin{align*}
  1^2 + 3(1) + 2 &= 6 \quad \text{composite} \\
  2^2 + 3(2) + 2 &= 12 \quad \text{composite} \\
  3^2 + 3(3) + 2 &= 20 \quad \text{composite} \\
  4^2 + 3(4) + 2 &= 30 \quad \text{composite} \\
  5^2 + 3(5) + 2 &= 42 \quad \text{composite}
  \end{align*}
  \]
- 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.

Proof

- 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.
- \[
  n^2 + 3n + 2 = n^2 + n + 2n + 2 \quad \text{(split 3n)}
  \]
  \[
  = n(n + 1) + 2(n + 1) \quad \text{(taking common factors)}
  \]
  \[
  = (n + 1)(n + 2) \quad \text{(distributive law)}
  \]
  \[
  = \text{composite} \quad (n + 1 > 1 \text{ and } n + 2 > 1)
  \]
- This proof style is called **proof by negation.**
**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
- This proof style is called proof by division into cases.
**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)
Proof 2 (continued)

1. Prove that \( n \) is even \( \Rightarrow \) \( n^2 + 3n + 2 \) is composite.

   \[ n \text{ is even} \]
   \[ \quad \Rightarrow \quad n^2 \text{ is even and } 3n \text{ is even} \quad (\text{even } \times \text{ integer } = \text{ even}) \]
   \[ \quad \Rightarrow \quad n^2 + 3n + 2 \text{ is even} \quad (\text{even } + \text{ even } = \text{ even}) \]
   \[ \quad \Rightarrow \quad n^2 + 3n + 2 \text{ is composite} \quad (2 \text{ is a factor}) \]

2. Prove that \( n \) is odd \( \Rightarrow \) \( n^2 + 3n + 2 \) is composite.

   \[ n \text{ is odd} \]
   \[ \quad \Rightarrow \quad n^2 \text{ is odd and } 3n \text{ is odd} \quad (\text{odd } \times \text{ odd } = \text{ odd}) \]
   \[ \quad \Rightarrow \quad n^2 + 3n \text{ is even} \quad (\text{odd } + \text{ odd } = \text{ even}) \]
   \[ \quad \Rightarrow \quad n^2 + 3n + 2 \text{ is even} \quad (\text{even } + \text{ even } = \text{ even}) \]
   \[ \quad \Rightarrow \quad n^2 + 3n + 2 \text{ is composite} \quad (2 \text{ is a factor}) \]

Proposition

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

• (Transitivity) For integers $a, b, c$, if $a | b$ and $b | c$, then $a | c$.  

If $a|b$ and $b|c$, then $a|c$

**Proposition**

- (Transitivity) For integers $a, b, c$, if $a|b$ and $b|c$, then $a|c$.

**Proof**

- Formal statement.
  \[ \forall \text{ integers } a, b, c, \text{ if } a|b \text{ and } b|c, \text{ then } a|c. \]
- $c$
  
  \[
  \begin{align*}
  &= bn \\
  &= (am)n \\ 
  &= a(mn) \\
  &= ak \\
  \implies a|c
  \end{align*}
  \]

  ($b|c$ and definition of divisibility)

  ($a|b$ and definition of divisibility)

  (multiplication is associative)

  (let $k = mn$ and multiplication is closed on integers)

  (definition of divisibility and $k$ is an integer)
### Problems

- **Handshakes.** During a college party, students shake hands with other students. What is the minimum number of students the party should have to achieve 100 handshakes?
- **Citations.** A scientist publishes research papers in a totally new field that nobody understands. He wants to get as many citations as possible for his papers but nobody cites his papers because his work is in a completely new field. Let’s assume that no one cites the scientist’s papers except himself. What is the minimum number of papers that the scientist has to publish to achieve 100 citations?
Let $n = \#\text{persons}$ and $H(n) = \#\text{handshakes}$

Try out a few examples.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$H(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0 + 1</td>
</tr>
<tr>
<td>3</td>
<td>0 + 1 + 2</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$n$</td>
<td>$0 + 1 + 2 + 3 + \cdots + (n - 1)$</td>
</tr>
</tbody>
</table>

Find a pattern.

It seems like $n$ people/papers can be used to obtain $\sum_{1}^{n-1} i$ handshakes/citations.
### Summation

**Workout**

- Let $n = \#\text{persons}$ and $H(n) = \#\text{handshakes}$
- **Try out a few examples.**

<table>
<thead>
<tr>
<th>$n$</th>
<th>$H(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$0 = \frac{0 \times 1}{2}$</td>
</tr>
<tr>
<td>2</td>
<td>$0 + 1 = \frac{1 \times 2}{2}$</td>
</tr>
<tr>
<td>3</td>
<td>$0 + 1 + 2 = \frac{2 \times 3}{2}$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$n$</td>
<td>$0 + 1 + 2 + 3 + \cdots + (n - 1) = \frac{(n-1) \times n}{2}$</td>
</tr>
</tbody>
</table>

- **Find a pattern.**
  It seems like $n$ people/papers can be used to obtain $n(n - 1)/2$ handshakes/citations.
Summation

Proposition

\[ 1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}. \]
**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{1cm} (adding the previous two equations)

  $\implies 2S = n(n + 1)$  
  (simplifying)

  $\implies S = n(n + 1)/2$  
  (divide both sides by 2)
Proposition

- 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.

\[
\begin{array}{|c|c|c|}
\hline
\text{Irrational} & \text{Irrational} & \text{Rational} \\
\hline
\sqrt{2} & \sqrt{2} & \sqrt{2}^{\sqrt{2}} = x = \text{rational} \\
\hline
\end{array}
\]

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

\[
\begin{array}{|c|c|c|}
\hline
\text{Irrational} & \text{Irrational} & \text{Rational} \\
\hline
x & \sqrt{2} & x^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2^2} = 2 \\
\hline
\end{array}
\]

- This proof style is called the nonconstructive proof.
Greatest integer

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• There is no greatest integer.</td>
</tr>
</tbody>
</table>
## Greatest integer

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• There is no greatest integer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| • **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.
• This proof style is called **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.

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

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

- $\sqrt{2}$ is irrational.
\[ \sqrt{2} \text{ is irrational} \]

**Proposition**

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

**Proof**

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

**Proposition**

- For any integer \( a \) and any prime \( p \), if \( p | a \), then \( p \nmid (a + 1) \).
If $p|a$, then $p \nmid (a + 1)$.

**Proposition**

- For any integer $a$ and any prime $p$, if $p|a$, then $p \nmid (a + 1)$.

**Proof**

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

  Eliminate $a$ to get:
  
  $1 = (a + 1) - a = ps - pr = p(s - r)$

  Hence, $p|1$, from the definition of divisibility.

  As $p|1$, we have $p \leq 1$.

  As $p$ is prime, $p > 1$.

  Contradiction! Hence, the proposition is true.
Proposition

- The set of prime numbers is infinite.
# 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>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
</table>
| **Negation.** Suppose the set of prime numbers is finite. Let \( p \) be the largest of all the prime numbers. 

Set of primes be \( \{2, 3, 5, 7, 11, \ldots, p\} \)

Let \( n = (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p) + 1 \).

As \( n > 1 \), \( q \mid n \) for some prime \( q \). (why?)

Because \( q \) is prime, \( q \) must be present in the set of primes.

\( q \mid (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p) \) by the definition of divisibility.

\( q \nmid (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p) + 1 \). (why?)

So, \( q \nmid n \).

It is not possible that both \( q \mid n \) and \( q \nmid n \) are true.

Contradiction! Hence, the proposition is true.
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.

This proof style is called proof by contraposition.
\( \text{Proposition} \)

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

\( \text{Proof} \)

- **Contrapositive.** For all integers, if \( n \) is odd, then \( n^2 \) is odd.
  
  \[
  n = 2k + 1 \quad \text{(definition of odd number)}
  \]
  \[
  \implies n^2 = (2k + 1)^2 \quad \text{(squaring both sides)}
  \]
  \[
  \implies n^2 = 4k^2 + 4k + 1 \quad \text{(expand)}
  \]
  \[
  \implies n^2 = 2(2k^2 + 2k) + 1 \quad \text{(taking 2 out from two terms)}
  \]
  \[
  \implies n^2 = 2m + 1 \quad \text{(set } m = 2k^2 + 2k) \]
  \[
  \quad \left(m \text{ is an integer as multiplication is closed on integers}\right)
  \]
  \[
  \implies n^2 = \text{odd} \quad \text{(definition of odd number)}
  \]

- Hence, the proposition is true.

- This proof style is called **proof by contraposition**.
$n \mid ab \implies n \mid a \text{ and } n \mid b$

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Let $a, b, n \in \mathbb{Z}$. If $n \mid ab$, then $n \mid a$ and $n \mid b$.</td>
</tr>
<tr>
<td>Proposition</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Let $a, b, n \in \mathbb{Z}$. If $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contrapositive.</strong> Let $a, b, n \in \mathbb{Z}$. If $n</td>
</tr>
<tr>
<td>**$n</td>
</tr>
<tr>
<td>$\implies a = nc$ (for some $c \in \mathbb{Z}$)</td>
</tr>
<tr>
<td>$\implies ab = (nc)b = n(cb)$ (multiply by $b$)</td>
</tr>
<tr>
<td>$\implies n</td>
</tr>
<tr>
<td>**$n</td>
</tr>
<tr>
<td>$\implies b = nd$ (for some $d \in \mathbb{Z}$)</td>
</tr>
<tr>
<td>$\implies ab = a(nd) = n(ad)$ (multiply by $a$)</td>
</tr>
<tr>
<td>$\implies n</td>
</tr>
<tr>
<td><strong>Hence, the proposition is true.</strong></td>
</tr>
</tbody>
</table>
$x^2 - 6x + 5$ is even $\iff$ $x$ is odd

**Proposition**

- Let $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then $x$ is odd.
**Proposition**

• Let $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then $x$ is odd.

**Proof**

• **Contrapositive.** If $x$ is even, then $x^2 - 6x + 5$ is odd.

• $x$ is even

  $\implies x = 2a$ for some integer $a$ \hspace{1cm} (defn. of even)

  $\implies x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5$ \hspace{1cm} (substitute $x = 2a$)

  $\implies x^2 - 6x + 5 = 2(2a^2) - 2(6a) + 2(2) + 1$ \hspace{1cm} (simplify)

  $\implies x^2 - 6x + 5 = 2(2a^2 - 6a + 2) + 1$ \hspace{1cm} (take 2 common)

  $\implies x^2 - 6x + 5$ is odd \hspace{1cm} (defn. of odd)

• Hence, the proposition is true.
\[ xy > 9 \iff x > 3 \text{ or } y > 3 \]

<table>
<thead>
<tr>
<th>Proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>For reals ( x ) and ( y ), if ( xy &gt; 9 ), then either ( x &gt; 3 ) or ( y &gt; 3 ).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contraposition.</strong> If ( x \leq 3 ) and ( y \leq 3 ), then ( xy \leq 9 ).</td>
</tr>
<tr>
<td>Suppose ( x \leq 3 ) and ( y \leq 3 ).</td>
</tr>
<tr>
<td>[ \implies xy \leq 9 ] (multiply the two inequalities)</td>
</tr>
<tr>
<td><strong>Hence, the proposition is true.</strong></td>
</tr>
</tbody>
</table>
Proposition

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

Proof

- **Contraposition.** 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?
Proposition

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

Proof

$n$ is odd $\Rightarrow n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$ (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. $n = 4q + 1$.

$\Rightarrow n^2 = (4q + 1)^2 = 8(2q^2 + q) + 1 = 8m + 1$, where $m = 2q^2 + q = integer$.

Case 2. $n = 4q + 3$.

$\Rightarrow n^2 = (4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8m + 1$, where $m = 2q^2 + 3q + 1 = integer$. 

\[ Odd^2 = 8m + 1 \]
**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: \((x^2 - y^2) \mod 4 \neq 2\).

Proof

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

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

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

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

- In all these four cases, \((x^2 - y^2) \mod 4 \neq 2\).
Bogus Proofs
Prove 1 = 2 using basic algebra

<table>
<thead>
<tr>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $a &gt; 0, b &gt; 0$</td>
</tr>
<tr>
<td>• $a = b$</td>
</tr>
<tr>
<td>• $ab = b^2$</td>
</tr>
<tr>
<td>• $ab - a^2 = b^2 - a^2$</td>
</tr>
<tr>
<td>• $a(b - a) = (b + a)(b - a)$</td>
</tr>
<tr>
<td>• $a = b + a$</td>
</tr>
<tr>
<td>• $0 = b$</td>
</tr>
<tr>
<td>• $b = 2b$</td>
</tr>
<tr>
<td>• $1 = 2$</td>
</tr>
<tr>
<td>• What is the problem with this proof?</td>
</tr>
</tbody>
</table>
## Prove $1 = 2$ using basic algebra

### Proof

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a &gt; 0, b &gt; 0$</td>
<td>Given</td>
</tr>
<tr>
<td>$a = b$</td>
<td>Given</td>
</tr>
<tr>
<td>$ab = b^2$</td>
<td>Multiply both sides by $b$</td>
</tr>
<tr>
<td>$ab - a^2 = b^2 - a^2$</td>
<td>Subtract $a^2$ from both sides</td>
</tr>
<tr>
<td>$a(b - a) = (b + a)(b - a)$</td>
<td>Factoring</td>
</tr>
<tr>
<td>$a = b + a$</td>
<td>Divide both sides by $(b - a)$</td>
</tr>
<tr>
<td>$0 = b$</td>
<td>Subtract $a$ from both sides</td>
</tr>
<tr>
<td>$b = 2b$</td>
<td>Add $b$ to both sides</td>
</tr>
<tr>
<td>$1 = 2$</td>
<td>Divide both sides by $b$</td>
</tr>
</tbody>
</table>

- 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

- \[ n^2 + 2n + 1 = (n + 1)^2 \]  
  ▶ Expand
- \[ n^2 = (n + 1)^2 - (2n + 1) \]  
  ▶ Subtract
- \[ n^2 - n(2n + 1) = (n + 1)^2 - (2n + 1) - n(2n + 1) \]  
  ▶ 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
- \[ n = n + 1 \]  
  ▶ Add
- \[ 1 = 2 \]  
  ▶ Subtract
- 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 basic algebra

## Proof

<table>
<thead>
<tr>
<th>Step</th>
<th>Equation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>$n^2 + 2n + 1 = (n + 1)^2$</td>
<td>Expand</td>
</tr>
<tr>
<td>2.</td>
<td>$n^2 = (n + 1)^2 - (2n + 1)$</td>
<td>Subtract</td>
</tr>
<tr>
<td>3.</td>
<td>$n^2 - n(2n + 1) = (n + 1)^2 - (2n + 1) - n(2n + 1)$</td>
<td>Subtract</td>
</tr>
<tr>
<td>4.</td>
<td>$n^2 - n(2n + 1) = (n + 1)^2 - (n + 1)(2n + 1)$</td>
<td>Factoring</td>
</tr>
<tr>
<td>5.</td>
<td>$n^2 - n(2n + 1) + (2n + 1)^2/4 = (n + 1)^2 - (n + 1)(2n + 1) + (2n + 1)^2/4$</td>
<td>Add</td>
</tr>
<tr>
<td>6.</td>
<td>$(n - (2n + 1)/2)^2 = ((n + 1) - (2n + 1)/2)^2$</td>
<td>Simplify</td>
</tr>
<tr>
<td>7.</td>
<td>$n - (2n + 1)/2 = (n + 1) - (2n + 1)/2$</td>
<td>Square roots</td>
</tr>
<tr>
<td>8.</td>
<td>$n = n + 1$</td>
<td>Add</td>
</tr>
<tr>
<td>9.</td>
<td>$1 = 2$</td>
<td>Subtract</td>
</tr>
</tbody>
</table>

- **What is the problem with this proof?**

## Error

<table>
<thead>
<tr>
<th>Step</th>
<th>Issue</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cannot take square roots directly</td>
<td>$a^2 = b^2$ does not imply $a = b$</td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td>E.g.: $1^2 = (-1)^2$ does not imply $1 = -1$</td>
</tr>
</tbody>
</table>
Prove 1 = 2 using calculus

Proof

• \( \int uv = uv - \int vdu \) \hspace{1cm} ▶ 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} ▶ Substitute

• \( \int \frac{1}{x} dx = 1 + \int \frac{1}{x} dx \) \hspace{1cm} ▶ Simplify

• \( 0 = 1 \) \hspace{1cm} ▶ Subtract

• \( 1 = 2 \) \hspace{1cm} ▶ Add

• What is the problem with this proof?

Error

Cannot subtract integrals from both sides

\[ \int dx = x + \text{const.} \] ▶ const. depends on conditions

E.g.

\[ \int \frac{d}{dx}(x + 1) = \int \frac{d}{dx}(x + 2) \] does not imply

\[ \int \frac{dx}{x + 1} = \int \frac{dx}{x + 2} \]
Prove $1 = 2$ using calculus

**Proof**

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

**Error**

- **Cannot subtract integrals from both sides**
- \[ \int dx = x + \text{const.} \] ▷ 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

### Proof

- \( x \neq 0 \) ▶ Given
- \( x = x \) ▶ Given
- \( x + x = 2x \) ▶ Add
- \( x + x + \cdots + x = x^2 \) ▶ Repeatedly add \( x \) times
- \( \sum_{i=1}^{x} 1 = 2x \) ▶ Differentiate
- \( x = 2x \) ▶ Simplify
- \( 1 = 2 \) ▶ Divide

- **What is the problem with this proof?**

---

**Error**

Cannot write \( x + x + \cdots + x \) times for non-integers

E.g.: Cannot write \( 1 + 1 + \cdots + 1 \) times

\( 1 + 1 + \cdots + 1 = 2 \)
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)
Proof

1. \[ 1 = \frac{2}{3-1} = \frac{2}{3-\frac{2}{3-1}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-1}}} = \ldots \]
2. \[ 2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-2}}} = \ldots \]

\[ 1 = 2 \] ▶ Continued fractions are the same

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

### Proof

1. \[ 1 = \frac{2}{3-1} = \frac{2}{3} = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{\ddots}}}}} \]

2. \[ 2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{\ddots}}}}} \]

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

### 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

<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} $\triangleright$ $S = 0$ and $S' = 1$
| • $1 = 2$  \hspace{1cm} $\triangleright$ Add
| • What is the problem with this proof? |
### Proof

- Consider Grandi’s series $S = 1 - 1 + 1 - 1 + \cdots$
- $S = (1 - 1) + (1 - 1) + \cdots = 0 + 0 + \cdots = 0$
- $S = 1 + (-1 + 1) + (-1 + 1) + \cdots = 1 + 0 + 0 + \cdots = 1$
- $0 = 1 \quad \triangleright S = 0$ and $S' = 1$
- $1 = 2 \quad \triangleright$ 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!
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.

- $1 = 2$

- What is the problem with this proof?
**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.

- $1 = 2$
- 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!
The Pythagorean theorem

• **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?)