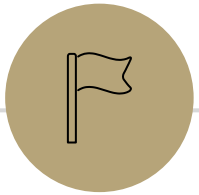
"Proof by contradiction is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game" - G. H. Hardy

Proof by Contradiction

CSE 311: Foundations of Computing I
Lecture 15

Announcements

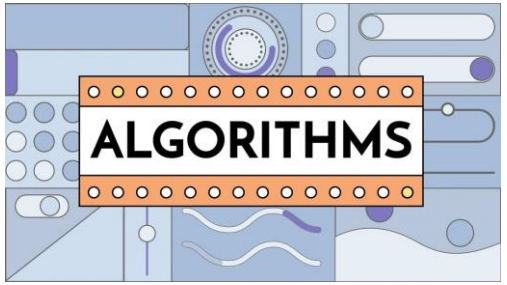
- HW5 due Wednesday at 11:59 pm.
  - Feedback before the midterm is only guaranteed if you don't use late days.
- Midterm is on Friday in class.
  - Optional review session tomorrow (Tuesday) from 3:00 – 4:20 in DEM 104. Will be recorded on Panopto.
  - Info about the exam has been published on the course website under the Exams tab. Includes problem categories and a practice exam.
- No new HW released this week.

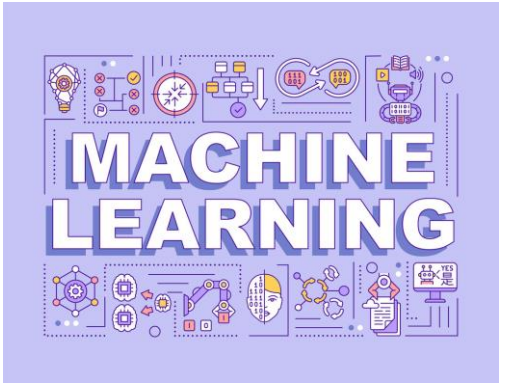


Proof by Contradiction

Proof Strategies

- Direct Proof
- Proof by Contrapositive
- Proof of Biconditional
- Proof by Cases
- Existence Proof
- Induction
  - Weak Induction
  - Strong Induction
  - Structural Induction (coming soon!)
- Proof by Contradiction

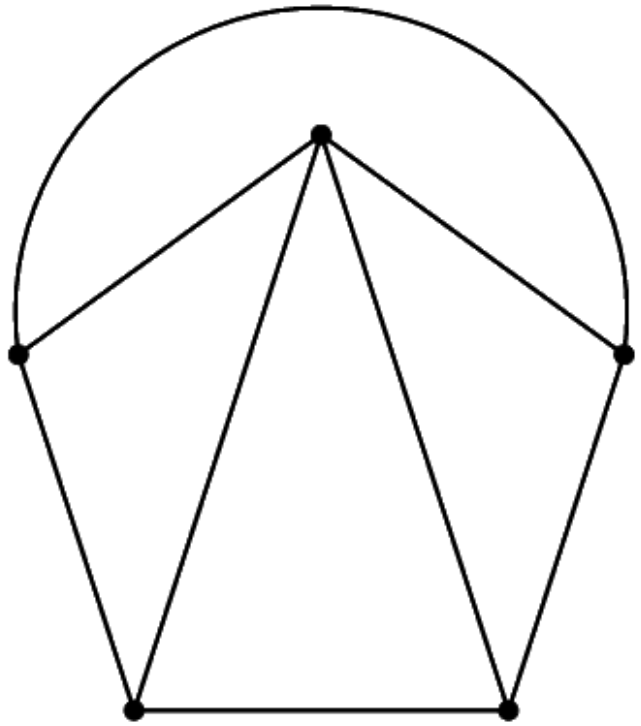




Warm-Up

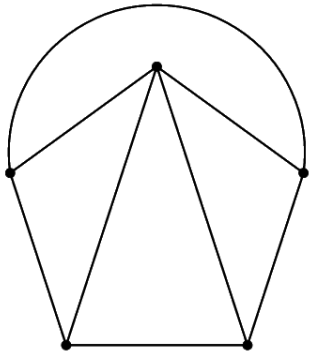
Traverse the following graph by traveling along each edge exactly once.

Any of the vertices may be selected as the starting or ending vertex.



There is no path!
Can we prove it?

Warm-Up



Claim: It is impossible to traverse this graph by traveling along each edge exactly once.

Proof: Suppose that it were possible to traverse the graph by traveling along each edge exactly once. Consider how many times each vertex would be passed through. For every time a vertex is entered, it is also exited. Therefore, if each edge is traveled exactly once, then each vertex should have an even number of edges coming from it. The exceptions to this are the starting vertex and ending vertex (in the case that these are distinct). However, there can only be one starting vertex and one ending vertex. However, this graph has 4 vertices with an odd number of paths coming from them.

Thus, it is impossible to traverse the above graph by traveling along each edge exactly once.

What did we just do?

To prove that the claim p holds:

1. We assumed that p does **not** hold, i.e. we assumed $\neg p$.
2. From $\neg p$, we then derived a false statement.

Why does that work?

Observe from our logical equivalences:

$$\neg p \to \mathrm{F} \equiv \neg\neg p \vee \mathrm{F} \qquad \text{Law of Implication}$$
$$\equiv p \vee \mathrm{F} \qquad \text{Double Negation}$$
$$\equiv p \qquad \text{Identity}$$

Proof by Contradiction

Proof by contradiction is a strategy for proving statements of any form.

- The strategy to prove p is to assume $\neg p$ and derive $\mathbf{False}$.
- E.g. the strategy to prove $p \to q$ is to assume $p \wedge \neg q$ and derive $\mathbf{False}$.
- E.g. the strategy to prove $p \vee q$ is to assume $\neg p \wedge \neg q$ and derive $\mathbf{False}$.

Proof by Contradiction Skeleton

Suppose for the sake of contradiction $\neg p$.

…

Then some statement s must hold.

…

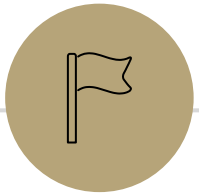
And some statement $\neg s$ must hold.

But s and $\neg s$ is a contradiction. So p must be true.

Proof by Contradiction: Remarks

- Unlike other proof techniques, we don't know *where* we're going. We're trying to find **any** contradiction. That can make it harder.
- Contradiction is a sledge-hammer.
  It can be used to prove many things. But it makes a mess.
- Use contradiction as a last-resort.

Contradiction is a sledge-hammer



Proof by Contradiction Examples

Claim 1: No integer is even and odd.

Suppose for the sake of contradiction that there exists an integer x that is both even and odd. Then $x = 2a$ for some integer a, and $x = 2b + 1$ for some integer b. Then:

$$2a = 2b + 1$$
$$2a - 2b = 1$$
$$a - b = \frac{1}{2}$$

Since a, b are integers, $a - b$ is an integer. But $\frac{1}{2}$ is not an integer. So $a - b$ cannot equal $\frac{1}{2}$. This is a contradiction.

Thus no integer can be even and odd.

Claim 2: For all sets A, B, we have $A \cap (B \backslash A) = \emptyset$.

Suppose for the sake of contradiction that there exists some sets A, B such that $A \cap (B \backslash A) \neq \emptyset$. Then $A \cap (B \backslash A)$ must have at least one element, call it x. Since $x \in A \cap (B \backslash A)$, by definition of intersection $x \in A$ and $x \in B \backslash A$. By definition of set difference, $x \in B$ and $x \notin A$.

Then we have $x \in A$ and $x \notin A$. This is a contradiction. Therefore for all sets A, B, $A \cap (B \backslash A) \neq \emptyset$ must hold.

[Exercise] Claim 3: The sum of any four consecutive integers is not divisible by 4.

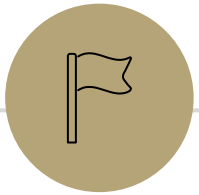
Suppose for the sake of contradiction that there exists four consecutive integers, call them $x, x+1, x+2, x+3$ (where x is an integer), that are divisible by 4. Then by definition of divides, there exists some integer k such that:

$$x + (x+1) + (x+2) + (x+3) = 4k$$

Then observe:

$$x + (x+1) + (x+2) + (x+3) = 4k$$
$$4x + 6 = 4k$$
$$6 = 4k - 4x$$
$$6 = 4(k - x)$$

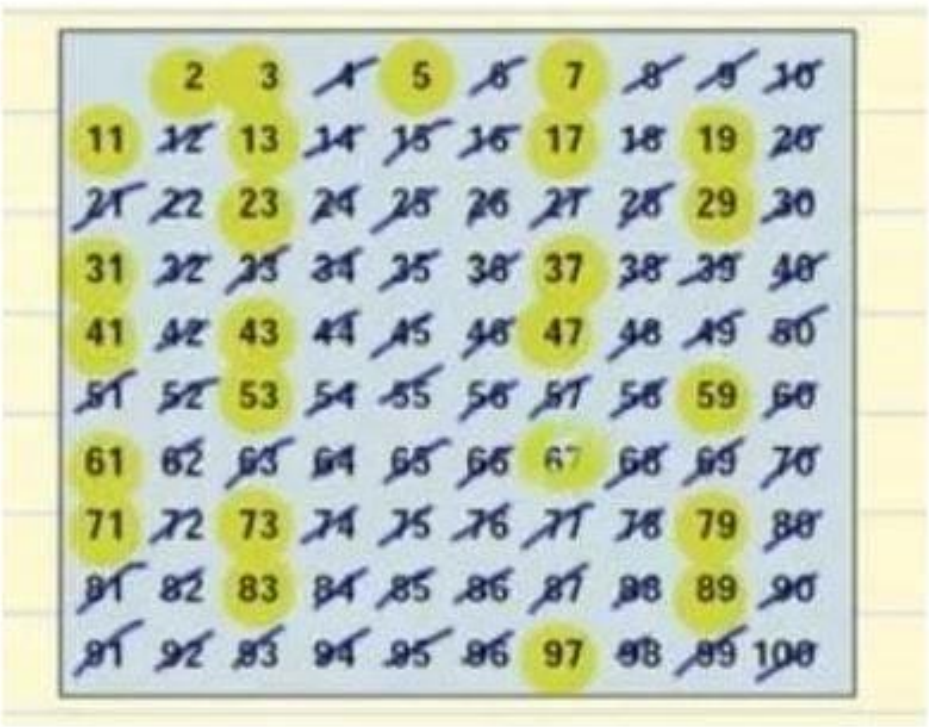
Since k, x are integers, $k - x$ is an integer. So $4 \mid 6$. However $4 \nmid 6$. This is a contradiction. So the sum of any four consecutive integers is not divisible by 4.

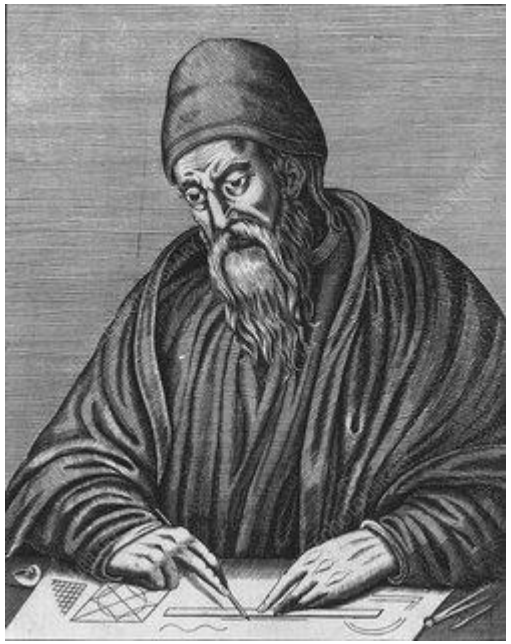


Euclid’s Theorem

Euclid's Theorem: There are infinitely many prime numbers.

2, 3, 5, 7, 11, 13, …





Euclid ~300 BC

Euclid's Theorem: There are infinitely many prime numbers.

Assume for the sake of contradiction that there are finitely many prime numbers. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdots p_k + 1$.

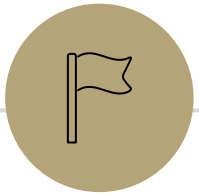
Case 1: q is prime. Then q is a prime that is larger than p_i for all $i \in \{1, \ldots, k\}$. But every prime was supposed to in the list $p_1, \ldots, p_k$. This is a contradiction.

Case 2: q is composite. Then q must have some prime factor. So there exists some i such that $p_i \mid q$. Then $q \,\%\, p_i = 0$. But

$$q \,\%\, p_i = (p_1 \cdot p_2 \cdots p_k + 1) \,\%\, p_i = 1$$

So we have $q \,\%\, p_i = 0$ and $q \,\%\, p_i = 1$. This is a contradiction.

In either case, we have a contradiction. Thus there must be infinitely many primes.



Discussion

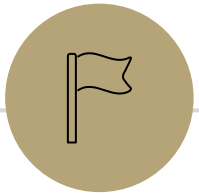
Several strategies to prove $p \rightarrow q$

1) Direct Proof
   Assume p is true. Show q is true.

2) Proof by Contrapositive
   Assume $\neg q$ is true. Show $\neg p$ is true.

3) Proof by Contradiction
   Assume p is true and $\neg q$ is true. Show $\mathbf{False}$.

   *The contrapositive *can* be thought of as a special case of contradiction, where we assume $\neg q$ and p, and the contradiction we find is $\neg p$. However, it's helpful for clarity to separate the terms out.



More Examples

There is no smallest positive rational number.

Recall: $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$

Suppose for the sake of contradiction that there is some smallest positive rational number, call it x. Then $x = \frac{m}{n}$ for some integers $m, n > 0$. Consider $\frac{m}{n+1}$. Since n is an integer and $n > 0$, certainly $n + 1$ is an integer and $n + 1 > 0$. So $m, n + 1$ are integers such that $n + 1 \neq 0$, so $\frac{m}{n+1}$ is rational.

Moreover, $0 < \frac{m}{n+1} < \frac{m}{n}$. This contradicts the claim that $\frac{m}{n}$ was the smallest positive rational. So there is no smallest positive rational number.