Books

1. Proof & Art of Mathematics
   Joel David Hamkins
2. Math... for C... Sci...
   Lehman, Leighton, Meyer
3. Invitation to D.M
   Matoušek & Nešetřil.
4. DM & it's Applications
   Kenneth Rossen

Course Topics

1. Logic and proofs
2. Set Theory
3. Combinatorics
4. Graph Theory
5. Discrete Probability.

Video Series

MIT OCW 6.042J

Grading

Test 1 : 20 } each test has 20% ques. from tutorials and
Test 2 : 30 } 20% from problem sets.
EndSem: 50   Tut & P.S are not graded.

---

* How many ways can you fill an empty sudoku puzzle?

---

* Is $\sqrt{2}$ a rational number?

Ans:

Let $\sqrt{2}$ be a rational number.

Then $\sqrt{2} = \frac{p}{q}$, where p, q are any 2 integers and p, q are coprimes, $q \neq 0$

$$p^2 = 2q^2$$

Then p^2 is an even number.

Then p is an even number, i.e; $p = 2n$.

$$4n^2 = 2q^2$$

$$2n^2 = q^2$$

Then q is also an even number

Here p, q are both even. They have a common factor of 2. Hence, they can't be co-primes.

Thus, by contradiction, $\sqrt{2}$ is irrational.

H.W

Exercises

1. Prove that $\sqrt{3}$ is not a rational number.
2. Do not prove that $\sqrt{4}$ is not a rational number.
3. Prove that $2^{1/3}$ is not a rational number.
4. Read the wikipedia article

https://en.wikipedia.org/wiki/Square_root_of_2

5. Read the 29 proofs of irrationality of $\sqrt{2}$ from https://www.cut-the-knot.org/proofs/sq_root.shtml
6. Watch the numberphile video about root 2

1) Def: A number which can be represented in the form of P/q, where p & q are integers, $q \neq 0$, p and q are co-primes is said to be a Rational Number

Thm:- $\sqrt{3}$ is not a rational number.

Proof:- Let $\sqrt{3}$ be a rational number
Then,

$$\sqrt{3} = \frac{p}{q}$$

$$p^2 = 3q^2.$$

Here, p^2 is a multiple of 3.
Thus, p is also a multiple of 3.

$$(3n)^2 = 3q^2 \Rightarrow 9n^2 = 3q^2 \Rightarrow q^2 = 3n^2.$$

Now, q^2 is also a multiple of 3.

As 3 is a common factor for p&q, p&q can't be co-primes. Thus $\sqrt{3}$ is not rational.

---

2) **Def:** A number which can be represented in the form of p/q, where p&q are integers, $q \neq 0$, p and q are co-primes is said to be a **Rational Number**.

Thm: $\sqrt{4}$ is a rational number.

Proof:

$$\sqrt{4} = \frac{p}{q}$$

$$p^2 = 4q^2$$

p is an even number. Let $p = 2n$, where $n \in \mathbb{Z}$

$$(2n)^2 = 4q^2 \Rightarrow 4n^2 = 4q^2 \Rightarrow n^2 = q^2$$

$$\Rightarrow n = \pm q$$

Thus $\sqrt{4}$ is rational.

3) **Def:** A number which can be represented in the form of p/q, where p & q are integers, $q \neq 0$, p and q are co-primes is said to be a **Rational Number**.

Thm: $2^{1/3}$ is not a rational number

Proof: Let $2^{1/3}$ be a rational number

$$2^{1/3} = p/q$$

$$p^3 = 2q^3$$

p^3 is an even number. Then p is even.

Let $p = 2n$, where n is an integer

Then, $q^3 = 4n^3 \Rightarrow q^3$ is even $\Rightarrow q$ is even

So, p and q have 2 as a common factor.

$\therefore$ $2^{1/3}$ is not a rational number.

Question:

Conjecture - I

1. For which natural number n is $\sqrt{n}$ rational?

Sol: For any natural no. 'n', $\sqrt{n}$ is rational iff n is a perfect square.

Perfect Square:- A natural number n is a perfect square, if it can be represented as k^2, where k is an integer.

Lemma:- A natural number n is a perfect square iff the prime factorization of n has only even powers

Proof:- if ($\Leftarrow$)

Prime factorization of n has only even powers

$$\Rightarrow n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}; \quad \alpha_i \in \mathbb{R}, \; p_i \in \mathbb{P}$$

$\Rightarrow n = k^2$, where

$$k = p_1^{\alpha_1/2} \cdot p_2^{\alpha_2/2} \cdots p_k^{\alpha_k/2}$$

only if ($\Rightarrow$)

Assume n is a perfect square, i.e; $n = k^2$

If $k = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_k}$

$$n = k^2 = q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdots q_k^{2\beta_k}$$

$\Rightarrow$ n has prime factors with even powers

Proof:

"if" ($\Leftarrow$)

If n is a perfect square, then by definition of perfect sq., $\exists\, k \in \mathbb{Z}$, s.t $n = k^2$. Therefore, $\sqrt{n} = \sqrt{k^2} = \pm k$, both of which are rational.

"only if" ($\Rightarrow$).

$$(\sqrt{n} \in \mathbb{Q}) \Rightarrow (\exists\, k \in \mathbb{Z} : n = k^2)$$

By definition of $\mathbb{Q}$,

$\exists\, p, q \in \mathbb{Z}$, $q \neq 0$, s.t

$$\sqrt{n} = \frac{p}{q}$$

We also choose p, q, s.t. $GCD(p, q) = 1$.

$$n = \frac{p^2}{\ldots}$$

$$q^2$$

$$p^2 = nq^2.$$

By hemme

p^2, q^2 are perfect squares and thus have all even powered prime-factorization. So, if n has odd powered prime factors, the total power on the left hand side becomes odd, which contradicts the fact that powers are even on RHS.

So, n must have even powered prime factors. Which means, n has to be a perfect square.

$$(p^2 = nq^2) \Rightarrow (p = kq), \text{ for some } k = \sqrt{n} \in \mathbb{Z}$$

2. For which real number n is $\sqrt{n}$ rational?

3. For which natural number n is $\sqrt[k]{n}$ rational?

4. For any natural number n, show that $n^2 - n$ is even.

Proof-I:- $n^2 - n = n(n-1)$

n & $n-1$ are any two consecutive nos.

If n is an odd number,

let $n = 2k+1$

then $n-1 = 2k$, which is even

So, for any 2 consecutive numbers, one of them will always be even. Hence, their product will also be even.

$\Rightarrow n^2 - n$ is even

Proof-II:-

If n is odd, $n = 2k+1$, $n^2 = 4k^2 + 4k + 1$

$n^2 - n = 4k^2 + 2k = 2(2k^2 + k) = 2t$, which is even

If n is even, $n = 2k$, $n^2 = 4k^2$

$n^2 - n = 4k^2 - 2k = 2(2k^2 - k) = 2t$, which is even

$\therefore$ $n^2 - n$ is even

Proof - III :-

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

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

$$\frac{1 \pm \sqrt{1 + 8k + 4}}{2}$$

$$\frac{1 \pm \sqrt{8k+5}}{2} \rightarrow$$ Need to prove $8k+5$ is never a perfect sq.

Proof - IV :-

Let $n = 1 \Rightarrow n^2 - n = 1^2 - 1 = 0$

Assume true for $n = k \Rightarrow k^2 - k$ is even

Assume true for $n = k \Rightarrow k^2 - k$ is even.

Then for $n = k+1$.

$$\Rightarrow (k+1)^2 - (k+1) = k^2 + 2k + \cancel{1} - k - \cancel{1}$$

$$= \underbrace{(k^2 - k)}_{\text{even}} + \underbrace{2k}_{\text{even}}$$

$$= \text{even}.$$

Proof - V :-

$$n^2 - n = n(n-1) = 2\sum n = \underline{\underline{\text{even}}}$$

Proof - VI :-

$${}^nC_2 = \frac{n(n-1)}{2} \text{ has to be a Natural No.}$$

$$\Rightarrow n(n-1) \text{ is even}$$

$$n^2 - n \text{ is even.}$$

Prime Numbers :-

X Natural numbers with only 2 factors, i.e; 1 and itself, are called prime numbers

✓ A number p is a positive integer greater than 1 and the only positive integers which divide p are 1 and itself

not necessary.

Fundamental Theorem of Arithmetic:-

⇒ Any positive integer can be written as a product of prime numbers. Moreover, the factorization is unique, upto the order of factors

* "1" is defined as a product of an empty set.

Prime Numbers:

> A Natural number other than 1 who is divisible by two and only two other natural number; that number itself and 1.

★ Fundamental Theorem of Arithematics: Any positive integer can be expressed as the product of prime numbers. Moreover, the factorisation is unique up to the order of factors.

A number p is prime if $p \geq 2$ and the only positive integer which divide p are 1 and p

★ Product of empty set = 1 ; Sum of empty set = 0
multiplicative Identity additive identity.

<u>Proof</u>

P(n) n can be written as a product of prime numbers.

Statement: $\forall\, n \geq 1$ P(n) is true.

Base case: n=1 ; P(1) is true because 1 is the empty product.

Strong Induction Hypothesis: P(i) is true for $1 \leq i \leq K$

Goal ⇒ Show that P(K+1) is true.

If K+1 is prime, we are done!
If K+1 is composite:
$\exists$ two integers a & b such that
$a < K+1$ & $b < K+1$
s.t $\underline{a \times b = K+1}$

Since a & b < K+1 ; they lie in the range (1, K)
we have already established this property in Strong Induction Hypothesis

Division Rule

For any 2 positive integers n & d, there exists unique non-negative integer q and r such that $n = qd + r$ and $0 \leq r < d$.

Proof :-

Suppose $n = q_1 d + r_1$

$n_2 = q_2 d + r_2$.

$\Rightarrow r_1 - r_2 = d(q_2 - q_1)$. So, $(r_1 - r_2)$ is a mul. of d.

$r_1, r_2 \in [0, d) \Rightarrow -(d-1) \leq r_1 - r_2 \leq d-1$

$\Rightarrow r_1 - r_2 = 0$, as 0 is the only mul. of d in the range.

$\Rightarrow \boxed{r_1 = r_2}$

$\Rightarrow \boxed{q_1 = q_2}$

Let r be the smallest non-neg int that cannot be written as $(n - qd)$, for some non-neg. q.

$r \geq 0$ and $r < d$ (If $r \geq d$, repeated subtr. can continue)

Bezout's Identity:- (This works for all integers)

For any 2 ~~positive~~ integers a and b which are relatively prime, there exists $\alpha, \beta \in \mathbb{Z}$ s.t,

$$\boxed{\alpha a + \beta b = 1}$$

Relatively prime: Only positive common factor is 1.

Proof:-

Let k be the smallest pos. int that can be represented as

$k = \alpha a + \beta b$, for $\alpha, \beta \in \mathbb{Z}$, a, b are co-primes

$S = \{ i : i \geq 1,\ i = a\alpha + b\beta \text{ for some } \alpha, \beta \in \mathbb{Z} \}$

Claim:- k divides a.

Let $a = qk + r$, $q, r \in \mathbb{Z}$, $0 < r < k-1$

$r = a - qk$.

$r = a - q(\alpha a + \beta b)$

$r = (1 - q\alpha)a - \beta q\, b$.

$r = \alpha' a - \beta' q$; $\alpha' = 1 - q\alpha$, $\beta' = -\beta$. $\in \mathbb{Z}$

Then $r \in S \cup \{0\}$

$\Rightarrow$ $r \notin S$, as then r will become the smallest counter example, which is a contradiction

So, $r = 0$ $\quad \boxed{a = qk} \Rightarrow$ k divides a.

* Similarly, k divides b

$\Rightarrow$ k is a common factor of a and b. As a and b are relatively prime, their only common factor is 1

Hence, $\boxed{k = 1}$

Euclid's Lemma:- $p \to$ prime, $a, b \in \mathbb{Z}$

If p divides ab then p will divide atleast one of a, b.

$$\boxed{(p \mid ab) \Rightarrow (p \mid a) \vee (p \mid b)}$$

Proof :-

Given $p | ab$.

* If $p | a$, we are done.
* Otherwise p, a are relatively prime. (Only pos. c.f is 1)

Then by Bezout's identity, $\exists\ \alpha, \beta \in \mathbb{Z}$ s.t.

$$\alpha a + \beta p = 1.$$

$$\Rightarrow \alpha ab + \beta pb = b.$$

$$\left.\begin{array}{l} * \ p \mid \alpha ab \ (\because p \mid ab) \\ * \ p \mid \beta pb \end{array}\right\} \Rightarrow \text{Their sum is a multiple of } p$$

Thus, b is a multiple of p.

Euclid's Lemma^{+} :-

If p is prime and $a_1, a_2, \ldots, a_k$ are any k integers such that $p | a_1 a_2 \cdots a_k$, then p divides atleast one of $a_1, a_2, \ldots, a_k$.

Proof :- Use Induction

Proof of Uniqueness of Prime Factorization :-

Let n be the smallest counter example.

Then, it has two different prime factorization

Let $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ (p_i, q_j are all primes)

From Euclid's Lemma[+], $p_1 \mid LHS \Rightarrow p_1 \mid RHS$

$\Rightarrow p_1 \mid q_1 \cdots q_l$

$\Rightarrow p_1 \mid q_j, \quad 1 \le j \le l$

$\Rightarrow p_1$ is either 1 or q_j

$\Rightarrow p_1 = q_j$.

$$\cancel{p_1} p_2 \cdots p_k = q_1 q_2 \cdots q_{j-1} \cancel{q_j} q_{j+1} \cdots q_k.$$

$\Rightarrow$ Then $p_2 \cdots p_k$ is a number less than n (say n_1)

* As n is the smallest counter example, n_1 will have unique prime factorization

* So, $p_2 \cdots p_k$ is the same thing as $q_1 \cdots q_{j-1} q_{j+1} \cdots q_l$

* As $p_1 = q_j$ also, this proves that the prime factorization of n is also unique.

$\Rightarrow$ $n^p - n$ is divisible by p, for any prime number p and an integer n.

Proof: (Proof by Induction on n).

i) $n = 0 \Rightarrow 0^p - 0 = 0$; 0 is divisible by p

ii) $n = k \Rightarrow k^p - k$, assume it's divisible by p.

(iii) $n = k+1$.

$$\Rightarrow (k+1)^p - (k+1) = \cancel{\binom{p}{0}k^0} + \binom{p}{1}k^1 + \dots\dots + \binom{p}{p}k^p - k - \cancel{1}$$

$$= \underbrace{\binom{p}{1}k^1 + \dots\dots\dots + \binom{p}{p-1}k^{p-1}}_{\text{All are multiples of } p} + \underbrace{k^p - k}_{\text{divisible by } p \text{ by induction}}$$

$$= p(N).$$

$$\boxed{\therefore\ n^p - n \text{ is divisible by } p, \text{ for any prime no. } p}$$

Induction:-

1: a. <u>Least element principle</u>

If there is a natural number with a certain property P, then there exists a smallest natural number with property P.

b. <u>Well ordering principle</u>

Every non-empty subset of $\mathbb{N}$ has a least element.

$\Rightarrow$ We can consider / "represent" a property as a set and vice versa.

$\rightarrow S = \{x : x \text{ has property } P\}$ for any property P

$\rightarrow x$ has property P iff $x \in S$.

x has property P iff $x \in S$

e.g:- $2 \in S$, If $x \in S$, then $x^2 \in S$

$$S = \{2, 4, 16, 256, 73216, \ldots\}$$

$$S = \{2^{2^n}, n \geqslant 0, n \in \mathbb{Z}\}.$$

Assume Least Element Principle and prove well-ordering principle.

Let S be any non-empty subset of $\mathbb{N}$.

Define property P as membership in S.

$\Rightarrow$ There exists a smallest natural no. which has prop. P (say x)

x has P $\Rightarrow x \in S$.

Proof by contradiction that x is the smallest nat. no. in S

2. Common Induction principle

a. Let P be any property of natural number.

If

A. 0 has P, and,

B. $\forall k \in \mathbb{N}$; $(k \text{ has } P) \Rightarrow (k+1 \text{ has } P)$

Then.

C. All natural numbers have P.

b. Let $S \subseteq \mathbb{N}$

If

A. $0 \in S$, and

B. $\forall k (k \in S \Rightarrow k+1 \in S)$

Then

C. $S = \mathbb{N}$

$$\boxed{\left[(0 \in S) \wedge \forall k\,(k \in S \Rightarrow k+1 \in S)\right] \Rightarrow S = \mathbb{N}}$$

3. Strong Induction Principle

a. Let Q be any property of Natural nos

If

A. 0 has Q, and,

B. $\forall k$ [(All natural no.s from 0 to k has Q) $\Rightarrow$ k+1 has Q]

Then.

C. All natural no.s have Q.

b. Let $S \subseteq \mathbb{N}$

If

A. $0 \in S$, and.

B. $\forall k (\{0, \ldots k\} \subset S \Rightarrow k+1 \in S)$

Then

C. $S = \mathbb{N}$

$$\boxed{[(0 \in S) \wedge \forall k\,(\{0, \ldots, k\} \subset S \Rightarrow k+1 \in S)] \Rightarrow S = \mathbb{N}}$$

$$\text{SIP} \Longleftrightarrow \text{CIP}$$

CIP → SIP

* Let k have Prop P, if all natural nos from 0 to k have prop Q.

$\Rightarrow$ 0 has P as 0 has Q.

$\Rightarrow$ k has P as $0, \ldots, k$ have Q

$\Downarrow$

$\Rightarrow$ $k+1$ has P as $0, \ldots, k+1$ have Q.

Applying Strong prop P on Q.

$\Rightarrow$ All natural nos have P, so, all natural nos have Q.

Prove CIP using LEP.

$\Rightarrow$ We have,

0 has P

$\forall k$ (k has $P \Rightarrow k+1$ has P)

Suppose, the prop (All $\mathbb{N}$ have P) be false. So, there will be a natural no. that has property NOT $P = \neg P = Q$ (let)

From LEP, there exists a smallest nat. no. (say x), which has Q.

$\rightarrow x \neq 0$ ($\because$ 0 has P).

$\rightarrow x > 0$, hence $x-1$ is a nat. no.

If x is smallest nat. no. with Q, then

$x-1$ will have P.

If $x-1$ has P $\Rightarrow (x-1)+1 = x$ has P.

So, no such x exist. By contradiction, we can say all Nat. no.s has prop Q.

Hence proved

My name is K. Parjanya

Fibonacci Sequence :-

$f_0 = 0$, $f_1 = 1$, $\forall n \geq 2$, $f_n = f_{n-1} + f_{n-2}$.

Theorem:- $\sum_{i=0}^{n} f_i^2 = f_n f_{n+1}$

Proof:- Base Case:- $n=0$

$0 = 0 \cdot 1 = 0$

Assume true for $n = k$. $\Rightarrow \sum_{i=0}^{k} f_i^2 = f_k f_{k+1}$

For $n = k+1$; $\sum_{i=0}^{k+1} f_i^2 = \sum_{i=0}^{k} f_i^2 + f_{k+1}^2$

$$= f_k \cdot f_{k+1} + f_{k+1}^2$$

$$= f_{k+1}(f_k + f_{k+1})$$

$$= f_{k+1} \cdot f_{k+2}$$

Hence proved

4-color Theorem:-

Theorem:- Any planar map formed using edge to edge or closed curves alone is 2-colorable.

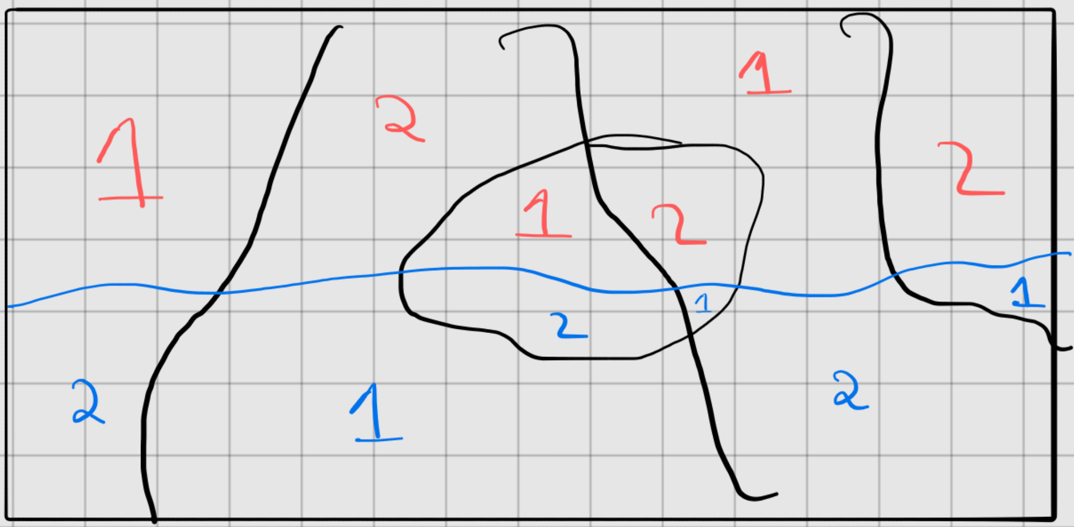
Proof: Base case: consider an empty rectangle. It is colored with 1-col.

consider it true for k-lines

n = k+1

For a new line added, it splits the region into 2 parts. Here, retain the coloring in one region and flip the coloring in the other..

Then, it becomes true for k+1



My name is K. Parjanya

Bezout's Theorem:-

For any 2 nat. no.s a, b ; GCD(a,b) is the smallest number that can be written as $\alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$.

Lemma:- $\gcd(a,b) = \gcd(b, a-b)$; $a > b$

```
def gcd(a,b):
    c = max(a,b)
    d = min(a,b).
```

```
    if d==0:
        return c.
    return gcd(d, c-d)
```

But $\gcd(b, a-b) = \gcd(b, a-2b) \ldots = \gcd(b, a\%b)$

```
def gcd(a,b):
    if b==0:
        return a
    else:
        return gcd(b, a%b)
```

Proof:-

$b=0$

$\gcd(a,0) = a = 1\cdot a + 0\cdot b$

Let be true for $b=k$.

$$\gcd(a,b) = d = \gcd\underbrace{(b, a-b)}_{\text{smaller case.}}$$

$d = \alpha'(b) + \beta'(a-b)$ (Using induction)

$a_2 = \beta^2 a + (\alpha^2 - \beta^2) b.$

Hence proved.

⇒ What is the maximum no. of slices into which we can cut a pizza using only straight line.

Sg

$0 \rightarrow 1$
$1 \rightarrow 2$) +1
$2 \rightarrow 4$) +2
$3 \rightarrow 7$) +3
$4 \rightarrow 11$) +4
$5 \rightarrow 16$) +5

Base Case :- $f(0) = 1$

Ind Step :- $f(k) = \frac{k(k+1)}{2} + 1$

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

Every time we create a new line, we cut through all the previous lines at diff. points.

$$\Rightarrow \text{Max} = \frac{n(n+1)}{2} + 1 = {}^{n+1}C_2 + 1$$

Base Case :- $f(0) = 0 + 1 = 1$

Ind. hyp :- $f(k)$ is the max no. of pieces with k lines

Ind. step:- $f(k+1) \leq f(k) + (k+1)$

Proof:- Let l be any of the lines

- Remove l.
- we get atmost $f(k)$ pieces
- l can intersect atmost $k+1$ pieces
- As the boundary b/w any 2 old pieces as one of the old lines

$$f(k+1) \leq f(k) + (k+1)$$

→ By adjusting the line l, we can make it intersect with all old lines at distinct points

$$f(k+1) \geq f(k) + (k+1)$$

$$\Rightarrow f(k+1) = f(k) + (k+1)$$

⇒ Find the min. no. of moves to solve the Towers of Hanoi puzzle with n-discs

$$f(n) = f(n-1) + 1 + f(n-1)$$

n	Moves
1	1
2	3
3	7

$$f(n) = 2f(n-1) + 1$$

$$f(n) + 1 = 2\left[f(n-1) + 1\right]$$

$$f(n) + 1 = 2^n [\ldots]$$

4	15
5	31

$f(n)+1 = 2\,[f(0)+1]$

$$f(n) = 2^n - 1$$