Foundations of Computer Science
Lecture 2

Discrete Objects and Proof

The Cast of Discrete Objects
Some Basic Proofs

Cinker with easy cases to build an understanding of the model

Like this?

Cinker with easy cases to build an understanding of the model

Like this?

(Niteesh Thangaraj, RPI Class of 2020)
A taste of discrete math and computing (ebola, speed dating, friendship networks)

$100
Distinct subsets with the same sum.

$1,000
Domino Program

$10
Create the best ‘math’-cartoon.

Create a cartoon to illustrate/make fun of some discrete math you learned in this class.

If you submit one, I can use it in the future.

If not, say it can’t be done.

Example:

Input: 32 21 15 7 4 1 Output: sequence that works or say it can’t be done.
Today: Discrete Objects and Proof

1. Discrete Objects
   - Sets
   - Sequences
   - Graphs

2. Proof
   - In 4 rounds of the speed-dating app, no one meets more than 12 people.
   - $x^2$ is even “is the same as” $x$ is even
   - Among any 6 people is a 3-clique or 3-war.
   - **Axioms.** The Well Ordering Principle.
   - $\sqrt{2}$ is not rational.
Collection of objects, order does not matter: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.

$F \cap V = \{o\}$  \hspace{1cm} $F \cup V = \{a, e, f, i, o, u, x\}$  \hspace{1cm} $F^\prime = ?$
1. Collection of objects, order does not matter: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.
   \[ F \cap V = \{o\} \quad F \cup V = \{a, e, f, i, o, u, x\} \quad \overline{F} = ? \]

2. Natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$
   Integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$

What is “...?”
Sets

1. Collection of objects, order does not matter: $F = \{ f, o, x \}; \quad V = \{ a, e, i, o, u \}$.
   
   $F \cap V = \{ o \} \quad F \cup V = \{ a, e, f, i, o, u, x \} \quad \overline{F} =$?

2. natural numbers $\mathbb{N} = \{ 1, 2, 3, 4, 5, \ldots \}$
   
   integers $\mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots \}$

   What is “…”?

3. $E = \{ 2, 4, 6, 8, 10, 12, \ldots \} \quad E' = \{ 2, 4, 6, 8, 10, 13, \ldots \}$

   What is “…”?
Sets

1. Collection of objects, order does not matter: \( F = \{f, o, x\}; \ V = \{a, e, i, o, u\}. \)
   \[ F \cap V = \{o\} \quad F \cup V = \{a, e, f, i, o, u, x\} \quad \overline{F} =? \]

2. natural numbers \( \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} \)
   integers \( \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\} \)

3. \( E = \{2, 4, 6, 8, 10, 12, \ldots\} \quad E' = \{2, 4, 6, 8, 10, 13, \ldots\} \)
   What is “…?”

4. \( E = \{n \mid n = 2k; \ k \in \mathbb{N}\} \quad \leftarrow \text{no “…”} \)

Pop Quiz: Define \( O = \{\text{odd numbers}\}. \)
Collections of objects, order does not matter: \( F = \{ f, o, x \}; \ V = \{ a, e, i, o, u \} \).

\[
F \cap V = \{ o \} \quad F \cup V = \{ a, e, f, i, o, u, x \} \quad F = ?
\]

2. natural numbers \( \mathbb{N} = \{ 1, 2, 3, 4, 5, \ldots \} \)  
integers \( \mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots \} \)

What is “…”?

3. \( E = \{ 2, 4, 6, 8, 10, 12, \ldots \} \)  
\( E' = \{ 2, 4, 6, 8, 10, 13, \ldots \} \)

What is “…”?

4. \( E = \{ n \mid n = 2k; \ k \in \mathbb{N} \} \)  
← no “…”

5. Rational numbers \( \mathbb{Q} = \{ r \mid r = \frac{a}{b}; \ a \in \mathbb{Z}, \ b \in \mathbb{N} \} \)

Pop Quiz: Define \( O = \{ \text{odd numbers} \} \).
Sets

1. Collection of objects, order does not matter: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.
   
   $F \cap V = \{o\}$\quad $F \cup V = \{a, e, f, i, o, u, x\}$\quad $\overline{F} =$?

2. natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$
   
   integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$

3. $E = \{2, 4, 6, 8, 10, 12, \ldots\}$\quad $E' = \{2, 4, 6, 8, 10, 13, \ldots\}$\quad What is “. . .?”

4. $E = \{n \mid n = 2k; \ k \in \mathbb{N}\}$\quad ← no “. . .”

5. Rational numbers $\mathbb{Q} = \{r \mid r = \frac{a}{b}; \ a \in \mathbb{Z}, \ b \in \mathbb{N}\}$

6. Subset $A \subseteq B$ (every element of $A$ is in $B$). $\emptyset \subseteq A$ for any $A$.
   Power set $\mathcal{P}(A) = \{\text{all subsets of } A\}$\quad Pop Quiz: Define $O = \{\text{odd numbers}\}$.

Pop Quiz: $A = \{a, b\}$. What is $\mathcal{P}(A)$?
Sets

1. Collection of objects, order does not matter: \( F = \{ f, o, x \}; \ V = \{ a, e, i, o, u \}. \)
   \[ F \cap V = \{ o \} \quad F \cup V = \{ a, e, f, i, o, u, x \} \quad \overline{F} = ? \]

2. Natural numbers \( \mathbb{N} = \{ 1, 2, 3, 4, 5, \ldots \} \)
   Integers \( \mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots \} \)

3. \( E = \{ 2, 4, 6, 8, 10, 12, \ldots \} \quad E' = \{ 2, 4, 6, 8, 10, 13, \ldots \} \)
   What is “…”?

4. \( E = \{ n \mid n = 2k; \ k \in \mathbb{N} \} \quad \leftarrow \text{no “…”} \)

5. Rational numbers \( \mathbb{Q} = \{ r \mid r = \frac{a}{b}; \ a \in \mathbb{Z}, \ b \in \mathbb{N} \} \)

6. Subset \( A \subseteq B \) (every element of \( A \) is in \( B \)). \( \emptyset \subseteq A \) for any \( A \).
   Power set \( \mathcal{P}(A) = \{ \text{all subsets of } A \} \)
   Pop Quiz: Define \( O = \{ \text{odd numbers} \} \).

7. Set equality, \( A = B \) means \( A \subseteq B \) and \( B \subseteq A \).
   Pop Quiz: \( A = \{ a, b \} \). What is \( \mathcal{P}(A) \)?
Sets

1. Collection of objects, order does not matter: \( F = \{f, o, x\} \); \( V = \{a, e, i, o, u\} \).
   \[ F \cap V = \{o\} \quad F \cup V = \{a, e, f, i, o, u, x\} \quad \overline{F} =? \]

2. natural numbers \( \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} \)
   integers \( \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\} \)

3. \( E = \{2, 4, 6, 8, 10, 12, \ldots\} \quad E' = \{2, 4, 6, 8, 10, 13, \ldots\} \)
   What is “...?”

4. \( E = \{n \mid n = 2k; \ k \in \mathbb{N}\} \quad \leftarrow \text{no “...”} \)

5. Rational numbers \( \mathbb{Q} = \{r \mid r = \frac{a}{b}; \ a \in \mathbb{Z}, \ b \in \mathbb{N}\} \)

6. Subset \( A \subseteq B \) (every element of \( A \) is in \( B \)). \( \emptyset \subseteq A \) for any \( A \).
   Power set \( \mathcal{P}(A) = \{\text{all subsets of } A\} \)
   Pop Quiz: Define \( O = \{\text{odd numbers}\} \).

7. Set equality, \( A = B \) means \( A \subseteq B \) and \( B \subseteq A \).

8. Set operations: Intersection, \( A \cap B \)
   Union, \( A \cup B \)
   Complement, \( \overline{A} \)
   Pop Quiz: \( A = \{a, b\} \). What is \( \mathcal{P}(A) \)?
Sets

1. Collection of objects, order does not matter: \( F = \{f, o, x\} \); \( V = \{a, e, i, o, u\} \).
   \[
   F \cap V = \{o\} \quad F \cup V = \{a, e, f, i, o, u, x\} \quad \overline{F} = ?
   \]

2. natural numbers \( \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} \)
   integers \( \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\} \)

3. \( E = \{2, 4, 6, 8, 10, 12, \ldots\} \quad E' = \{2, 4, 6, 8, 10, 13, \ldots\} \)
   What is “…?”

4. \( E = \{n \mid n = 2k; \ k \in \mathbb{N}\} \quad \leftarrow \text{no “…”} \)

5. Rational numbers \( \mathbb{Q} = \{r \mid r = \frac{a}{b}; \ a \in \mathbb{Z}, \ b \in \mathbb{N}\} \)

6. Subset \( A \subseteq B \) (every element of \( A \) is in \( B \)). \( \emptyset \subseteq A \) for any \( A \).
   Power set \( \mathcal{P}(A) = \{\text{all subsets of } A\} \)
   Pop Quiz: \( A = \{a, b\} \). What is \( \mathcal{P}(A) \)?

7. Set equality, \( A = B \) means \( A \subseteq B \) and \( B \subseteq A \).

8. Set operations: Intersection, \( A \cap B \)
   Union, \( A \cup B \)
   Complement, \( \overline{A} \)

9. Venn Diagrams are a convenient way to represent sets.

Lives in Troy, NY

Creator: Malik Magdon-Ismail
List of objects: order and repetition matter.

\[ tap \neq taap \neq atp \]
Sequences

1. List of objects: order and repetition matter.

   \[ \text{tap} \neq \text{taap} \neq \text{atp} \]

2. We are mostly concerned with binary sequences composed of bits (ASCII code).

   \[
   \begin{array}{ccc}
   t & a & p \\
   01110100 & 01100001 & 01110000 \\
   \end{array}
   \]
Friendships between Alice, Bob, Charles, David, Edward, Fiona:
Friendships between Alice, Bob, Charles, David, Edward, Fiona:
Friendships between Alice, Bob, Charles, David, Edward, Fiona:

\[
V = \{A, B, C, D, E, F\}.
\]
Friendships between Alice, Bob, Charles, David, Edward, Fiona:

\[ V = \{A, B, C, D, E, F\}. \]

\[ E = \{(A, C), (A, D), (C, D), (B, D), (B, E), (D, E), (E, F)\}. \]
Friendships between Alice, Bob, Charles, David, Edward, Fiona:

\[ V = \{A, B, C, D, E, F\} \]

\[ E = \{(A, C), (A, D), (C, D), (B, D), (B, E), (D, E), (E, F)\} \]

What matters is:
- who the people are, that is the set \( V \) of objects; and,
- who is friends with whom, that is the set \( E \) of relationships.
Friendships between Alice, Bob, Charles, David, Edward, Fiona:

\[ V = \{A, B, C, D, E, F\} \]

\[ E = \{(A, C), (A, D), (C, D), (B, D), (B, E), (D, E), (E, F)\} \]

What matters is:
- who the people are, that is the set \( V \) of objects; and,
- who is friends with whom, that is the set \( E \) of relationships.

The picture with circles and links is a convenient *visualization* of the graph.
Graphs and Different Types of Relationships

**Affiliation graphs**

Students and their courses.

**Conflict graphs**

Courses with students in common conflict. (Why?)
Graphs and Different Types of Relationships

Affiliation graphs

| A | 1100 |
| B | 1200 |
| C | 2200 |
| D | 2300 |
| E | 2400 |
| F |       |

Students and their courses.

Conflict graphs

Courses with students in common conflict. (Why?)
Graphs and Different Types of Relationships

Affiliation graphs

Courses with students in common conflict. (Why?)

Conflict graphs

Students and their courses.
Graphs and Different Types of Relationships

Affiliation graphs

Students and their courses.

Conflict graphs

Courses with students in common conflict. (Why?)
Graphs and Different Types of Relationships

Affiliation graphs

Students and their courses.

Conflict graphs

Courses with students in common conflict. (Why?)
It is Human to seek verification – proof.
Proof

It is Human to seek verification – proof.

- The sun has risen every morning in history. \((\text{inductive proof})\)
It is Human to seek verification – proof.

- The sun has risen every morning in history. \textit{(inductive proof)}

- In the speed dating ritual, no-one meets more than 12 people. \textit{deductive proof:}
Proof

It is Human to seek verification – proof.

- The sun has risen every morning in history. (*inductive proof*)

- In the speed dating ritual, no-one meets more than 12 people.
  
  *deductive proof:*
  
  In any round a person meets *at most* 3 new people. (Why?)
It is Human to seek verification – proof.

- The sun has risen every morning in history. (*inductive proof*)

- In the speed dating ritual, no-one meets more than 12 people.
  
  *deductive proof:*
  
  In any round a person meets *at most* 3 new people. (Why?)
  There are 4 rounds, *ergo* at most $4 \times 3 = 12$ people can be met.
Proof

It is Human to seek verification – proof.

- The sun has risen every morning in history. (*inductive proof*)

- In the speed dating ritual, no-one meets more than 12 people.

  *deductive proof:*
  
  In any round a person meets *at most* 3 new people. (Why?)
  
  There are 4 rounds, *ergo* at most $4 \times 3 = 12$ people can be met.

Do you have any doubts?
Proof

It is Human to seek verification – proof.

- The sun has risen every morning in history. \((inductive\ proof)\)

- In the speed dating ritual, no-one meets more than 12 people.
  
  \(\text{deductive proof:}\)
  
  In any round a person meets \textit{at most} 3 new people. (Why?)
  
  There are 4 rounds, \textit{ergo} at most \(4 \times 3 = 12\) people can be met.

  Do you have any doubts? That is the beauty of deductive proof.
When is a Number a Square

Tinker!
## When is a Number a Square

### Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\pm 1$</th>
<th>$\pm 2$</th>
<th>$\pm 3$</th>
<th>$\pm 4$</th>
<th>$\pm 5$</th>
<th>$\pm 6$</th>
<th>$\pm 7$</th>
<th>$\pm 8$</th>
<th>$\pm 9$</th>
<th>$\pm 10$</th>
<th>$\pm 11$</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>
**Conjecture.**
Even squares come from even numbers and even numbers have even squares.
Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?)
When is a Number a Square

<table>
<thead>
<tr>
<th>Tinker!</th>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td></td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

- $n$ is even
When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>$0$</th>
<th>$±1$</th>
<th>$±2$</th>
<th>$±3$</th>
<th>$±4$</th>
<th>$±5$</th>
<th>$±6$</th>
<th>$±7$</th>
<th>$±8$</th>
<th>$±9$</th>
<th>$±10$</th>
<th>$±11$</th>
<th>$\ldots$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>$0$</td>
<td>$1$</td>
<td>$4$</td>
<td>$9$</td>
<td>$16$</td>
<td>$25$</td>
<td>$36$</td>
<td>$49$</td>
<td>$64$</td>
<td>$81$</td>
<td>$100$</td>
<td>$121$</td>
<td>$\ldots$</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

**Proof.** (How do I convince you this is true, *without a doubt*) Let’s look at the cases

- $n$ is even $\rightarrow$ $n = 2k$

Creator: Malik Magdon-Ismail
Discrete Objects and Proof: 9 / 14

3-war or 3-clique →
Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

- **n is even**  \( \rightarrow \)  \( n = 2k \)  \( \rightarrow \)  \( n^2 = 4k^2 \)
When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.

Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, *without a doubt*?) Let’s look at the cases:

- $n$ is even $\rightarrow$ $n = 2k$ $\rightarrow$ $n^2 = 2(2k^2)$ $\rightarrow$ $n^2$ is even.
Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.

Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

1. **$n$ is even** → $n = 2k$ → $n^2 = 2(2k^2)$ → $n^2$ is even.
2. **$n$ is odd**
When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>n</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>n^2</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

- **i.** If $n$ is even, then $n = 2k$.
  - $n^2 = 2(2k^2)$
  - $n^2$ is even.

- **ii.** If $n$ is odd, then $n = 2k + 1$. 

When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

1. $n$ is even $\rightarrow$ $n = 2k$ $\rightarrow$ $n^2 = 2(2k^2)$ $\rightarrow$ $n^2$ is even.
2. $n$ is odd $\rightarrow$ $n = 2k + 1$ $\rightarrow$ $n^2 = 2(2k^2 + 2k) + 1$
When is a Number a Square

<table>
<thead>
<tr>
<th>$n$</th>
<th>$0$</th>
<th>$±1$</th>
<th>$±2$</th>
<th>$±3$</th>
<th>$±4$</th>
<th>$±5$</th>
<th>$±6$</th>
<th>$±7$</th>
<th>$±8$</th>
<th>$±9$</th>
<th>$±10$</th>
<th>$±11$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>$0$</td>
<td>$1$</td>
<td>$4$</td>
<td>$9$</td>
<td>$16$</td>
<td>$25$</td>
<td>$36$</td>
<td>$49$</td>
<td>$64$</td>
<td>$81$</td>
<td>$100$</td>
<td>$121$</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

1. $n$ is even $→$ $n = 2k$ $→$ $n^2 = 2(2k^2)$ $→$ $n^2$ is even.
2. $n$ is odd $→$ $n = 2k + 1$ $→$ $n^2 = 2(2k^2 + 2k) + 1$ $→$ $n^2$ is odd.
When is a Number a Square

<table>
<thead>
<tr>
<th>Tinker!</th>
<th>0 ±1 ±2 ±3 ±4 ±5 ±6 ±7 ±8 ±9 ±10 ±11 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n^2 )</td>
<td>0 1 4 9 16 25 36 49 64 81 100 121 ...</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

1. \( n \) is even \( \rightarrow \) \( n = 2k \) \( \rightarrow \) \( n^2 = 2(2k^2) \) \( \rightarrow \) \( n^2 \) is even.
2. \( n \) is odd \( \rightarrow \) \( n = 2k + 1 \) \( \rightarrow \) \( n^2 = 2(2k^2 + 2k) + 1 \) \( \rightarrow \) \( n^2 \) is odd.

\( n \) must be even or odd, and we made no assumptions about \( n \) (\( n \) is general).
When is a Number a Square

Tinker!

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

- $n$ is even $\rightarrow$ $n = 2k$ $\rightarrow$ $n^2 = 2(2k^2)$ $\rightarrow$ $n^2$ is even.
- $n$ is odd $\rightarrow$ $n = 2k + 1$ $\rightarrow$ $n^2 = 2(2k^2 + 2k) + 1$ $\rightarrow$ $n^2$ is odd.

$n$ must be even or odd, and we made no assumptions about $n$ ($n$ is general).

Are you convinced?
When is a Number a Square

<table>
<thead>
<tr>
<th>n</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>n²</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>36</td>
<td>49</td>
<td>64</td>
<td>81</td>
<td>100</td>
<td>121</td>
<td>...</td>
</tr>
</tbody>
</table>

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, without a doubt?) Let’s look at the cases

1. **n is even** → \( n = 2k \) → \( n² = 2(2k²) \) → \( n² \) is even.
2. **n is odd** → \( n = 2k + 1 \) → \( n² = 2(2k² + 2k) + 1 \) → \( n² \) is odd.

\( n \) must be even or odd, and we made no assumptions about \( n \) (\( n \) is general).

Are you convinced?

Theorem.
*Every* even square came from an even number and *every* even number has an even square.
3-war or 3-clique

friend clique
3-war or 3-clique
Theorem.
Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).
Theorem. Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

Proof. For a general network with 6 people, there are two cases:

(i) $A$ has more friends than enemies.
Theorem. Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

Proof. For a general network with 6 people, there are two cases:

(i) A has more friends than enemies.

(ii) A has more enemies than friends.
Theorem. Any 6-person friend network has a 3-person friend clique or a 3-person war (or both).

Proof. For a general network with 6 people, there are two cases:

(i) $A$ has more friends than enemies.

(ii) $A$ has more enemies than friends.

Two friends are linked $\rightarrow$ 3-clique.
Theorem. Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

Proof. For a \textit{general} network with 6 people, there are two cases:

(i) \( A \) has more friends than enemies.

(ii) \( A \) has more enemies than friends.

Two friends are linked \( \rightarrow \) 3-clique.
None are linked \( \rightarrow \) 3-war.
Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

**Proof.** For a *general* network with 6 people, there are two cases:

(i) A has more friends than enemies.  

Two friends are linked → 3-clique.  
None are linked → 3-war.

(ii) A has more enemies than friends.

Two friends are enemies → 3-war.
Theorem. Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

Proof. For a general network with 6 people, there are two cases:

(i) $A$ has more friends than enemies.

Two friends are linked $\rightarrow$ 3-clique.
None are linked $\rightarrow$ 3-war.

(ii) $A$ has more enemies than friends.

Two friends are enemies $\rightarrow$ 3-war.
None are enemies $\rightarrow$ 3-clique.
We Can’t Prove Everything

- **Axioms**: A self-evident statement that is asserted as true without proof.
• **Axioms:** A self-evident statement that is asserted as true without proof.

• **Conjectures:** A claim that is believed true but is not true until proven so.
We Can’t Prove Everything

- **Axioms:** A self-evident statement that is asserted as true without proof.
- **Conjectures:** A claim that is believed true but is not true until proven so.
- **Theorems:** A proven truth. You can take it to the bank.
We Can’t Prove Everything

- **Axioms:** A self-evident statement that is asserted as true without proof.
- **Conjectures:** A claim that is believed true but is not true until proven so.
- **Theorems:** A proven truth. You can take it to the bank.

**Axiom. The Well-Ordering Principle**

*Any* non-empty subset of $\mathbb{N}$ has a minimum element.

\[
\{2, 5, 4, 11, 7, 296, 81\}; \text{ or,}
\{6, 19, 24, 18, \ldots\}.
\]
We Can’t Prove Everything

- **Axioms:** A self-evident statement that is asserted as true without proof.

- **Conjectures:** A claim that is believed true but is not true until proven so.

- **Theorems:** A proven truth. You can take it to the bank.

**Axiom. The Well-Ordering Principle**

*Any* non-empty subset of \( \mathbb{N} \) has a minimum element.

\[ \{2, 5, 4, 11, 7, 296, 81\}; \text{ or, } \{6, 19, 24, 18, \ldots\}. \]

**Exercises.**

- Construct a subset of \( \mathbb{Z} \) (integers) that has no minimum element.

- Construct a **positive** subset of \( \mathbb{Q} \) (rationals) that has no minimum element.
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.
A Gift from Hipassus: \( \sqrt{2} \) is Irrational

It may not be so.

In which case \( \sqrt{2} \) is rational,

\[
\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},
\]

where \( a_1, a_2, \ldots \) are all integers and \( b_1, b_2, \ldots \) are all natural numbers.
A Gift from Hipassus: \( \sqrt{2} \) is Irrational

It may not be so.

In which case \( \sqrt{2} \) is rational,

\[
\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \cdots \right\},
\]

where \( a_1, a_2, \ldots \) are all integers and \( b_1, b_2, \ldots \) are all natural numbers.

Well ordering principle: there is a minimum \( b_i \), call it \( b_* \).

\[ \sqrt{2} = a_*/b_* \] and \( a_* \) and \( b_* \) have no factor in common. (\( b_* \) is the minimum possible)
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

\[
\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \cdots \right\},
\]

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$. 

$\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. (\(b_*\) is the minimum possible)

\[
\sqrt{2} = \frac{a_*}{b_*}
\]
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$. $\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. ($b_*$ is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2$$
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\}$,

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$. $\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. ($b_*$ is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?)}. $$
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$.  

$\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common.  ($b_*$ is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?).}$$

So, $a_* = 2k$ and
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_\ast$.

$\sqrt{2} = a_\ast/b_\ast$ and $a_\ast \text{ and } b_\ast \text{ have no factor in common.}$  \((b_\ast \text{ is the minimum possible})\)

$$\sqrt{2} = \frac{a_\ast}{b_\ast} \quad \rightarrow \quad a_\ast^2 = 2b_\ast^2 \quad \rightarrow \quad a_\ast \text{ is even (why?)}.$$  

So, $a_\ast = 2k$ and

$$4k^2 = 2b_\ast^2$$
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$.

$\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. ({$b_*$ is the minimum possible})

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?)}. $$

So, $a_* = 2k$ and

$$4k^2 = 2b_*^2 \quad \rightarrow \quad b_*^2 = 2k^2$$
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \cdots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_\ast$.

$\sqrt{2} = a_\ast/b_\ast$ and $a_\ast$ and $b_\ast$ have no factor in common. (This $b_\ast$ is the minimum possible)

$$\sqrt{2} = \frac{a_\ast}{b_\ast} \quad \rightarrow \quad a_\ast^2 = 2b_\ast^2 \quad \rightarrow \quad a_\ast \text{ is even (why?)}. $$

So, $a_\ast = 2k$ and

$$4k^2 = 2b_\ast^2 \quad \rightarrow \quad b_\ast^2 = 2k^2 \quad \rightarrow \quad b_\ast \text{ is even (why?)}. $$
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b*$.

$\sqrt{2} = a*/b*$ and $a*$ and $b*$ have no factor in common.  ($b*$ is the minimum possible)

$$\sqrt{2} = \frac{a*}{b*} \quad \rightarrow \quad a^2 = 2b^2 \quad \rightarrow \quad a* \text{ is even} \quad \text{(why?)}.\]

So, $a* = 2k$ and

$$4k^2 = 2b^2 \quad \rightarrow \quad b^2 = 2k^2 \quad \rightarrow \quad b* \text{ is even} \quad \text{(why?)}.\]

So, $a*$ and $b*$ have the factor 2 in common.
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$.

$\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. ($b_*$ is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?)}. $$

So, $a_* = 2k$ and

$$4k^2 = 2b_*^2 \quad \rightarrow \quad b_*^2 = 2k^2 \quad \rightarrow \quad b_* \text{ is even (why?)}. $$

So, $a_*$ and $b_*$ have the factor 2 in common.

**FISHY!**
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots \right\},$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$.

$\sqrt{2} = a_*/b_*$ and $a_*$ and $b_*$ have no factor in common. ($b_*$ is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?)}. $$

So, $a_* = 2k$ and

$$4k^2 = 2b_*^2 \quad \rightarrow \quad b_*^2 = 2k^2 \quad \rightarrow \quad b_* \text{ is even (why?)}. $$

So, $a_*$ and $b_*$ have the factor 2 in common.

FISHY!

It must be so!
A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\sqrt{2} = \{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots\}$$

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ are all natural numbers.

Well ordering principle: there is a minimum $b_i$, call it $b_*$.

$\sqrt{2} = \frac{a_*}{b_*}$ and $a_*$ and $b_*$ have no factor in common. $\quad (b_* \text{ is the minimum possible})$

$$\sqrt{2} = \frac{a_*}{b_*} \rightarrow a_*^2 = 2b_*^2 \rightarrow a_* \text{ is even (why?).}$$

So, $a_* = 2k$ and

$$4k^2 = 2b_*^2 \rightarrow b_*^2 = 2k^2 \rightarrow b_* \text{ is even (why?).}$$

So, $a_*$ and $b_*$ have the factor 2 in common.

It must be so!
A proof strings together “truths” to convince the reader of something new.
A proof strings together “truths” to *convince* the reader of something *new*.

Our proof that $\sqrt{2}$ is irrational strung together several “truths”:
A proof strings together “truths” to *convince* the reader of something *new*.

Our proof that $\sqrt{2}$ is irrational strung together several “truths”:

- The well ordering principle.
A proof strings together “truths” to convince the reader of something new.

Our proof that $\sqrt{2}$ is irrational strung together several “truths”:

- The well ordering principle.
- High-school algebra for manipulating equalities.
A proof strings together “truths” to convince the reader of something new.

Our proof that $\sqrt{2}$ is irrational strung together several “truths”:

- The well ordering principle.
- High-school algebra for manipulating equalities.
- Our Theorem on when a square is even.
A proof strings together “truths” to *convince* the reader of something *new*.

Our proof that $\sqrt{2}$ is irrational strung together several “truths”:

- The well ordering principle.
- High-school algebra for manipulating equalities.
- Our Theorem on when a square is even.

A proof’s goal is always, always, ALWAYS to convince a reader of something.
Making and Proving Claim

Three Steps for Making and Proving a Claim
Three Steps for Making and Proving a Claim

Step 1: Precisely state the right thing to prove. Often, creativity and imagination are needed. The claim should be non-trivial, i.e. useful, but also “provable” given the tools you have. Most importantly, the claim should be true (and how do you know that).
Three Steps for Making and Proving a Claim

**Step 1: Precisely state the right thing to prove.** Often, creativity and imagination are needed. The claim should be non-trivial, i.e. useful, but also “provable” given the tools you have. Most importantly, the claim should be true (and how do you know that).

**Step 2: Prove the claim.** Sometimes a simple “genius” idea may be needed. Again, creativity and imagination play a role. Sometimes standard proof techniques can be used; you can become proficient in these techniques through training and practice.
Three Steps for Making and Proving a Claim

**Step 1: Precisely state the right thing to prove.** Often, creativity and imagination are needed. The claim should be non-trivial, i.e. useful, but also “provable” given the tools you have. Most importantly, the claim should be true (and how do you know that).

**Step 2: Prove the claim.** Sometimes a simple “genius” idea may be needed. Again, creativity and imagination play a role. Sometimes standard proof techniques can be used; you can become proficient in these techniques through training and practice.

**Step 3: Check the proof for correctness.** No creativity is needed to look a proof in the eye and determine if it is correct; to determine if you are convinced. Become an expert at this task. Don’t allow anyone to claim bogus things and “convinced” you with invalid proofs.
Three Steps for Making and Proving a Claim

**Step 1: Precisely state the right thing to prove.** Often, creativity and imagination are needed. The claim should be non-trivial, i.e. useful, but also “provable” given the tools you have. Most importantly, the claim should be true (and how do you know that).

**Step 2: Prove the claim.** Sometimes a simple “genius” idea may be needed. Again, creativity and imagination play a role. Sometimes standard proof techniques can be used; you can become proficient in these techniques through training and practice.

**Step 3: Check the proof for correctness.** No creativity is needed to look a proof in the eye and determine if it is correct; to determine if you are convinced. Become an expert at this task. Don’t allow anyone to claim bogus things and “convince” you with invalid proofs.

Next. How to make precise claims.