Date: _____

Number Theory:

Prime Numbers:

A prime is a positive Integer greater than 1, that is divisible by no positive Integer other than 1 and itself.

e.g:- 2, 3, 5, 101, 103

Composite Numbers:

A positive integer, which is not prime and not 1 is called composite number.

e.g: 4, 6, 10, 100, 9

Date: _____

Lemma:

Every positive integer greater than 1, has a prime divisor.

Thearom:

There are infinitly many prime.

Thearem:

If n iis a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.

note

20

1, 2, 4, 5, 10, 20 (2 and 5: prime factor)

$\sqrt{20}$

hence 2 is that factor

Sieve of Eratosthenes
name of find the prime number method

Function $\pi(x)$:

The function $\pi(x)$, where x is a positive real number, donate the number of prime not exceeding x

e.g $\pi(10) = 4$ 2, 3, 5, 7

$\pi(20) = 8$ 2, 3, 5, 7, 11, 13, 17, 19

$\pi(100) = 25$

preposition

lemma → Theorem

Corollary

Date: _____

The Prime number Theorm:

The ratio of $\pi(x)$ to $x/\log x$ approaches one as x grown without bound.

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

$\leftrightarrow$ Greatest common divisor:

$(4, 8, 10) = ((4, 8), 10)$
$= (4, 10)$
$= 2$

$(252, 198) = 18$

$198 \overline{)252}$ (1)
198
$54 \overline{)198}$ (3)
162
$36 \overline{)54}$ (1)
36
$18 \overline{)36}$ (2)
36
0

$\therefore (105, 140, 350) = ?$

$((105, 140), 350)$
$= (35, 350)$
$= 35$

Date: _____

Fibonacci Sequence:

The Fibonacci number $u_1, u_2, u_3, \ldots$ are defined recursively by the equation

$$u_1 = 1$$
$$u_2 = 1$$
$$u_n = u_{n-1} + u_{n-2} \text{ for } n \geq 3$$

$u_3 = u_2 + u_1$

$u_3 = 1 + 1$

$u_3 = 2$

$u_4 = u_3 + u_2$

$u_4 = 2 + 1$

$u_4 = 3$

The Fundamental Theorm of Axithmetic

Every positive integer can be written uniquely as a product of prime.

$(18, 24)$

2 | 18
3 | 9
3 | 3
| 1

2 | 24
2 | 12
2 | 6
3 | 3
| 1

$18 = 2 \times 3^2$

$24 = 2^3 \times 3^1$

$(18, 24) = 2 \times 3^2$

$= 6$

2 | 12
2 | 6
3 | 3
| 1

$12 = 2 \cdot 2 \cdot 3$

$(252, 198)$

2 | 252
2 | 126
3 | 63
3 | 21
7 | 7
| 1

2 | 198
3 | 99
3 | 33
11 | 11
| 1

$252 = 2^2 \times 3^2 \times 7^1 = 2^2 \times 3^2 \times 7^1 \times 11^0$

$198 = 2 \times 3^2 \times 11 = 2 \times 3^2 \times 11^1 \times 7^0$

$(252, 198) = 2^1 \times 3^2 \times 11^0 \times 7^0 = 18$

Date: _____

Least Common Multiple:

The least common multiple of two positive integers, a and b is the smallest positive integer that is divisible by a and b.

LCM

4 → 4, 8, 12, 16, (20), 24, 28, 32, 36, (40)

5 → 5, 10, 15, (20), 25, 30, 35, (40) —

⇒ The least common multiple of two integers a & b is denoted by [a, b].

$$[4, 5] = 20$$

Formula of GCD & LCM By using prime factorization:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

$$b = p_1^{a_1} p_2^{a_2} \dots p_n^{b_n}$$

$$D:(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

$$M:[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

Example:

$\min(2, 5) = 2$

$\max(4, 7) = 7$

Date: _____

GCD

$(42, 60) = 6$

$42 \mid 60$ (1)

$18 \mid 42$ (2)

$6 \mid 36$ (6)

36

$60 = 2^2 \cdot 3^1 \cdot 5^1$

$42 = 2^1 \cdot 3^1 \cdot 7^1$

$60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$

$42 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$

prime factorization

$\min(1,2) \quad \min(1,1) \quad \min(0,1)$

$(42, 60) = 2^{\min(1,2)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,1)} \cdot 7^{\min(1,0)}$

$= 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0$

$= 6$

$[42, 60] = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$

$= 4 \cdot 3 \cdot 5 \cdot 7$

$= 420$

$42 \times 60 = 2520$

$\frac{2520}{6} = 420$

Theorem: If a and b are positive integers, then $[a, b] = \frac{ab}{(a, b)}$

Proof:

Let the prime factorization of a be

$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$

$(a, b) = \frac{ab}{[a, b]}$

$[a, b](a, b) = ab$

LCM GCD

Suppose the prime factorization of b is

Date: _____

$b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$

jo chota ha ga a_i, b_i no m jo bara ha no M

let $\min(a_i, b_i) = m_i$

& $\max(a_i, b_i) = M_i$

so, $(a, b) = p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}$ —— (1)

$[a, b] = p_1^{M_1} \cdot p_2^{M_2} \cdots p_n^{M_n}$ —— (2)

By multiplying eq (1) & (2)

$(a, b)[a, b] = (p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n})(p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n})$

$\min(4_0, 6_0) = 4_0$

$\max(4_0, 6_0) = 6_0$

$\min(4_0, 6_0) + \max(4_0, 6_0) = 4_0$

$\min(a_1, b_1) + \max(a_1 + b_1) = a_1 + b_2$

$= p_1^{m_1 + M_1} \cdot p_2^{m_2 + M_2} \cdots p_n^{m_n + M_n}$

$= p_1^{a_1 + b_1} \cdot p_2^{a_2 + b_2} \cdots p_n^{a_n + b_n}$

$(a, b)[a, b) = (p_1^{a_1} \cdot p_1^{b_1})(p_2^{a_2} \cdot p_2^{b_2}) \cdots$

$(p_n^{a_n} \cdot p_n^{b_n})$

$\therefore x^{a+b} = x^a x^b$

Date: _____

$$= \left(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}\right)\left(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}\right)$$

$$(a,b)[a,b] = ab$$

Fermat's Numbers:

The integer of the form

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

are called Fermat Numbers.

$F_1 = 5$, $F_2 = 16 + 1 = 17$ $F_3 = 2^{2^3} + 1$

$F_2 = 17$ $= 2^8 + 1$

$= 256 + 1$

$= 257$

$\therefore F_1 = 2^{2^1} + 1$

$= 4 + 1 = 5$

$\therefore$ Fermat's said that the Fermat's no answer should be prime number.

$F_4 = 2^{2^4} + 1$

$= 2^{16} + 1$

$= 65537 \longrightarrow$ Fermat's Numbers.

$\therefore$ prime number ja 1 aur apne par divide ho.

Date: _____

Divisibility :-

Let a and b be integer we say that a divides b. if there is an integer c. such that $b = ac$. if a divides b. we also say that a is a divisor or factor of b.

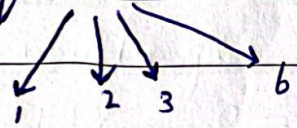
For example:

$\underset{a}{2} \quad \underset{b}{b}$

$b = (2)(3)$

$b = ac$

factor of b are



If a divides b, we write $a|b$. if a does not divide b we write $a \nmid b$.

→ Lemma ⇒ short result.

→ proposition ⇒ short result of any domain

→ Theorm ⇒ long result of any domain

Proposition:

If a, b and c are integers with $a|b$ and $b|c$ then $a|c$.

Proof:

if $a|b$ then $\exists$ an integer d $\exists$ $b = ad$ —— ①

if $b|c$ then $\exists$ an integer e $\exists$ $c = be$ —— ②

Date: _____

Use ① into ②:

$c = (ad)e$

$c = a(de)$

Since both d & e integer therefor de in integer. Therefor ③ implies that $\frac{a}{b}$.

Proposition:

if a, b m and n are integer if c/a and c/b then

$c/(ma + nb)$

Proof:

Given c/a and c/b.

if c/a then ∃ an integer d

∃ $a = cd$ —— ①

if c/b then ∃ an integer e

∃ $b = ce$ —— ②

multiplying eq ① by m

$ma = mcd$ —— ③

Multiplying eq ② by n

$nb = nce$ —— ④

Adding both ③ and ④.

$ma + nb = mcd + nce$

$ma + nb = c(md + ce)$

$\Rightarrow c/ma+nb$.

Greatest integer function:
Let x be a real number the greatest in x, is denoted by $[x]$, is the largest integer less than or equal to x.

$[2.2] = 2$

$[0.5] = 0$

The divisar Algorithm:
if a and b are integer such that $b>0$, then there exist unique integer q or r such that
$a = bq + r \quad 0 \leq r < b$.

Radix / Base / Expansion:
Let b be a positive integer with $b>1$. Then every positive integer 'n' can be written uniqly in the form.

$$n = a_k b^k + a_{k+1} b^{k-1} + \dots a_1 b_1 + a_2 b_2$$

where a_j is an integer with $0 \leq a_j < b$ for $J = 0, 1, 2, \dots, k$ an intial coffecient $a_n \neq 0$.

In (1), b is called radix base/

Date: _____

Example:

$34765 = 3.10^4 + 4.10^3 + 7.10^2 + 6.10^1 + 5.10^0$

are called

2 - binary

8 - atal

16 - Hexa

10 - decimal

$(a_k a_{k-1}, \ldots, a, a_0) = (34765)_{10}$

Example:

$(1001)_2 = 1.2^3 + 0.2^2 + 0.2^1 + 1.2^0$

$= 8 + 1$

$= (9)_{10}$ $(\because 2^0 = 1)$

$(236)_7 = 2 \times 7^2 + 3 \times 7^1 + 6 \times 7^0$

$= 98 + 21 + 6$

$= (125)_{10}$

$(1864)_{10}$

2	1864
2	932 — 0
2	466 — 0
2	233 — 0
2	116 — 1
2	58 — 0
2	29 — 0
2	14 — 0
2	7 — 0
2	3 — 1
	1 — 1

$(1864)_{10} = (100001000111)_2$

Date: _____

main points

A	10
B	11
C	12
D	13
E	14
F	15

Example:

$(A35B0F)_{16} = 10 \times 16^5 + 3 + 16^4 + 5 \times 16^3 + 11 \times 16^2 + 0 \times 16^1 + 15 \times 16^0$

$= 10485760 + 196608 + 20480 + 2816 + 15$

$= 10705678$

Example:

$(9A0B)_{16} = 9 \times 16^3 + 10 \times 16^2 + 0 \times 16^1 + 11 \times 16^0$

$= 36864 + 2560 + 0 + 11$

$= (36435)_{10}$

2	39435
2	19717 — 1
2	9858 — 1
2	4929 — 0
2	2464 — 1
2	1232 — 0

$(1001101000001001 1)_2$

Date: _____

Example:

$(1101)_2$
$+(1001)_2$
$\overline{10110}$

$(657)_8$
$+(526)_8$
$\overline{1405}$

$(11011)_2$
$-(10110)_2$
$\overline{101}$

$(FEED)_{16}$
$(CAFE)_{16}$
$\overline{33EF}$

Greatest common divisor:
The greatest common divisor of two integers a and b that are not both zero. is the largest integer which divides both a and b.

Ex:

i) 16, 20
↓
1, 2, (4)

ii) 4, 8
↓
1, 2, (4)

iii) 0, 5
↓
1, (5)

iv) 0, 0
↓
we can't find gcd because both are zero

v) 2, 2
↓
1, 2

Relatively prime:

The integers a and b are called relatively prime if

$$(a, b) = 1.$$

Ex:

$$(5, 7) = 1$$

$$(25, 42) = 1$$

Proposition:

Let a, b & c are integers with $(a, b) = d$

Then

i) $(a/d, b/d) = 1$

ii) $(a + cd, b) = (a, b)$

$$\left(\frac{a}{b}, \frac{b}{d}\right) = \left(\frac{15}{3}, \frac{21}{3}\right)$$

$$(5, 7) = 1$$

$$(a + cd, b) = (15 + 2(21), 21)$$

$$= (57, 21)$$

$$= 3$$

$$= (a, b)$$

$$\text{If } (a, b) = d \Rightarrow \left(\frac{a}{b}, \frac{b}{d}\right) = 1$$

Proof:

Let a, b be two integer with $(a, b) = d$

Assume 'e' is GCD of a/d and b/d.

Date: _____

$\left(\frac{a}{d}, \frac{b}{d}\right) = e$

So e divide a/d and e/ b/d

Since $e / a/d$, $\exists\ k \in \mathbb{Z}$

$a/d = ke$

$a = dek$ — ①

Sine $e / b/d$, $\exists\ l \in \mathbb{Z}$

$b/d = le$

$b = de\ l$ — ②

eq ① & eq ② implies that de in common divisor of a & b

$(a, b) = d$

Since d is GCD of a & b

So e must be 1

Hence $\left(\frac{a}{d}, \frac{a}{d}\right) = 1.$

$641 - 5^4 = 2^7$

$5 \cdot 2^7 = 641 - 1$

Date: _____

Proposition The formal number $F_5 = 2^{2^5} + 1$ is divisible by 641.

Proof:

Note that

$$641 = 5 \times 2^7 + 1 = 2^4 + 5^4$$

Hence $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 =$

$$(641 - 5^4)\, 2^{28} + 1$$

$$= 641 \cdot 2^{28} - 5^4 \cdot 2^{28} + 1$$

$$= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1$$

$$= 641 \cdot 2^{28} - (641 - 1)^4 + 1$$

$2^4 = 641 - 5^4$

$5 \overline{)641}$ 2^7 1

$\therefore (a-b)^2 = a^2 - 2ab + b^2$

$(a-b)^4 = (a-b)^2 (a-b)^2$

$= (a - 2ab + b^2)(a^2 - 2ab + b^2)$

$= a^4 - 2ab + a^2 b^2$

$- 2ab + 4a^2 b^2 - 2ab^3$

$a^2 b^2 - 2ab^3 + b^4$

$$(641 - 1)^4 = (641)^4 - 2(641)(1) + (641)^2 (1)^2$$

$$- 2(641)(1) + 4(641)^2 (1)^2 - 2(641)(1)^3$$

$$(641)^2 (1)^2 - 2(641)(1)^3 + (1)^4$$

$$= 641 \cdot 2^{28} - \Big[(641)^4 - 2(641)(1) + (641)^2 (1)^2$$

$$- 2(641)(1) + 4(641)^2 (1)^2 - 2(641)(1)^3$$

$$(641)^2 (1)^2 - 2(641)(1)^3 + (1)^4\Big] + 1$$

$$= 641\Big[2^{28} - (641)^3 + 2(641)^2 (1) - (641)^1 (1)^2$$

$$+ 2(641)^2 (1) - 4(641)^1 (1)^2 + 2(1)^3$$

Date: _____

$-(641)^1 (1)^2 + 2(1)^4)$

$\Rightarrow 641 \mid F_5$

Linear Diophantine Equation:

The equation of the form

$$ax + by = c$$

where a, b and c are integers is called a linear diophantine equation in two variable. The solution are required to be integers.

Theorm:

Let a and b be two integers with $d = (a, b)$

The equation $ax + by = c$ has no integral solution if $a \nmid c$

If $d \mid c$, then there are infinitly many solution. Moreover if $x = x_0$, $y = y_0$ is a particular solution of the equation then all solution are given by.

$$x = x_0 + \left(\frac{d}{d}\right)n \qquad y = y_n - \left(\frac{b}{d}\right)n$$

Date: _____

Example:

$172x + 20y = 1000$

By ÷ with 4

$43x + 5y = 250$

$a = 172$
$b = 20$
$c = 1000$
$d =$

$5 \overline{)250}\ 50$
0

$(5 + 38)x + 5y = 5 \cdot 50 + 0$

$5x + 38x + 5y = 5 \cdot 50$

~~Let $5x + 5y = z$~~

~~$z + 38x = 5.50$~~

$5x + 5y - 5 \cdot 50 + 38x = 0$

$5x + 5y - 5 \cdot 50 = z$

$x = -1$

$z = 38$

$z + 38x = 0$