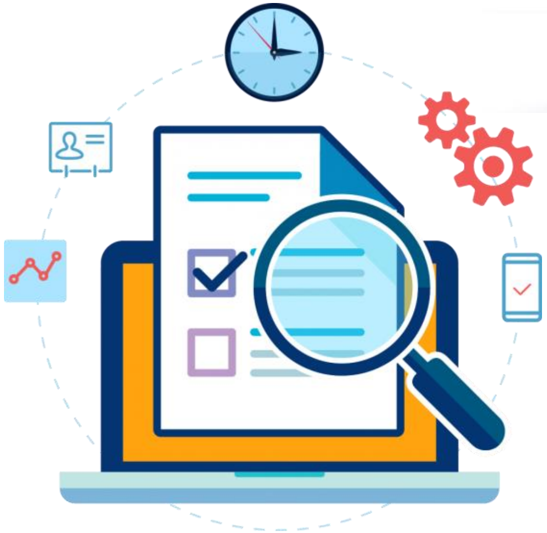
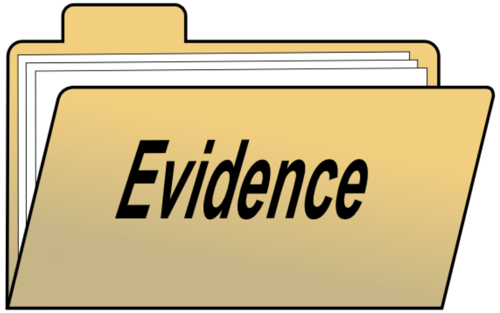
Lecture 5:
Proofs





Ms. Togzhan Nurtayeva
Course Code: IT 235/A
Semester 3
Week 9
Date: 20.11.2023

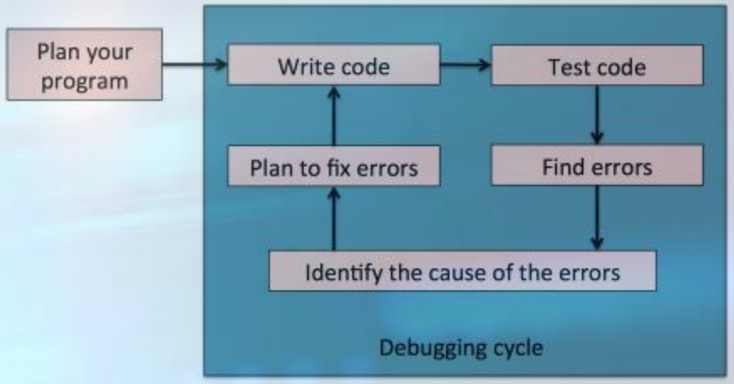
- Computing systems are doing so much:

Why Study Proofs?

- How can we guarantee they work?

- Many advanced topics in computer science, such as cryptography, artificial intelligence, and formal verification, heavily rely on proofs. Understanding proofs lays a solid foundation for comprehending and working with these complex topics.

Why Study Proofs?



Why not just testing?

– Integrates well with programming
– No new languages, tools required
– Conclusive evidence for bugs

Because…

– Difficult to assess coverage
– Cannot demonstrate absence of bugs
– No guarantees for safety-critical systems

Formal Verification

1. SOFTWARE

– If you want to debug a program beyond a doubt, prove that it's bug-free! Deduction and proof provides universal guarantees.

2. HARDWARE

– Proof-theory has recently also been shown to be useful in discovering bugs in pre-production hardware.

https://cse.buffalo.edu/~erdem/cse331/support/proofs/index.html

With the ever-increasing complexity of software and the layers of abstraction, we have reached a time when writing secure, efficient and resilient code requires some level of formal verification to be done, if not for the whole software at least for the important sub-systems involved. In recent times we have seen more widespread adoption of formal verification by the industry leaders like Intel, Amazon or Microsoft, in products where we have enormous complexity and multiple systems interacting with one another.

https://www.moritz.systems/blog/an-introduction-to-formal-verification/

Objectives

- ✓ Direct Proof
- ✓ Proof by Case
- ✓ Proof by Induction
- ✓ Proof by Contradiction

Terminology

- Definition: Something given (no proof)

  E.g. Let $M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

- Theorem: Something to be proved

  Results corollary (sub-proofs): any number divisible by 2 is even.

Direct Proof.

EXAMPLES

If φ, then φ.

Assume φ.

Show that φ.

Prove: If x is odd, then x^2 is odd.

Assume x is odd.

Odd number: $x = 2n + 1$

$$x^2 = (2n+1)^2$$
$$= 4n^2 + 4n + 1$$
$$= 2\underbrace{(2n^2 + 2n)}_{k} + 1$$

#

Direct Proof.

Prove:

If x, y are odd, then xy is odd.

$x = 2k + 1$

$y = 2j + 1$

$$xy = (2k + 1)(2j + 1)$$

$$= 4kj + 2k + 2j + 1$$

$$= 2(2kj + k + j) + 1$$

odd

Direct Proof.

Prove:

- If $5|2a$ for $a \in \mathbb{Z}$, then $5|a$.

Assume $5|2a$, $\forall\, a \in \mathbb{Z}$.

$5j = 2a$ **some** $j \in \mathbb{Z}$.

odd

even

even $j = 2k$ for some $k \in \mathbb{Z}$

$5(2k) = 2a$

$5k = a$

$5|a$

Direct Proof.

Prove:

- ❑ If $7|4a$ for $a \in \mathbb{Z}$, then $7|a$.
- ❑ Every odd integer is a difference of two squares. $(13 = 7^2 - 6^2)$

Direct Proof.

❑ **Every odd integer is a difference of two squares.** $(13 = 7^2 - 6^2)$

$$1 = 1^2 - 0^2$$

$$3 = 2^2 - 1^2$$

$$5 = 3^2 - 2^2$$

$$2(0) + 1 = 1^2 - 0^2$$

$$2(1) + 1 = 2^2 - 1^2$$

$$2(2) + 1 = 3^2 - 2^2$$

trial-and-error method

Trial and error is a fundamental method of problem-solving. It is characterized by repeated, varied attempts which are continued until success, or until the practicer stops trying.

$$2k + 1 = (k + 1)^2 - k^2$$

$$= k^2 + 2k + 1 - k^2$$

$$= 2k + 1$$

E.g. $2(69) + 1 = 139 = 70^2 - 69^2$

Direct Proof.

- **if m and n are both perfect squares, then nm is also a perfect square.**

An integer that can be expressed as the square of another integer is called a **perfect square**.

- $m = s^2$
- $n = t^2$

$$m \cdot n = s^2 \cdot t^2 = s \cdot s \cdot t \cdot t = s \cdot t \cdot s \cdot t = (st)^2$$

#

Direct Proof.

- [ ] Prove that if x and y are nonnegative real numbers, then: $\frac{x+y}{2} \geq \sqrt{xy}$

This is called the Arithmetic-Geometric Mean Inequality.

$$\frac{x+y}{2} \geq \sqrt{xy}$$

$$\left(\frac{x+y}{2}\right)^2 \geq (\sqrt{xy})^2$$

$$\frac{x^2+2xy+y^2}{4} \geq xy$$

$$x^2+2xy+y^2 \geq 4xy$$

$$x^2+2xy+y^2-4xy \geq 0$$

$$x^2-2xy+y^2 \geq 0$$

$$(x-y)^2 \geq 0$$

#

Direct Proof.

- Use a direct proof to show that the sum of two odd integers is even.

- Prove that if n and m are positive, even integers, then nm is divisible by 4.

- A perfect number is a positive integer n such that the sum of the factors of n is equal to 2n (1 and n are considered factors of n). So, 6 is a perfect number since 1 +2+3+6 = 12 = 2∗6. Prove that a prime number cannot be a perfect number.

For any prime number P, its divisors are P and 1. The sum of these divisors is (P+1), which is always less than 2P.

- If x and y are integers and $x^2 + y^2$ is even, prove that $x + y$ is even.

Proof by Case

Prove: $\varphi \vee \psi \rightarrow x$

Assume φ

Show x

Assume ψ

Show x

(If either φ (phi) or ψ(psi) is true, then x is true)

Prove:

If $n \in \mathbb{Z}$, $n^2 + 3n + 4$ is even

Case 1: n is odd

$$(2k+1)^2 + 3(2k+1) + 4$$

$$= 4k^2 + 4k + 1 + 6k + 3 + 4$$

$$= 4k^2 + 10k + 8$$

Case 2: n is even

$$(2k)^2 + 3(2k) + 4$$

$$= 4k^2 + 6k + 4$$

Proof by Case

- **Prove: If** $m + n$ **and** $n + p$ **are even, where** $m, n, p \in \mathbb{Z}$**, then** $m + p$ **is even.**

- **Prove: If** $x, y \in \mathbb{R}$**, then** $\max(x, y) + \min(x, y) = x + y$.

Proof by Case

- **Prove: If $m + n$ and $n + p$ are even, where $m, n, p \in \mathbb{Z}$, then $m + p$ is even.**

Case 1:
$\boldsymbol{m + n}$ = **even** so, there are 2 possibilities:
- m and n are both even
- m and n are both odd

Case 2:
$\boldsymbol{n + p}$ = **even** so, there are 2 possibilities:
- n and p are both even
- n and p are both odd

✓ If n is even, then from the first case, m has to be even and from the second case, p has to be even - hence, $m + p$ = even
✓ If n is odd, then from the first case, m has to be odd and from the second case, p has to be odd - hence, $m + p$ = even

So, $\boldsymbol{m + p}$ is always even

Proof by Case

- **Prove: If** x, y ∈ ℝ, **then** $\max(x, y) + \min(x, y) = x + y$.

- **How many cases are there?**

Case 1: $x \geq y$

$$
\begin{array}{rl}
 & \min(x, y) = y \\
+ & \\
 & \max(x, y) = x \\
\hline
 & x + y
\end{array}
$$

Case 2: $x < y$

$$
\begin{array}{rl}
 & \min(x, y) = x \\
+ & \\
 & \max(x, y) = y \\
\hline
 & x + y
\end{array}
$$

Proof by Case

$|x| = a$ → $x = +a$, $x = -a$

- Prove that for all $x \in \mathbb{R}$,

$$-5 \leq |x+2| - |x-3| \leq 5$$

Case 1: $\boldsymbol{x \leq -2}$: $-5 \leq -(x+2) + (x-3) \leq 5$

Case 2: $\boldsymbol{-2 < x \leq 3}$: $-5 \leq (x+2) + (x-3) \leq 5$

Case 3: $\boldsymbol{x > 3}$: $-5 \leq (x+2) - (x-3) \leq 5$

For any real number x, prove $|x-6| + x > 3$

By Cases and Direct Proof.

- If x ***or*** y are odd, check if xy is odd.

Case 1:

$x = 2k + 1$

$y = 2j + 1$

Case 2:

$x = 2k$

$y = 2j + 1$

Case 3:

$x = 2k + 1$

$y = 2j$

Tips for proof by Cases

When the hypothesis is, "n is an integer."	Case 1: n is an even integer. Case 2: n is an odd integer.
When the hypothesis is, "m and n are integers."	Case 1: m and n are even. Case 2: m is even and n is odd. Case 3: m is odd and n is even. Case 4: m and n are both odd.
When the hypothesis is, "x is a real number."	Case 1: x is rational. Case 2: x is irrational.
When the hypothesis is, "x is a real number."	Case 1: $x = 0$ OR Case 1: $x > 0$ Case 2: $x \neq 0$ Case 2: $x = 0$ Case 3: $x < 0$
When the hypothesis is, "a and b are real numbers."	Case 1: $a = b$ OR Case 1: $a > b$ Case 2: $a \neq b$ Case 2: $a = b$ Case 3: $a < b$

Proof by Case

- If n is an integer, prove that $n^3 - n$ is even.

- If n is an integer, prove $n \leq n^2$.

- If $n \in \mathbb{Z}$, prove $n^2 + 3n + 2$ is even.

- Show that if an integer n is not divisible by 3, then $n^2 = 3k + 1$ for some integer k.

- If $n \in \mathbb{Z}$, prove $n^2 + 3n + 5$ is an odd integer.

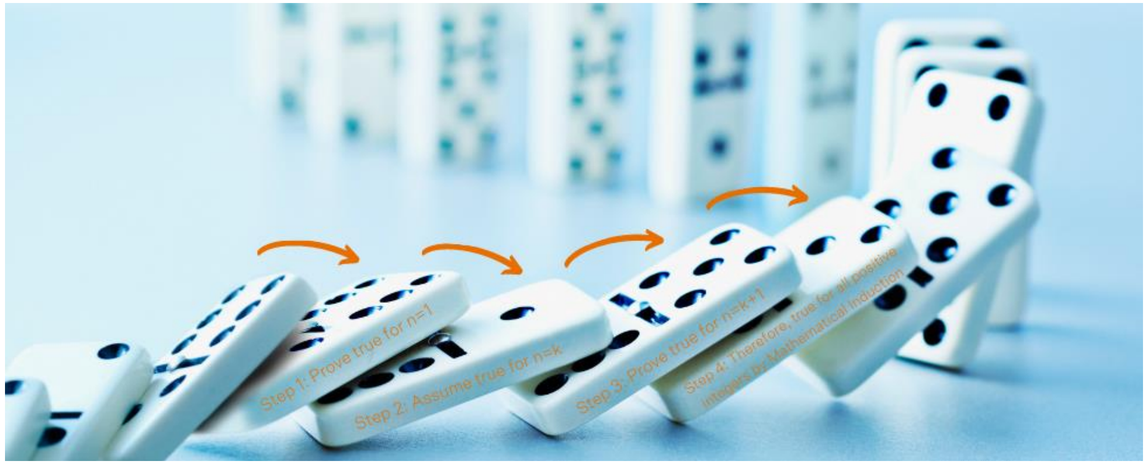
- If x is a real number such that $\frac{x^2-1}{x+2} > 0$, then either $x > 1$ or $-2 < x < -1$.

Proof by Induction

Base Case: 1st thing is true.

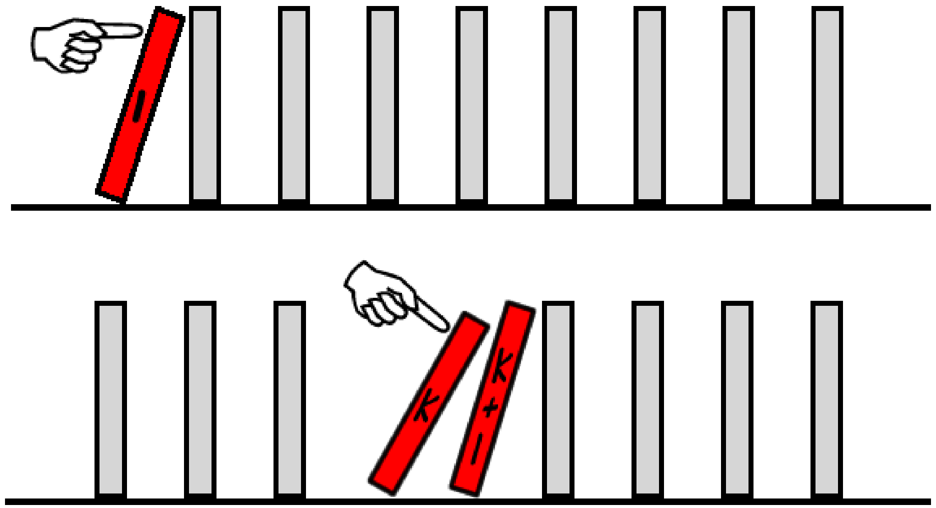
Inductive Hypothesis: Assume is true $n \leq k$. Show $k + 1$ is true.

Conclusion: Every n is true.



How Mathematical Induction Works

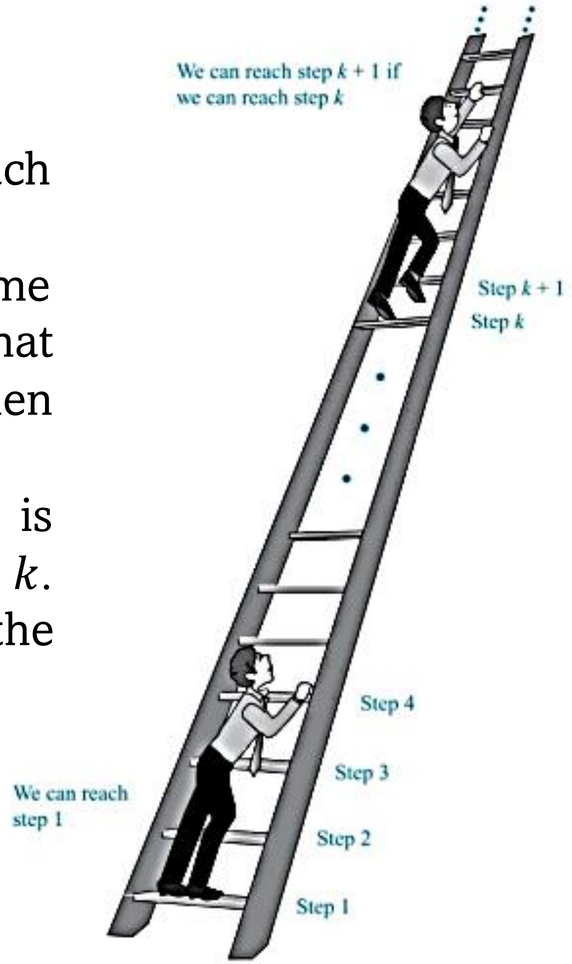
Consider an infinite sequence of dominoes, labeled 1,2,3, … , where each domino is standing.
Let $P(n)$ be the proposition that the nth domino is knocked over. Know that the first domino is knocked down, i.e., $P(1)$ is true. We also know that if whenever the kth domino is knocked over, it knocks over the $(k+1)th$ domino, i.e, $P(k) \rightarrow P(k+1)$ is true for all positive integers k. Hence, all dominos are knocked over. $P(n)$ is true for all positive integers n.



Climbing an Infinite Ladder

- ✓ BASIS STEP: we can reach rung 1.
- ✓ INDUCTIVE STEP: Assume the inductive hypothesis that we can reach rung k. Then we can reach rung $k + 1$.

Hence, $P(k) \rightarrow P(k+1)$ is true for all positive integers k. We can reach every rung on the ladder.

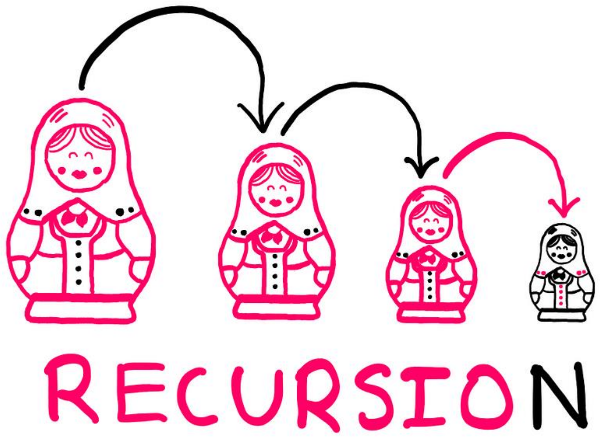


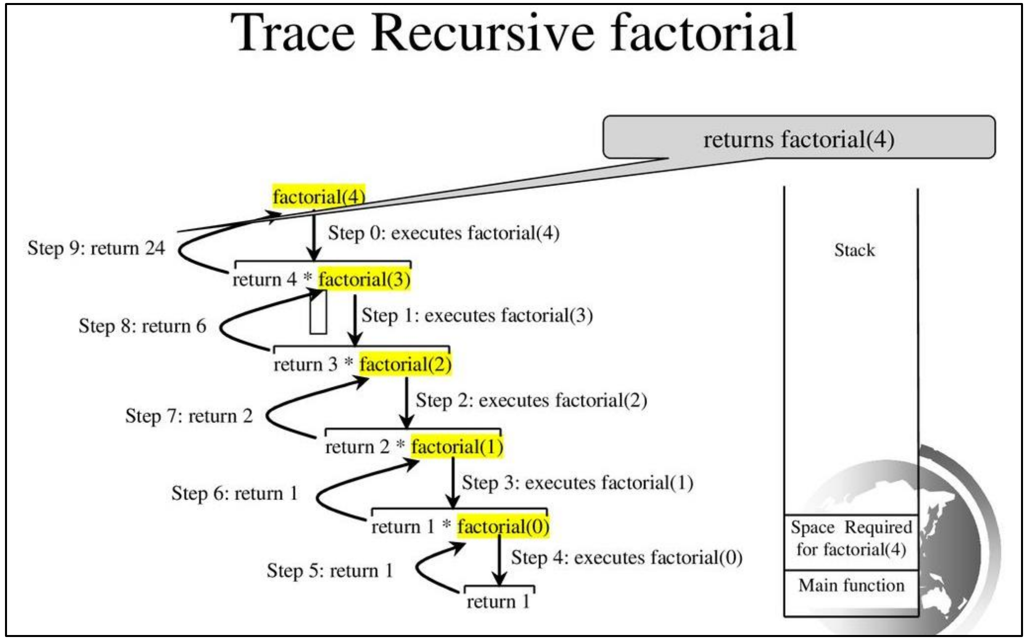
Why Base Case?

- Recursive functions are functions that calls itself. It is always made up of 2 portions, the base case and the recursive case. The base case is the condition to stop the recursion. The recursive case is the part where the function calls on itself.

- The base case is a way to return without making a recursive call. In other words, it is the mechanism that stops this process of ever more recursive calls and an ever-growing stack of function calls waiting on the return of other function calls.

- If a recursion never reaches a base case, it will go on making recursive calls forever and the program will never terminate. This is known as infinite recursion, and it is generally not considered a good idea. In most programming environments, a program with an infinite recursion will not really run forever.





Proof by Induction

Show $1+2+\cdots+n=\frac{n(n+1)}{2}$

Base Case: **Assume n = 1.**

$$1=\frac{1(1+1)}{2}$$

Inductive Hypothesis: **Assume $n \leq k$ is true.**

$$1+2+\cdots+k=\frac{k(k+1)}{2}$$

Show $k+1$ is true.

$$1+2+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}$$

$$\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)(k+2)}{2}$$

$$\frac{k(k+1)+2(k+1)}{2}=\frac{k^2+3k+2}{2}$$

$$\frac{k^2+k+2k+2}{2}=\frac{k^2+3k+2}{2}$$

$$\frac{k^2+3k+2}{2}=\frac{k^2+3k+2}{2}$$

$k \Longrightarrow k+1$ is true, inductively proved.

Proof by Induction

Prove that $n^3 + 2n$ is divisible by $3\ \forall n \in \mathbb{Z}^+$

Base: **Assume** $n = 1.$

$$1^3 + 2 \times 1 = 3 \qquad \frac{3}{3}$$

I.H: **Assume** $n = k$ **is true.**

$$3 | (k^3 + 2k)$$

$$3m = k^3 + 2k, \qquad m \in \mathbb{Z}^+$$

Show $n = k + 1$ **is true.**

$$\underbrace{(k+1)^3 + 2(k+1)}_{} = k^3 + 3k^2 + 3k + 1 + 2k + 2$$

$$= k^3 + 3k^2 + 5k + 3$$

$$= k^3 + 2k + 3k^2 + 3k + 3$$

$$= 3m + 3(k^2 + k + 1)$$

$$= 3\underbrace{(m + k^2 + k + 1)}_{\in \mathbb{Z}}$$

divisible by 3

$3 | n^3 + 2n, \forall n \in \mathbb{Z}$ ⟷ $3 | (k+1)^3 + 2(k+1)$

Proof by Induction

Prove that $2^n < n!$ **for** $n \in \mathbb{Z}^+$ **and** $n > 3$.

$n \geq 4$

Base: **Assume n = 4.**

$(2^4 = 16) < (4! = 24)$

I.H: **Assume n = k is true.**

$2^k < k!$

$2 < 4$, $k + 1 \geq 4$ } $k + 1 > 2$

$2^{k+1} = 2^k \cdot 2 < k!(k+1) = (k+1)!$

Show $n = k + 1$ **is true.**

$k \Longrightarrow k + 1$ **is true, inductively proved.**

$2^n < n!$ **for** $n \in \mathbb{Z}^+$ **and** $n > 3$

Proof by Induction with Derivatives

Show that $f(x) = x^n$ **implies** $f'(x) = nx^{n-1}$ **for all** $n \geq 1$.

Base: **Assume** $n = 1$.

$$f(x) = x \qquad f'(x) = 1x^0 = 1$$

I.H: **Assume n = k is true.**

$$f(x) = x^k \qquad f'(x) = kx^{k-1}$$

Show $n = k + 1$ **is true.**

$$f(x) = x^{k+1} = x^k x$$

$$f'(x) = kx^{k-1}x + x^k \cdot 1$$

$$= kx^k + x^k$$

$$= x^k(k + 1)$$

Proof by Induction with Matrices

Show that $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ **implies** $A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}$ **for all** $n \geq 1$.

Base: **Assume** $n = 1$.

$$A^1 = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a^1 & 0 \\ 0 & b^1 \end{bmatrix}$$

I.H: **Assume** $n = k$ **is true.**

$$A^k = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix}$$

Show $n = k + 1$ **is true.**

$$A^{k+1} = A^k A = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$$= \begin{bmatrix} a^k a + 0 \cdot 0 & a^k \cdot 0 + 0 \cdot b^k \\ 0 \cdot a + b^k \cdot 0 & 0 \cdot 0 + b^k b \end{bmatrix}$$

$$= \begin{bmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{bmatrix}$$

Proof by Induction

- Prove that $\sum_{i=0}^{n} 2i = n(n+1)$.

- Prove that $n^3 - n$ is divisible by 3 for any integer n ≥ 0.

- Prove $\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}^n = \begin{bmatrix} a^n & na^{n-1} \\ 0 & a^n \end{bmatrix}$ for every natural number n.

Proof by Contradiction

We want to prove φ

1. Assume $\neg\varphi$
2. Find some contradiction $\psi \wedge \neg\psi$
3. Claim $\neg\neg\varphi$
   $= \varphi$

Proof by Contradiction

φ

Show that $\sqrt{2}$ is irrational.

Assume $\sqrt{2}$ is rational.

$$\sqrt{2} = \frac{a}{b},$$ *where a, b in lowest terms*

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2 \rightarrow a^2 \text{ is even} \rightarrow (a \cdot a)\text{even} \rightarrow a \text{ is even}$$

$$2b^2 = (2k)^2$$

$$2b^2 = 4k^2$$

$$b^2 = 2k^2 \rightarrow b^2 \text{ is even} \rightarrow b \text{ is even}$$

$$\frac{a(even)}{b(even)}$$

not in lowest terms

by contradiction $\sqrt{2}$ **not rational**

Proof by Contradiction

Prove that $(A - B) \cap (B - A) = \emptyset$.

$$(A \cap \bar{B}) \cap (B \cap \bar{A}) = \emptyset$$

Assume $(A \cap \bar{B}) \cap (B \cap \bar{A}) \neq \emptyset$

$$\exists x \in U \mid x \in ((A \cap \bar{B}) \cap (B \cap \bar{A}))$$

$x \in A \cap \bar{B}$ **and** $x \in B \cap \bar{A}$

$x \in A$ **and** $x \in \bar{B}$ **and** $x \in B$ **and** $x \in \bar{A}$

by contradiction **set is empty** $\emptyset$

Proof by Contradiction

- Show that at least four of any 22 days must fall on the same day of the week.

$$p = \{at\ least\ four\ of\ 22\ chosen\ days\ fall\ on\ the\ same\ day\ of\ the\ week\}$$

$$\neg p\ is\ true\ (not\ 4, \boldsymbol{3\ days})$$

$Suppose, within\ 22\ days\ we\ can\ have\ 3\ same\ week\ days.$

$21\ days\ but\ this\ {\color{red}contradicts}\ the\ premise\ that\ we\ have\ 22\ days\ under\ consideration.$

$7\ days\ in\ a\ week$

#

Proof by Contradiction

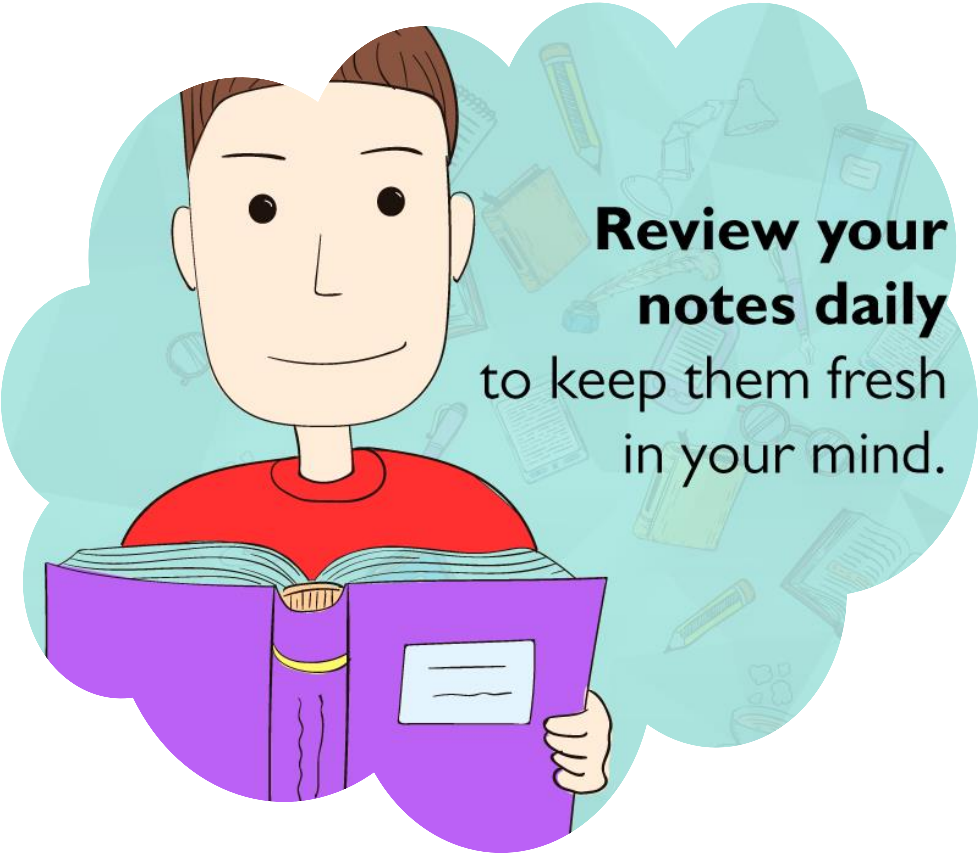
- Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

- Show that at least ten of any 64 days chosen must fall on the same day of the week.

- Show that if you pick three socks from a drawer containing just blue socks and black socks, you must get either a pair of blue socks or a pair of black socks.

- Prove that if n is a perfect square, then $n + 2$ is not a perfect square.

- Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.


Review your notes daily
to keep them fresh in your mind.

Practice time

Direct proof

- Prove that if m and n are integers and mn is even, then m is even or n is even.

- Prove that if x is irrational, then $1/x$ is irrational.

- Prove that if x is rational and $x \neq 0$, then $1/x$ is rational.

- Use a direct proof to show that the product of two rational numbers is rational.

- Prove that if n is a positive integer, then n is even if and only if $7n + 4$ is even.

- Prove that if n is a positive integer, then n is odd if and only if $5n + 6$ is odd.

Proof by Cases

- Prove that if n is an integer, then $3n^2 + n + 14$ is even
- Prove that if n is an integer, then $2n^2 + n + 1$ is not divisible by 3
- $\forall x \in \mathbb{R}$ prove if $|x - 3| > 3$ then $x^2 > 6x$
- Prove that the equation $2x^2 + y^2 = 14$ has no positive integer solutions.
- If x and y are integers and both $x \cdot y$ and $x + y$ are even, then both x and y are even.
- Prove that if m and n are consecutive integers, then the sum $\mathrm{m} + n$ is odd.
- Let $x, y \in \mathbb{Z}$, prove that x and y are of the same parity if and only if $x + y$ is even.

Proof by Induction

- Prove that:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

- Prove that:

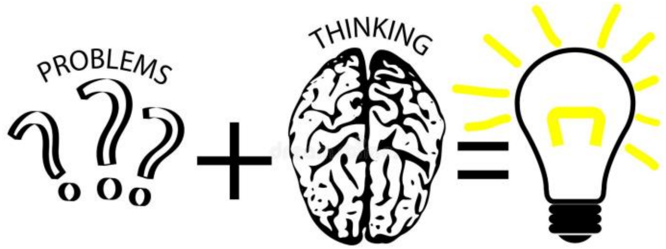
$$1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

- Prove that $9^n + 3$ is divisible by 4.

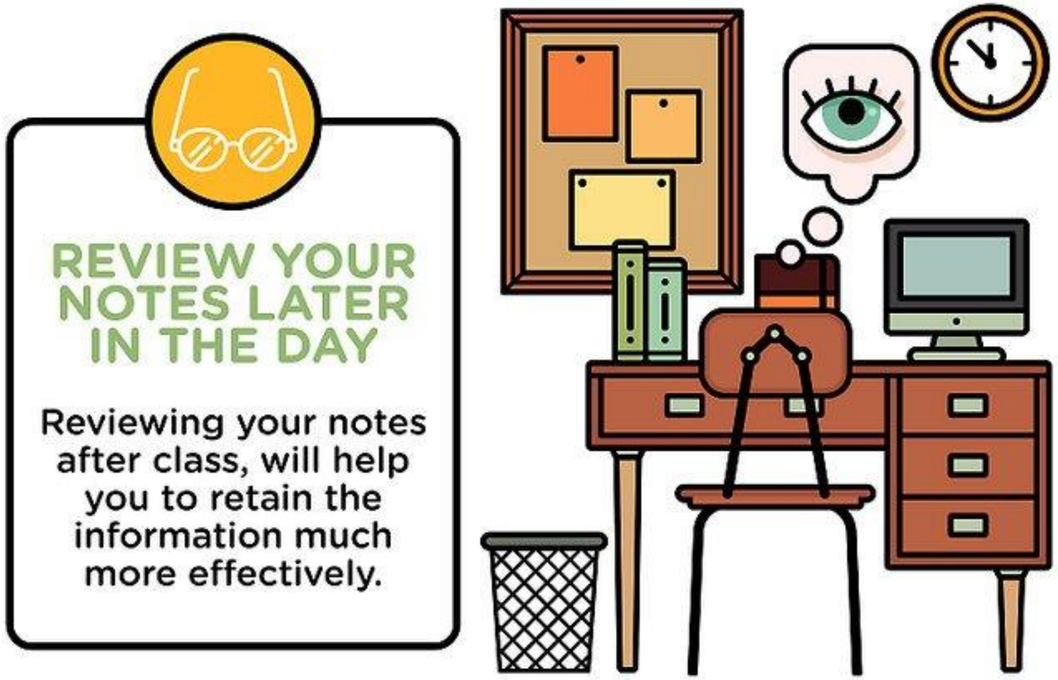
- Suppose $a_0 = 1$, $a_1 = 2$ and for every $n > 1$, $a_n = 3a_{n-1} - 2a_{n-2}$. Find a simple formula for the value of a_n and prove that it is correct.

- Prove that any $n \geq 8$ can be expressed as $3x + 5y$ where $x \geq 0$ and $0 \leq y < 3$.

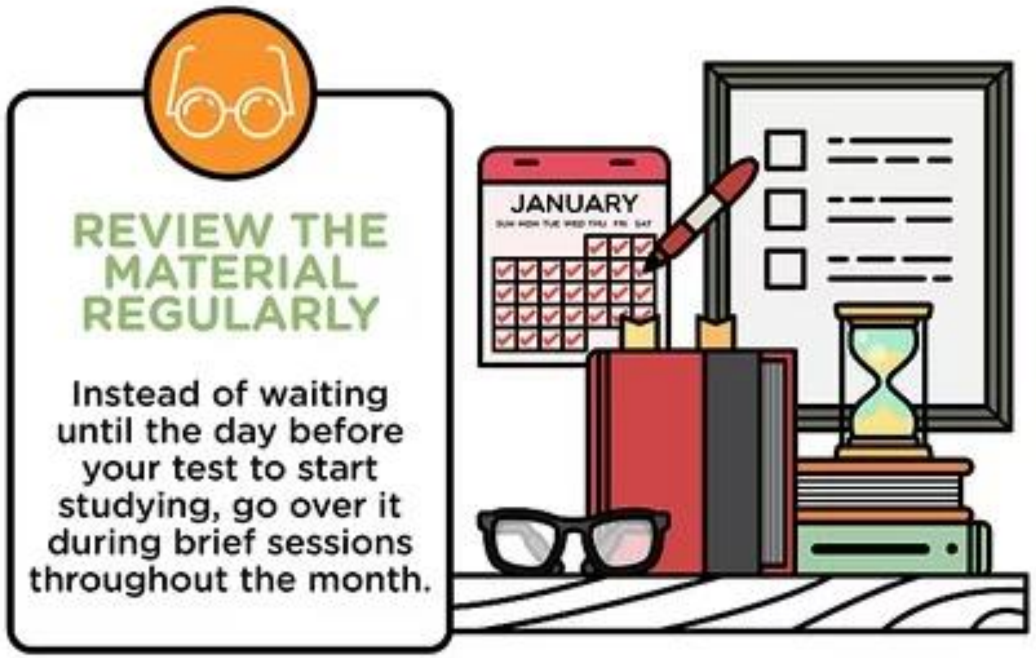
Proof by Contradiction



- Suppose $n \in Z$. If n^2 is odd, then n is odd.
- If $a, b \in Z$, then $a^2 - 4b - 2 \neq 0$
- If $a, b \in Z$, then $a^2 - 4b - 3 \neq 0$
- If A and B are sets, then $A \cap (B - A) = \emptyset$.
- There exist no integers a and b for which $21a + 30b = 1$.
- There exist no integers a and b for which $18a + 6b = 1$.
- For every $n \in Z, 4 \nmid (n^2 + 2)$
- Show that if n is an integer and $n^3 + 5$ is odd, then n is even.


REVIEW YOUR NOTES LATER IN THE DAY
Reviewing your notes after class, will help you to retain the information much more effectively.

Study Tip


REVIEW THE MATERIAL REGULARLY
Instead of waiting until the day before your test to start studying, go over it during brief sessions throughout the month.
JANUARY