The Fundamental Course

Next Chapter:

Proof Techniques

- By Deepak Poonia(IISc Bangalore)

Instructor:

Deepak Poonia

IISc Bangalore

GATE CSE AIR 53; AIR 67; AIR 206; AIR 256;

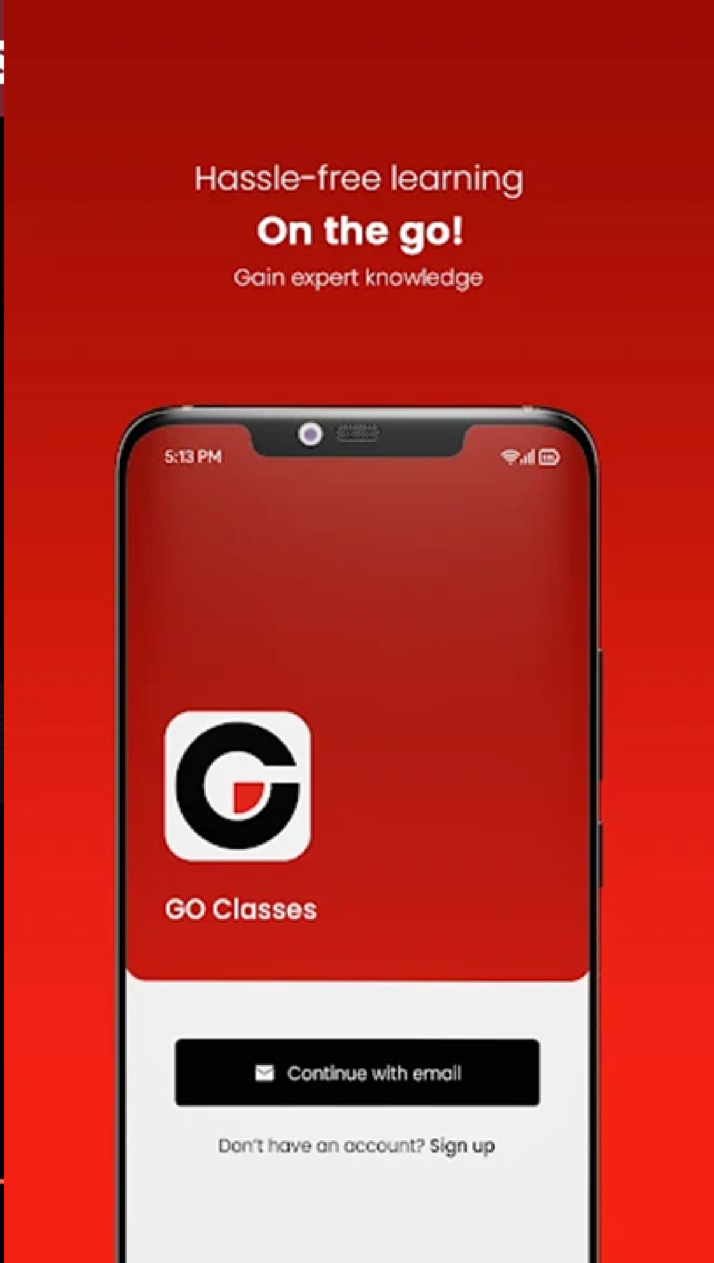
Discrete Mathematics Complete Course:

https://www.goclasses.in/courses/Discrete-Mathematics-Course

Download the GO Classes Android App:

https://play.google.com/store/apps/details?id=com.goclasses.courses

Search “GO Classes” on Play Store.



NOTE :

Complete Discrete Mathematics & Complete Engineering Mathematics Courses, by GO Classes, are **FREE** for ALL learners.

Visit here to watch : https://www.goclasses.in/s/store/

SignUp/Login on Goclasses website for free and start learning.

We are on Telegram. **Contact us** for any help.

Link in the Description!!

Join GO Classes **Doubt Discussion** Telegram Group :

Username:

@GATECSE_Goclasses

We are on Telegram. **Contact us** for any help.

Join GO Classes Telegram Channel, Username: @GOCLASSES_CSE

Join GO Classes **Doubt Discussion** Telegram Group :

Username: @GATECSE_Goclasses

(Any doubt related to Goclasses Courses can also be asked here.)

Join GATEOverflow Doubt Discussion Telegram Group :

Username: @GateOverflow_CSE

"Proof Techniques:"

"Prove that ......"

Proof Techniques:

GATE is an Objective Exam.. Then..

1. WHY study Proof Techniques??

GATE is an Objective Exam.. Then WHY study Proof Techniques??

1. To improve Analytical Skills.
2. To improve Problem Solving Skills.

GATE is an Objective Exam.. Then WHY study Proof Techniques??

3. To "Understand" concepts... Without Rote-Learning them.

4. To Feeeel Good.

GATE is an Objective Exam.. Then WHY study Proof Techniques??

5. For MTech/MS(or MTech RA) Interviews in IITs, IISc etc.

6 → "Proof Technique"

"Joy" = $\checkmark$

Proof Techniques:

Q 2: Can anyone Ever become "Expert" at proving things?? → NO

Goldbach's $\boxed{\text{conjecture}}$

Article Talk

From Wikipedia, the free encyclopedia

Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states that every even natural number greater than 2 is the sum of two prime numbers.

No one knows

True or false

Goldbach Conjecture

Any even integer $n > 2$

$$\boxed{n = p_1 + p_2}$$

Statement
Not Yet Proven
& Not Yet Disproven

Open Statement

Goldbach Conjecture:

Any even integer $n > 2$ then $n = p_1 + p_2$

$4 = 2 + 2$

$6 = 3 + 3$

$8 = 3 + 5$

$10 = 5 + 5$

$12 = 7 + 5$

$\vdots$

Proof Techniques:

Our Purpose:

Understand the Proofs once it is taught to you...

Proof Techniques:

Our Purpose:

Understand the Proofs..

"Coming up with proof yourself" is HARD.

Don't get demotivated

- if you couldn't come up with a proof,
- if you couldn't write a proof,
- if you couldn't think in a particular way of proving.

Be happy when you understand a proof which is taught to you.

Let's start...

Some

Basic Terminology:

TERMINOLOGY

Definition: Something given (No Proof)

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

Theorem: Something to be proved → proven Result

Even Number:

Definition:

$\boxed{\text{an integer which is multiple of 2.}}$

Ex:

Let a matrix of size 2*2 with all values being negative be called "tiktik".

Definition of TikTik

$$\begin{bmatrix} -2 & -1.5 \\ -\pi & -2 \end{bmatrix}_{2\times 2} \rightarrow \text{a TikTik}$$

Definition 1. *An integer number n is **even** if and only if there exists a number k such that $n = 2k$.*

Definition 2. *An integer number n is **odd** if and only if there exists a number k such that $n = 2k + 1$.*

Definition 3. *Two integers a and b are **consecutive** if and only if $b = a + 1$.*

Integer n ;

n is even iff there is some integer k such that $n = 2k$.

$-10 = 2(k)$

$k \to -5$

integer

even

$0 = 2(0)$

$0 \to k$

integer

Not even

$19 = 2(k)$

integer

No such integer k

Integer n ;

n is odd iff there is some integer k such that $n = 2k+1$

$3 = 2(k)+1$

integer $= 1$

NOT odd

$0 = 2(k)+1$

No such integer k

integer

Consecutive Integers;

Int a, b

$\boxed{b = a + 1}$ or $\boxed{a = b + 1}$

$4, 3$

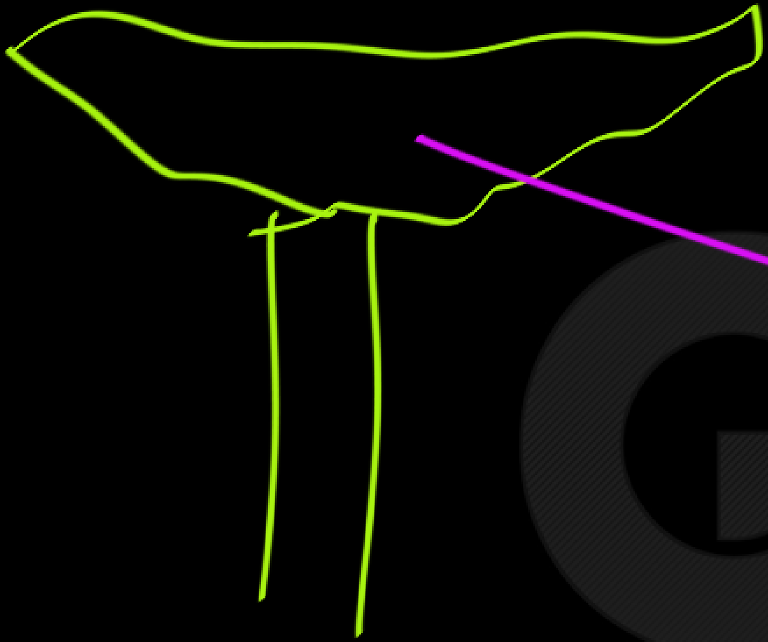
$4 = 3 + 1$

$5, 6$

$6 = 5 + 1$

Some Terminologies

- Axioms: Statements that are always true.
  - Example: Given two distinct points, there is exactly one line that contains them.
- Definitions: Used to create new concepts in terms of existing ones
- Theorem: A proposition that has been proved to be true.



Analogy

Euclid's 5 Axioms

Tree of Geometry

seed → axiom

Axioms are like Seeds... the whole Tree grows over them.

Axiom : Considered to be True
Assumed " " "
Taken " " "

by ALL People

Probability: we will study later.

3 Axioms

① $\boxed{0 \leq P(E) \leq 1}$ → Axiom

we have Assumed it to be True.

②

③

Example of Axioms:

Some Axioms for the Real Numbers:

1. For all real numbers x and y, x + y is a real number.
2. For all real numbers x and y, x · y is a real number.

Example of Axioms:

Some Axioms for the Real Numbers:

3. For all real numbers x and y, exactly one of

$x = y$, $x > y$, or $y > x$ is true.

Real a, b

$a = b$ OR $a > b$ OR $b > a$

Exactly one of them will be True.

Example of Axioms:

AXIOMS AND POSTULATES OF EUCLID

This version is given by Sir Thomas Heath (1861-1940) in *The Elements of Euclid.* (1908)

AXIOMS

1. Things which are equal to the same thing are also equal to one another.
2. If equals be added to equals, the wholes are equal.
3. If equals be subtracted from equals, the remainders are equal.
4. Things which coincide with one another are equal to one another.
5. The whole is greater than the part.

numbers:

$c = a$

$a = b$

$b = c$? Yes

$a = b \rightsquigarrow a + c = b + c$

Did you know?

In mathematics or logic, an *axiom* is an unprovable rule or first principle accepted as true because it is self-evident or particularly useful. “Nothing can both be and not be at the same time and in the same respect” is an example of an axiom. The term is

7 Axioms are the truths you cannot deduce from other axioms :) – user65203 May 3, 2016 at 10:57

12 @emory: "axioms are true" is an axiom. – user65203 May 3, 2016 at 12:04

4 "axioms are true" is an axiom, is an axiom – Matt May 3, 2016 at 14:44

28

In mathematics, every result known descends from something else: it is proven to be true from other facts.

The one exception is axioms: these things we choose to accept without proving them.

We have to choose some axioms, since we cannot prove anything with nothing, but we try and make them as simple and obvious as possible.

For example, Euclidean geometry rests on five axioms, the first of which is "given two points on a plane, it is always possible to construct a straight line passing through these two points". Another states that it is possible to draw a circle with any center and radius.

Using these simple statements, Euclid then proceeds to prove more complex properties of figures on the plane.

Basic Definitions

An integer n is an even number
if there exists an integer k such that $n = 2k$.

An integer n is an odd number
if there exists an integer k such that $n = 2k+1$.

$2.2 \rightarrow$ Not even

$\rightarrow$ Not odd

even, odd : for integers

Q :

Take Two Same integers

a, a

Q :

Take Two Same even integers

Q :

Take Two Same even integers

$2k$, $2k$

Q :

Take Two Same odd integers

$2k+1, \quad 2k+1$

Q :

Take Two even integers

Q :

Take Two even integers

2, 4 ✓

2, 2 ✓

$\boxed{2k, 2k}$ ✗

Can't cover 2, 4 type of possibilities

2a, 2b

2, 4

2, 2

Q :

Take Two odd integers

$\boxed{2k+1, \quad 2k+1}$ ✗

$2a+1, \quad 2b+1$

int int

Q :

Take Two different odd integers

$\boxed{2a+1,\ 2b+1}$ & $a \neq b$

int int

Q :

Take Two different even integers

$2a, 2b$ where $a \neq b$.

int int

Proof Techniques
(Basic)

- Disproof by counterexample
- Exhaustive proof
- Direct proof
- Proof by contraposition
- Proof by contradiction

" " Induction

Tools

IISc B'l

Graph Theory

My Specialization

Gallai's Path Decomposition Conjecture

open problem

for All Graphs → Conjecture

for all Complete Graphs → Proven ✓

for all bipartite Graphs → Proven

for Block Graphs → proven ✓

Methods of Proof:

1 Direct Proof

→ Proof Technique

To prove: $\boxed{\text{If } P \text{ then } Q}$

Direct Proof Technique:

Start with P (Assume)

Apply facts you already know

Derive Q

Direct proof of $P \Rightarrow Q$

This is the simplest, and most natural, method of proof. *Try this first before considering other methods.*

Assume P.
...
[Logical deductions]
...
Therefore Q.

Q : We know that even number is a integer which is multiple of 2.

Prove that every integer which is multiple of some even number, is even number.

(i.e. Even Integer * Any Integer = Even Integer)

$\boxed{\text{Even} \times \text{Integer} = \text{Even}}$ To prove.

To Prove: If $\boxed{a \text{ is even}}$ then $ab = \text{even}$

p

b: any integer

P: → a is even ; b is any integer

$a = 2k$ → integer

$ab = (2k)b = 2(kb)$

k → int, b → int

$ab = 2(\text{some int})$

facts you know

So

Q: → ab = even = 2 (some int)

Note:

Int a is Divisible by int b

means: $\boxed{a = bk}$ → Some integer k

8 is Divisible by 2 $\equiv$ $8 = 2(k)$ → 4

- Example 1: show that every integer divisible by 6 is divisible by 3

- Example 1: show that every integer divisible by 6 is divisible by 3

Int a

If 'a' is divisible by 6 then 'a' is Divisible by 3.

P: int a ; a is Divisible by 6

$a = 6k$ → int

$a = (3 * 2)k$

$a = 3(2k)$ → int

$a = 3(\text{int})$

Apply knowledge that you have

Q: $\boxed{\text{a is Divisible by 3}} \equiv a = 3(\text{some int})$

- Example 1: show that every integer divisible by 6 is divisible by 3
  - Pf. Let x be an integer divisible by 6. There exists an integer y S.T. $x = 6 \cdot y$. Therefore $x = 3 \cdot 2 \cdot y$, and x is divisible by 3.

Theorem 1. *If a and b are consecutive integers, then the sum $a + b$ is odd.*

Prove it.

Theorem 1. *If a and b are consecutive integers, then the sum $a + b$ is odd.*

P: a, b are Cons. Ints.

$$a = b + 1$$

$$a + b = (b+1) + b = 2b + 1$$

$$\underbrace{2b}_{\text{int}}$$

$$a + b = 2(\text{int}) + 1$$

Q: $a + b = \text{odd} = 2(\text{int}) + 1$

Theorem 1. *If a and b are consecutive integers, then the sum $a+b$ is odd.*

Proof. Assume that a and b are consecutive integers. Because a and b are consecutive we know that $b = a+1$. Thus, the sum $a+b$ may be re-written as $2a+1$. Thus, there exists a number k such that $a+b = 2k+1$ so the sum $a+b$ is odd. $\square$

Prove "The sum of two even integers is even".

Prove "The sum of two even integers is even".

P : Two even integers

$(2k) + (2k) = 4k = 2(2k)$ even

same even int

WRONG

Prove "The sum of two even integers is even".

P : Two even integers

Same

Same

$2k + 2k = 2(2k)$

int

even

Hence Proves

Prove "The sum of two even integers is even".

P : Two even integers

Any two even int

2, 4 ✓

2, 2 ✓

6, 100 ✓

Prove "The sum of two even integers is even".

P : Two even integers

$$\underbrace{2a}_{\text{int}} + \underbrace{2b}_{\text{int}} = 2(\underbrace{a+b}_{\text{int}})$$

$$= 2(\text{int}) = \text{even}$$

Prove "The sum of two even integers is even".

$p \to q$ $\boxed{\text{If}}$ I add 2 even integers, $\boxed{\text{then}}$ the sum is even.

$\underbrace{\text{I add 2 even integers}}_{p}$, $\underbrace{\text{the sum is even}}_{q}$

Assume a and b are even integers. Then $a = 2k$ for some $k \in \mathbb{Z}$ and $b = 2m$ for some $m \in \mathbb{Z}$.

$$\begin{aligned} a + b &= 2k + 2m \\ &= 2(k+m) \\ &= 2r \text{ where } r = k+m,\ r \in \mathbb{Z} \end{aligned}$$

$\therefore$ The sum of two even integers is even

QED

Prove " If n is an odd integer, then n^2 is odd "

EXAMPLE 1 Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

HW

Source: Discrete Mathematics and Its Applications

Seventh Edition Kenneth H. Rosen

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

Assume x is odd

$$x = 2n+1$$

$$x^2 = (2n+1)^2$$

$$= 4n^2 + 4n + 1$$

Prove " $\boxed{\text{If}}$ n is an odd integer, $\boxed{\text{then}}$ $\boxed{n^2 \text{ is odd}}$ "

$\boxed{p} \rightarrow q$

$p \longrightarrow q$

Even integer

$n = 2k, \ k \in \mathbb{Z}$

Odd integer

$$\boxed{n = 2k+1, \ k \in \mathbb{Z}}$$

Assume n is an odd integer. Then $n = 2k+1, \ k \in \mathbb{Z}$ by defn. of an odd integer.

$(n)^2 = (2k+1)^2 \longrightarrow (2k+1)(2k+1)$

$n^2 = 4k^2 + 4k + 1$

$n^2 = 2(\underline{2k^2 + 2k}) + 1$

$n^2 = 2r + 1$ where $r = 2k^2 + 2k, \ r \in \mathbb{Z}$

$\therefore n^2$ is odd $\square$ Δ QED

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

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

$\to p$

$\to q$

P : x, y are odd

$$\left\{\begin{array}{l} x = 2k+1 \\ y = 2k+1 \end{array}\right\}$$

Proving for same odd numbers

NOT what Ques is asking

Q : $xy = \text{odd} = 2(\text{int}) + 1$

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

$\rightarrow p$ $\quad$ $\rightarrow q$

p : x, y are odd

$$x = 2a + 1 \quad a \rightarrow \text{int}$$
$$y = 2b + 1 \quad b \rightarrow \text{int}$$

$$xy = 4ab + 2a + 2b + 1$$
$$= 2(2ab + a + b) + 1 \implies xy = 2(\text{int}) + 1$$

$xy = \text{odd}$

q : $xy = \text{odd} = 2(\text{int}) + 1$

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

$$x = 2k+1$$
$$y = 2j+1$$

$$xy = (2k+1)(2j+1)$$
$$= 4kj + 2k + 2j + 1$$

Perfect Square: $\rightarrow$ for integer

Int a

a is PS iff $a = b^2$ $\rightarrow$ some integer

2 is PS ✗

$2 \neq (\text{int})^2$

Perfect Squares:

$1^2, 2^2, 3^2, 4^2, \ldots$

0

$4 = 2^2$

$9 = 3^2$

$16 = 4^2$

$0 = 0^2$

2 ✗

6 ✗

36 ✓

EXAMPLE 2 Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square. (An integer a is a **perfect square** if there is an integer b such that $a = b^2$.)

Source: Discrete Mathematics and Its Applications

Seventh Edition Kenneth H. Rosen

P : $\underline{m, n}$ are $\underline{ps}$

$m = a^2$; $n = b^2$

$a \rightarrow$ int, $b \rightarrow$ int

$mn = a^2 b^2 = (\underbrace{ab}_{\text{int}})^2 = (\text{int})^2$

fact you know

Q : $\boxed{mn \text{ is ps}} \equiv mn = (\text{int})^2$

HW

If m and n are perfect square, then $m+n+2\sqrt{(mn)}$ is a perfect square.

If m and n are perfect square, then $m+n+2\sqrt{(mn)}$ is a perfect square.

Proof

$m = a^2$ and $n = b^2$ for some integers a and b

Then $m + n + 2\sqrt{(mn)} = a^2 + b^2 + 2ab$

$= (a + b)^2$

So $m + n + 2\sqrt{(mn)}$ is a perfect square.

Note:

$a|b$: a divides b

Divides

a → int, b → int

$a/b \neq a|b$

$2 | 4$

$\boxed{\text{2 Divides 4}}$ → 2 ✗

→ Yes ✓

Divides

$4/2 = 2$

$4 \div 2 = 2$

$2 | 4 = \text{Yes}$

$4 | 2 = \text{No}$

$\div$, /

Same (Return Quotient)

$8 \div 4 = 2$

$4 \div 8 = 0.5$

|

Divides

boolean operator

$4 | 8$ = Yes

$8 | 4$ = No

$4 \mid 4$ True

$a \mid b$

a Divides b

int int

means $\boxed{b = a(\text{some int})}$

$$0 \mid 0$$

a b

Divides

$$\boxed{a \mid b = \text{True}}$$

iff

$$b = a(\text{some int})$$

$$0 = 0(\underbrace{\text{some int}}_{y})$$

$$a = 0$$

$$b = 0$$

$0/0$ = Indeterminate

value

Divides Relation

$0 \mid 0$ = True

$0/5 \rightarrow$ false ✓

$5 = 0$ (some int)

$5/0 \rightarrow 0 = 5$ (some int) $\rightarrow 0$

$\div$

Used in Group Theory

$|$

Divides Relations

Prove: If $5 \mid 2a$ for $a \in \mathbb{Z}$, then $5 \mid a$

Prove: If $5 | 2a$ for $a \in \mathbb{Z}$, then $5 | a$

5 Divides 2a

a is integer

integers

5 Divides a

$\mathbb{Z}$: integers $= 0, +1, -1, +2, -2, \ldots$

Given: P : $5 \mid 2a$ → some integer

$2a = 5k$ → int

even odd

→ $\boxed{\text{even}}$ ✓

$\cancel{2}a = 5(\cancel{2}b) \Rightarrow \boxed{a = 5(b)}$

⇒ $k = 2b$ → int

To prove

Q : $5 \mid a \equiv a = 5(\text{int})$

$2a = 5k$

int

$a = \frac{5k}{2}$

Stuck

Tutt's

4.5 Hours
for prove it

① ~
② ~
③ ~

1.5 Hour

$5 \mid 2a$

$2a = 5k$ — k: int

even = odd × even

$\boxed{k = 2m}$ — m: int

$2a = 5(2m)$

$a = 5m$

Odd * even = even

$\boxed{\text{Any Integer} * \text{even} = \text{even}}$

was the 1st Question

Prove: If $5 \mid 2a$ for $a \in \mathbb{Z}$, then $5 \mid a$

Assume $5 \mid 2a$ $\quad \forall a \in \mathbb{Z}$

$5j = \underbrace{2a}_{\text{even}}$ $\quad$ some $j \in \mathbb{Z}$

odd

even

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

$5(2k) = 2a$

$5k = a \longrightarrow 5 \mid a$

Prove

$7 \mid 4a \rightarrow 7 \mid a$

HW

Try your Best

- Show that

  if m and n are both square numbers,

  then m n is also a square number.

- Proof :

  Assume that m and n are both squares. This implies that there are integers u and v such that

  $$m = u^2 \quad \text{and} \quad n = v^2.$$

  Then $m n = u^2 v^2 = (uv)^2$. Thus, m n is a square.

5, 6, 7 → Not Consecutive

Consecutive

a, b

Cons iff $\boxed{b = a + 1}$

Methods of Proof: Proof by Contraposition