Sunrise 6-40 AM

Introduction

New Year's Day

Unit I

Sunset 5-52 PM

Number theory, branch of Mathematics concerned with properties of the positive integers (1, 2, 3 ....).

These numbers, together with the negative integers and zero, form the set of integers, Z.

Known Facts:

1. An integer is divisible by 3 iff the sum of its digits are divisible by 3.

Ex: 852 → 8+5+2 = 15

2. The sequence of prime 2, 3, 5, 7, 11, 13, 17 ... is endless.

→ known to Euclid, who lived about 350 B.C

3. Irrational number - a number that cannot be expressed as the quotient a/b of two integers.

Examples: $\sqrt{2}$, 2/7, 13/5, -14/9 & 99/100

4. Integers are themselves rational numbers.

Ex: 7 = 7/1

Rational numbers - recurring - repeating

Sunrise 6-41 AM

Sunset 5-53 PM

Irrational number π

22/7 is rational or irrational

The number 22/7 is a fraction so it is rational.

You may think it is irrational, because its a famous approximation for pi.

But $22/7 \simeq \pi$ → close but not accurate

It is not equal to π

22/7 has digits that repeat every 6 times, pi's digits never repeat.

5. Therefore, the rational number 22/7 is a good approximation to π, close but not precise.

The fact that π is irrational means, that there is no fraction a/b that is exactly equal to π, with a and b integers.

Number Theory abounds with unsolved problems → exists in large numbers

Conjecture:

A statement or idea that has not yet been proved.

Sunrise 6-41 AM Sunset 5-54 PM

Example: Fermat's last theorem: not a Theorem at all because it has not yet been proved.
Pierre de fermat (1601 - 1665) stated that the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, z for any exponent $n > 2$.

1. Leonhard Euler: 2m
Conjecture that no n^{th} power is a sum of fewer than 'n' n^{th} powers.
Example: For $n = 3$, no cube is the sum of two smaller cubes.
$3^3 = n^3 / 2^3 + 1^3 \Rightarrow 27 > 8 + 1$

A counter-example to Euler's conjecture was provided in 1968 by L. J. Lander and Thomas.
as $144^5 = 27^5 + 84^5 + 110^5 + 133^5$ fifth power

2. Goldbach Conjecture 2m
Every even integer greater than 2 is the sum of two primes.
Examples: $4 = 2+2$, $6 = 3+3$, $50 = 7+13$
$50 = 3+47$, $100 = 29+71$

All of you must now give full support to Grandfather Bhishma, as you stand at your respective strategic points

3. Mathematical Induction. 2m

P(n) is a statement with integer parameter 'n' and the following two conditions hold then P(n) is true for every positive integer 'n'.

(i) P(1) is true

(ii) $\forall n \geq 1$, P(n) is true

$\Rightarrow$ P(n+1) is true.

1.2 Divisibility

Divisors, multiples and prime & Composite numbers - are concepts known & studied since the time of Euclid, about 350 B.C

The fundamental ideas are developed in this & next section.

Definition 1.1 - Divisibility.

An integer 'b' is divisible by an integer 'a', not zero, if there is an integer x s.t $b = ax$. Notation: $a|b$ a divides b

If b is not divisible by a then we write $a \nmid b$.

Sunrise 6-42 AM Sunset 5-55 PM

Note:

1. If $a|b$ and $0 < a < b$, then 'a' is called a proper divisor of 'b'.

2. $a|0$ for every integer $a \neq 0$

3. The symbol $a^k \| b \Rightarrow a^k | b$ but $a^{k+1} \nmid b$

Example: $5^2 | 100$ but $5^{2+1} \nmid 100$

Theorem 1.1

1. $a|b$ implies $a|bc$ for any integer c;
2. $a|b$ and $b|c$ imply $a|c$;
3. $a|b$ and $a|c$ imply $a|(bx+cy)$ for any integers x and y;
4. $a|b$ and $b|a$ imply $a = \pm b$;
5. $a|b$, $a>0$, $b>0$, imply $a \leq b$;
6. if $m \neq 0$, $a|b$ implies and is implied by $ma|mb$.

Sunrise 6-43 AM

Proof:

1. Given $a|b \Rightarrow b = ax$ for any integer x

Multiply both sides by $c \Rightarrow bc = acx$ for $x \in Z$

$\Rightarrow bc = a(cx)$

$\Rightarrow a|bc$ for $cx \in Z$

2. Given $a|b \Rightarrow b = ax$ for any integer $x \in Z$

Given $b|c \Rightarrow c = by$ " " " $y \in Z$

Consider $c = by$

$\Rightarrow c = (ax)y \quad \because b = ax$

$\Rightarrow c = a(xy)$

$\Rightarrow a|c$ for $xy \in Z$

3. Given $a|b \Rightarrow b = ax_1$ for any integer $x_1 \in Z$

$a|c \Rightarrow c = ay_1$ " " " $y_1 \in Z$

To prove $a|bx+cy$

Consider $bx+cy = (ax_1)x + (ay_1)y \quad x_1, x \in Z$

$= a[x_1x + y_1y] \quad y_1, y \in Z$

$\Rightarrow a|bx+cy$

4. Given $a|b$ and $b|a$

$\Rightarrow b = ax$ & $a = by$ for $x, y \in Z$

Sunrise 6-44 AM Sunset 5-57 PM

To prove: $a = \pm b$

Consider: $a = by$

$\Rightarrow a = a x y$ $\because b = ax$ for $xy \in Z$

$\Rightarrow xy = 1$

Both x & y are positive

or

x & y are negative

when $x = 1$, $b = ax \Rightarrow b = a(1) \Rightarrow b = a$

$x = -1$, $b = a(-1) \Rightarrow b = -a$

$\Rightarrow b = \pm a$

when $y = 1$, $a = by \Rightarrow a = b(1) \Rightarrow a = +b$

$y = -1$, $a = by \Rightarrow a = b(-1) \Rightarrow a = -b$

$\Rightarrow a = \pm b$

Hence $a|b$ and $b|a \Rightarrow a = \pm b$.

5. Given $a|b$, $a > 0$, $b > 0$

$\Rightarrow b = ax$ for $x \in Z$

$\Rightarrow \frac{b}{x} = a$ ——— ①

$\because a > 0$, $b > 0$ we have $x > 0$

$\therefore x \geq 1 \Rightarrow \frac{1}{x} \leq 1$

Multiply by $b \Rightarrow \frac{b}{x} \leq b \Rightarrow a \leq b$ [$\because b > 0$]

6. Given $a|b$

$a|b \Leftrightarrow b = ax$ for $x \in Z$

Multiply both sides by m $\Leftrightarrow mb = max$ for $m \neq 0$, $m \in Z$

$\Leftrightarrow mb = ma(x)$

$\Leftrightarrow mb|ma$ for $x \in Z$.

Extension of Property 3:

If $a|b_1, a|b_2, \ldots a|b_n$ then

$a|\sum_{i=1}^{n} b_i x_i$ for $x_i \in Z$.

Proof: We prove this by Induction Principle

By property (3) $a|b, a|c \Rightarrow a|bx+cy$

$\therefore a|b_1, a|b_2 \Rightarrow a|b_1x_1 + b_2x_2$ for $x_1, x_2 \in Z$

$\therefore$ The result is true for two integers.

Now assume that the result is true for $(n-1)$ integers.

ie $a|b_1, a|b_2 \ldots a|b_{n-1}$

$\Rightarrow a|b_1x_1 + b_2x_2 + \ldots + b_{n-1}x_{n-1}$ for $x_1, x_2 \ldots x_{n-1} \in Z$

To prove: The result is true for 'n' integers

Consider $a|b_1, a|b_2 \ldots a|b_{n-1}, a|b_n$

$\Rightarrow a|b_1x_1 + b_2x_2 + \ldots + b_{n-1}x_{n-1}, a|b_n$

$\Rightarrow a \mid (b_1x_1 + b_2x_2 + \cdots + b_{n-1}x_{n-1})c_1 + b_n c_2$ for $c_1, c_2 \in Z$

$\Rightarrow a \mid b_1x_1c_1 + b_2x_2c_1 + \cdots + b_{n-1}x_{n-1}c_1 + b_n c_2$

$\Rightarrow a \mid b_1x_1 + b_2x_2 + \cdots b_{n-1}x_{n-1} + b_n x_n$

for $x_i = x_i c_1$ $i = 1, 2 \cdots n-1$

$c_2 = x_n$

$\Rightarrow a \mid \sum_{i=1}^{n} b_i x_i$ for $x_i \in Z$.

Hence the result is true for all 'n' integers.

Problems:

1. Show that if $ac \mid bc$ then $a \mid b$

Proof: Given $ac \mid bc$

$\Rightarrow bc = ac(x)$ for $x \in Z$

$\Rightarrow b = ax$ for $x \in Z$

$\Rightarrow a \mid b$

2. Given $a \mid b$ and $c \mid d$ Prove that $ac \mid bd$.

Proof: $a \mid b \Rightarrow b = ax$, $x \in Z$

$c \mid d \Rightarrow d = cy$, $y \in Z$

Consider $bd = (ax)(cy)$ for $x, y \in Z$

$= ac(xy)$ for $xy \in Z$

$\Rightarrow ac \mid bd$

3. Prove that n^2-n is divisible by 2 for every integer 'n'.

Proof: Consider n^2-n

$\Rightarrow n(n-1)$

$\Rightarrow n^2-n$ is an multiple of product of 2 consecutive integers.

ie one must be even and other must be odd

$\rightarrow$ Product of odd and even is also even.

$\Rightarrow$ Every even integers is divisible by 2.

$\therefore n^2-n$ is divisible by 2 $\forall$ integer 'n'.

4. Prove that n^3-n is divisible by 6.

Proof: To prove $6 \mid n^3-n$

Consider $n^3-n \Rightarrow n(n^2-1)$

$\Rightarrow n(n-1)(n+1)$

$n^3-n = n(n-1)(n+1)$ is a product of 3 consecutive integers

$n(n-1)$ is divisible by 2 — problem 3

And $n+1$ is divisible by 3 or multiple of 3

$\therefore n^3-n$ is divisible by $2 \times 3 = 6$

$\therefore 6 \mid n^3-n$.

Sunrise 6-45 AM

Theorem 1.2 : Division Algorithm Sunset 5-59 PM

Given any integers 'a' and 'b', with $a > 0$, $\exists$ unique integers 'q' & 'r' $\ni$ $b = qa + r$, $0 \leq r < a$. If $a \nmid b$, then 'r' satisfies the stronger inequalities $0 < r < a$.

Proof : Consider the Arithmetic Progression

$\ldots (b-3a), (b-2a), (b-a), b, (b+a), (b+2a), (b+3a) \ldots$

From this select the smallest non-negative number and denote it by 'r'.

Then r satisfies the inequality $0 \leq r < a$

Also r is of the form $b - qa$

$\Rightarrow r = b - qa$

$\Rightarrow b = qa + r$, $0 \leq r < a$ ——— (1)

To prove : q and r are unique.

Suppose $\exists$ q_1 and r_1 $\ni$ $b = q_1 a + r_1$ ——— (2)

Then to prove $r = r_1$ and $q = q_1$

(i) To prove $r = r_1$

If $r \neq r_1$, then either $r > r_1$ or $r < r_1$

If $r < r_1 \Rightarrow r_1 > r$

$\Rightarrow r_1 - r > 0$

$\Rightarrow 0 < r_1 - r < a$ ——— (3)

from (2), $r_1 = b - q_1 a$

(1) − (2) $\Rightarrow r - r_1 = b - qa - b + q_1 a$

$\Rightarrow r - r_1 = (q_1 - q)a$ ——— (*)

$\Rightarrow a \mid r - r_1$ $\quad r_1 - r = (q - q_1)a$

$\Rightarrow a \mid r_1 - r$

$\Rightarrow a \leq r_1 - r$ ——— (4) by property (5)

(4) is a Contradiction to (3)

$\therefore r < r_1$ is not possible.

Why $r \neq r_1$ is not proved?

$r > r_1 \rightarrow r - r_1 > 0$ $\quad r - r_1 = b - q_1 a - b + q_1 a > 0$

$\Rightarrow 0 < r - r_1 < a$ $\quad r - r_1 = (q_1 - q)a > 0$ $\quad a \mid r - r_1$

Contradiction $\rightarrow a \leq r - r_1$

$\therefore r = r_1$

Sub $r = r_1$ in (*)

we have $r - r_1 = 0 = (q_1 - q)a$

$\because a > 0$, we have $q_1 - q = 0$

$\Rightarrow q_1 = q$

$\therefore$ the integers q and r are unique.

Given $a > 0$ and $a \nmid b$

$\Rightarrow$ 'b' is not a multiple of 'a'

$\therefore 0 < r < a$ $\quad \Rightarrow b \neq qa$

$\Rightarrow b = qa + r$

Hence for $a \nmid b$, it satisfies the stronger inequality $0 < r < a$.

Hence if $a|b$, $\exists$ a unique integer q and r

$\rightarrow b = qa + r$, $0 \leq r < a$.

Definition 1.2: Greatest Common Divisor

The integer a is a common divisor of b and c if $a|b$ and $a|c$.

Since there is only a finite number of divisors of any non-zero integer, there is only a finite number of common divisors of b and c, except in the case $b = c = 0$. If at least one of b and c is not '0', the greatest among their common divisors is called the greatest common divisor of b and c & it is denoted by (b, c).

The greatest common divisor g of the integers $b_1, b_2 \cdots b_n$ not all zero by $(b_1, b_2 \cdots b_n)$.

The greatest common divisor (b, c) is defined & pair of integers b, c except $b = 0$, $c = 0$ and $(b, c) \neq 1$.

Properties of GCD

Bhogi

Given integers b and c there is only one number d with the following property

i) $d > 0$

ii) $d|b$ and $d|c \Rightarrow d$ is the common divisor of $b + c$.

iii) $e|b$ and $e|c \Rightarrow e|d$

Every common divisor of b and c divides d then the number d is called the gcd of b and c and is denoted by (b, c).

Theorem 1.3:

If g is the greatest common divisor of b and c, then there exist integers x_0 and y_0 such that $g = (b, c) = bx_0 + cy_0$

Proof: Consider the set of linear combination of b and c.

ie $A = \{bx + cy \mid x, y \in Z\}$

This set A has positive, negative values and also '0' by the choice $x = y = 0$.

Let l be the least the integer in the set A.

$l = bx_0 + cy_0$, $x_0, y_0 \in Z$

To prove: $l \mid b$ and $l \mid c$

ie to prove l is the common divisor of b & c.

Suppose,

$l \nmid b$, then by the 'division Algorithm'

$\exists$ integers q and r $\ni$ $b = lq + r$, $0 < r < l$.

$\Rightarrow r = b - lq$

$r = b - (bx_0 + cy_0)q$

$r = b - bx_0 q - cy_0 q$

$r = b[1 - x_0 q] - cy_0 q$

$r = b(1 - qx_0) + c(-qy_0)$

$1 - qx_0 \in Z$,

$-qy_0 \in Z$

This is of the form $bx + cy$

$\therefore r \in A$, $0 < r < l$

a $\Rightarrow\Leftarrow$ to the fact that l is the least +ve integer in A.

$\therefore l \mid b$

III'ly we can prove $l \mid c$

$\therefore l$ is a common divisor of b and c.

To prove: g is the linear combination of b & c.

Let g be the gcd of b and c

$l < g$ ——— (*)

$g|b \Rightarrow b = gB$, $B \in Z$

$g|c \Rightarrow c = gC$, $C \in Z$

Now, $l = bx_0 + cy_0$

$= gBx_0 + gCy_0$

$= g[Bx_0 + Cy_0]$

$\Rightarrow g|l$

By property (5) $g \leq l$.

Since g is the gcd of b and c.

$g \leq l$ is not possible by (*)

$\therefore g = l$

$\Rightarrow g = l = bx_0 + cy_0$

Theorem 1.4:

The greatest common divisor g of b and c can be characterized in the following 2 ways:

i) It is the least positive value of $bx + cy$, where x and y range over all integers

ii) It is the positive common divisor of b and c that is divisible by every common divisor.

Sunrise 6-45 AM

Sunset 6-02 PM

Proof:

i) Same as proof of Theorem 1.3

ii) Assume that $\exists$ another common divisor d of b and c.

$\Rightarrow d|b$ and $d|c$

$\Rightarrow d|bx+cy$ [$\because$ by property (3)]

$\Rightarrow d|g$ [$\because g = bx+cy$]

[Given gcd g of b and c

$\Rightarrow g|b$ and $g|c$

$\Rightarrow g|=bx+cy$]

Theorem 1.5: Given any integers $b_1, b_2 \cdots b_n$ not all zero, with greatest common divisor g, there exist integers $x_1, x_2 \cdots x_n$ such that

$$g = (b_1, b_2 \cdots b_n) = \sum_{j=1}^{n} b_j x_j$$

Furthermore, g is the least positive value of the linear form $\sum_{j=1}^{n} b_j y_j$ where the y_j range over all integers; also g is the positive common divisor of $b_1, b_2 \cdots b_n$ that is divisible by every common divisor.

Sunrise 6-45 AM

Proof:

Sunset 6-02 P

Let us prone this theorem by Induction hypothesis.

When $n=2$; $(b_1, b_2) = g_1$

Then by Theorem 1.3, we have

$$g_1 = b_1 x_1 + b_2 x_2$$
$$= (b_1, b_2)$$

The theorem is true for $n=2$.

When $n=3$; $(b_1, b_2, b_3) = g_2$

$\Rightarrow$ $g_2 = b_1 x_1 + b_2 x_2 + b_3 x_3$ not necessary

$\Rightarrow$ $g_2 = (b_1, b_2, b_3)$

$\Rightarrow (b_1, b_2, b_3) = ((b_1, b_2), b_3) = g_2$

By theorem 1.3,

$$g_2 = (b_1, b_2) y_1 + b_3 y_2$$
$$= (b_1 x_1 + b_2 x_2) y_1 + b_3 y_2$$
$$= b_1 (x_1 y_1) + b_2 (x_2 y_1) + b_3 y_2$$

$$g_2 = (b_1, b_2, b_3)$$

The Theorem is true for $n=3$.

Assume that the result is true for $n-1$

ie $(b_1, b_2 \cdots b_{n-1}) = g_3$

ie $g_3 = b_1 x_1 + b_2 x_2 + \cdots + b_{n-1} x_{n-1}$

To prone the theorem is true for n.

Let $(b_1, b_2 \cdots b_n) = g$

$g = ((b_1, b_2, \ldots b_{n-1}), b_n)$

$= (g_3, b_n)$

By Theorem 1.3 : $g = g_3 y_1 + b_n y_2$

$g = (b_1 x_1 + b_2 x_2 + \cdots + b_{n-1} x_{n-1}) y_1 + b_n y_2$

$= b_1 (x_1 y_1) + b_2 (x_2 y_1) + \cdots + b_{n-1} (x_{n-1} y_1) + b_n y_2$

$g = b_1 c_1 + b_2 c_2 + \cdots + b_{n-1} c_{n-1} + b_1 c_n$

$c_1, c_2 \cdots c_n \in Z$

ie $g = (b_1, b_2 \cdots b_n)$

∴ The theorem is true for all 'n' $\in Z$

Theorem 1.6:

For any positive integer m, $(ma, mb) = m(a, b)$

Proof: By theorem 1.4

(ma, mb) = least +ve value of $max + mby$

$\forall\ x, y \in Z$

= least +ve value of $m(ax + by)$

$\forall\ x, y \in Z$

$= m$ (least +ve value of $(ax + by)$)

$= m(a, b)$

Sunrise 6-45 AM

Theorem 1.7 : 5 m (X)

Sunset 6-03 p

(i) If $d|a$ and $d|b$ and $d>0$, then

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

(ii) If $(a,b) = g$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

Proof:

(i) Given $d|a$, $d|b$

$\Rightarrow a = ld$ and $b = md$, $\forall l, m \in Z$

$\Rightarrow \frac{a}{d} = l$ and $\frac{b}{d} = m$

Now, $\left(\frac{a}{d}, \frac{b}{d}\right) = (l, m)$

$=$ least +ve value of $lx+my$, $x, y \in Z$

$=$ least +ve value of $\frac{a}{d}x + \frac{b}{d}y$

$=$ least +ve value of $\frac{1}{d}(ax+by)$

$= \frac{1}{d}$ [least +ve value of $(ax+by)$]

$= \frac{1}{d}(a,b)$

(ii) Consider $(a,b) = g$ (Given)

$\hookrightarrow \left(\frac{a}{g}, \frac{b}{g}\right) = \frac{1}{g}(a,b) = \frac{1}{g} \cdot g = 1$

$\because$ by (i)

Sunrise 6-45 AM

Sunset 6-04 PM

Theorem 1.8:

If $(a,m) = (b,m) = 1$, then $(ab,m) = 1$.

Proof:

$(a,m) = 1 \Rightarrow \exists\ x_0, y_0 \in Z \ni ax_0 + my_0 = 1$ ——— (1)

$(b,m) = 1 \Rightarrow \exists\ x_1, y_1 \in Z \ni bx_1 + my_1 = 1$ ——— (2)

From (1) $ax_0 = 1 - my_0$

From (2) $bx_1 = 1 - my_1$

Consider $ax_0(bx_1) = (1 - my_0)(1 - my_1)$

$ab(x_0x_1) = 1 - my_1 - my_0 + m^2 y_0 y_1$

$= 1 - m(y_1 + y_0 - my_0y_1)$

$\Rightarrow ab\,x_2 = 1 - my_2$ [$\because x_0x_1 = x_2 \in Z$, $y_1 + y_0 - my_0y_1 = y_2 \in Z$]

$\Rightarrow abx_2 + my_2 = 1$

$\Rightarrow (ab, m) = 1$

Theorem 1.9: (X. 5m or 10m)

For any integer 'x' then $(a,b) = (b,a) = (a,-b) = (a,b+ax)$

Proof:

(i) To prove $(a,b) = (b,a)$

Let $(a,b) = g$

(a,b) = least +ve value of $ax + by$, $\forall x, y \in Z$

= least +ve value of $by + ax$ $\forall y, x \in Z$

$(a,b) = (b,a)$ ——— (1)

(ii) To prove $(a,b) = (a,-b)$

(a,b) = least +ve value of $ax+by$, $\forall x,y \in Z$

= least +ve value of $ax-b(-y)$ $\forall x,-y \in Z$

$= (a,-b)$

$\Rightarrow (a,b) = (a,-b)$ ——— (2)

(iii) To prove $(a,b) = (a, b+ax)$

Let $(a,b) = d_1$ and $(a, b+ax) = d_2$

$(a,b) = d_1 \Rightarrow d_1 | a$ and $d_1 | b$

$\Rightarrow d_1 | a$, $d_1 | ax$ and $d_1 | b$

$\Rightarrow d_1 | a$, $d_1 | b+ax$ [by property (3)]

$\Rightarrow d_1 | d_2$ [$\because d_2 = (a, b+ax)$]

$\Rightarrow d_1 \leq d_2$ — (3) [by property (5)]

Now, $(a, b+ax) = d_2$

$\Rightarrow d_2 | a$, $d_2 | b+ax$

$\Rightarrow d_2 | a$, $d_2 | -ax$, $d_2 | b+ax$

$\Rightarrow d_2 | a$, $d_2 | -ax+b+ax$

$\Rightarrow d_2 | a$, $d_2 | b$

$\Rightarrow d_2 | d_1$ [$\because d_1 = (a,b)$]

$\Rightarrow d_2 \leq d_1$ ——— (4)

From (3) & (4), $d_1 = d_2$

$\Rightarrow (a,b) = (a, b+ax)$ ——— (5)

Sunrise 6-45 AM

Sunset 6-05 PM

From ①, ② and ⑤, we have

$(a,b) = (b,a) = (a,-b) = (a, b+ax)$

Theorem 1.10: Euclid's lemma 5m

If $c|ab$ and $(b,c)=1$ then $c|a$

Proof: Given $(b,c)=1$ and $c|ab$

W.k.T $(ma, mb) = m(a,b)$

III^{ly} $(ab, ac) = a(b,c)$

$= a \cdot 1$

$= a$

$\therefore a = abx + acy \quad \forall\ x, y \in \mathbb{Z}$

Now, $c|ab \Rightarrow c|abx,\ c|acy$ →?

$\Rightarrow c|abx+acy$ [∵ by property ③]

$\Rightarrow c|a$

Problems:

1. Find $(64, 43)$

$64 = (1 \times 43) + 21$

$43 = (2 \times 21) + 1$

$21 = (1 \times 21) + 0$

$1 = 43 - 2(21)$

$= 43 - 2[64 - (1 \times 43)]$

$= 43 - 2 \times 64 + 2 \times 43$

$1 = 43 \times 3 - 2 \times 64$

$\therefore x = -2 \ ; y = 3$

$gcd = 1$

Sunrise 6-45 AM

2. Find (93, 81) $x = 7$, $y = -81$, GCD = 3

3. Find (963, 657) $x = -15$, $y = 22$, GCD = 9

After Theorem 1.11.

4. By using the Euclidean Algorithm, find the GCD
   i) 7469 and 2464
   ii) 2689 " 4001
   iii) 2947 " 3997
   iv) 1109 " 4999

5. Find the GCD of the numbers 1819 and 3587, and find the integer x & y to satisfy
   $1819x + 3587y = 9$

6. Find the value of x & y to satisfy
   a. $423x + 198y = 9$
   b. $71x - 50y = 1$
   c. $43x + 64y = 1$
   d. $93x - 81y = 3$

Sunrise 6-45 AM

Theorem 1.11 : Euclidean Algorithm

Sunset 6-06 PM

Given integers b and $c > 0$, we make a repeated application of the division algorithm, Theorem 1.2, to obtain a series of equations

$$b = cq_1 + r_1, \quad 0 < r_1 < c$$
$$c = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2,$$
$$\cdots\cdots$$
$$r_{j-2} = r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}$$
$$r_{j-1} = r_j q_{j+1} \quad \text{(1)}$$

The greatest common divisor (b, c) of b and c is r_j, the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b, c) = bx_0 + cy_0$ can be obtained by writing each r_i as a linear combination of b and c.

Proof:

Divide b by c $\Rightarrow$ $b = cq_1 + r_1, \quad 0 < r_1 < c$

" c " r_1 $\Rightarrow$ $c = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$

" r_1 " r_2 $\Rightarrow$ $r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$

Proceeding like this, we get the set of equations (1)

By using the Theorem 1.9,

$$(a, b) = (a, b + ax)$$

$$\Rightarrow (b, c) = (b - cq_1, c)$$
$$= (r_1, c)$$
$$= (r_1, c - r_1 q_2)$$
$$= (r_1, r_2)$$
$$= (r_1 - r_2 q_3, r_2)$$
$$= (r_3, r_2)$$
$$\vdots$$
$$= (r_{j_0-1}, r_{j_0})$$
$$= (r_{j_0} q_{j_0+1}, r_{j_0})$$
$$= r_{j_0} (q_{j_0+1}, 1)$$
$$= r_{j_0}(1) \quad [\because (q_{j+1}, 1) = 1]$$
$$= r_{j_0}$$

In equation (1), r_{j_0} can be written as a linear combination of b and c by eliminating r_i's

$$r_{j_0} = (b, c)$$
$$r_{j_0} = bx_0 + cy_0, \quad x_0, y_0 \in Z$$

Note: We also note that the remainders $r_1, r_2 \cdots r_{j_0}$ are always greater than '0'.

If $r_1 = 0 \Rightarrow b = cq_1 + r_1$

$$b = cq_1$$
$$(b, c) = (cq_1, c) = c(q_1, 1) = c$$

The Lord of Sri said: While speaking learned words, you lament for those not worthy of lamentation

Illy if $r_2 = 0 \Rightarrow c = r_1 q_2$

$(c, r_1) = (r_1 q_2, r_1)$

$= r_1 (q_2, 1)$

$(c, r_1) = r_1$.

Definition 1.4 : Least Common Multiple [LCM]

The integers $a_1, a_2 \cdots a_n$ all different from zero, have a common multiple 'b' if $a_i | b$, $i = 1, 2 \cdots n$. The least of the common multiple is called the LCM and it is denoted by $[a_1, a_2 \cdots a_n]$.

Example : Consider the integers 6 and 10.

Multiples of 6 = 1, 6, 12, 18, 24, 30, 36, ...

" " 10 = 1, 10, 20, 30, 40, 50, 60, ...

Common multiples of 6 and 10 are

30, 60, 90, ...

LCM of 6 and 10 is 30.

$[6, 10] = 30$

Note: LCM of a and b is always greater than a and b.

ie if $[a, b] = h$ Then $h \geq a$, $h \geq b$

Also $a | h$ and $b | h$

$\Rightarrow$ If $\exists$ another multiple then h will divide that multiple

$\Rightarrow$ h is the LCM, then the other multiples are

0, $\pm h$ $\pm 2h$, ----

Theorem 1.12: If m is any common multiple of $a_1, a_2 \cdots a_n$ then $[a_1, a_2 \cdots a_n] \mid m$ (or) if $h = [a_1, a_2 \cdots a_n]$ then $0, \pm h, \pm 2h$ --- comprise all the common multiples of $a_1, a_2 \cdots a_n$

Proof:

Let 'm' be any common multiple of $a_1, a_2 \cdots a_n$ and $h = [a_1, a_2 \cdots a_n]$, then $h \mid m$.

Divide 'm' by 'h' by Division Algorithm

$$m = qh + r \quad , \quad 0 \le r < h \qquad \text{---------} (1)$$

To prove: $r = 0$

If $r \neq 0$, Then for each i,

$a_i \mid h$ and $a_i \mid m$, $i = 1, 2 \cdots n$

$\therefore$ $a_i \mid hx + my$, $x, y \in Z$

ie $a_i \mid h(-q) + m(1)$, $x = -q$, $y = 1$

ie $a_i \mid -qh + m$

$\Rightarrow$ $a_i \mid r$ [by (1)]

Thus r is the common multiple of $a_1, a_2 \cdots a_n$ which is less than the +ve LCM h.

O son of Kunti happiness

Sunrise 6-45 AM

Sunset 6-07 PM

$a \Rightarrow \Leftarrow$ to the fact that $r \neq 0$

$\therefore r = 0$

$\therefore m = qb$

ie $b \mid m$

Theorem 1.13 :

If $m > 0$, $[ma, mb] = m[a, b]$ also $[a,b] \cdot (a,b) = |ab|$

Proof :

Let $[ma, mb] = b_1$ and $[a, b] = b_2$

$[a,b] = b_2 \Rightarrow b_2$ is the LCM of a and b

$\Rightarrow b_2$ is a multiple of a

$\Rightarrow b_2 = ka$

$\Rightarrow mb_2 = mka$

$\Rightarrow mb_2$ is a multiple of 'ma'

III^{ly} mb_2 is a multiple of 'mb'

Thus mb_2 is a multiple of ma and mb.

Since $[ma, mb] = b_1$, $b_1 \leq mb_2$ ——— (1)

Now, $[ma, mb] = b_1$

$\Rightarrow b_1$ is a multiple of ma and mb

$\Rightarrow b_1 = mak$

$\Rightarrow \frac{b_1}{m} = ak$

$\Rightarrow \frac{b_1}{m}$ is a multiple of 'a'

Similarly $\frac{b_1}{m}$ is a multiple of 'b'

Thus, $\frac{b_1}{m}$ is a multiple of 'a' and 'b'

Since $b_2 = [a,b]$, $b_2 \leq \frac{b_1}{m}$ or $mb_2 \leq b_1$

$\Rightarrow b_1 \geq mb_2$

From (1) & (2) $b_1 = mb_2$ ——— (2)

$\Rightarrow [ma, mb] = m[a,b]$

Let $(a,b) = 1$ (*)

It is enough to prove for the integers a and b

Since $[a,-b] = [a,b]$??

$[a,b]$ is a multiple of 'a' (say)

$[a,b] = ma$

$\Rightarrow b \mid ma$

$\Rightarrow b \mid m$ [by Theorem 1.10 Euclid's lemma]

$\Rightarrow b \leq m$

$\Rightarrow ba \leq ma$

But ba, being a +ve common multiple of a and b, cannot be less than the LCM of ba and ma.

$\therefore ba = ma$

$\therefore [a,b] = ma = ba$

$\therefore [a,b](a,b) = [a,b] \cdot 1 = ab$ [$\because (a,b) = 1$ Assumption ✗]

General Case :

Let $(a,b) = g > 1$

Then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ [$\because$ by Theorem 1.7]

$$\left[\frac{a}{g}, \frac{b}{g}\right]\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{a}{g} \cdot \frac{b}{g}$$

$$g^2\left[\frac{a}{g}, \frac{b}{g}\right]\left(\frac{a}{g}, \frac{b}{g}\right) = g^2 \frac{a}{g} \cdot \frac{b}{g}$$

$$g^2 \cdot \frac{1}{g}[a,b]\frac{1}{g}(a,b) = ab$$

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

Sunrise 6-44 AM

1.3 Primes

Sunset 6-10 PM

Definition 1.5 :

An integer $p > 1$ is called a prime number if there is no divisor 'd' of 'p' satisfying $1 < d < p$.

If an integer $p > 1$ is not a prime, it is called a composite number.

Theorem 1.14 :

Every integer $n > 1$ can be expressed as a product of primes.

Proof :

If 'n' is a prime, it is a product of a single factor.

If 'n' is not a prime, it can be factorised as $n = n_1 \times n_2$, $1 < n_1 < n$, $1 < n_2 < n$.

If 'n_1' is prime, keep it as it is.... otherwise factorize it as $n_1 = n_3 \times n_4$, $1 < n_3 < n_1$, $1 < n_4 < n_1$

Similarly if 'n_2' is prime, keep it as it is .... otherwise, factorize it is $n_2 = n_5 \times n_6$, $1 < n_5 < n_2$ $1 < n_6 < n_2$

Continue till all factors are prime and the result can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where $p_1, p_2 \cdots$ are primes and $\alpha_1, \alpha_2 \cdots$ are integers.

Hence every integer $n > 1$ can be expressed as a product of primes.

Theorem 1.15

If $p \mid ab$, 'p' being a prime then $p \mid a$ or $p \mid b$, more generally if $p \mid a_1 * a_2 * \cdots a_n$, then p divides atleast one 'a_i' of the product.

Proof:

If $p \nmid a$ then $(a, p) = 1$, then by theorem 1.10

$p \mid b$

General Case:

This is proved by induction

Given $p \mid a_1 * a_2 * \cdots * a_n$

To prove: $p \mid a_i$ for some 'i'

$n = 2 \Rightarrow p \mid a_1 a_2 \Rightarrow p \mid a_1$ or $p \mid a_2$

Assume the theorem is true for $n-1$

$p \mid a_1 a_2 \cdots a_{n-1} \Rightarrow p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_{n-1}$

Sunrise 6-44 AM Sunset 6-10 PM

Consider $p \mid a_1 a_2 \ldots a_n$

$\Rightarrow p \mid (a_1 a_2 \ldots a_{n-1})\, a_n$

$\Rightarrow p \mid k a_n$ ie $k = a_1 a_2 \ldots a_{n-1}$

If $p \mid a_n$ Then the proof is over

If $p \nmid a_n$ Then $p \mid k$

ie $p \mid a_1 a_2 \ldots a_{n-1}$

$\Rightarrow p$ divides atleast one 'a_i'

Hence The theorem is true for 'n'.

Thus it is true for all the integers.

Theorem 1.16

The fundamental theorem of Arithmetic (or) Unique Factorization Theorem.

The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.

Proof:

To prove: Uniqueness

$n = 2$ is a prime.

∴ The theorem is true for $n = 2$.

Assume that the theorem is true for all integers less than 'n' and greater than one.

ie $1 < x < n$

The 'x' can be written as a product of prime factors.

Now, take the integer 'n', if 'n' is prime the proof is over.

Assume 'n' is composite.

Suppose 'n' has a prime factorization

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

To prove: $r = s$

Take a prime number p_1

$p_1 \mid p_1 p_2 \cdots p_r$

$\Rightarrow p_1 \mid n$

$\Rightarrow p_1 \mid q_1 q_2 \cdots q_s$

$\Rightarrow p_1$ divides atleast one q_i

$\Rightarrow p_1 \mid q_1$ (say)

$\Rightarrow p_1 = q_1$ [$\because p_1, q_1$ both are primes] ???

Now, $\frac{n}{p_1} = \frac{p_1 p_2 \cdots p_r}{p_1} = \frac{q_1 q_2 \cdots q_s}{p_1}$

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s \quad \text{——— (1)}$$

$\therefore \frac{n}{p_1} < n$

By induction hypothesis $\frac{n}{p_1}$ is a product of prime factors in one and only one way.

① $\Rightarrow$ $r = s$ and each 'p_i' is some 'q_i', $2 \le i \le t$

$\therefore \frac{n}{p_1} = p_2 \cdot p_3 \cdots p_r$

$n = p_1 p_2 p_3 \cdots p_r$

Thus 'n' has a prime factorization in one and only one way.

$\therefore$ By Induction every integer $n \ge 1$ can be expressed as a product of prime factors.

ie one and only one way apart from the order of factors.

Theorem 1.17 : Euclid's Theorem (-X-) 300 BC

The number of primes is infinite (or) there is no end to the sequence of primes.

Proof :

Assume that there are finite no of primes $p_1, p_2 \cdots p_n$ set $p_1 < p_2 < \cdots < p_n$.

Consider a number of the form $n\not{N} = 1 + p_1 \cdot p_2 \cdot \cdots \cdot p_n$

$$n\not{N} = 1 + p_1 p_2 \cdots p_n$$

Here $n\not{N}$ is an integer and $n > p_i \ \forall i = 1, 2 \cdots n$

$\therefore$ n is not a prime number

$\Rightarrow$ n is a composite number

By Theorem 1.14

n is a product of primes.

$\therefore$ n is divisible by some prime

Suppose $p_i \mid n$ for $i = 1, 2 \cdots n$

$\Rightarrow p_i \mid n - p_1 p_2 \cdots p_n$

$\Rightarrow p_i \mid 1$

$a \Rightarrow \Leftarrow$

$\therefore$ n is divisibb by some prime except $p_1, p_2 \cdots p_n$

$\therefore$ There are infinitely many primes.

Theorem 1.18 :

There are arbitrarily large gaps in the series of primes (or) Given any (+ve) positive integer 'k', $\exists$ 'k' consecutive Composite numbers.

Proof : Consider the integer k that makes the sequence,

$(k+1)! + 2, (k+1)! + 3, \ldots (k+1)! + k, (k+1)! + (k+1)$

$(k+1)! + 2$ is divisible by 2

$(k+1)! + 3$ is " " 3

⋮

$(k+1)! + k+1$ " " $k+1$

∴ the above 'k' numbers are composite for different values of 'k', we get 'k' composite numbers.

There are arbitrarily large gaps in the sequence of primes.

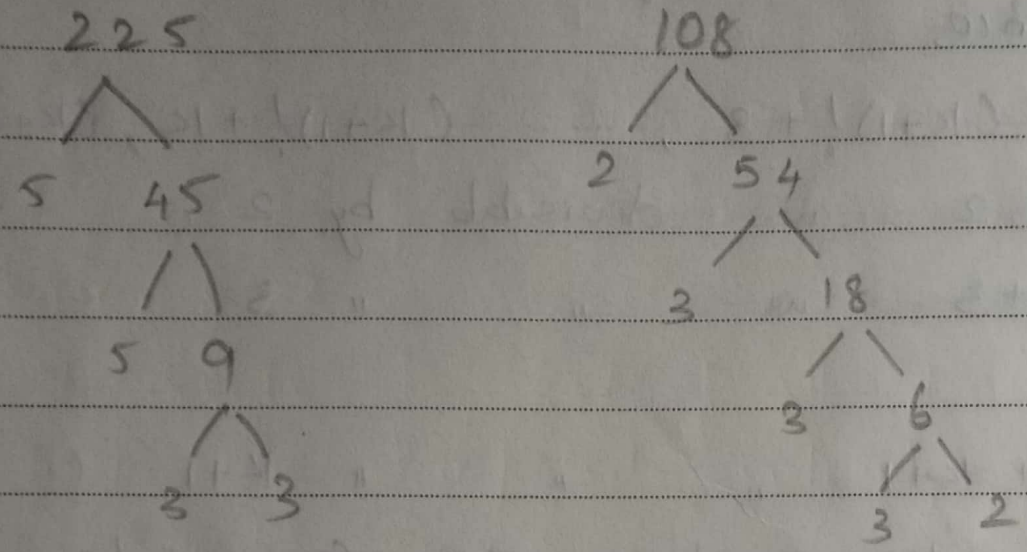
Note :

Sunrise 6-43 AM

Problems:

Sunset 6-12 PM

1. Find $(108, 225)$, $[108, 225]$



$108 = 2^2 \cdot 3^3 \cdot 5^0$

$225 = 3^2 \, 5^2 \cdot 2^0$

$(108, 225) = 2^{\min(2,0)} \; 3^{\min(3,2)} \; 5^{\min(0,2)}$

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

$= 3^2$

$= 9$

$[108, 225] = 2^{\max[2,0]} \; 3^{\max[3,2]} \; 5^{\max[0,2]}$

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

$= 4 \times 27 \times 25$

$= 2700$

2. $(30, 60)$, $[30, 60]$

3. $(60, 61)$, $[60, 61]$

Sunrise 6-44 AM

Theorem 1.19: 10 marks (X)

Sunset 6-14 PM

For every real number $y \geq 2$, $\sum_{p \leq y} \frac{1}{p} > (\log(\log y) - 1)$

here the sum is over all primes $p \leq y$.

Proof:

Given $y \geq 2$

Let N denote the set of all positive integers 'n' that are composed entirely of primes 'p' not exceeding 'y'.

ie $N = \{n \mid p \leq y\}$

Since there are only finitely many primes $p \leq y$, the terms of an absolutely convergent infinite series may be arbitrarily rearranged.

$$\prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum_{n \in N} \frac{1}{n}$$

$$\Rightarrow \prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \in N} \frac{1}{n} \quad \text{——— (1)}$$

If 'n' is a positive integer $\leq y$, then $n \in N$, the above sum includes $\sum_{n \in N} \frac{1}{n}$.

Let N denote the largest integer $\leq y$.

Sunrise 6-42 AM

Sunset 6-14 PM

By the integral test,

$$\sum_{n=1}^{N} \frac{1}{n} \geq \int_1^{N+1} \frac{dx}{x} = \log x \Big|_1^{N+1}$$

$$= \log N+1 - \log 1$$

$$= \log N+1$$

$$> \log y$$

ie $$\sum_{n \in N} \frac{1}{n} > \log y \quad \text{——— (2)}$$

$\therefore$ (1) becomes, $\prod_{p \leq y} (1 - \frac{1}{p})^{-1} > \log y$ ——— (3)

Now, Assume that, $e^{v+v^2} \geq (1-v)^{-1}$ ——— (4) holds for all real nos v in the interval $0 \leq v \leq 1/2$.

Taking $v = 1/p$.

(4) $\Rightarrow e^{v+v^2} \geq (1 - \frac{1}{p})^{-1}$

$$\therefore \prod_{p \leq y} e^{\frac{1}{p} + \frac{1}{p^2}} \geq \prod_{p \leq y} (1 - \frac{1}{p})^{-1}$$

$$\exp \sum_{p \leq y} \left(\frac{1}{p} + \frac{1}{p^2}\right) > \log y \quad [\because \text{by (3)}]$$

Since $\prod \exp(a_i) = \exp(\sum a_i)$

Taking log on both sides

$$\sum_{p \le y} \left(\frac{1}{p} + \frac{1}{p^2} \right) > \log \log y$$

$$\Rightarrow \sum_{p \le y} \frac{1}{p} + \sum_{p \le y} \frac{1}{p^2} > \log \log y \quad \text{—— (5)}$$

Using Comparison test,

$$\sum_{p \le y} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2}$$

$$< \int_1^{\infty} \frac{dx}{x^2}$$

$$= \left(-\frac{1}{x} \right)_1^{\infty}$$

$$= 0 - (-1)$$

$$= 1$$

(5) $\Rightarrow$

$$\sum_{p \le y} \frac{1}{p} + 1 > \log \log y$$

$$\Rightarrow \sum_{p \le y} \frac{1}{p} > \log \log y - 1$$