$n-1$

① → Fermats theorem [→ Fermats Primality test]

$$a^{p-1} \equiv 1 \pmod{p}$$ (p — prime, $p > a$)

ie $7^{6} \equiv 1 \pmod{7}$

② $4^{6} \equiv 1 \pmod{7}$

② Property —

$\sigma(n)$ → Sum divisors of n $\quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

($p_1, p_2 \cdots p_n$ are prime numbers)

total number of divisors $= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$

$\sigma(n)$ = Sum of divisors $= (1+p_1+p_1^2 \cdots p_1^{\alpha_1})(1+p_2+\cdots p_2^{\alpha_2})(1+p_3 \cdots p_3^{\alpha_3})$
$(1+p_n+p_n^2 \cdots p_n^{\alpha_n})$

Eulers Functions

1 — $\phi(n)$ = no. of integer which are less than n and coprime with n

[Where $\phi(n) = z(n)$ [set of no. in $\phi(n)$]]

$i < n$ && coprime

2 — $\phi(p) \rightarrow$ all $[1, 2 \cdots p-1]$ → no. of integer

ie → $\phi(25) \rightarrow 20$

3 — $\phi(p^{\alpha}) = \left(\frac{p-1}{p}\right) p^{\alpha}$ ($p \rightarrow$ prime)

ie = $\phi(27) =$

↳ (3^3) 3 → prime

$\phi(3^3)$

non copr → 3, 6, 9, 12, 15, 18, 21, 24, 27

($p^{\alpha-1}$)

pd Total ~~prime~~ coprime no → $p^{\alpha} - p^{\alpha-1}$ → coprime

$= p^{\alpha-1}(p-1)$

$= \boxed{\frac{(p-1)}{p} p^{\alpha}}$

4- $\phi(n)$ → n → can be any no.

$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$

p_n → prime

$\phi(n) = \frac{p_1 - 1}{p_1} \cdot p_1^{\alpha_1} \frac{p_2 - 1}{p_2} p_2^{\alpha_2} \cdots \frac{p_n - 1}{p_n} p_n^{\alpha_n}$

~~ie~~ → ~~n = 24~~

$\phi(n) = n \times \prod_{i=1}^{n} \frac{p_i - 1}{p_i}$

→

ie - ⊙ n = 24

~~$\phi(n) =$~~

$\phi(24) = \phi(2^3 \cdot 3^1)$

$= 24 \frac{3-1}{3} \frac{2-1}{2}$

$= 8$ ✓

1, 5, 7, ~~8~~, 11, 13, 17, 19, 23, ~~24~~.

→ modulo multiplicative inverse

$$A x \equiv 1 \pmod{M}$$

here x is mod. mult. inverse of A such that x is from 1 to M-1 and A and M coprime [↔ then and only then such x can exist]

ie - ~~3 (mod 4)~~

~~3 ≡ 1 (mod 4)~~

ie $3^{-1} \pmod{11} = x$

A = 3
M = 11 x = ?

$3x \equiv 1 \pmod{11}$

[1 ≤ x ≤ 11]

So we have to multiply and check each no.

→ 4

3 × 4 → 12/11 → 1

↳ R

ie $10^{-1} \pmod{17} = x = ?$

↳A ↳M

↳ coprime

$1 \le x < 17$

$16x \equiv 1 \pmod{17}$

$x = 12$

12 - / 119 →

7 ×
8 ×
80
~~100~~
110
120 17
102
(113)

→ Part of → Fermat's primality test

$[a^i \bmod p]$ is forming cyclic group $0 \leq i < p$ [

Wilson theorem

$(p-1)! \equiv -1 \pmod p$

$(p-1)! = 1 \times 2 \times \cdots \times p-1$

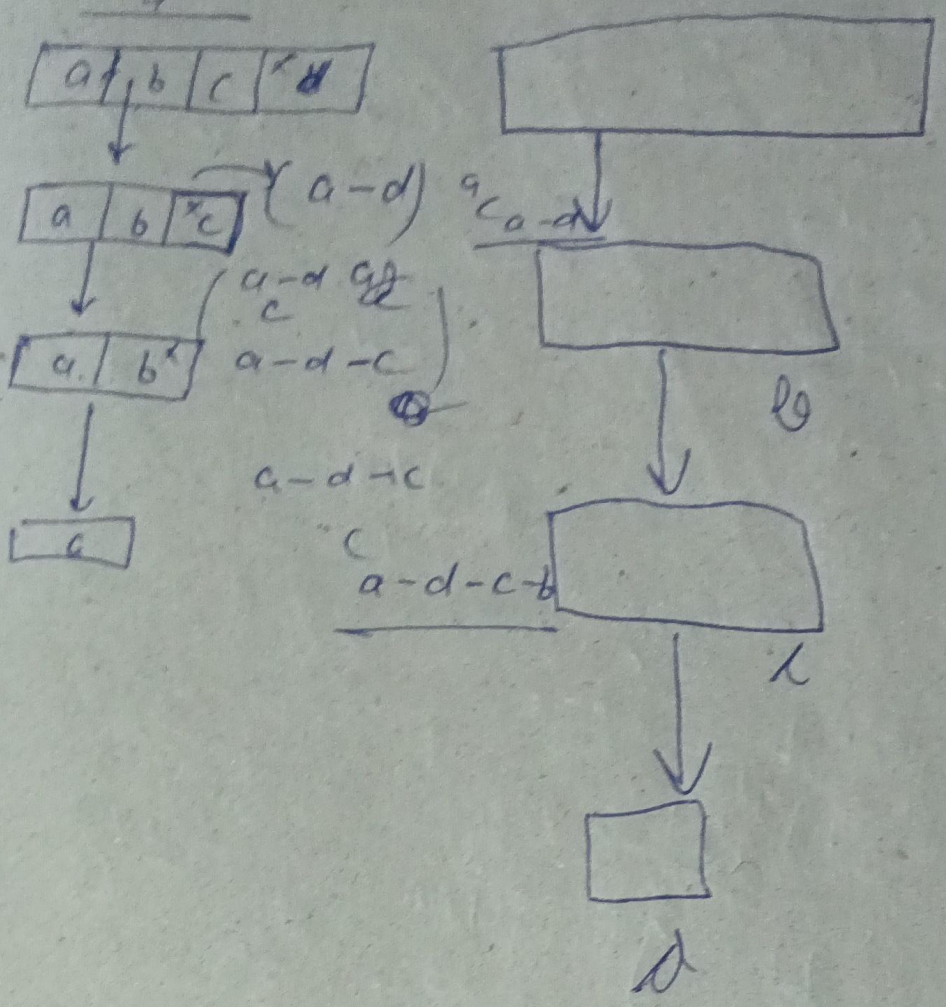
Such that from 1 to p-2 all the numbers within them will be classified into multiplication inverse pairs

for eg.

$6! \equiv -1 \pmod 7$

$1 \times 2 \times 3 \times 4 \times 5 \times 6 = 6 \bmod 7 = -1$

1 1 1



$$n(A) = n(U) - n(A')$$

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$$

$$^{a}C_{a-d} \times {}^{a-d}C_{c} \times {}^{c}C_{a-d-c} \times {}^{a-d-c}C_{b}$$

→ Modulo multiplicative matrix

$Z_6^* = \{1, 5\}$

$\phi(6) = 2$

$Z_9^* = \{1, 2, 4, 5, 7, 9\} =$

$\phi(9) = 6$

↳ no. of elements

$|Z_n^*| = \phi(n)$

c →

i ↓	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

} → mod 9

$(i \times j) \bmod = [a]_{ij}$

Some example

ie → $4^3 \rightarrow [4^2]^2$

$(4 \cdot (4^2 \bmod 9) \bmod 9)$

↳ $(7 \times 4) \bmod 9$

↳ 8 From table

ie → 2^{12}

$2^4 \bmod 9 \quad 2^4 \bmod 9 \quad (2^4 \bmod 9)$

↳ 7 ↳ 7 ↳ 7 → 4×7 (1)

Worpitzky identity

$$n^2 = {}^{n}C_2 + {}^{n+1}C_2$$

$$n^3 = {}^{n}C_3 + {}^{n+1}C_3 + {}^{n+2}C_3$$

$$\vdots$$

$$n^k = \sum a_k \, {}^{n}C_k$$

↳ no. of permitutions of n with k run / and it is eular no.

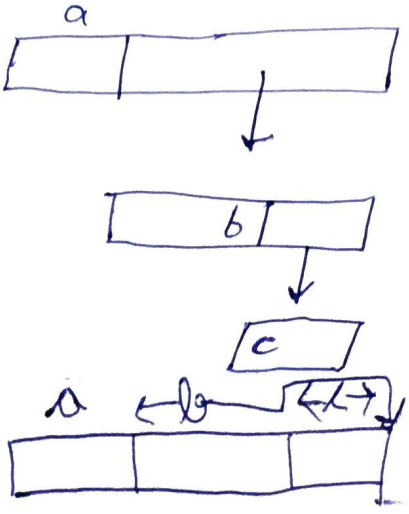
Where, $a_k = T(n,k) = \sum_{m=0}^{n+1} (-1)^m \, {}^{n+1}C_m \, (k+1-m)^k$

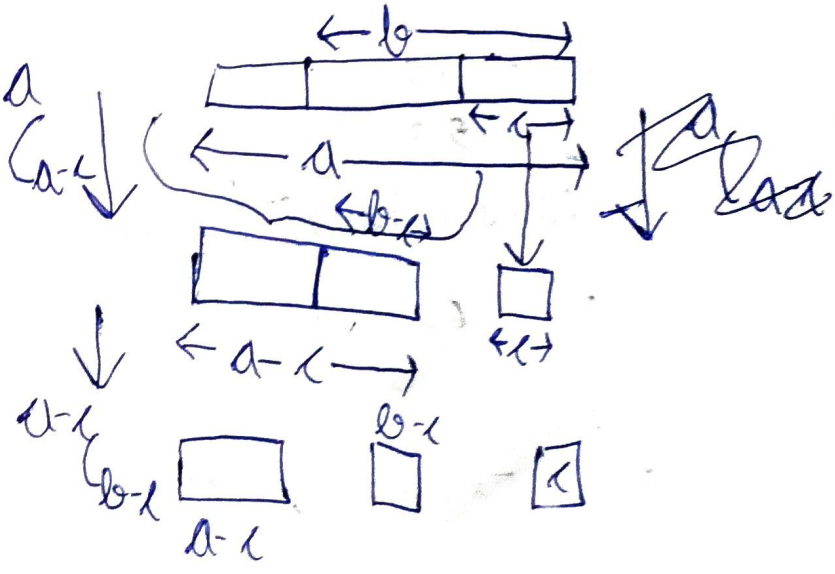
2 → Prove

$${}^{n}C_k = \frac{n}{k} \, {}^{n-1}C_{k-1}$$

imp

3 — $${}^{a}C_b \cdot {}^{b}C_c = {}^{a}C_{a-c} \cdot {}^{a-c}C_{b-c}$$





4- Properties

(a) $2^{n-1} \leq n! \leq n^{n-1}$

(b) $2^n < n!$ for all $n > 4$

(c) Strin

*

5→ Chinees rimindar fheorem

$x \equiv 4 \mod 11$

$x \equiv 6 \mod 13$

$x \equiv 2 \mod 5$

$B_1 \equiv 0 \mod 11$ $B_2 \equiv 0 \mod 11$ $B_3 \equiv 1$

$B_2 \equiv 0 \mod 13$ $B_2 \equiv 1 \mod 13$ $B_3 \equiv 0$

$B_1 \equiv 1 \mod 5$ $B_2 \equiv 0 \mod 5$ $B_3 \equiv 0$

$B_1 = (11 \cdot 13 \cdot 5)\,[(11 \cdot 13 \cdot 4)^{-1} \mod 5]$

$= 146 \times 2$

$= 286$

$B_2 = 11 \times 5\,[(11 \times 5)^{-1} \mod 13)$

$= 55 \times 9$

$= 495$

$B_3 = 13 \times 5\,[(13 \times 5)^{-1} \mod 11]$

$= 65 \times 10$

$= 650$

$= 5 \times 286 + 13 \times 495 + 650 \times 11$

6 → m(~~x~~) — 1 2 3 4 5 6 7 8 9 10 11 12

gcd(m,12) → 1 2 3 4 1 6 1 4 3 2 1 12

$|S_1| = 4$ $|S_3| = 2$ $|S_6| = 1$

$|S_2| = 2$ $|S_4| = 2$ $|S_{12}| = 1$

$|S_1| = \phi\left(\frac{n}{d}\right)$ $S_1 = \{1, 5, 7, 11\}$; $S_3 = \{3, 9\}$

$S_2 = \{2, 10\}$; $S_4 = \{4, 8\}$

$S_6 = \{6\}$; $S_{12} = \{12\}$

7 → if d/n then Prove $n = \sum \phi(d)$

Skiping

→ 8 Properties

$(u+a)^n \equiv u^n + a \pmod n$, where n is prime

~~Proove~~

1. $(u+a)^n = {}^nC_0\, u^{n-0} a^0 + {}^nC_1\, u^{n-1} a \ldots\ldots + {}^nC_n\, u^0 a^n$

except last and 1 element all can be divided by n

$= {}^nC_0\, u^n + {}^nC_n\, a^n$

$= u^n + a\, a^{n-1}$

$\equiv u^n + a \pmod n$

Well ordering Principle

$S = \{a_i\}$; $a_i \in N$

Then there is a least element $a_x \in S$

$a_x < a_j \quad \forall a_j \in S$

Q.) Prove that no integers b/w 0 & 1

$S = \{a \quad a \in N^+, \ 0 < a < 1$

$a < 1$

$a^2 < a$

$(a^2)^2 < a^2$

⋮

There is no least element thus it Contradicts well ordering Principle. ~~so it Can't be~~

Q.) In a bag there are 10 red marbels, 10 blue & 10 green marbels. You are taking marbels in the bag in the random order. What is the minimum no. of marbels so that 4 marbels of same colour are picked always.

Ans.) 10.

worst case: we pick 3 marbels of each colour so $3+3+3=9$ and now whatever colour is chosen 4 marbels of same colour will be picked.

Q.) A group can be formed with 10 members from 1st year or 8 members of 2nd year or 6 members of 3rd year or 4 members of final year. We Randomly Pick. students. What is the minimum no. of students to be picked so that group is formed always

Ans.) 25

$9 \times 2 + 7$

$3 \times 3 \times 3 + 1 = 25$

Induction

$P(1)$ is true

Assume $P(n)$ is true

To show $P(n+1)$ is True

$\Rightarrow P$ is true

Strong Induction

$P(1)$ is true

Assume $P(\ell)$ is true $\forall \ell < K$

To show $P(K)$ is true

$\Rightarrow P$ is true

Fibonacci Series : 0, 1, 1, 2, 3, 5, 8, 13, 21, ...

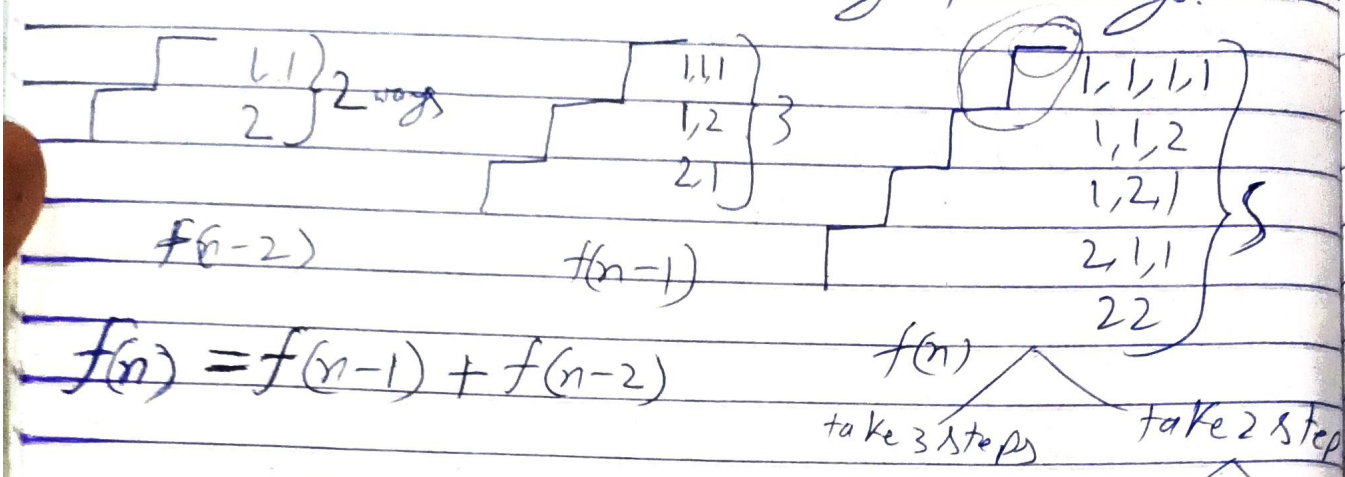
$F_1 = 1$; $F_2 = 1$

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{\sqrt{5}+1}{2}\right)^n - \left(\frac{\sqrt{5}-1}{2}\right)^n\right]$$

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{\sqrt{5}+1}{2}\right)^n\right]$$

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Q) There are n steps in a staircase & You can take 1 (or) 2 steps at a time how many possible ways?



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

$$f(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

$$\lim_{n\to\infty} \frac{F_{n-1}}{F_n} \longrightarrow C$$

$$\frac{F_{n-1}}{F_n} = \frac{F_{n-1}}{F_{n-1}+F_{n-2}} = \frac{1}{1+\frac{F_{n-2}}{F_{n-1}}} = \frac{1}{1+\frac{F_{n-2}}{F_{n-2}+F_{n-3}}} = \frac{1}{1+\frac{1}{1+\frac{F_{n-3}}{F_{n-2}}}}$$

$$= \frac{1}{1+\frac{1}{1+\frac{1}{1+1}}} \cdots$$

$$C = \frac{1}{1+C} \Rightarrow C^2 + C - 1 = 0 \Rightarrow C = \frac{-1 \pm \sqrt{1+4}}{2}$$

$$= \frac{-1 \pm \sqrt{5}}{2} = \frac{\sqrt{5}-1}{2}$$

$$\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Using Induction;

$$F(1) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)\right]$$

$$F(1) = 1$$

Assumption is Strong induction

$$F_n + F_{n-1}$$

$$\frac{1}{\sqrt{5}}\left[a^n - b^n\right] + \frac{1}{\sqrt{5}}\left[a^{n-1} - b^{n-1}\right]$$

$$\frac{1}{\sqrt{5}}\left[a^{n-1}(a+1) - b^{n-1}(b+1)\right]$$

1 1 2 3 5 8 13 21

2 4 7 12 20

$F_1 + F_2 = F_4 - 1$

$F_1 + F_2 + F_3 = F_5 - 1$

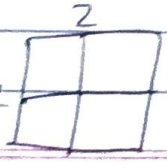
$F_1 + F_2 + F_3 + \ldots F_n = F_{n+2} - 1$

Using induction

$F_1 + F_2 + F_3 \ldots F_n + F_{n+1} = F_{n+2} + F_{n+1} - 1$

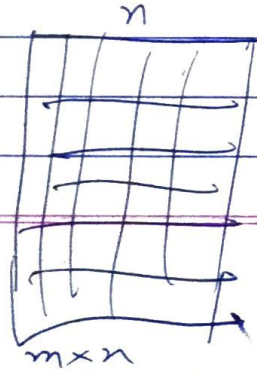
$= F_{n+3} - 1$

Bar of Chocolate How many breaks are required



= 3 breaks

→ 5 breaks



Elementary Number Theory

a b $\quad a \mid b \Rightarrow b/a$ is an integer

a divides b

$b = c \cdot a$ for some integer c

$a \nmid b \Rightarrow b/a$ is a fraction

a doesn't divides b

Q) $a \mid b$ & $a \mid c$ then prove $a \mid (b+c)$

$b = K_1 a$; $c = K_2 a$; $b + c = (K_1 + K_2) a$

Q) $a \mid b$ & $a \mid c$ then prove $a \mid bc$

Q) If $a \mid b$ & $b \mid c$ then prove $a \mid c$

If we take $c \triangleright a$

$c = a \cdot q + b$ ← This is Unique

Such that $0 \leq b < a$

Assume 2 different representation

$c = a q_1 + b_1$

$c = a q_2 + b_2$

$0 = a(q_1 - q_2) + (b_1 - b_2)$

$a(q_2 - q_1) = (b_1 - b_2)$

$a \mid (b_1 - b_2)$

$\Rightarrow b_1 - b_2 = 0$

$b_1 = b_2 \Rightarrow q_1 = q_2$

Integers

a b

$a+b \in Z$

$a-b$

$a*b$

Ring of Integers

1.) Closed $a+b$, $a-b$

2.) Inverse : $a+(-a)=0$

3.) $0+a=a$ Identity

$a \cdot 1 = a$

4.) $a+b=b+a$ Commutative

Field , of real & complex nos

if $a \equiv b \mod n$

$c \equiv d \mod n$

$a+c \equiv b+d \mod n$

$a \equiv b \mod m$

Then, $a = mK + b$

~~$m(a-b)$~~ $m/(a-b)$

~~$mK = a-b$~~ $mK = a-b$

$a = mK_1 + b$

$c = mK_2 + d$

$(a+c) = m[K_1+K_2] + (b+d)$ ~~mod m~~

$a+c \equiv b+d \mod m$

similarly $ac \equiv bd \mod m$

Sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54						
61	62	63	64						
71	72	73	74						
81	82	83	84						
91	92	93	94						

Mersenne primes
$2^p - 1$ when p is a prime

Q) Prove that $2^{ab} - 1$ can be a composite

$$(2^a)^b - 1 = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \dots\right)$$

Q) $f(n) = n^2 - n + 41$ always produces prime no.
disprove it.
For $n = 41$, $(41)^2 - 41 + 41 = 41^2$ not prime

Prime Counting Function $\pi(x)$

no of Primes $\leq x$

$\pi(x) \sim \frac{x}{\ln x}$

eg) no of Primes ≤ 100 is approx $\frac{100}{\ln 100} \approx 21.7$

$\frac{50}{\ln 50} = 12.7$

GCD (Greatest common Divisor)

a b

largest $d | a$ & $d | b$

$d = gcd(a, b)$

LCM (lowest common multiple), l

$a | l$ & $b | l$

$A = p_1^2 p_2^5 p_3$

$B = p_1^3 p_2^5 p_3^0$

$gcd(A, B) = p_1^2 p_2^5 p_3^0$

$lcm(A, B) = p_1^3 p_2^5 p_3^1$

$A * B = gcd * lcm$

if $a = bq + r$ $\quad 0 \leq r \leq b$

then $gcd(a, b) = gcd(b, r)$

$gcd(a, b) = gcd(b, a - bq)$

Prime Counting fcn $\pi(x)$

no. of Primes $\leq x$

$$\pi(x) \sim \frac{x}{\ln x}$$

eg.) no of Primes ≤ 100 is approx $\frac{100}{\ln 100} \approx 21.7$

$\frac{50}{\ln 50} \approx 12.7$

GCD (Greatest common Divisor)

a, b

largest $d|a$ & $d|b$

$d = \gcd(a, b)$

LCM (Lowest common multiple), l

$a|l$ & $b|l$

$A = p_1^2 p_2^3 p_3$

$B = p_1^3 p_2^5 p_3^0$

$\gcd(A,B) = p_1^2 p_2^3 p_3^0$

$\text{lcm}(A,B) = p_1^3 p_2^5 p_3^1$

$A * B = \gcd * \text{lcm}$

if $a = bq + r$ $\quad 0 \leq r \leq b$

then $\gcd(a,b) = \gcd(b,r)$

$$\gcd(a,b) \equiv \gcd(b, a-bq)$$

Euclids Algorithm

$(a,b) \rightarrow$

$a = bq + r_1 \quad ; \quad r_1 < b \quad , \quad gcd(a,b) = gcd(b, r_1)$

$b = r_1 q_2 + r_2 \quad ; \quad r_2 < r_1 \quad , \quad gcd(b, r_1) = gcd(r_1, r_2)$

$r_1 = r_2 q_3 + r_3 \quad ; \quad r_3 < r_2 \quad , \quad gcd(r_1, r_2) = gcd(r_2, r_3)$

$r_2 = r_3 q_4 + r_4 \quad ;$

$\vdots$

$r_{n-1} = r_n q_n + 0 \qquad gcd(r_{n-1}, r_n) = gcd(r_n, 0)$

Bezouts Theorem

$\exists$ s such that

$$gcd(a,b) = sa + tb$$

then $a \mid bc \implies a \mid c$

$at + sb = 1$

$atc + sbc = c \qquad$ as $a \mid bc \quad \therefore ak = bc$

$atc + ak = c$

$a[k + tc] = c \quad \therefore a \mid c$

Q) There are certain number of things (n) whose no. is unknown; $n \% 3 = 2$

$n \% 5 = 3$ How many things are there

$n \% 7 = 2$

Tutorial

Q) Let R be a ~~relation~~ set of binary relations on {1, 2, 3}. If U chose a random relation from R. What is the Probability that it is reflexive?

Total ordered pairs Possible $= n^2 = 3^2 = 9$

Total relations $= 2^9$

	1	2	3
1	1	2	-
2	-	1	-
3	-	-	1

$R = \{(1,2), (1,3)\}$

$Ans = 2^6$

Total Symmetric $= 2^6$

Q) let $A = \{(X, X) \mid X \subseteq U, x \in X\}$

~~$\phi \subseteq \phi$~~

~~$\phi \subseteq U$~~

(i) $|A| = n 2^{n-1}$

$$|A| = \sum_{k=1}^{n} k \cdot {}^nC_k$$

$$n^2 = 1 \cdot {}^nC_1 + 2 \cdot {}^nC_2 + 3 \cdot {}^nC_3 + \dots$$

$$\sum_{k=1}^{n} {}^nC_k x^k = (1+x)^n - 1$$

$$\sum_{k=1}^{n} k \cdot {}^nC_k x^{k-1} = n(1+x)^{n-1}$$

$x = 1$

$$\sum k \cdot {}^nC_k = n 2^{n-1}$$

Q) $A = \{1, \omega, \omega^2\}$ & $\omega^3 = 1$

* operation $1 * \omega = \omega$

$\{A, *\}$

$\omega, \omega^2, \omega^3$

$a, b \in A \quad a * b \in A$

$a(bc) = (ab)c$

$a \cdot 1 = a$

$a \cdot a^{-1} = 1$

$ab = ba$

Abedion Group

$\exists$ [redacted] $c^{-1}ac \equiv bcc^{-1} \pmod m$ & $\gcd(c, m) = 1$

then $a \equiv b \pmod m$

[redacted] $3 \cdot 7 \equiv 3 \cdot 2$

$1 = 1$

$7 \equiv 2 \pmod 5$

$2 = 2$

$m \mid ac - bc$

$m \mid c(a-b)$

$m \mid a-b$

$a \equiv b \pmod m$

$\gcd(c, m) = 1$

$sc + tm = 1$

$sc \equiv 1 \pmod m$

$ax \equiv b \pmod{n}$

$x \equiv (a^{-1})b \pmod{n}$

$\gcd(a, n) = 1$

eg. $7x \equiv 2 \pmod{21}$ 7 14 0 7 14 0

~~$7x3 = 1 \pmod{20}$~~

eg. $7x^3 \equiv 2 \pmod{20}$

$7 \cdot 3 \equiv 1$

$3 \cdot 7x \equiv 3 \cdot 2 \pmod{20}$

$x \equiv 6 \pmod{20}$

eg. $\sum_{K=0}^{n-1} K \equiv 0 \pmod{n}$ When n is odd

$\frac{(n-1)(n-2)}{2} \equiv 0$

Assignment-1

eg. $\sum_{K=0}^{p-1} K^m \equiv 0 \pmod{p}$ When $p(>2)$ is a prime number

1	2	3	4	5	6	7	8	9
1	1	3	1	1	3	1	1	9

$S_d = \{m \mid \gcd(m, n) = d\}$

$12 \rightarrow$

d	1	2	3	4	6	12
	1	1	2	2	2	4

m	1	2	3	4	5	6	7	8	9	10	11	12
gcd(m,12)	1	2	3	4	1	6	1	4	3	2	1	12

$|S_1| = 4$, $|S_3| = 2$; $|S_6| = 1$
$|S_2| = 2$, $|S_4| = 2$, $|S_{12}| = 1$

$$|S_d| = \phi\left(\frac{n}{d}\right)$$

$S_1 \{1, 5, 7, 11\}$; $S_3 = \{3, 9\}$
$S_2 = \{2, 10\}$; $S_4 = \{4, 8\}$
$S_6 = \{6\}$; $S_{12} = \{12\}$

To Prove $\sum_{d \mid n} \phi(d) = n$

Define: $S_d = \{m \mid \gcd(m, n) = d\}$

Since, $\gcd(m, n) = d$

$$\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

$$|S_d| = \phi\left(\frac{n}{d}\right)$$

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} |S_d| \quad r = n$$

Q] Given we have 'n' non-zero integers $S_n = \{a_1, a_2, a_3 \ldots a_n\}$

$A \subset S_n$ $\quad A = \{a \in A\}$

Such that $\sum a_i$ is divisible by n $\quad a \in A$

Subset

$$S_n = \{a_1\ a_2\ a_3 \ldots\ldots\ldots a_n\}$$

$b_1 = a_1 \quad r_1$

$b_2 = a_1 + a_2 \quad r_2$

$b_3 = a_1 + a_2 + a_3 \quad r_3$

$\vdots$

$b_n = a_1 + a_2 + \ldots a_n \quad r_n$

} at least two remainders are same

$b_i = a_1 + \ldots + a_i \quad r$

$b_j = a_1 + \ldots + a_j \quad r$

$= a_{i+1} + \ldots a_j \quad 0$

$(x+a)^n \equiv x^n + a \pmod n$ A-K-S Primality test

↳ Expanding n is a prime

$^nC_0 x^n a^0 + {}^nC_1 x^{n-1} a^1 + \ldots + {}^nC_n x^{n-n} a^n$