	GOVERNMENT ARTS AND SCIENCE COLLEG, KOVILPATTI – 628 503. (AFFILIATED TO MANONMANIAM SUNDARANAR UNIVERSITY, TIRUNELVELI) DEPARTMENT OF MATHEMATICS STUDY E - MATERIAL CLASS : II M.Sc. (MATHEMATICS) SEM: III SUBJECT : ALGEBRAIC NUMBER THEORY(PMAE31)

Algebraic Number Theory (60 Hours)

L	T	P	C
2	2	0	3

Objective:

- To acquire knowledge about recent developments in Algebra have its impact on Number Theory and Number Theory too has its own contribution to the development of algebra.
- To understand and appreciate the role played by Algebra in Number Theory.

Prerequisite:

Basic knowledge in Distribution of primes, Mathematical Induction and Congruence..

Outcome:

Knowledge gained about various types of numbers such as algebraic Numbers, Pythagorean triples and representation of number as sum of positive squares.

Unit I: **Diophantine equations :**Diophantine equations – The equation ax+by=c – Positive solutions – Other linear equations. L 12

Unit II: **Some special equations:**The equation $x^2+y^2=z^2$ – The equation $x^4+y^4=z^2$.The equation $4x^2+y^2=n$ L 12

Unit III: **Infinite continued functions :**The equation $ax^2+by^2+cz^2=0$- Infinite continued functions – Irrational numbers. L 13

Unit IV: **Approximation to irrational numbers :**Approximation to irrational numbers- Algebraic integers . L 11

Unit V: **Quadratic Fields :**Quadratic Fields – Units in quadratic fields. L 12

Text book: **An introduction to the theory of Numbers – Ivan Nivan and Herbert S. Zukerman** – II edition, Wiley Eastern Ltd.

Book for Reference:

Elements of Number Theory – Kumaravelu and SuseelaKumaravelu (2002), Raja Shankar Printers,Sivakasi(V Edition).

Algebraic Number Theory

Syllabus

UNIT-I Diophantine equations: Diophantine eqns – The equation $ax+by=c$ – positive solutions – other linear equations

UNIT-II Some special equations: The eqn $x^2+y^2=z^2$ – the equation $x^4+y^4=z^2$ – The equation $4x^2+y^2=n$

UNIT-III Infinite continued functions: The equation $ax^2+by^2+cz^2=0$ – Infinite continued functions – Irrational Infinite continued functions – Irrational Numbers

UNIT-IV Approximation to irrational numbers – Approximation to irrational numbers – Algebraic integers.

UNIT-V Quadratic Fields: Quadratic fields – units in quadratic fields.

Text Book:

An Introduction to the theory of Numbers - Ivan Nivan and Herbert S. Zukerman - II Edition, Wiley Eastern Limited.

Book for reference:

Elements of Number theory - Kumaravelu & Suseela Kumaravelu (2002), Raja Shankar Printers, Sivakasi (5th Edition)

9/6/18

UNIT-I

Some Diophantine Equation

Pb: Finding the solution of this problem is called solving the Diophantine equation

The eqn $ax+by=c$

Let $ax+by=c$ be a linear equation in two variables x, y with (a,b,c) 3 integer co-efficients.

The solution of this eqn is trivial.

Unless neither a nor b is zero,

So we can assume that $a \neq 0$ and $b \neq 0$

Let $(a,b)=g$

If $g \nmid c$, then the eqn $ax+by=c$ has no solution.

Suppose $g \mid c$

$\because (a,b)=g$ $\exists$ integers x_0 and y_0 s.t

$ax_0+by_0=g$

put $x_1 = \frac{c}{g}x_0$. $y_1 = \frac{c}{g}y_0$

Then $ax_1+by_1 = \frac{c}{g}(ax_0+by_0)$

$= \frac{c}{g} \times g$

$= c$

$\therefore x_1, y_1$ is a solution of $ax+by=c$.

To find all solutions.

Let r, s be any integers

Solution of $ax+by=c$

Then $ar+bs=c = ax_1+by_1$

$\therefore a(r-x_1) = -b(s-y_1)$

$\Rightarrow \frac{a}{g}(r-x_1) = -\frac{b}{g}(s-y_1)$ —— (*)

Now, $(a,b)=g \Rightarrow \left(\frac{a}{g}, \frac{b}{g}\right)=1$ (by thm)

$\frac{a}{g} \mid (s-y_1)$ and $\frac{b}{g} \mid (r-x_1)$

$\Rightarrow s-y_1 = \frac{a}{g}u$ and $r-x_1 = \frac{b}{g}t$

$\therefore r = x_1 + \frac{b}{g}t$ and $s = y_1 + \frac{a}{g}u$

(*) $\Rightarrow \frac{a}{g} \times \frac{b}{g}t = \frac{-b}{g}\frac{a}{g}u$

$t = -u$

$\therefore r = x_1 + \frac{b}{g}t$ and $s = y_1 - \frac{a}{g}t$

where t is any integer.

Notes:

1) The eqn $ax+by=c$ has integers soln's if $(a,b) \mid c$.

2) Suppose a, b and c have a

~~Common~~ Common ~~division~~ divisor. ~~Pick~~

Dividing out the g.c.d we get $(a,b,c)=1$. Then the eqn $ax+by=c$ is solvable iff $(a,b)=1$ and the soln is $x=x_1+bt$ and $y=y_1-at$ where x_1, y_1 is one of the solutions.

Pb: P.T $ax+by=a+c$ is solvable iff $ax+by=c$ is solvable.

proof: Let $(a,b)=g$

$ax+by=c$ is solvable iff $g|c$ — (1)

Also, $g|a$ and $g|b$

Now, $g|a$ & $g|c$

$\Rightarrow g|a+c$

$ax+by=a+c$ is solvable (by (1))

Conversely,

Assume that $ax+by=a+c$ is solvable

$\Rightarrow g|a+c$

Also, $g|a$

$\Rightarrow g|a+c-a$

$\Rightarrow g|c$

$ax+by=c$ is solvable.

2. P.T $ax+by=c$ is solvable iff $(a,b)=(a,b,c)$

proof: Let $(a,b)=(a,b,c)=g$

$\Rightarrow g|a,\ g|b\ \&\ g|c$

$g|c \Rightarrow ax+by=c$ is solvable

Conversely,

Assume that $ax+by=c$ is solvable

$\Rightarrow g|c = (a,b)|c$

$(a,b,c) = ((a,b),c)$

$= (g,c)$ $\quad (\because g|c \Rightarrow c=gx_0$

$= g$ $\quad \therefore (g,gx_0)=g)$

$= (a,b)$

3. Show that soln of the eqn $3x+5y=1$ is in the form $x=2+5t$, $y=-1-3t$ also in the form $x=2-5t$, $y=-1+3t$ also in the form $x=-3+5t$ $y=2-3t$.

Soln: $(3,5)=1$

$\therefore 1|c$ where $c=1$

$\Rightarrow 3x+5y=1$ has a solution

Let x_0, y_0 be the soln of $ax+by=g$

ii) x_0, y_0 be the soln of $3x+5y=1$.

$x_0 = 2$, $y_0 = -1$

$x_1 = \frac{c}{g} x_0 = \frac{1}{1}(2) \Rightarrow x_1 = 2$

$y_1 = \frac{c}{g} y_0 = \frac{1}{1}(-1) \Rightarrow y_1 = -1$

The other solutions are

$x_1 = 2$ $y_1 = -1$.

$$\left.\begin{array}{l} r = x_1 + \frac{b}{g} t \quad s = y_1 - \frac{a}{g} t \end{array}\right\} \text{—} ①$$

$r = 2+5t$ $\quad s = -1-3t$

$x_0 = 7$ $y_0 = -4$

$x_1 = 7$ $y_1 = -4$

$r = 7+5t$ $\quad s = -4-3t$

$x_0 = -3$ $y_0 = 2$

$x_1 = -3$ $y_1 = 2$.

$r = -3+5t$ $\quad s = 2-3t$

put $u = -t$ in ①

$\therefore r = 2-5t$ and $s = -1+3t$.

4. Solve the eqn $6x+9y = 13$

Soln: $(6,9) = 3$, $3 \nmid 13$

$\therefore 6x+9y = 13$ has ~~a~~ no integer solution.

5. Solve $10x - 7y = 17$

Soln: $a = 10 \quad b = -7$

$(10, -7) = (10, 7) = 1$

$\therefore 1 \mid 17$

$\Rightarrow 10x - 7y = 17$ has a soln.

Let x_0, y_0 be the soln of $ax + by = g$

$x_0 = 5 \quad y_0 = 7$ be a soln of $10x - 7y = 1$

1 Here $g = 1$, $c = 17$

$$x_1 = \frac{c}{g} x_0 \ \& \ y_1 = \frac{c}{g} y_0.$$

$$x_1 = 85, \quad y_1 = 119$$

$$r = x_1 + \frac{b}{g} t \qquad s = y_1 - \frac{a}{g} t$$

$$r = 85 + \frac{(-7)}{1} t \qquad s = 119 - \frac{10}{1} t$$

ie) $r = 85 - 7t \qquad s = 119 - 10t$

$$x_0 = -2 \qquad y_0 = -3$$

$$x_1 = \frac{c}{g} x_0 \qquad y_1 = \frac{c}{g} y_0$$

$$x_1 = -34 \qquad y_1 = -51$$

$$r_1 = -34 - 7t \qquad s = -51 - 10t$$

Positive solns:

We find the ~~non~~ +ve integer soln of $ax+by=c$.

Let $(a,b)=g$

$ax+by=c$ is solvable iff $g|c$ and the solns are $x=x_1+\frac{b}{g}t$

$y=y_1-\frac{a}{g}t$

where x_1, y_1 is a particular soln and t is any integer.

we want the soln $x>0$ & $y>0$.

i.e) $x_1+\frac{b}{g}t>0$ and $y_1-\frac{a}{g}t>0$.

i.e) $t>\frac{-g}{b}x_1$ and $t<\frac{gy_1}{a}$.

i.e) $-\frac{gx_1}{b}<t<\frac{gy_1}{a}$.

The lowest possible value of t is $\left[\frac{-gx_1}{b}\right]+1$

The highest possible value of t is $-\left[\frac{-gy_1}{a}+1\right]$.

Let N be the no of positive integer solns.

Then

$$N = -\left[-\frac{gy_1}{a}+1\right] - \left[-\frac{gx_1}{b}+1\right]+1$$

$$N = -\left[-\frac{gy_1}{a}\right] - \left[-\frac{gx_1}{b}\right] - 1 \quad \left[\because [x+m] = [x]+m \text{ if } m \text{ is an integer}\right]$$

ie) $N = -\left(\left[-\frac{gy_1}{a}\right] + \left[-\frac{gx_1}{b}\right] + 1\right)$.

W.K.T,

$$[x]+[y] \le [x+y] \le [x]+[y]+1$$

$$[x+y] \le [x]+[y]+1$$

$$-[x+y] \geq -\{[x]+[y]+1\}$$

$$-\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right] \geq -\left\{\left[-\frac{gy_1}{a}\right] + \left[-\frac{gx_1}{b}\right]+1\right\}.$$

$$-\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right] \geq N \text{ ——— } (1).$$

$$[x]+[y]+1 \le [x+y]+1$$

$$-\{[x]+[y]+1\} \geq -\{[x+y]+1\}$$

$$-\left\{\left[-\frac{gy_1}{a}\right] + \left[-\frac{gx_1}{b}\right]+1\right\} \geq -\left\{\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right]+1\right\}$$

$$N \geq -\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right] - 1 \text{ ——— } (2).$$

From (1) & (2), we get

$$-\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right] - 1 \le N \le -\left[-\frac{gy_1}{a} - \frac{gx_1}{b}\right].$$

$$-\left[\frac{-gy_1}{a} - \frac{gx_1}{b}\right] - 1 \le N \le -\left[\frac{-gy_1}{a} - \frac{gx_1}{b}\right]$$

ie) $$-\left[\frac{-g}{ab}(by_1 + ax_1)\right] - 1 \le N \le -\left[\frac{-g}{ab}(by_1 + ax_1)\right]$$

ie) $$-\left[\frac{-gc}{ab}\right] - 1 \le N \le -\left[\frac{-gc}{ab}\right].$$

This shows that the eqn has atleast one positive integer solution if $gc > ab$.

1) Find the +ve integer solutions of $5x+3y=52$.

soln: $a=5$ $b=3$ $c=52$

$(a,b)=1$

Also, $1 | 52$.

$\therefore 5x+3y=52$ has a solution.

Let x_0, y_0 be the solution of $5x+3y=1$.

$x_0 = -1$ $y_0 = 2$

$x_1 = \frac{c}{g} x_0$ $y_1 = \frac{c}{g} y_0$

$y_1 = (52)(2) = 104.$

$x_1 = -52$

$\therefore$ The other solutions are

$x = -52 + 3t$ $y = 104 - 5t$ — (1).

$52 > 15$

$\therefore$ There is atleast one positive solution.

$x > 0$, $y > 0$.

$-52+3t>0$ $\qquad$ $104-5t>0$

$3t>52$ $\qquad$ $5t<104$

$t>\frac{52}{3}$ $\qquad$ $t<\frac{104}{5}$

$t>17.3$ $\qquad$ $t<20.8$

$\therefore 17.3<t<20.8$

$\therefore t=18, 19, 20$

$① \Rightarrow x=-52+3(18)=2$

$y=104-5(18)=14$

$x=-52+3(19)=5$

$y=104-5(19)=9$

$x=-52+3(20)=8$

$y=104-5(20)=4.$

$\therefore$ The solutions are $(2,14), (5,9), (8,4)$

2) Find all +ve integers solns of $97x+98y=1000$

Soln: $a=97$ $\quad b=98$ $\quad c=1000$

$(97,98)=1$

$1 \mid 1000.$

$\therefore 97x+98y=1000$ has soln.

Let x_0, y_0 be the soln of $97x+98y=1$

$x_0=-1$ $\quad y_0=1$

$x_1 = \frac{c}{g} x_0 \qquad y_1 = \frac{c}{g} y_0.$

$x_1 = -1000 \qquad y_1 = 1000$

The other solns are

$x = -1000 + 98t \qquad y = 1000 - 97t$

$x > 0 \qquad y > 0.$

$-1000 + 98t > 0 \qquad 1000 - 97t > 0.$

$98t > 1000 \qquad t < \frac{1000}{97}$

$t > \frac{1000}{98} \qquad t < 10.3$

$t > 10.2$

$10.2 < t < 10.3$

$\therefore$ This is impossible.

$\therefore$ The given eqn has no solution.

3) $12x + 501y = 274$

Soln: $a = 12 \quad b = 501 \quad c = 274$

$(12, 501) = 3$

$3 \nmid 274.$

$\therefore$ The given eqn has no solution.

4) ~~97+9~~ $15x + 7y = 111$

$a = 15 \quad b = 7 \quad c = 111$

$(15, 7) = 1$

$1 \mid 111$

$\therefore 15x + 7y = 111$ has solution.

Let x_0, y_0 be the soln of $15x + 7y = 1$

$x_0 = 1 \quad y_0 = -2$

$x_1 = \frac{c}{g} x_0 \qquad y_1 = \frac{c}{g} y_0$

$x_1 = 111 \qquad y_1 = -222$

The other solutions are

$x = 111 + 7t \qquad y = -222 - 15t$ — (1)

$x > 0 \qquad y > 0.$

$111 + 7t > 0. \qquad -222 - 15t > 0$

$7t > -111 \qquad -222 > 15t$

$t > \frac{-111}{7} \qquad \frac{-222}{15} > t$

$t > -15.85 \qquad t < -14.8$

$-15.85 < t < -14.8$

$\therefore t = -15,$

(1) $\Rightarrow$ $x = 111 + 7(-15) \qquad y = -222 - 15(-15)$

$x = 6 \qquad y = 3.$

The solutions are $(6, 3)$

5) $12x + 501y = 531$

$a = 12 \quad b = 501 \quad c = 531$

$(12, 501) = 3$

$3 \mid 531$

$\therefore 12x + 501y = 531$ has a soln.

Let x_0, y_0 be the soln of $12x + 501y = 3$.

$x_0 = 42 \qquad y_0 = -1$

$x_1 = \frac{531}{3}(42) \qquad y_1 = \frac{531}{3}(-1)$.

$x_1 = 7434 \qquad y_1 = -177$.

The other solutions are

$x = 7434 + \frac{501}{3}t \qquad y = -177 - \frac{12}{3}t$

$y = -177 - 4t$

$x = 7434 + 167t$

$x > 0, y > 0$.

$7434 + 167t > 0 \qquad -177 - 4t > 0$.

$-177 > 4t$

$167t > -7434 \qquad t < \frac{-177}{4}$.

$t > -\frac{7434}{167} \qquad t < -44.25$.

$t > -44.51$

$-44.51 < t < -44.25$.

There is no integer in this range

$gc > ab \Rightarrow 3(531) > 12(501)$

$\Rightarrow 1593 \not> 6012$

$\therefore$ This equation has no positive integer solution.

General method of other linear equations

Consider the equation

$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ — (1) where $k > 2$

Let $g = (a_1, a_2, \cdots, a_k)$

If the eqn (1) has ~~a linear~~ integer solution then $g | c$

Conversely,

Suppose $g | c$

Then $c = gr$ for some integer r

Now, $(a_1, a_2, \cdots, a_k) = g \Rightarrow \exists$ an integer $y_1, y_2, \cdots, y_k$ s.t $a_1y_1 + a_2y_2 + \cdots + a_ky_k = g$

$$a_1 \cdot ry_1 + a_2 \cdot ry_2 + \cdots + a_k \cdot ry_k = g \cdot r = c$$

Clearly,

$x_1 = ry_1 \quad x_2 = ry_2 \cdots x_k = ry_k$ is a solution of (1).

Thus, eqn (1) has integer solution iff $g | c$

To find the solutions

To solve this eqn by reducing the variable

put $x_{k-1} = \alpha u + \beta v$ — (2)

$x_k = \gamma u + \delta v$ — (3)

where $\alpha, \beta, \gamma, \delta$ are integers s.t $\alpha\delta - \beta\gamma = 1$

$$\alpha\delta u + \beta\delta v = \delta x_{k-1}$$
$$\beta\gamma u + \beta\delta v = \beta x_k$$
$$(\alpha\delta - \beta\gamma) u = \delta x_{k-1} - \beta x_k$$

$$\delta x_{k-1} - \beta x_k = 1 \cdot u, \quad \boxed{\alpha\delta - \beta\gamma = 1}$$

put this in (1),

$$x_{k-1} = \alpha(\delta x_{k-1} - \beta \cdot x_k) + \beta v$$
$$x_{k-1} - \alpha\delta x_{k-1} + \alpha\beta x_k = \beta v$$
$$v = \frac{x_{k-1}(1-\alpha\delta) + \alpha\beta x_k}{\beta}$$
$$v = \frac{x_{k-1}(1-\alpha\delta)}{\beta} + \alpha x_k.$$
$$= \frac{x_{k-1}(-\beta\gamma)}{\beta} + \alpha x_k \quad (\because \alpha\delta - \beta\gamma = 1)$$
$$v = \alpha x_k - \gamma x_{k-1}$$

This shows that u & v are integers iff x_k, x_{k-1} are integers

Take $\beta = \dfrac{a_k}{(a_{k-1}, a_k)}$ & $\delta = \dfrac{-a_{k-1}}{(a_{k-1}, a_k)}$

$$(\beta, \delta) = \left(\frac{a_k}{(a_{k-1}, a_k)}, \frac{-a_{k-1}}{(a_{k-1}, a_k)} \right)$$
$$= \frac{1}{(a_{k-1}, a_k)} (a_k, -a_{k-1})$$
$$(\beta, \delta) = 1$$

The eqn $\alpha\delta - \beta\gamma = 1$ has integer soln.

Now,

① $\Rightarrow a_1x_1 + a_2x_2 + \dots + x_{k-1}(-\delta(a_{k-1}, a_k)) + x_k(\beta(a_{k-1}, a_k))$
$= c_1$

$a_1x_1 + a_2x_2 + \dots + a_{k-2}x_{k-2} - \delta(a_{k-1}, a_k)(\alpha u + \beta v)$
$+ \beta(a_{k-1}, a_k)(\gamma u + \delta v) = c$

$a_1x_1 + a_2x_2 + \dots + a_{k-2}x_{k-2} - (a_{k-1}, a_k)(\delta(\alpha u + \beta v) + \beta(\gamma u + \delta v))$
$= c$

$a_1x_1 + a_2x_2 + \dots + a_{k-2}x_{k-2} - (a_{k-1}, a_k)(\alpha\delta u + \beta\delta v - \beta\gamma u - \beta\delta v) = c_1$

$a_1x_1 + a_2x_2 + \dots + a_{k-2}x_{k-2} - (a_{k-1}, a_k)(u(\alpha\delta - \beta\gamma)) = c_1$

$a_1x_1 + a_2x_2 + \dots + a_{k-2}x_{k-2} - (a_{k-1}, a_k)\cdot u = c_1$ — ④

This is a eqn with one less than k unknowns ie) k-1 unknowns

Now, $(a_1, a_2, \dots a_{k-2}, (a_{k-1}, a_k))$
$= (a_1, a_2, \dots a_{k-2}, a_{k-1}, a_k) = g.$

This shows that eqn ④ has the same properties as eqn ① that the coefficients are not zero and the g.c.d of the coefficients divides c.

If $k = 3$ eqn ④ has 2 unknowns and can be solved by the method of solving linear eqn in two unknowns

If $k > 3$, the process can be repeated to reduce the eqn with $k-2$ unknowns

Repeating the above process finally the given equations reduces to an eqn with two unknown.

Pb 1) $5x-2y-4z=10$

Here $a=5$ $b=-2$ $c=-4$

$(a,b,c) = (5,-2,-4) = 1 = g$

clearly, $1 | 10$.

The equation has soln

put $y = \alpha u + \beta v$

$z = \gamma u + \delta v$ — (1)

where $\alpha, \beta, \gamma, \delta$ are integers s.t $\alpha\delta - \beta\gamma = 1$ — (2).

W.K.T. $\beta = \frac{a_k}{(a_{k-1}, a_k)}$ $\delta = \frac{-a_{k-1}}{(a_{k-1}, a_k)}$

Here $(a_{k-1}, a_k) = (-2,-4) = 2$

$\beta = \frac{-4}{2} = -2$ $\delta = -\frac{(-2)}{2} = \frac{2}{2} = 1$

$\alpha\delta - \beta\gamma = 1 \Rightarrow \alpha + 2\gamma = 1$ (by (2))

Now $(1,2) = 1$

It has soln.

$1 + 2(0) = 1$

$\Rightarrow \alpha = 1$ $\gamma = 0$.

(1) $\Rightarrow y = u - 2v$

$z = v$

$5x - 2y - 4z = 10$

$5x - 2(u-2v) - 4v = 10$

$5x - 2u + 4v - 4v = 10$

$5x - 2u = 10$

$\cancel{5x = 10 + 2u}$

$(5, -2) = 1$ & $1 | 10$

Here $a = 5$ $b = -2$

$5 = (-2)(-2) + 1$

$\Rightarrow 1 = 5 - (-2 \times -2)$

$\Rightarrow 1 = 1(5) - 2(2)$

$\Rightarrow 10 = 5(10) - 2(20)$

$x_0 = 10$ $u_0 = 20$

$x' = x_0 + \frac{b}{g} t$ $u' = u_0 + \frac{a}{g} t$

$x' = 10 + (-2t)$ $u' = 20 - 5t$ $10 > 2t$, $t < 5$

$x' = 10 - 2t$ $u' = 20 - 5t$ $20 > 5t$, $t < 4$.

$x' > 0$ $u' > 0$

$10 - 2t > 0$ & $20 - 5t > 0$

t has no integer soln.

$\therefore x = 10 - 2t$ $u = 20 - 5t$

$y = 20 - 5t - 2v$

$z = v$.

b: 2) $5x-2y-4z=1$

Here $a=5 \quad b=-2 \quad c=-4$.

G.c.d of $(5,-2,-4) = (5,-2)(-4) = 1$

$\therefore 1 | 1$.

$\therefore$ The eqn is solvable

put $y = \alpha u + \beta v \quad z = \gamma u + \delta v$ — (1)

where $\alpha, \beta, \gamma, \delta$ are integers s.t

$\alpha\delta - \beta\gamma = 1$ — (2).

W.K.T $\beta = \dfrac{a_k}{(a_{k-1}, a_k)} \qquad \delta = \dfrac{-a_{k-1}}{(a_{k-1}, a_k)}$

Here $(a_{k-1}, a_k) = (-2, -4) = 2$

$\beta = \dfrac{-4}{2} = -2 \qquad \delta = \dfrac{-(-2)}{2} = 1$

$\therefore \alpha + 2\gamma = 1$ (by (1))

$-1 + 2(1) = 1$

$\Rightarrow \alpha = -1 \qquad \gamma = 1$

(1) $\Rightarrow y = -u - 2v$

$z = u + v$

$5x - 2y - 4z = 1$

$5x - 2(-u-2v) - 4(u+v) = 1$

$5x + 2u + 4v - 4u - 4v = 1$

$5x - 2u = 1$

$(5, -2) = 1$

Here $a=5 \quad b=-2$.

$5 = (-2)(-2) + 1$

$1 = 5 + (-2 \times -2)$

$1 = 1(5) - 2(2)$

~~$10 = 5(10) - 2(20)$~~

$x_0 = 1 \quad u_0 = 2.$

$x' = x_0 + \frac{b}{g} t \qquad u' = u_0 - \frac{a}{g} t$

$x' = 1 - 2t \qquad u' = 2 - 5t.$

$x' > 0 \qquad u' > 0.$

$\therefore$ t has no integer soln.

$\therefore x = 1 - 2t \qquad u = 2 - 5t$

$x = 1 - 2t$
$y = -2 + 5t - 2v$
$z = 2 - 5t + v$

Pb:3) $x + 2y + 5z = 10.$

Here $a = 1, \quad b = 2 \quad c = 5$

$(a, b, c) = (1, 2, 5) = 1 = g$

Clearly $1 / 10.$

$\therefore$ The eqn is solvable

put $y = \alpha u + \beta v$ and $z = \gamma u + \delta v$ — (1)

where $\alpha, \beta, \gamma, \delta$ are integers s.t $\alpha\delta - \beta\gamma = 1$ — (2)

W.K.T, $\beta = \frac{a_k}{(a_{k-1}, a_k)} \qquad \delta = \frac{-a_{k-1}}{(a_{k-1}, a_k)}$

$(a_{k-1}, a_k) = (2,5) = 1$

$\beta = \frac{5}{1} = 5 \quad \delta = \frac{-2}{1} = -2$

(2) $\Rightarrow x(-2) - 5(\gamma) = 1$

$\Rightarrow 2x + 5\gamma = -1$

$2(2) + 5(-1) = 4 - 5 = -1$

$x = 2 \quad \gamma = -1$

(1) $\Rightarrow y = 2u + 5v$ and $z = -u - 2v$

$x + 2(2u + 5v) + 5(-u - 2v) = 10.$

$x + 4u + 10\cancel{v} - 5u - 10\cancel{v} = 10.$

$x - u = 10 \Rightarrow 1(x) + (-1)u = 10.$

$(1, -1) = 1$

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

$10 = 1(-10) - 1(-20)$

$10 = -10 + 20.$

$\therefore 1(-10) - 1(-20) = 10.$

$x_0 = -10 \quad u_0 = -20.$

$x' = x_0 + \frac{b}{g} t \qquad u' = u_0 - \frac{a}{g} t$

$x' = -10 + 2t \qquad u' = -20 - t$

$x' > 0 \quad \& \quad u' > 0$

$-20 - t > 0$

$-10 + 2t > 0$

$-t > 20$

$-10 > -2t$

$-5 > -t$

$20 < -t < -5 \Rightarrow -20 \gtrless t \gtrless 5$

$x = 10 + u$

$y = 2u + 5v$

$z = -u - 2v$

pb:4) $x + 2y + 3z = 1$

Here $a = 1$ $b = 2$ $c = 3$

$(a, b, c) = (1, 2, 3) = 1 = g$

clearly $1 | 1$

The eqn is solvable

put $y = \alpha u + \beta v$ $z = \gamma u + \delta v$ — (1)

where $\alpha, \beta, \gamma, \delta$ are integers s.t $\alpha\delta - \beta\gamma = 1$ — (2)

W.K.T $\beta = \frac{a_k}{(a_{k-1}, a_k)}$ $\delta = \frac{-a_{k-1}}{(a_{k-1}, a_k)}$

$(a_{k-1}, a_k) = (2, 3) = 1$

$\beta = \frac{3}{1} = 3$ $\delta = \frac{-2}{1} = -2$

(2) $\Rightarrow$ $-2\alpha - 3\gamma = 1 \Rightarrow 2\alpha + 3\gamma = 1$

$2(1) + 3(-1) = 2 - 3 = -1$

$\therefore \alpha = +1$ $\gamma = -1$

(1) $\Rightarrow$ $y = u + 3v$ $z = -u - 2v$

$x + 2(u + 3v) + 3(-u - 2v) = 1$

$x + 2u + 6v - 3u - 6v = 1$

$x - u = 1$

$1 = 1(2) - 1(1)$

$\therefore x_0 = 2 \quad u_0 = 1.$

$x' = x_0 + \frac{b}{g} t \qquad u' = u_0 - \frac{a}{g} t$

$x' = 2 + 2t \qquad u' = 1 - t$

$x' > 0 \qquad u' > 0$

$2 + 2t > 0 \qquad 1 - t > 0$

$2t > -2 \qquad 1 > t \Rightarrow t > -1$

$-1 < t < 1$

$x = 1 + u$

$y = u + 3v$

$z = -u - 2v$

6:5) $3x - 6y + 5z = 11$

Here $a = 3 \quad b = -6 \quad c = 5$

$(a, b, c) = (3, -6, 5) = 1 = g$

clearly $1 | 11$

The eqn ~~has~~ is solvable.

put $y = \alpha u + \beta v \quad z = \gamma u + \delta v$ — (1).

where $\alpha, \beta, \gamma, \delta$ are integers $\alpha\delta - \beta\gamma = 1$ — (2).

w.k.T $\beta = \frac{a_k}{(a_{k+1}, a_k)} \qquad \delta = -\frac{a_{k+1}}{(a_{k+1}, a_k)}$

$(a_{k+1}, a_k) = (-6, 5) = 1$

$\beta = 5 \qquad \delta = 6$

(2) $\Rightarrow 6\alpha - 5\gamma = 1$

$6(1) - 5(1) = 6 - 5 = 1.$

$\alpha = 1 \qquad \gamma = 1$

$y = u + 5v \qquad z = u + 6v$

$3x - 6(u+5v) + 5(u+6v) = 11$

$3x - 6u - \cancel{30v} + 5u + \cancel{30v} = 11$

$(3, -1) = 1$

$3(3) - 1(-2) = 11$

$x_0 = 3 \qquad u_0 = -2$

$x' = x_0 + \frac{b}{g} t \qquad u' = u_0 - \frac{a}{g} t$

$x' = 3 - 6t \qquad u' = -2 - 3t$

$x' > 0 \qquad u' > 0$

$3 - 6t > 0 \qquad -2 - 3t > 0$

$3 > 6t \qquad -3t > 2$

$\frac{1}{2} > t \qquad t > -\frac{2}{3}$

$-\frac{2}{3} < t < \frac{1}{2}$

(1) (2) — t has no positive integer soln.

$\therefore x = 3 - 6t \qquad u = -2 - 3t$

$y = -2 - 3t + 5v$

$z = -2 - 3t + 6v$

UNIT-II

The equation $x^2+y^2=z^2$

Suppose $(x,y)=g$ then $g^2|x^2$ and $g^2|y^2$

$\Rightarrow g^2|x^2+y^2 \Rightarrow g^2|z^2$

$\Rightarrow g|z$

$(x,y,z)=g=((x,y),z)$

By symmetry,

$(x,z)=(z,y)=(x,y)=(x,y,z)=g$

$\therefore \frac{x^2}{g^2}+\frac{y^2}{g^2}=\frac{z^2}{g^2}$ where $\left(\frac{x}{g},\frac{y}{g}\right)=\left(\frac{y}{g},\frac{z}{g}\right)$

$=\left(\frac{x}{g},\frac{z}{g}\right)=1$

If x_1, y_1, z_1 is such a way is called primitive solution.

Defn: A soln x,y,z of the equation $x^2+y^2=z^2$ such that these three are relatively prime in pairs is called primitive solution.

Theorem:

A primitive soln of the eqn $x^2+y^2=z^2$ with y is even is of the form $x=r^2-s^2$, $y=2rs$ $z=r^2+s^2$ where $r>s>0$ & $(r,s)=1$, r and s are integers and of opposite parity.

Proof: Let x, y, z be a primitive soln of $x^2+y^2=z^2$

Then x & y are not both even.

Also, x & y are not both odd.

For, if both x & y are odd.

Then $x^2 \equiv 1 \pmod 4$ & $y^2 \equiv 1 \pmod 4$

$$x^2+y^2 \equiv 2 \pmod 4$$

$$z^2 \equiv 2 \pmod 4$$

This is impossible. ($\because$ a square is congruent to either 1 (or) 0 mod 4)

$\therefore x$ & y are not both odd

we assume that y is even, then x is odd

Consequently z is odd.

$$\cancel{z^2 = x^2}$$

$$z^2 - x^2 = y^2$$

$$(z+x)(z-x) = y^2$$

$\therefore z, x$ are odd

$\Rightarrow z+x, z-x$ is even

$\therefore \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = \left(\frac{y}{2}\right)^2$ where $\frac{z+x}{2}, \frac{z-x}{2}$, $\frac{y}{2}$ are integers

$\rightarrow$ (1)

claim: $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$

clearly, $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| \frac{z+x}{2} + \frac{z-x}{2} = z$.

$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| \frac{z+x}{2} - \frac{z-x}{2} = x$.

$\Rightarrow \left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| z$ & $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| x$.

$\Rightarrow \left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| (z, x) = 1$

$\Rightarrow \left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$ $(\because (z, x) = 1)$

Since $\frac{z+x}{2} \times \frac{z-x}{2}$ is a square, $\exists$ integer r & s s.t $\frac{z+x}{2} = r^2$, $\frac{z-x}{2} = s^2$ — (*)

Also, $\frac{z+x}{2} > \frac{z-x}{2}$

$\Rightarrow r^2 > s^2$

$\Rightarrow r > s > 0$.

from (*), $z = r^2 + s^2$

$x = r^2 - s^2$

(1) $\Rightarrow r^2 s^2 = \left(\frac{y}{2}\right)^2$

$y^2 = 4r^2 s^2$

$\boxed{y = 2rs}$

Since $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1 \Rightarrow (r^2, s^2) = 1$

$\Rightarrow (r, s) = 1$

Since x is odd, r^2+s^2 is odd

$\therefore$ r and s are of opposite parity

(ie) neither r (or) s is odd)

Conversely, Suppose r & s are any two integers s.t $(r,s)=1$, $r>s>0$, r & s are of opposite parity.

<u>To prove:</u> $x^2+y^2=z^2$

Given $x=r^2-s^2$ $y=2rs$

$$(r^2-s^2)^2+(2rs)^2 = r^4-2r^2s^2+s^4+4r^2s^2$$

$$= r^4+2r^2s^2+s^4$$

$$= (r^2+s^2)^2$$

$$x^2+y^2=z^2$$

<u>To prove:</u> x, y, z are primitive

Let $(z, x)=g$

Since z & x are odd, g is odd

Also $g \mid z+x$, $g \mid z-x$

$\Rightarrow g \mid 2r^2$ & $g \mid 2s^2$

$\Rightarrow g \mid r^2$ & $g \mid s^2$

$(r^2, s^2)=g$

But $(r^2, s^2)=1$

$\therefore g = 1 \Rightarrow (z, x) = 1$

By Symmetry,

$(z, x) = (x, y) = (y, z) = (x, y, z) = 1$

<u>Defn</u>: The positive integer soln of $x^2 + y^2 = z^2$ are called pythagorean triples.

<u>Problem</u>:

Q1) Find the pythagorean triples forming

a) an arithmetic progression

b) a Geometric progression.

All positive integer solution of $x^2 + y^2 = z^2$ are +ve multiple of +ve primitive soln.

A +ve primitive soln of $x^2 + y^2 = z^2$ are of the form

$x = r^2 - s^2 \quad y = 2rs \quad z = r^2 + s^2$ where $(r, s) > 0$.

$(r, s) = 1$ & r, s are of opposite parity.

If x, y, z form an A.p then

$x = a - d \quad y = a \quad z = a + d$.

clearly $y = \frac{z + x}{2}$

ie) $2rs = \frac{2r^2}{2} \Rightarrow 2s = r$.

$$\boxed{r = 2s}$$

$x = (2s)^2 - s^2 = 3s^2$

$y = 2(2s)s = 4s^2$

$z = (2s)^2 + s^2 = 5s^2$

$x = 3s^2 \quad y = 4s^2 \quad z = 5s^2$ which is a pythagorean triples forming A.P.

Now, we claim that no pythagorean triples form an G.P.

For W.K.T the pythagorean triples are of the form ~~x, y~~ $x_1 g, y_1 g, z_1 g$ where x_1, y_1, z_1 are primitive soln & g is +ve integer.

clearly, $x_1 g, y_1 g, z_1 g$ are in G.P iff x_1, y_1, z_1 are in G.P.

A primitive soln are in G.P iff $r^2 - s^2, 2rs, r^2 + s^2$ where r and s of opposite parity $r > s > 0$ with $(r, s) = 1$ are in G.P

$$\frac{2rs}{r^2 - s^2} = \frac{r^2 + s^2}{2rs} \Rightarrow \underset{\text{even}}{4r^2 s^2} = \underset{\text{odd}}{(r^2 + s^2)} \underset{\text{odd}}{(r^2 - s^2)}$$

This is impossible

$\therefore r^2-s^2, 2rs, r^2+s^2$ are not in G.P.

$\Rightarrow$ No pythagorean triple is an G.P.

Pb:) If $x^2+y^2=z^2$. P.T one of x, y is a multiple of 3 and one of x, y, z is a multiple of 5

Soln: It is enough to consider the positive primitive solution of $x^2+y^2=z^2$.

Any positive primitive soln of $x^2+y^2=z^2$ when y is even given by $x=r^2-s^2$, $y=2rs$, $z=r^2+s^2$, where r and s are integers of opposite parity $r>s>0$ and $(r,s)=1$.

Let y is a multiple of 3.

A part of the proof is over

Suppose y is not a multiple of 3.

$\therefore 3\nmid r$ and $3\nmid s$

$\therefore r \equiv 1, 2 \pmod 3$ $\quad s \equiv 1, 2 \pmod 3$.

$r^2 \equiv 1 \pmod 3$ $\quad s^2 \equiv 1 \pmod 3$

$\Rightarrow r^2-s^2 \equiv 0 \pmod 3$

$\Rightarrow x \equiv 0 \pmod 3$

$\therefore x$ is a multiple of 3.

Let y is a multiple of 5 then the next part of the proof is over.

Suppose y is not a multiple of 5

$\therefore 5 \nmid r$ and $5 / s$.

$r \equiv 1,2,3,4 \pmod 5$ $\quad s \equiv 1,2,3,4 \pmod 5$

$r^2 \equiv 1,4 \pmod 5$ $\quad s^2 \equiv 1,4 \pmod 5$

<u>Case (i)</u> $r^2 \equiv 1 \pmod 5$ $\quad s^2 \equiv 1 \pmod 5$

$\Rightarrow r^2 - s^2 \equiv 0 \pmod 5$.

$\Rightarrow x \equiv 0 \pmod 5$

x is a multiple of 5

<u>Case (ii)</u> $r^2 \equiv 4 \pmod 5$ $\quad s^2 \equiv 1 \pmod 5$

$r^2 + s^2 \equiv 0 \pmod 5$

$\Rightarrow z \equiv 0 \pmod 5$.

z is a multiple of 5

<u>Case (iii)</u>

$r^2 \equiv 1 \pmod 5$ $\quad s^2 \equiv 4 \pmod 5$

$r^2 + s^2 \equiv 0 \pmod 5$

$\Rightarrow z \equiv 0 \pmod 5$

z is a multiple of 5

<u>Case (iv)</u>

$r^2 \equiv 4 \pmod 5$ $\quad s^2 \equiv 4 \pmod 5$

$r^2 - s^2 \equiv 0 \pmod 5$

$x \equiv 0 \pmod 5$

x is a multiple of 5

From all, we conclude one of the multiple of x, y, z is 5.

Pb For which integer n are there solution of $x^2-y^2=n$

Soln:

Case (i) x and y are both even

Then $x^2 \equiv 0 \pmod 4$ $y^2 \equiv 0 \pmod 4$

$\therefore x^2-y^2 \equiv 0 \pmod 4$

$n \equiv 0 \pmod 4$

Case (ii) x & y are both odd

Then $x^2 \equiv 1 \pmod 4$ $y^2 \equiv 1 \pmod 4$

$x^2-y^2 \equiv 0 \pmod 4$

$n \equiv 0 \pmod 4$

Case (iii) x is odd and y is even

Then $x^2 \equiv 1 \pmod 4$ $y^2 \equiv 0 \pmod 4$

$x^2-y^2 \equiv 1 \pmod 4$

$n \equiv 1 \pmod 4$

Case (iv) x is even and y is odd

$x^2 \equiv 0 \pmod 4$ $y^2 \equiv 1 \pmod 4$

$x^2-y^2 \equiv -1 \pmod 4$

$n \equiv -1 \pmod 4$

$n \equiv 3 \pmod 4$

$n \equiv 0, 1, 3 \pmod 3$

Pb: Find all positive primitive solutions of $x^2+y^2=z^2$ with $0<z<30$.

Soln: The positive primitive solutions are $x=r^2-s^2$, $y=2rs$ $z=r^2+s^2$ with

with $0 < r^2+s^2 < 30$, $r > s > 0$, r & s are opposite parity $(r,s)=1$

i) when $s=1$ $r=2$

Then $x = 2^2 - 1^2 = 3$

$y = 4$

$z = 5$

ii) when $s=1$ $r=4$

Then $x = 4^2 - 1^2 = 15$

$y = 2(1)(4) = 8$

$z = 4^2 + 1^2 = 17$

iii) when $s=2$ $r=3$

Then $x = 3^2 - 2^2 = 5$

$y = 12$

$z = 3^2 + 2^2 = 13$

iv) when $s=2$ $r=5$

Then $x = 5^2 - 2^2 = 21$

$y = 2(2)(5) = 20.$

$z = 5^2 + 2^2 = 29$

v) when $s=3$ $r=4$

Then $x = 4^2 - 3^2 = 7$

$y = 2(4)(3) = 24$

$z = 4^2 + 3^2 = 25$

Prove that if x, y, z is a +ve primitive solutions of $x^2+y^2=z^2$ then xyz is a multiple of 60.

proof: The +ve primitive soln of $x^2+y^2=z^2$ is given by $x=r^2-s^2$, $y=2rs$, $z=r^2+s^2$ where r & s are integers of opposite parity and $(r,s)=1$ with $r>s>0$

Since r and s are of opposite parity either r is even or s is even.

$\therefore 2rs$ is a multiple of 4

$\therefore y$ is a multiple of 4, if y is even

$\therefore 4 \mid xyz$ — (1) if x, y, z, is a primitive solution.

Also, we have proved that one of x, y is a multiple of 3

$\Rightarrow 3 \mid xyz$ — (2).

Again one of x, y, z is a multiple of 5

$\therefore 5 \mid xyz$ — (3)

$\therefore 3, 4, 5$ are relatively prime in pairs

$3 \times 4 \times 5 \mid xyz$

ie) $60 \mid xyz$

Hence the proof.

pb: Prove that +ve integer n can be expressed as $n = x^2+y^2-z^2$

soln: Case (i) n is even

put $x=1$ $y=\frac{n}{2}$ $z=\frac{n}{2}-1$

$$x^2+y^2-z^2 = 1+\frac{n^2}{4}-\frac{n^2}{4}+n-1 = n$$

Case (ii) n is odd

Then $n+1$ is even.

put $x=0$ $y=\frac{n+1}{2}$ $z=\frac{n+1}{2}-1$

$$x^2+y^2-z^2 = 0+\left(\frac{n+1}{2}\right)^2-\left(\frac{n+1}{2}-1\right)^2 = n.$$

There is no integer solution except the trivial solution

pb: If n is any integer ≥ 3, then P.T there is atleast one pythagorean triple which contains n as one of its number.

proof: Case (i) n is odd

then n^2 is odd.

Let $n^2 = 2k-1$ $k \geq 5$ (since $n \geq 3$)

Consider the triple $n, k-1, k$

Clearly, $n^2+(k-1)^2 = 2k-1+(k^2-2k+1)$

$= k^2$.

This shows that $n, k-1, k$ is a pythagorean triple

Case (ii) n is even

Sub case (i) $n \equiv 0 \pmod 4$

W.K.T any positive primitive solution with y is even is given by $x = r^2 - s^2$ $y = 2rs$ $z = r^2 + s^2$ where r & s are integer of opposite parity with $(r, s) = 1$ & $r > s > 0$

Fixing $s = 1$ and ranging r over all positive even integers we have y varies over all the multiples of 4.

This shows that every $n \equiv 0 \pmod 4$ is one of the memebers of a pythagorean triple.

Sub case (ii) $n \equiv 2 \pmod 4$

Then $n = 2m$ where m is odd

By Case (i), there is a pythagorean triple which contains m as one of its member say $m, k-1, k$ where $m^2 = 2k-1$

Then $2m, 2(k-1), 2k$ is also a pythagorean triple

(ie) $n, 2(k-1), 2k$ is a pythagorean triple.

Thus in all cases, we have n is a member of a pythagorean triple.

Pb Prove that the solution of the equation $x^2+2y^2=z^2$ with $(x,y,z)=1$ are of the form $x=|u^2-2v^2|$, $y=2uv$, $z=u^2+2v^2$ where n is odd and $(u,v)=1$

proof: First we claim that y is even

For, if y is odd say $y=2k+1$

then $y^2=4k^2+4k+1$

$$2y^2 = 8k^2+8k+2$$

$$2y^2 \equiv 2 \pmod 8$$

$$z^2-x^2 \equiv 2 \pmod 8$$

This is impossible

$z^2 \equiv 0,1,4 \pmod 8$ & $x^2 \equiv 0,1,4 \pmod 8$

$$z^2-x^2 \equiv 0,1,4 \pmod 8$$

$\therefore y$ is even

$(x,y,z)=1$, x & z are odd

For ~~Suppose~~ x & z are even

$\Rightarrow\Leftarrow$ to $(x,y,z)=1$

Also $(x,z)=1$

For if $(x,z)=g$, then g is odd and

$$g \mid z^2-x^2 = 2y^2$$

$$\Rightarrow g \mid y$$

$\therefore g$ is a common divisor of x,y,z

But $(x,y,z)=1$

ie) $(x,z)=1$

Now, $z^2-x^2=2y^2 \Rightarrow (z+x)(z-x)=2y^2$

ie) $\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)=2\left(\frac{y}{2}\right)^2$ —— (1)

$$\left(\frac{z+x}{2},\frac{z-x}{2}\right) \Big| \frac{z+x}{2}+\frac{z-x}{2}=z$$

$$\& \left(\frac{z+x}{2},\frac{z-x}{2}\right) \Big| \frac{z+x}{2}-\frac{z-x}{2}=x$$

But $(x,z)=1$

$$\therefore \left(\frac{z+x}{2},\frac{z-x}{2}\right)=1$$

Also one of $\frac{z+x}{2}$ & $\frac{z-x}{2}$ is odd and the other is even.

Suppose $\frac{z-x}{2}$ is even

Then $\frac{z-x}{2} = 2t$ where t is a +ve integer

Also, $\left(\frac{z+x}{2}, 2t\right) = 1$

and $\frac{z+x}{2} \times t = \left(\frac{y}{2}\right)^2$ (by (1))

Let $\frac{z+x}{2} = u^2$ & $t = v^2$ where $(u, v) = 1$

$\because \frac{z+x}{2}$ is odd then u is odd

we have $\frac{z+x}{2} = u^2$ and $\frac{z-x}{2} = 2v^2$

$\therefore x = u^2 - 2v^2$ and $z = u^2 + 2v^2$

$$\left(\frac{y}{2}\right)^2 = u^2 v^2$$

$$y = 2uv$$

If $\left(\frac{z+x}{2}\right)$ is even and $\left(\frac{z-x}{2}\right)$ is odd

then $\frac{z+x}{2} = 2v^2$ & $\frac{z-x}{2} = u^2$

$\Rightarrow x = 2v^2 - u^2$, $y = 2uv$ $z = u^2 + 2v^2$

$\therefore x = |u^2 - 2v^2|$ $y = 2uv$ $z = u^2 + 2v^2$

where u is odd and $(u, v) = 1$

is a solution of $x^2 + 2y^2 = z^2$ with $(x, y, z) = 1$

Conversely, suppose $x = |u^2 - 2v^2|$

$y = 2uv$ $z = \cancel{v^2}\, u^2 + 2v^2$

Then $x^2+2y^2 = (u^2-2v^2)^2 + 2(4u^2v^2)$

$$= (u^2-2v^2)^2 + 8u^2v^2$$

$$= u^4 - 4u^2v^2 + 4v^4 + 8u^2v^2$$

$$= u^4 + 4u^2v^2 + 4v^4$$

$$= (u^2+2v^2)^2 = z^2$$

The equation $x^4+y^4 = z^2$

The only integral solution of $x^4+y^4=z^2$ are the trivial solutions $x=0$; y; $z=\pm y^2$ and x; $y=0$; $z=\pm x^2$

proof: Suppose that the eqn $x^4+y^4=z^2$ has atleast one positive solution

Consider the +ve solution x, y, z s.t no other ~~be~~ +ve solution has a smaller value of z.

First claim that $(x, y, z) = 1$

Suppose $\exists$ a prime p s.t $(x, y, z) = p$

$\Rightarrow p \mid x$ & $p \mid y$

$\Rightarrow p^4 \mid x^4$ & $p^4 \mid y^4$

$\Rightarrow p^4 \mid x^4+y^4 \Rightarrow p^4 \mid z^2$

$$\frac{x^4}{p^4} + \frac{y^4}{p^4} = \frac{z^2}{p^4} \Rightarrow \left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$$

$\therefore \cancel{\left(\frac{x}{p}\right), y}$

$\therefore \frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}$ is a solution of

$x^4+y^4=z^2$

which is a contradiction $\left(\because \left(\frac{z}{p^2} < z\right)\right)$

$\therefore (x,y,z)=1$

$\Rightarrow x,y,z$ are not all even

Now, we claim that one of x,y is odd and other is even

Suppose x & y are odd

$x^4 \equiv 1 \pmod 8$ $\quad y^4 \equiv 1 \pmod 8$

$x^4+y^4 \equiv 2 \pmod 8$

$z^2 \equiv 2 \pmod 8$

$\Rightarrow \Leftarrow$

Assume that x is even and y is odd.

$\Rightarrow z$ is odd

Now, $y^4 = z^2 - x^4$

$y^4 = (z+x^2)(z-x^2)$

$\therefore (z+x^2)$ & (z^2-x^2) are odd

Now, $y^4 = z^2 - x^4$

$y^4 = (z+x^2)(z-x^2)$

$\therefore (z+x^2)$ & $(z-x^2)$ are odd

<u>claim:</u> $(z+x^2, z-x^2) = 1$

For if $(z+x^2, z-x^2) = p \Rightarrow p \mid z+x^2$ and

$p \mid z-x^2$

$p \mid z+x^2+z-x^2$ & $p \mid z+x^2 - z+x^2$

$\Rightarrow p \mid 2z \;, \; p \mid 2x^2 \;, \; p \mid y^4$

$\Rightarrow p \mid z \;, \; p \mid x \;, \; p \mid y$

$\Rightarrow (x,y,z) = p$

put $(x,y,z) = 1 \Rightarrow \boxed{p=1}$

$\therefore (z+x^2, z-x^2) = 1$

$\therefore z+x^2$ and $z-x^2$ are fourth power of some integers

Let $z-x^2 = u^4$ — ①, $z+x^2 = v^4$ — ②

Clearly, both u & v are odd,

Also, $v^4 - u^4 = 2x^2$

$(v^2+u^2)(v^2-u^2) = 2x^2$

$\therefore u$ & v are odd $\Rightarrow u^2 \equiv 1 \pmod 4$ &

$v^2 \equiv 1 \pmod 4$

$v^2 - u^2 \equiv 0 \pmod 4$ & $v^2 + u^2 \equiv 2 \pmod 4$

$(v^2+u^2)(v^2-u^2) \equiv 0 \pmod 4$

$\therefore$ v^2-u^2 is a square &

v^2+u^2 is twice a square

Let $v^2 - u^2 = a^2$ & $v^2 + u^2 = 2b^2$

$\Rightarrow v^2 = u^2 + a^2$

A +ve primitive solution of this equation is given by

$u = r^2 - s^2$, $a = 2rs$, $v = r^2 + s^2$

with $r > s > 0$ and $(r, s) = 1$

where r & s are of opposite parity.

Now, $v^2 + u^2 = 2b^2$ — (3)

$$(r^2+s^2)^2 + (r^2-s^2)^2 = 2b^2$$

$$r^4 + s^4 + 2r^2s^2 + r^4 + s^4 - 2r^2s^2 = 2b^2$$

$$2(r^4+s^4) = 2b^2$$

$$r^4 + s^4 = b^2$$

We claim that $b < z$

(1) + (2) $\Rightarrow z = \frac{1}{2}(u^4 + v^4) > \frac{1}{2}(u^2+v^2) = b^2$ ($\because$ from (3))

$z > b^2 \Rightarrow z > b$.

$\therefore b < z$. which is a

Contradiction.

$\therefore$ Thus, we have a positive solution r, s, b of the equation $x^4+y^4=z^2$ where $b<z$, which is a contradiction

There is no integral soln except the trivial solution

<u>Defn:</u> A solution x, y of the equation $x^2+y^2=n$ is called primitive solution if $(x, y)=1$

<u>Notations:</u>

i) $N(n)$ = No. of solns of $x^2+y^2=n$.

ii) $P(n)$ = No. of non-negative primitive solution of $x^2+y^2=n$.

iii) $Q(n)$ = No. of primitive solutions $x^2+y^2=n$

iv) $R(n)$ = No. of solns of the congruence $s^2 \equiv -1 \pmod n$

v) $R(n) = p(n)$ if $n>1$

vi) $N(n) = 4 \sum_{d^2 \mid n} R(n/d^2)$.

The Equation $4x^2+y^2=n$

Let n be any integer $n>1$, $n \equiv 1 \pmod 4$.

If n is prime, the equation $4x^2+y^2=n$ has only one non-negative solution and it is primitive. If n is not prime then the equation has either no primitive solution more than one non-negative primitive solution or one non-negative primitive solution & atleast one non-negative non-primitive solution.

proof: Let $N'(n)$, $P'(n)$, $Q'(n)$ denote respectively no of solns of $4x^2+y^2=n$, the no. of non-negative primitive solns of $4x^2+y^2=n$, the no. of primitive solns of $4x^2+y^2=n$

Let $N(n)$, $P(n)$, $Q(n)$ be the usual notation connected with the eqn $x^2+y^2=n$

First we prove that

$$N'(n) = \frac{N(n)}{2}, \quad P'(n) = \frac{P(n)}{2} \quad \& \quad Q'(n) = \frac{Q(n)}{2}$$

For let x, y be solutions of $x^2+y^2=n$

Since $n \equiv 1 \pmod 4$ either x is even and y is odd or y is even & x is odd.

If x is even put $u=\frac{x}{2}$ & $v=y$.

If y is even put $u=\frac{y}{2}$ & $v=x$

then $4u^2+v^2=n$

Also, $(x,y)=(2u,v)=(u,v)$ ($\because v$ is odd)

But $x^2+y^2=y^2+x^2$ & $x \neq y$.

This shows that two solution of $x^2+y^2=n$ correspond to one solution of $4u^2+v^2=n$

$\therefore N'(n)=\frac{N(n)}{2}$, $p'(n)=\frac{p(n)}{2}$ $Q'(n)=\frac{Q(n)}{2}$.

If $n \equiv 1 \pmod 4$ is prime, then

$$N(n) = 4\sum_{d|n} h(d)$$

$$= 4\left[h(1)+h(n)\right]$$

$$= 4(1+1)$$

$N(n) = 8 \Rightarrow N'(n) = 4$

Now, $p(n) = R(n) = 2 \Rightarrow p'(n) = 1$

This shows that the equation $4x^2+y^2=n$ has exactly one non-negative primitive solution.

Since $N'(n) = 4$, there are 3 other solutions which will be obtained by changing the sign of non-negative solution.

$\therefore$ The eqn $4x^2+y^2=n$ has exactly one non-negative solution and it is primitive solution.

Suppose n is not prime and if some prime.

<u>Case (i)</u>

$p \equiv 3 \pmod 4$ divide n where p is prime.

Then $Q(n) = 4\,p(n) = 4\,R(n) = 4\times 0 = 0$.

$$\therefore Q'(n) = \frac{Q(n)}{2} = 0.$$

In this case, eqn has no primitive solution.

<u>Case (ii)</u> If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$; $p_i \equiv 1 \pmod 4$

To each i, $e_i > 0$ for $i = 1$ to r ($r > 1$)

$$p(n) = R(n) = \prod_{i=1}^{r} R(p_i^{e_i})$$

$$= \prod_{i=1}^{r} (R(p_i)) = 2^r.$$

$\therefore p'(n) = \frac{p(n)}{2} = \frac{2^r}{2} = 2^{r-1} > 2$

This shows that in this case the eqn $4x^2+y^2=n$ has more than one non-negative primitive solution

Case (iii)

If $n = p^e$, $e > 1$, $p \equiv 1 \pmod 4$.

Then $p(n) = R(n) = R(p^e) = R(p) = 2$

$\therefore p'(n) = 1$

$N(n) = 4\left[h(1) + h(p) + h(p^2) + \cdots + h(p^e)\right]$

$= 4(e+1)$

$N'(n) = e(e+1) \geq 6 \geq 4$

$\Rightarrow N'(n) \geq 4$

& $p'(n) = \frac{p(n)}{2} = \frac{R(n)}{2} = \frac{R(p^e)}{2} = \frac{R(p)}{2}$

$= \frac{2}{2} = 1$

$\therefore p'(n) = 1$

$\therefore$ The eqn has exactly one non-negative primitive soln and it has more than 4 solutions.

It must have some non-primitive solns, say a & b.

Then $|a|, |b|$ is a non-negative non-primitive solution

Thus, in this case, the eqn $4x^2+y^2=n$ has one non-negative primitive solution and atleast one non-negative non primitive solution

$K_{-1}=1$ $K_{-2}=1$

$h_{-1}=1$ $h_{-2}=0$

$h_i=a_ih_{i-1}+h_{i-2}$

$K_i=a_iK_{i-1}+K_{i-2}$

UNIT - III

Infinite Continued fraction

We define two sequence of integers $\{k_n\}$ and $\{h_n\}$ as follows

$h_{-2} = 0,\ h_{-1} = 1;\ h_i = a_i h_{i-1} + h_{i-2}$ for $i \geq 0$

$k_{-2} = 1\ \ k_{-1} = 1\ \ k_i = a_i k_{i-1} + k_{i-2}$ for $i \geq 0$.

$$k_0 = a_0 k_{-1} + k_{-2} = k_{-2} = 1$$

$$k_1 = a_1 k_0 + k_{-1} = a_1 k_0 \geq k_0 \quad (a_1 \geq 1)$$

$$k_2 = a_2 k_1 + k_0 > a_2 k > k_1 \quad (a_2 \geq 1)$$

Thus we have $1 = k_0 \leq k_1 \leq k_2 \leq k_3 \cdots$

pb: Let x be any real number then

$$\langle a_0, a_1, \ldots, a_{n-1} \rangle = \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}$$

proof: We prove that the result by induction on n.

For $n=0$, $\langle a_0, a_1, \ldots, a_{n-1}, x \rangle = \langle x \rangle = x$

$$\frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}} = \frac{x h_{-1} + h_{-2}}{x k_{-1} + k_{-2}}$$

$$= \frac{x \cdot 1 + 0}{x \cdot 0 + 1}$$

$$= \frac{x}{1}$$

$$= x.$$

$\therefore$ For $n=0$, the result is true for $n=1$

$\langle a_0, a_1, a_2, \ldots, a_{n-1}, x\rangle = \langle a_0, x\rangle$

$= a_0 + 1/x$

$$\frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}} = \frac{x h_0 + h_{-1}}{x \cdot 1 + 0}$$

$$= \frac{x a_0 + 1}{x}$$

$$= a_0 + 1/x$$

$\therefore$ For $n=1$, the result is true

Assume that the result is true for n

ie) $\langle a_0, a_1, a_2, \ldots, a_{n-1}, x\rangle = \dfrac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}$

For $n+1$,

$\langle a_0, a_1, \ldots, a_{n-1}, x\rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n + 1/x\rangle$

$$= \frac{(a_n + 1/x) h_{n-1} + h_{n-2}}{(a_n + 1/x) k_{n-1} + k_{n-2}}$$

$$= \frac{(x a_n + 1) h_{n-1} + h_{n-2}\, x}{(x a_n + 1) k_{n-1} + k_{n-2}\, x}$$

$$= \frac{x a_n h_{n-1} + h_{n-1} + x h_{n-2}}{x a_n k_{n-1} + k_{n-1} + x k_{n-2}}$$

$$= \frac{x(a_n h_{n-1} + h_{n-2}) + h_{n-1}}{x(a_n K_{n-1} + K_{n-2}) + K_{n-1}}$$

$$\langle a_0, a_1, \ldots, a_n, x\rangle = \frac{x h_n + h_{n-1}}{x K_n + K_{n-1}}.$$

The result is true for $n+1$

By induction

$$\langle a_0, a_1, \ldots a_{n-1}, x\rangle = \frac{x h_{n-1} + h_{n-2}}{x K_{n-1} + K_{n-2}}$$

Result:

If $r_n = \langle a_0, a_1, \ldots, a_n\rangle$ then $r_n = \frac{h_n}{K_n}$.

~~proof~~ put $x = a_n$ in above thm.

Then $r_n = \langle a_0, a_1, \ldots, a_{n-1}, a_n\rangle$.

$$= \frac{a_n h_{n-1} + h_{n-2}}{a_n K_{n-1} + K_{n-2}}$$

$$= \frac{h_n}{K_n}.$$

b) Prove that equation

i) $h_i K_{i-1} - K_i h_{i-1} = (-1)^{i-1}$

ii) $r_i - r_{i-1} = \frac{(-1)^{i-1}}{K_i K_{i-1}}$ for $i \geq 1$

iii) $h_i K_{i-2} - K_i h_{i-2} = (-1)^{i-2} a_i$ and

iv) $r_i - r_{i-2} = \frac{(-1)^{i-2} a_i}{K_i K_{i-2}}$ for $i \geq 1$.

proof: i) we prove $h_i k_{i-1} - k_i h_{i-1} = (-1)^{i-1}$ by induction on i.

For $i=0$, $h_0 k_{-1} - k_0 h_{-1} = (-1)^{-1} = \frac{1}{(-1)} = -1$

$= (-1)^{0-1}$

For $i=1$, $h_1 k_0 - k_1 h_0 = (-1)^0 = (-1)^{1-1}$

Assume that result is true for $i \geq 1$.

$h_{i-1} k_{i-2} - k_{i-1} h_{i-2} = (-1)^{i-2}$

Now,

$h_i k_{i-1} - k_i h_{i-1} = (a_i h_{i-1} + h_{i-2}) k_{i-1}$

$- (a_i k_{i-1} + k_{i-2}) h_{i-1}$

$= a_i \cancel{h_{i-1}} k_{i-1} + h_{i-2} k_{i-1} - a_i \cancel{k_{i-1}} h_{i-1}$

$- k_{i-1} h_{i-1}$

$= h_{i-2} k_{i-1} - k_{i-2} h_{i-1}$

$= -[h_{i-1} k_{i-2} - k_{i-1} h_{i-2}]$

$h_i k_{i-1} - k_i h_{i-1} = -(-1)^{i-2}$

$= (-1)^{i-1}$

By induction $h_i k_{i-1} - k_i h_{i-1} = (-1)^{i-1}$

for $i \geq 1$

ii) Dividing by $k_i k_{i-1}$

$$\frac{h_i k_{i-1} - k_i h_{i-1}}{k_i k_{i-1}} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$$

$$\frac{h_i}{k_i} - \frac{h_{i-1}}{k_{i-1}} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$$

$$r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}} \text{ for } i \geq 1$$

iii) Consider

$$h_i k_{i-2} - k_i h_{i-2} = (a_i h_{i-1} + h_{i-2}) k_{i-2} - (a_i k_{i-1} + k_{i-2}) h_{i-2}.$$

$$= a_i h_{i-1} k_{i-2} + k_{i-2} h_{i-2} - a_i k_{i-1} h_{i-2} - k_{i-2} h_{i-2}$$

$$= a_i h_{i-1} k_{i-2} - a_i k_{i-1} h_{i-2}$$

$$= a_i (h_{i-1} k_{i-2} - k_{i-1} h_{i-2})$$

$$= a_i (-1)^{i-2}$$

by induction $h_i k_{i-2} - k_i h_{i-2} = (-1)^{i-2} a_i$.

iv) Dividing by $k_i k_{i-2}$ we have

$$\frac{h_i k_{i-2} - k_i h_{i-2}}{k_i k_{i-2}} = \frac{(-1)^{i-2} a_i}{k_i k_{i-2}}.$$

$$\frac{h_i}{k_i} - \frac{h_{i-2}}{k_{i-2}} = \frac{(-1)^{i-2} a_i}{k_i k_{i-1}}.$$

$$r_i - r_{i-2} = \frac{(-1)^{i-2} a_i}{k_i k_{i-1}}.$$

Pb) The infinite sequence $r_0, r_1, r_2, \ldots$ satisfying the following inequality $r_0 < r_2 < r_4 < \ldots < r_7 < r_5 < r_3 < r_1$. stated inwards r_n with even suffices form an increasing sequence and r_n with odd suffices form an decreasing sequence and $r_{2n} < r_{2j-1}$ for every n and j furthermore $\lim_{n\to\infty} r_n$ exists.

proof: we have $r_{2j} - r_{2j-2} = \dfrac{(-1)^{2j-2} a_{2j}}{k_{2j}\, k_{2j-2}} > 0$.

Since a_{2j}, k_{2j} and k_{2j-2} are +ve

$r_{2j} - r_{2j-2} > 0 \Rightarrow r_{2j} > r_{2j-2}$ for $i \geq 1$

ie) $r_0 < r_2 < r_4 < \ldots$ — (1)

Now, $r_{2j+1} - r_{2j-1} = \dfrac{(-1)^{2j-1} a_{2j+1}}{k_{2j+1}\, k_{2j-1}}$

$= \dfrac{-a_{2j+1}}{k_{2j+1}\, k_{2j-1}} < 0$ for $i \geq 1$.

$r_{2j+1} - r_{2j-1} < 0$

$r_{2j+1} < r_{2j-1}$ for $j \geq 1$

i.e) $r_1 > r_3 > r_5 > \cdots$ — (2)

Now, $r_{2j} - r_{2j-1} = \dfrac{(-1)^{2j-1} a_{2j}}{k_{2j}\, k_{2j-1}} < 0$

$\Rightarrow r_{2j} - r_{2j-1} < 0$ — (3).

Comparing (1), (2), (3), we have

$r_{2n} < r_{2n+2j} < r_{2n+2j-1} < r_{2j-1}$

i.e) $r_{2n} < r_{2j-1}$ for any n and j

the sequence $\{r_{2j}\}$ is monotonic increasing and bounded above by r_1.

Also, the sequence $\{r_{2j-1}\}$ is monotonic decreasing and bounded below by r_0.

The l.u.b of $\{r_n\}$ = g.l.b of $\{r_{2j-1}\}$.

This shows that $\lim\limits_{n\to\infty} r_n$ exists.

Defn

Let $a_0, a_1, \dots, a_n$ are integers then $\langle a_0, a_1, \dots, a_n \rangle$ is known as simple finite continued fraction

Formula:

$$\langle a_0, a_1, \dots, a_{n-1}, a_n \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3} + \dots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

$$= a_0 + \langle a_1, a_2, \dots, a_n \rangle$$

$$= \langle a_0, \dots, a_{n-2}, a_{n-1} + 1/a_n \rangle$$

Defn 7.1

An infinite sequence $a_0, a_1, \dots$ of all integers determine an infinite simple continued fraction $\langle a_0, a_1, \dots \rangle$.

$$\langle a_0, a_1, \dots \rangle = \lim_{n \to \infty} \langle a_0, a_1, \dots, a_n \rangle.$$

Theorem: 7.7

The value of any infinite simple continued fraction $\langle a_0, a_1, \dots \rangle$ is irrational.

proof: ~~The value of any infinite sum~~

Let $\theta = \langle a_0, a_1, a_2, \ldots \rangle$ which is not irrational

Also, $r_n < \theta < r_{n+1}$

$$0 < |\theta - r_n| < |r_{n+1} - r_n|$$

Also we know that

$$r_{n+1} - r_n = \frac{(-1)^n}{k_{n+1} k_n}$$

$$|r_{n+1} - r_n| = \frac{1}{k_{n+1} \cdot k_n} = (k_{n+1} \cdot k_n)^{-1}$$

$$\therefore (1) \Rightarrow 0 < |\theta - r_n| < (k_{n+1} k_n)^{-1} = \frac{1}{k_{n+1} k_n}$$

Multiplying by k_n,

$$0 < |\theta k_n - r_n k_n| < \frac{1}{k_{n+1} \cdot \cancel{k_n}} \cdot \cancel{k_n}$$

$$\frac{h_n}{k_n} = r_n$$

$$0 < |\theta k_n - h_n| < \frac{1}{k_{n+1}}$$

$\because \theta$ is rational, denote $\theta = \frac{a}{b}$ where a and b are integers and $b > 0$

$$\therefore 0 < \left| \frac{a}{b} k_n - h_n \right| < \frac{1}{k_{n+1}}$$

$$0 < |a k_n - b h_n| < \frac{b}{k_{n+1}}$$

$\therefore$ The integers k_n increases with n, we choose n sufficiently large so that $b < k_{n+1}$.

Then $\frac{b}{k_{n+1}} < 1$

$\therefore |k_n a - h_n b|$ lies between 0 and 1

$\Rightarrow \Leftarrow$ to $k_n a - h_n b$ is an integer.

$\therefore \langle a_0, a_1, a_2, \ldots, \rangle$ is irrational.

Lemma: 7.8

Let $\theta = \langle a_0, a_1, a_2, \ldots \rangle$ be a simple continued fraction. Then $a_0 = [\theta]$. Furthermore, if θ_1 denotes $\langle a_1, a_2, \ldots, \rangle$ then $\theta = a_0 + \frac{1}{\theta_1}$.

proof: Given $\theta = \langle a_0, a_1, a_2, \ldots \rangle$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

$$< a_0 + \frac{1}{a_1}$$

$$\therefore a_0 < \theta < a_0 + \frac{1}{a_1}$$

Also; $a_1 > 1 \Rightarrow \frac{1}{a_1} < 1$

$$\therefore a_0 < \theta < a_0 + 1.$$

$$\Rightarrow a_0 = [\theta]$$

Also, $\theta = \langle a_0, a_1, a_2, \ldots \rangle$.

$$= \lim_{n \to \infty} \langle a_0, a_1, \ldots, a_n \rangle$$

$$= \lim_{n\to\infty}\left(a_0 + \frac{1}{\langle a_1, a_2, \dots, a_n\rangle}\right)$$

$$= a_0 + \frac{1}{\lim_{n\to\infty}\langle a_1, a_2, \dots, a_n\rangle}$$

$$= a_0 + \frac{1}{\langle a_1, a_2, \dots\rangle}$$

$$\theta_0 = a_0 + \frac{1}{\theta_1}.$$

Theorem: 7.7

Two distinct infinite simple continued fractions converge to different values

Proof: Suppose that $\langle a_0, a_1, a_2, \dots\rangle = \langle b_0, b_1, \dots\rangle = \theta$

By above lemma, $[\theta] = a_0 = b_0$

Also, $\theta = a_0 + \frac{1}{\langle a_1, a_2, \dots\rangle} = b_0 + \frac{1}{\langle b_1, b_2, \dots\rangle}$

$\Rightarrow \langle a_1, a_2, \dots\rangle = \langle b_1, b_2, \dots\rangle.$

Repeat the same argument gives $a_1 = b_1$ and so by mathematical induction.

$a_n = b_n \ \forall n$

$\therefore$ Two distinct infinite simple continued fractions converges to different values.

Irrational Numbers

Theorem: 7.10

Any irrational number ξ is uniquely expressible by $a_i = [\xi_i]$, $\xi_{i+1} = \frac{1}{\xi_i - a_i}$, as an infinite simple continued fraction $\langle a_0, a_1, a_2, \cdots \rangle$ conversely any such continued fraction determined by integers a_i which are positive for all $i>0$, represents an irrational number ξ

proof We have already P.T any infinite simple continued fraction represents irrational number.

Conversely, Let ξ be an irrational number

T.P. ξ can be expressed as an infinite simple continued fraction.

Let $\xi = \xi_0$

define $a_0 = [\xi_0]$ and $\xi_1 = \frac{1}{\xi_0 - a_0}$

next $a_1 = [\xi_1]$ and $\xi_2 = \frac{1}{\xi_1 - a_1}$

and so by inductive define

$a_i = [\xi_i]$ and $\xi_{i+1} = \frac{1}{\xi_i - a_i}$

$\therefore$ By defn, a_i are integers and ξ_i are irrationals for all i.

<u>claim</u>: $a_i \geq 1 \ \forall i$.

$$a_{i-1} < \xi_{i-1} < 1 + a_{i-1}$$

$$0 < \xi_{i-1} - a_{i-1} < 1$$

$$\frac{1}{\xi_{i-1} - a_{i-1}} > 1.$$

$$\Rightarrow \xi_i > 1$$

$$\therefore a_i = [\xi_i] \geq 1$$

$$\therefore \xi_{i+1} = \frac{1}{\xi_i - a_i}$$

$$\Rightarrow \xi_i - a_i = \frac{1}{\xi_{i+1}}$$

$$\Rightarrow \xi_i = a_i + \frac{1}{\xi_{i+1}}$$

Now $\xi_0 = \xi_0 = a_0 + \dfrac{1}{\xi_1}$

$$= \langle a_0, \xi_1 \rangle$$

$$= \langle a_0, a_1 + \frac{1}{\xi_2} \rangle$$

$$= \langle a_0, a_1, \xi_2 \rangle.$$

$$\vdots$$

$$= \langle a_0, a_1, \dots, a_{n-2}, a_{n-1}, \xi_n \rangle$$

$$= \frac{\xi_n h_{n-1} + h_{n-2}}{\xi_n k_{n-1} + k_{n-2}}.$$

$$\xi - r_{n-1} = \xi - \frac{h_{n-1}}{k_{n-1}}$$

$$= \frac{\xi_n h_{n-1} + h_{n-2}}{\xi_n k_{n-1} + k_{n-2}} - \frac{h_{n-1}}{k_{n-1}}.$$

$$\frac{\xi_n h_{n-1} k_{n-1} + h_{n-2} k_{n-1} - \xi_n k_{n-1} h_{n-1} - h_{n-1} k_{n-2}}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} = \frac{-(h_{n-1} k_{n-2} - h_{n-2} k_{n-1})}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})}$$

$$= \frac{(-1)^{n-1}}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})}$$

This fraction tends to zero as $n \to \infty$ because the integers k_n are increasing with n and ξ_n is positive as $n \to \infty$.

$\therefore \xi - r_{n-1} \to 0$

$\therefore \xi = r_n$ as $n \to \infty$

$$\therefore \xi = \lim_{n \to \infty} r_n = \lim_{n \to \infty} \langle a_0, a_1, \ldots, a_n \rangle$$

$$= \langle a_0, a_1, \ldots \rangle$$

$\therefore$ Every irrational number can be expressed as infinite continued fraction.

UNIT- IV

Approximation to irrational numbers.

(6) we have for any $n \geq 0$, $\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}}$

& $\left|\xi k_n - h_n\right| < \frac{1}{k_{n+1}}$.

proof: we have $\xi = \langle a_0, a_1, \dots, a_n, \xi_{n+1} \rangle$

(ie) $$\xi = \frac{\xi_{n+1} h_n + h_{n-1}}{\xi_{n+1} k_n + k_{n-1}}$$

$$\xi - \frac{h_n}{k_n} = \frac{\xi_{n+1} h_n + h_{n-1}}{\xi_{n+1} k_n + k_{n-1}} - \frac{h_n}{k_n}.$$

$$= \frac{\xi_{n+1} h_n k_n + k_n h_{n-1} - \xi_{n+1} k_n h_n - h_n k_{n-1}}{(\xi_{n+1} k_n + k_{n+1}) k_n}$$

$$= \frac{k_n h_{n-1} - h_n k_{n-1}}{(\xi_{n+1} k_n + k_{n+1}) k_n}$$

$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}}$.

$$= \frac{-(h_n k_{n-1} - k_n h_{n-1})}{k_n(\xi_{n+1} k_n + k_{n-1})}$$

$\left|\xi k_n - h_n\right| < \frac{1}{k_{n+1}}$.

$$= \frac{-(-1)^{n-1}}{k_n(\xi_{n+1} k_n + k_{n-1})}.$$

$$= \frac{(-1)^n}{k_n(\xi_{n+1} k_n + k_{n-1})}.$$

$$\left|\xi - \frac{h_n}{k_n}\right| = \left|\frac{(-1)^n}{k_n(\xi_{n+1}k_n + k_{n-1})}\right|$$

$$= \frac{1}{k_n(\xi_{n+1}k_n + k_{n-1})} \quad \text{--- (1)}$$

But $a_{n+1} = [\xi_{n+1}] < \xi_{n+1}$

$\xi_{n+1}k_n > a_{n+1}k_n$

$\therefore \xi_{n+1}k_n + k_{n-1} > a_{n+1}k_n + k_{n-1} = k_{n+1}$ By defn.

$$\xi_{n+1}k_n + k_{n-1} > k_{n+1}.$$

$$\frac{1}{\xi_{n+1}k_n + k_{n-1}} < \frac{1}{k_{n+1}}$$

$$(1) \Rightarrow \left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}}.$$

Multiplying both sides by k_n, we have

$$|\xi k_n - h_n| < \frac{1}{k_{n+1}}.$$

7) For any irrational no. ξ,

$\left|\xi - \frac{h_n}{k_n}\right| < \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|$ Moreover, the stronger inequality $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$ holds.

proof: First we prove the stronger inequality $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$

implies the inequality $\left|\xi - \frac{h_n}{k_n}\right| < \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|$

Assume that $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$ holds

Now,

$$\left|\xi - \frac{h_n}{k_n}\right| = \frac{1}{k_n}|\xi k_n - h_n| < \frac{1}{k_n}|\xi k_{n-1} - h_{n-1}|$$

But $k_{n-1} < k_n$.

$$\frac{1}{k_{n-1}} \geq \frac{1}{k_n}$$

ie) $\frac{1}{k_n} \leq \frac{1}{k_{n-1}}$.

$$\therefore \left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_{n-1}}|\xi k_{n-1} - h_{n-1}|$$

$$= \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|.$$

$$\therefore \left|\xi - \frac{h_n}{k_n}\right| < \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|$$

Now we prove the second inequality

$$\left|\xi - \frac{h_{n-1}}{k_{n-1}}\right| = \frac{1}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} \quad \text{(1)}$$

(by above thm)

Consider $\xi_n k_{n-1} + k_{n-2}$

we have $a_n < \xi_n < 1 + a_n$.

$$\xi_n k_{n-1} + k_{n-2} < (1+a_n)k_{n-1} + k_{n-2}$$

$$= k_{n-1} + \underline{a_n k_{n-1} + k_{n-2}}$$

$$= k_{n-1} + k_n \quad \text{(by defn)}$$

$$\le a_{n+1}k_n + k_{n-1} = k_{n+1} \quad (\because a_{n+1} \geq 1)$$

$$\therefore \xi_n k_{n-1} + k_{n-2} < k_{n+1}$$

$$k_{n-1}(\xi_n k_{n-1} + k_{n-2}) < k_{n-1} k_{n+1}$$

$$\frac{1}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} > \frac{1}{k_{n-1} k_{n+1}}$$

But $\dfrac{1}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} = \left|\xi - \dfrac{h_{n-1}}{k_{n-1}}\right|$.

$$\therefore \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right| > \frac{1}{k_{n-1} k_{n+1}}.$$

Multiplying both sides by k_{n-1} we get

$$|\xi k_{n-1} - h_{n-1}| > \frac{1}{k_{n+1}}$$

By above thm, $\dfrac{1}{k_{n+1}} > |\xi k_n - h_n|$

$$\therefore |\xi k_{n-1} - h_{n-1}| > |\xi k_n - h_n|$$

ie) $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$

Hence the proof) II 1st internal

8) If $\frac{a}{b}$ is rational with +ve denominator and if $\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$ for some $n \geq 1$ Then $b > k_n$. Moreover, if $|b\xi - a| < |k_n\xi - h_n|$ for some $n \geq 0$ then $b \geq k_{n+1}$.

__Proof:__ First we prove that the second part of them implies the first part.

Second part states that if $|b\xi - a| < |k_n\xi - h_n|$, $n \geq 0$ then $b \geq k_{n+1}$.

Suppose that $\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$ & $b \leq k_n$

$$\text{Now, } |b\xi - a| = b\left|\xi - \frac{a}{b}\right|$$

$$< b\left|\xi - \frac{h_n}{k_n}\right|$$

$$< k_n\left|\xi - \frac{h_n}{k_n}\right|$$

$$|b\xi - a| < |k_n\xi - h_n|$$

$$\Rightarrow b \geq k_{n+1}$$

Thus, we have $b \leq k_n < k_{n+1} \leq b$

which is $\Rightarrow\Leftarrow$.

If $\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$ then $b > k_n$

Now, we want to prove the second part of thm

Suppose that $|b\xi - a| < |k_n\xi - h_n|$ then $b < k_{n+1}$

Consider the linear eqn.

$x h_n + y h_{n+1} = a$ & $x k_n + y k_{n+1} = b$

$\therefore$ These eqns have integral soln

Now, we claim that neither x nor y is zero.

For if $x = 0$ then $b = y k_{n+1}$

This implies that $y \neq 0$

$\therefore y \geq 1$

$\therefore b \geq k_{n+1}$

$x h_n + y h_{n+1} = a$

$x k_n + y k_{n+1} = b$

which is $\Rightarrow\Leftarrow$ to hypothesis, that $|b\xi - a| < |k_n\xi - h_n|$ & $b < k_{n+1}$.

$\therefore x \neq 0$.

If $y = 0$ then $a = x h_n$ & $b = x k_n$

$$|b\xi - a| = |x k_n \xi - x h_n|$$
$$= |x|\,|k_n \xi - h_n|$$

$\geq |k_n \xi - h_n| \quad (\because |x| \geq 1)$

which is $\Rightarrow\Leftarrow$ to assumption.

$\therefore y \neq 0$.

Now we claim that x & y are of opposite signs.

For if $y < 0$ then $x k_n = b - y k_{n+1}$

$\Rightarrow x > 0$.

$(\because x k_n = b - y k_{n+1})$

If $y > 0$, & $b < k_{n+1}$ $\quad$ & $x k_n = b - y k_{n+1}$

$\Rightarrow b < y k_{n+1}$

implies $x k_n < 0$ which implies $x < 0$.

Hence our claim.

Now for $n = 0, 2, 4, 6, \ldots$

$\frac{h_n}{k_n}$ is an increasing sequence

for $n = 1, 3, 5, 7, \ldots$

$\frac{h_n}{k_n}$ is a decreasing sequence and

$\xi = \lim_{n \to \infty} \frac{h_n}{k_n}$.

$k_n \xi_1 - h_n$ & $k_{n+1}\xi_1 - h_{n+1}$ are of opposite signs

$\therefore x(k_n \xi_1 - h_n)$ & $y(k_{n+1}\xi_1 - h_{n+1})$ are of the same sign.

$\therefore$ Absolute value of the sum equals the sum of separate absolute values.

$|x(k_n\xi_1 - h_n) + y(k_{n+1}\xi_1 - h_{n+1})|$

$= |x(k_n \xi_1 - h_n)| + |y(k_{n+1}\xi_1 - h_{n+1})|$

ie) $|(xk_n + yk_{n+1})\xi_1 - (xh_n + yh_{n+1})| > |x(k_n\xi_1 - h_n)|$

ie) $|b\xi_1 - a| > |x|\,|k_n\xi_1 - h_n|$

ie) $|b\xi_1 - a| > |k_n \xi_1 - h_n|$ $(\because |x| \geq 1)$

which is $\Rightarrow\Leftarrow$

$\therefore b \geq k_{n+1}$

4) Let ξ_1 be an irrational. Let $\frac{a}{b}$ be rational with $b \geq 1$ such that $\left|\xi_1 - \frac{a}{b}\right| < \frac{1}{2b^2}$. Then $\frac{a}{b}$ is equal to one of the convergent to ξ_1.

~~proof~~ W.l.g, assume that $(a,b)=1$

Suppose $\frac{a}{b}$ is not equal to any of the convergents $\frac{h_n}{k_n}$ choose +ve integer n such that $k_n \le b \le k_{n+1}$.

For this n, $|b\xi_1 - a| \geq |k_n\xi_1 - h_n|$

Now, $\frac{a}{b} \neq \frac{h_n}{k_n} \Rightarrow bh_n - ak_n$ is a non-zero integer.

$\therefore |bh_n - ak_n| \geq 1$.

Consider $\frac{1}{bk_n} \le \frac{|bh_n - ak_n|}{bk_n} = \left|\frac{h_n}{k_n} - \frac{a}{b}\right|$

$\le \left|\xi_1 - \frac{h_n}{k_n}\right| + \left|\xi_1 - \frac{a}{b}\right|$

(using triangular inequality)

$\frac{1}{bk_n} \le \frac{1}{k_n}|k_n\xi_1 - h_n| + \left|\xi_1 - \frac{a}{b}\right|$

$\le \frac{1}{k_n}|b\xi_1 - a| + \left|\xi_1 - \frac{a}{b}\right|$

$\le \frac{b}{k_n}\left|\xi_1 - \frac{a}{b}\right| + \left|\xi_1 - \frac{a}{b}\right|$

$\frac{1}{bk_n} < \frac{\cancel{b}}{k_n} \cdot \frac{1}{2b^{\cancel{2}}} + \frac{1}{2b^2}$

$\frac{1}{bk_n} < \frac{1}{2bk_n} + \frac{1}{2b^2}$

$$\cancel{\frac{1}{2bk_n}} + \frac{1}{2bk_n} < \cancel{\frac{1}{2bk_n}} + \frac{1}{2b^2}$$

$$\frac{1}{2bk_n} < \frac{1}{2b^2} \Rightarrow \frac{1}{k_n} < \frac{1}{b} \Rightarrow b < k_n$$

$$\Rightarrow \Leftarrow \text{ to } k_n \le b \le k_{n+1}$$

$\therefore \frac{a}{b}$ is equal to one of convergent to ξ.

Defn: A complex number ξ is called an algebraic number if it satisfies some polynomial equation $f(x) = 0$ where $f(x)$ is a polynomial over $\mathbb{Q}$.

Defn: An algebraic number ξ is an algebraic integer if it satisfies some monic polynomial equation.

$f(x) = x^n + b_1 x^{n-1} + \dots + b_n = 0$ with integral coefficients.

Theorem: Among the rational number the only ones that are algebraic integers are the integers $0, \pm 1, \pm 2, \dots$

Defn: Algebraic Number field

Consider the collection of all

numbers of the form $\left\{ \frac{f(\xi_1)}{h(\xi_1)} \middle| \begin{array}{l} h(\xi_1) \neq 0 \\ f(x), h(x) \in Q(x) \end{array} \right\}$

For a ~~field~~ fixed complex number ξ_1, this collection forms a field and is denoted by $Q(\xi_1)$ and it is called the extentions of Q by ξ_1.

Note: If ξ_1 is an algebraic number, then $Q(\xi_1)$ is called an algebraic number field.

Algebraic Integers.

Thm: If α is algebraic number, there is a rational integer b s.t αb is an algebraic integer.

proof: Let $f(x) = 0$ be the polynomial eqn satisfied by α where $f(x) \in Q[x]$.

We may persume that $f(x) = 0$ has rational integer coefficients by multiplying the rational coefficients by lest common multiple of denominators of the rational coefficients.

Let the eqn thus obtained be

$bx^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$ where $b, a_1, a_2, \ldots a_n$ are rational integer.

Let $h(x) = bx^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$

Let $h(\alpha) = 0$.

Now, $h\left(\frac{x}{b}\right) = b\left(\frac{x}{b}\right)^n + a_1\left(\frac{x}{b}\right)^{n-1} + a_2\left(\frac{x}{b}\right)^{n-2} + \cdots + a_n$

$= \frac{x^n}{b^{n-1}} + a_1 \frac{x^{n-1}}{b^{n-1}} + a_2 \frac{x^{n-2}}{b^{n-2}} + \cdots + a_n$

$b^{n-1} h\left(\frac{x}{b}\right) = x^n + a_1 x^{n-1} + \cdots + a_n b^{n-1}$.

put $x = \alpha b$.

Then $b^{n-1} h(\alpha) = (\alpha b)^n + a_1(\alpha b)^{n-1} + \cdots + a_n b^{n-1}$

$0 = (\alpha b)^n + a_1(\alpha b)^{n-1} + a_2 b(\alpha b)^{n-2} + \cdots + a_n b^{n-1}$.

This shows that αb satisfies the monic polynomial $x^n + a_1 x^{n-1} + \cdots + a_n b^{n-1}$

$\therefore \alpha b$ is an algebraic integer.

Theorem: The integer of an algebraic number field F forms a ring under addition and multiplication.

proof: Let $\alpha, \beta \in F$

If α, β are algebraic integer then $\alpha+\beta$, $\alpha\beta$ and $-\alpha$, are algebraic integer.

Also the additive identity 0 and multiplicative identity 1 are algebraic integer

$\therefore$ The closure of algebraic integer in any algebraic number field form a ring under addition and multiplication.

Defn: An algebraic integer $\alpha \neq 0$ in an algebraic number field is said to be divisor of algebraic integer β if $\exists$ an algebraic integer γ in the field s.t $\beta = \alpha\gamma$. In this case we write $\alpha | \beta$.

Any divisor of 1 is called unit.

Two non-zero algebraic integer α and β are said to be associates if $\alpha|\beta$ is unit.

(we say that α is called a unit if $\alpha|1$ or we say that β is an associate of α if $\alpha|\beta$ is a unit).

Theorem: The reciprocal of a unit is a unit. The unit of an algebraic number field forms a group.

proof: Let ϵ_1 be a unit.

Then ϵ_1 is divisor of 1.

$\therefore \exists$ an algebraic integer ϵ_2 s.t $\epsilon_1 \epsilon_2 = 1$

This shows that ϵ_2 is unit and is the reciprocal of ϵ_1.

$\Rightarrow$ reciprocal of unit is a unit.

Let ϵ_3 be a unit

Then $\exists$ algebraic integer ϵ_4 s.t $\epsilon_3 \epsilon_4 = 1$.

Now, $(\varepsilon_1, \varepsilon_3)(\varepsilon_2, \varepsilon_4) = 1$.

This shows that $\varepsilon_1 . \varepsilon_3$ is a unit.

1 is multiplicative identity and 1 is a unit we have already prove that reciprocal of unit is a unit.

$\therefore$ The unit form multiplicative group.

pb: The unit of Q are ± 1 and if α and β are associates then $\alpha = \pm \beta$.

Soln: Let ε_1 be a unit in the field Q.

Then $\exists \ \delta \in Q$ s.t $\varepsilon_1 . \delta = 1$.

By defn, ε_1 and δ must be algebraic integer of Q.

But the only algebraic integer in the rational field are rational integers.

$\therefore \varepsilon_1$ and δ are rational integer.

In particular ε_1 and $\frac{1}{\varepsilon_1}$ are rational integer

This is possible only if $\varepsilon_1 = \pm 1$ unit in the rational field are ± 1.

If α and β are associates then α/β is a unit

$$\therefore \frac{\alpha}{\beta} = \pm 1 \Rightarrow \alpha = \pm \beta$$

UNIT-5

Quadratic field

Defn: A quadratic field is the algebraic number field $Q(\xi_e)$ where ξ_e is root of an irreducible quadratic polynomial equation.

Note: The roots of an irreducible quadratic polynomial equation is of the form $\frac{a \pm b\sqrt{m}}{c}$ where a, b, c, m are rational integers and m is square free integer which is +ve or -ve but not one and $c > 0$.

Theorem: Every Quadratic field is of the form $Q(\sqrt{m})$ where m is a square free rational integer, positive or negative but not equal to 1. Numbers of the form $a + b\sqrt{m}$ with rational integers a and b are integers of $Q(\sqrt{m})$. These are the only integers of $Q(\sqrt{m})$ if $m \equiv 2$ or $3 \pmod 4$.

If $m \equiv 1 \pmod 4$, the numbers $\left(\frac{a + b\sqrt{m}}{2}\right)$ with odd rational integer a and b are also integer of $Q(\sqrt{m})$ and there are no further algebraic integers.

proof Let $Q(\xi)$ be quadratic field then ξ is root of an irreducible quadratic polynomial.

$\therefore \xi_1$ is of the form $\frac{a+b\sqrt{m}}{c}$ where a, b, c, m are rational integer

then $Q(\xi_1) = Q\left(\frac{a+b\sqrt{m}}{c}\right)$

$= Q(a+b\sqrt{m})$

$= Q(b\sqrt{m})$

$= Q(\sqrt{m})$.

Any number α in $Q(\sqrt{m})$ can be taken as $\alpha = \frac{a+b\sqrt{m}}{c}$, $c>0$.

W.L.G, assume that $(a, b, c) = 1$ so that α is its lowest term.

If $b=0$, then α is rational and it is an algebraic iff it is rational integer (by thm.)

$\therefore$ In this case, α is algebraic integer iff $c=1$.

If $b \neq 0$ then minimal equation α is quadratic namely

$$\left(x - \frac{a+b\sqrt{m}}{c}\right)\left(x - \frac{a-b\sqrt{m}}{c}\right) = 0.$$

ii) $x^2 - \frac{2a}{c}x + \frac{a^2-mb^2}{c^2} = 0$.

By known thm, α is algebraic integer iff minimal equation of α is monic with integral coeffiuents.

$\therefore$ α is an algebraic integer iff $c / 2a$ and c^2 / a^2-mb^2 ——— (*)

Claim: $(a,c)=1$ if α is an algebraic integer.

For, if $(a,c)>1$ and $c/2a$ then a & c have common prime say p.

But $p \nmid b$ [$\because (a,b,c)=1$].

$x^2 - \frac{2a}{c}x + \frac{a^2-mb^2}{c^2} = 0$

Now, p^2 / c^2 and p^2 / a^2

If c^2 / a^2-mb^2 then p^2 / a^2-mb^2

$\Rightarrow p^2 / mb^2 \Rightarrow p^2 / m$.

which is a $\Rightarrow\Leftarrow$ to the fact that m is a square free

$\therefore$ α is an algebraic integer iff $(a,c)=1$.

Next we claim $c \nmid 2$.

For, suppose $c>2$.

Let $c = 2^n,\ n > 1$

Then $c \mid 2a \Rightarrow 2^n \mid 2a$

$\Rightarrow 2^{n-1} \mid a$.

$\Rightarrow (a, c) \geq 2^{n-1} \geq 2$

which is a $\Rightarrow\Leftarrow$.

If c has an odd prime factors p

and $c \mid 2a \Rightarrow p \mid 2a \Rightarrow p \mid a$

$\Rightarrow (a, c) \geq p > 1$

which is a $\Rightarrow\Leftarrow$.

$\therefore c \nmid 2$

$\therefore \alpha$ is an algebraic integer iff

$c = 1$ or 2.

If $c = 1$ then ⊛ holds true.

$\therefore a + b\sqrt{m}$ are algebraic integer of $\mathbb{Q}(\sqrt{m})$

If $c = 2$ then $4 \mid a^2 - mb^2$

$\Rightarrow a^2 \equiv mb^2 \pmod 4$

which in turn implies that a is odd

Since m is square free

when a is odd $a^2 \equiv 1 \pmod 4$

$\therefore mb^2 \equiv 1 \pmod 4$.

which in turn implies that b is odd
when b is odd, $b^2 \equiv 1 \pmod 4$.

$$\therefore m \equiv 1 \pmod 4$$

This shows that $\frac{a+b\sqrt{m}}{2}$ are also algebraic integer if $m \equiv 1 \pmod 4$.

Defn: Consider a quadratic field $Q(\sqrt{m})$. Any number in the quadratic field is of form $\alpha = \frac{a+b\sqrt{m}}{c}$. we define norm of α denoted by $N(\alpha)$

$$N(\alpha) = \alpha\bar{\alpha} = \frac{a^2-b^2m}{c^2}$$ [$\bar{\alpha}$ is rational conjugate of α].

$\frac{a+b\sqrt{m}}{c}$ $\frac{a-b\sqrt{m}}{c}$

Theorem:
1) If $\alpha \in Q(\sqrt{m})$ is an algebraic integer then $N(\alpha)$ is rational integer.
2) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$
3) $N(\alpha) = 0$ iff $\alpha = 0$.
4) An algebraic integer γ is unit in $Q(\sqrt{m})$ iff $N(\gamma) = \pm 1$.

proof: 1) If α is an algebraic integer then
c^2 / a^2-b^2m.

$\therefore \frac{a^2-b^2m}{c}$ is rational integer.

$\Rightarrow N(\alpha)$ is rational integer

2) clearly $\alpha, \beta \in Q(\sqrt{m})$

$$\Rightarrow (\overline{\alpha\beta}) = \bar{\alpha}\,\bar{\beta}.$$

$$N(\alpha\beta) = (\alpha\beta)\,(\overline{\alpha\beta})$$
$$= (\alpha\beta)(\bar{\alpha}\,\bar{\beta})$$
$$= (\alpha\bar{\alpha})\,(\beta\bar{\beta})$$
$$= N(\alpha)\,N(\beta).$$

3) $N(\alpha) = 0$ iff $\alpha\bar{\alpha} = 0$ iff either $\alpha = 0$ (or) $\bar{\alpha} = 0$

But $\bar{\alpha} = 0 \Rightarrow \alpha = 0$.

$\therefore N(\alpha) = 0$ iff $\alpha = 0$.

4) Let γ be an algebraic integer which is unit in $Q(\sqrt{m})$

Then deg γ is either 1 or 2

If deg γ is 1 then minimal eqn is

$x - \gamma = 0$ with integral coefficients

This shows that γ itself is rational integer.

$\therefore N(\gamma) = \gamma\bar{\gamma}$ is rational integer.

$\because \gamma$ is unit, $\bar{\gamma}$ is also unit

Hence $\gamma\bar{\gamma}$ is unit $\Rightarrow \gamma\bar{\gamma} = \pm 1$

$\therefore N(\gamma) = \pm 1$.

If γ is of degree 2, then the minimal eqn is $x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} = 0$ with integral coefficients

$\therefore N(\gamma) = \gamma\bar{\gamma}$ is rational integer since γ is unit $\bar{\gamma}$ is also unit.

Hence $\gamma\bar{\gamma}$ is unit $\Rightarrow \gamma\bar{\gamma} = \pm 1$ $(\because N(\gamma) = \pm 1)$

Conversely, Suppose $N(\gamma) = 1$

$$\Rightarrow \gamma\bar{\gamma} = 1 \Rightarrow \gamma / 1$$

$\therefore \gamma$ is unit.

UNITS IN QUADRATIC FIELD

If $m<0$ the quadratic field $Q(\sqrt{m})$ is called imaginary quadratic field.

$m>0$ is called the real quadratic field.

1) Let m be -ve rational Integer which is square free. The units in the field $Q(\sqrt{m})$ are ± 1 except in 2 cases where $m=-1$ & $m=-3$. The units of $Q(i)$ are $\pm 1, \pm i$ and units of $Q(\sqrt{-3})$ are $\frac{1 \pm \sqrt{-3}}{2}$, $\frac{-1 \pm \sqrt{-3}}{2}$

Proof:

The algebraic Integers of $Q(\sqrt{m})$ are of two forms $x+y\sqrt{m}$ and $\frac{x+y\sqrt{m}}{2}$ where x, y are rational Integers and in latter case x, y are odd and $m \equiv 1 \pmod 4$

Suppose $m<0$ then $x^2 - my^2 \geq 0$

If α is unit, then $N(\alpha) = \pm 1$ and if α is unit of $Q(\sqrt{m})$, then $N(\alpha) = 1$ $[\alpha / 1 \Rightarrow 1 = \alpha\bar{\alpha} = N(\alpha)]$

ie) $x^2 - my^2 = 1$

$\therefore$ The eqn $x^2 - my^2 = 1$ has the only soln $x = \pm 1$

and $y = 0$

$\therefore$ The unit is ± 1

when $m = -1$, $x^2 - my^2 = x^2 + y^2$

$\therefore x^2 - my^2 = 1 \Rightarrow x^2 + y^2 = 1$

The soln of the eqn are $x = \pm 1, y = 0$ and

$x = 0, y = \pm 1$

The units are $\pm 1, \pm\sqrt{-1} = \pm\sqrt{i}$

Suppose $m = -3$ then $m \equiv 1 \pmod 4$ and $(N(\alpha) = \alpha\bar{\alpha})$

$$N\left(\frac{x + y\sqrt{m}}{2}\right) = \frac{x^2 - my^2}{4} = \frac{x^2 + 3y^2}{4}$$

and the eqn $\frac{x^2 + 3y^2}{4} = 1$ has soln $x = 1, y = \pm 1$

and $x = -1, y = \pm 1$

Since x & y are odd, the units of $Q(\sqrt{-3})$

are $\frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2}$ apart from ± 1

Summing up units of $Q(\sqrt{-1})$ are $\pm 1, \pm i$

$Q(\sqrt{-3})$ are $\frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2}$ and for all other $m < 0$,

the only units are ± 1

2) The units of real Quadratic field $Q(\sqrt{m})$ are

Infinite

Proof:

The algebraic integer of $Q(\sqrt{m})$ are $x + y\sqrt{m}$

and $\frac{x + y\sqrt{m}}{2}$ in case $m \equiv 1 \pmod 4$ with x & y odd

If $x + y\sqrt{m}$ is unit then $x^2 - my^2 = 1$

W.K.T the eqn has infinitely many soln.

$\therefore$ The units of $Q(\sqrt{m})$ are infinite

If $\frac{x+y\sqrt{m}}{2}$ is unit then $\frac{x^2-my^2}{4}=1$

ie) $x^2-my^2=4$ and this eqn has infinitely many soln.

$\therefore$ Units of real quadratic field are infinite

Problems:

1) If $\alpha = \alpha_1 + i\alpha_2$ where α_1 & α_2 are real. If α is algebraic no/-. Can α_1, α_2 be algebraic number?

If α is algebraic integer then α_1 & α_2 are algebraic integer.

Since α and $\bar{\alpha}$ satisfying same polynomial eqn with rational coefficients both α and $\bar{\alpha}$ are algebraic number if α is an algebraic number

W.K.T the algebraic number form a field

$\therefore \alpha_1 = \frac{\alpha+\bar{\alpha}}{2}$ is an algebraic number

$\alpha_2 = \frac{\alpha-\bar{\alpha}}{2i}$ is algebraic number

Since i is algebraic no/- satisfying poly eqn

$x^2+1=0$

Ans: NO

For consider $\alpha = \frac{1 \pm i\sqrt{3}}{2}$

This is an algebraic integer since it satisfies the monic poly eqn $x^2-x+1=0$.

But $\alpha_1 = 1/2$ $\alpha_2 = \sqrt{3}/2$ are not algebraic integer

Since this minimal eqn are $2x-1=0$ and $4x^2-3=0$ which are not monic

2) If α is an algebraic integer in $Q(\sqrt{m})$ and ε_1 is unit PT ε_1 / α

Clearly $\alpha = \varepsilon_1 (\varepsilon_1^{-1} \alpha)$

Put $B = \varepsilon_1^{-1} \alpha$ which is an algebraic integer

Since ε_1^{-1} is unit which is algebraic integer

$\therefore \alpha = \varepsilon_1 B \Rightarrow \varepsilon_1 / \alpha$

3. If α is an algebraic integer which is neither 0 nor unit P.T $|N(\alpha)| > 1$

Since α is an algebraic integer

$\Rightarrow N(\alpha)$ is rational integer

$\because \alpha$ is not 0, $N(\alpha) \neq 0$.

$\because \alpha$ is not a unit, $N(\alpha) \neq \pm 1$

$\therefore |N(\alpha)| > 1$

4) D.T the following assertion is false. If $N(\alpha)$ is rational integer in $Q(i)$ then α is algebraic integer

Consider $\alpha = \dfrac{1+7i}{5}$

Clearly. $N(\alpha) = \left(\dfrac{1+7i}{5}\right)\left(\dfrac{1-7i}{5}\right) = \dfrac{1+49}{25} = \dfrac{50}{25} = 2$

But minimal eqn of α is,

$$\left(x - \frac{1+7i}{5}\right)\left(x - \frac{1-7i}{5}\right) = 0$$

$$\left(x - \frac{1}{5}\right)^2 + \frac{49}{25} = 0$$

$$x^2 - 2x + \frac{1}{25} + \frac{49}{25} = 0 \Rightarrow x^2 - \frac{2x}{5} + 2 = 0$$

$$5x^2 - 2x + 10 = 0$$

which is not monic poly with integer coeffs

$\alpha = \frac{1+7i}{5}$ is not an algebraic integer

5) If $m \equiv 1 \pmod 4$ P.T the algebraic integer in $Q(\sqrt{m})$ are of the form $a + b\left(\frac{1+\sqrt{m}}{2}\right)$

Since $m \equiv 1 \pmod 4$ the algebraic integer in $Q(\sqrt{m})$ are of the form $\frac{\alpha + \beta\sqrt{m}}{2}$ where α, β are rational integers

$\because \alpha$ & β are odd we can write $\alpha = 2a + \beta$ where a is rational integer which may be +ve or -ve or zero

Then $\frac{\alpha + \beta\sqrt{m}}{2} = \frac{2a + \beta + \beta\sqrt{m}}{2} = a + \beta\left(\frac{1+\sqrt{m}}{2}\right)$

Put $\beta = b$

$$\frac{\alpha + \beta\sqrt{m}}{2} = a + b\left(\frac{1+\sqrt{m}}{2}\right)$$

$\therefore$ algebraic integers in $Q(\sqrt{m})$ are of form

$a + b\left(\frac{1+\sqrt{m}}{2}\right)$

6. If $\alpha \neq 0, \beta \neq 0$ are algebraic integer s.t $\alpha | \beta$ P.T $\bar{\alpha} | \bar{\beta}$ and $N(\alpha) | N(\beta)$

$\because \alpha | \beta$ $\exists$ an algebraic integer $\nu \neq 0$ such that

$\beta = \alpha\nu$

$$\bar{\beta} = \bar{\alpha}\bar{\nu} \Rightarrow \bar{\alpha} | \bar{\beta}$$

$$N(\beta) = N(\alpha\nu) = N(\alpha)N(\nu)$$

$$\therefore N(\alpha) | N(\beta)$$

7) P.T units in $Q(\sqrt{2})$ are of form $\pm(1+\sqrt{2})^n$ where n is any integer.

The units in $Q(\sqrt{2})$ are of form $x+y\sqrt{2}$

Since $2 \not\equiv 1 \pmod 4$

$\because x+y\sqrt{2}$ is unit $x^2-2y^2=\pm 1$

The least +ve soln of eqn $x^2-2y^2=-1$ are $x=1, y=1$.

Put $x_1=1, y_1=1$ then all soln of $x^2-2y^2=$ are x_n, y_n where

$$x_n+y_n\sqrt{2} = (x_1+y_1\sqrt{2})^n \quad n=1,2,3$$

$\therefore$ The units are $(1+\sqrt{2})^n$ $n=1,2,3$

The soln of $x^2-2y^2=1$ are x_n, y_n where

$x_n+y_n\sqrt{2} = (1+\sqrt{2})^n$ $n=2,4,6,\ldots$

UNIT-III

The equation $ax^2+by^2+cz^2=0$.

Let a, b, c be non-zero integer and abc is squarefree. The necessary and sufficient condition that $ax^2+by^2+cz^2=0$ has a solution in integers x, y, z not all zero are that a, b, c do not have same sign & that $-bc, -ca, -ab$ are quadratic residue modulo a, b, c respectively.

proof: Before proving the thm we see the following lemma

Lemma-1

Let λ, μ, δ be the +ve real no. ~~such that~~ $\lambda\mu\delta = m$ an integer.

Then the congruence, $\alpha x + \beta y + \gamma z \equiv 0 \pmod{m}$ has a solution x, y, z not all zero s.t $|x| \le \lambda, |y| \le \mu, |z| \le \delta$.

Proof of the lemma-1

Let x ranges over all values $0, 1, 2, \ldots [\lambda]$. y ranges over all values $0, 1, 2, \ldots [\mu]$, z ranges over all values $0, 1, 2, \ldots [\delta]$.

Then there are $(1+[\lambda])(1+[\mu])(1+[\delta])$ different triples x, y, z

Clearly, $1+[\lambda] > \lambda$, $1+[\mu] > \mu$, $1+[\delta] > \delta$

$\therefore (1+[\lambda])(1+[\mu])(1+[\delta]) > \lambda\mu\delta = m$.

$\therefore$ there exist three different triples x_1, y_1, z_1 & x_2, y_2, z_2 s.t

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \pmod m$$

$$\alpha(x_1 - x_2) + \beta(y_1 - y_2) + \gamma(z_1 - z_2) \equiv 0 \pmod m$$

ie) $\alpha x + \beta y + \gamma z \equiv 0 \pmod m$ has a soln

s.t $|x| = |x_1 - x_2| \le [\lambda] \le \lambda$

$|y| = |y_1 - y_2| \le [\mu] \le \mu$

$|z| = |z_1 - z_2| \le [\delta] \le \delta$

Lemma-2

Suppose $ax^2 + by^2 + cz^2$ is congruent to 2 linear factors modulo m & modulo n.

ie) $ax^2 + by^2 + cz^2 \equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \pmod m$

and $ax^2 + by^2 + cz^2 \equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \pmod n$

If $(m,n)=1$ then $ax^2+by^2+cz^2$ is congruent to 2 linear factors modulo mn.

proof of lemma-2:

proof: Since $(m,n)=1$, the congruence $x \equiv \alpha_1 \pmod{m}$ & $x \equiv \alpha_3 \pmod{n}$ has a soln satisfies by chinese remainder thm

Similarly,

$x \equiv \alpha_2 \pmod{m}$ & $x \equiv \alpha_4 \pmod{n}$ has a common soln.

Let α, β, γ and α', β', γ' be s.t $\alpha_1 \equiv \alpha \pmod{m}$,

$\alpha_3 \equiv \alpha \pmod{n}$, $\alpha_2 \equiv \alpha' \pmod{m}$; $\alpha_4 \equiv \alpha' \pmod{n}$

$\beta_1 = \beta \pmod{m}$; $\beta_3 = \beta \pmod{n}$; $\beta_2 \equiv \beta' \pmod{m}$

$\beta_4 \equiv \beta' \pmod{n}$

$\gamma_1 \equiv \gamma \pmod{m}$; $\gamma_3 \equiv \gamma (\bmod n$; $\gamma_2 \equiv \gamma' \pmod{m}$

$\gamma_4 \equiv \gamma' \pmod{n}$

Then $ax^2+by^2+cz^2 \equiv (\alpha x+\beta y+\gamma z)(\alpha' x+\beta' y+\gamma' z) \pmod{m}$

& $(ax^2+by^2+cz^2) \equiv (\alpha x+\beta y+\gamma z)(\alpha' x+\beta' y+\gamma' z) \pmod{n}$

Since $(m,n)=1$

$ax^2+by^2+cz^2 \equiv (\alpha x+\beta y+\gamma z)(\alpha' x+\beta' y+\gamma' z) \pmod{mn}$

Hence the lemma.

Proof of main theorem:

Suppose $ax^2+by^2+cz^2=0$ has a soln say x_0, y_0, z_0 not all zero

obviously, a, b, c do not have the same sign

If x_0, y_0, z_0 is soln then

$$x_1 = \frac{x_0}{(x_0, y_0, z_0)} ; \; y_1 = \frac{y_0}{(x_0, y_0, z_0)} ; \; z_1 = \frac{z_0}{(x_0, y_0, z_0)} .$$

is also a soln.

But $(x_1, y_1, z_1) = 1$

Consider the soln x_1, y_1, z_1 s.t

$ax_1^2 + by_1^2 + cz_1^2 = 0.$

We claim that $(c, x_1) = 1$

Suppose not, Let p be a prime factor of c & x_1

Then $p \mid ax_1^2 + cz_1^2 \Rightarrow p \mid -by_1^2 \Rightarrow p \mid by_1^2$

But $p \nmid b$ for if $p \mid b$ then

$p^2 \mid bc$ & hence abc is not squarefree

which is a $\Rightarrow\Leftarrow$.

$\therefore p \mid y_1^2 \Rightarrow p^2 \mid y_1^2$

$\therefore p^2 \mid ax_1^2 + by_1^2 \quad (\because p \mid x_1 \Rightarrow p^2 \mid x_1^2)$

$\therefore p^2 \mid cz_1^2$

Since c is square free

$p^2 / z_1^2 \Rightarrow p / z_1$

Thus we have p is a prime factor of x_1, y_1, z_1 which is contradiction to the fact that $(x_1, y_1, z_1) = 1$

$\therefore (c, x_1) = 1$

The congruence $ux_1 \equiv 1 \pmod{c}$ has soln.

Now $ax_1^2 + by_1^2 \equiv 0 \pmod{c}$

Multiply by u^2b we have.

$u^2bax_1^2 + u^2bby_1^2 \equiv 0 \pmod{c}$

Since $ux_1 \equiv 1 \pmod{c}$

$\Rightarrow u^2x_1^2 \equiv 1 \pmod{c}$

$\therefore ab + (uby_1)^2 \equiv 0 \pmod{c}$

$(uby_1)^2 \equiv -ab \pmod{c}$

This shows that $-ab$ is quadratic residue modulo c

Similarly,
we prove that $-bc$ is quadratic residue modulo a & $-ac$ is quadratic residue modulo b.

Conversely,
Suppose a, b, c do not have the same sign, abc is square free and $-bc$, $-ca$, $-ab$ are quadratic residue modulo a, b, c respectively.

Changing the sign of a, b, c will not affect the quadratic residue modulo character of $-bc, -ca, -ab$.

$\therefore$ we can change the signs of a, b, c so that one of positive & other two are negative.

By rearranging, we take 'a' to be positive & b, c are negative.

Since abc is square free $(a, c) = 1$ and hence the congruence
$aa_1 \equiv 1 \pmod{c}$ has a solution.

Since ab is quadratic residue modulo c, the congruence $x^2 \equiv -ab \pmod{c}$ has a solution say r.

$$ax^2+by^2 = 1\,(ax^2+by^2)$$

$$ax^2+by^2 \equiv aa_1(ax^2+by^2) \pmod{c}$$

$$\equiv a_1(a^2x^2+aby^2) \pmod{c}$$

$$\equiv a_1(a^2x^2-r^2y^2) \pmod{c}$$

$$\equiv a_1(ax+ry)(ax-ry) \pmod{c}$$

$$\equiv (ax+ry)(a_1ax-a_1ry) \bmod c.$$

$$\equiv (ax+ry)(x-a_1ry) \pmod{c}.$$

$$ax^2+by^2 \equiv (ax+ry)(x-a_1ry) \pmod{c}$$

Now, $cz^2 \equiv 0 \pmod{c}$

Since $ax^2+by^2+cz^2 \equiv (ax+ry)(x-a_1ry) \pmod{c}$

$ax^2+by^2+cz^2$ is product of two linear factor of mod c.

Similarly, $ax^2+by^2+cz^2$ is a product of two linear factor modulo b & modulo a.

Applying lemma 2, two times we have $ax^2+by^2+cz^2$ is a product of 2 linear factors modulo abc.

Let $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ be s.t ~~$ax^2+by^2+cz^2$~~

$ax^2+by^2+cz^2 \equiv (\alpha x+\beta y+\gamma z)(\alpha' x+\beta' y+\gamma' z) \bmod (abc)$ — (1).

Consider the congruence $\alpha x+\beta y+\gamma z \equiv 0 \pmod{abc}$ — (2).

Applying lemma 1, with
$\lambda = \sqrt{|bc|}$, $\mu = \sqrt{|ac|}$, $\delta = \sqrt{|ab|}$

(2) has a solution x_1, y_1, z_1 not all zero such that

$|x_1| \le \sqrt{bc}$ ie) $x_1^2 \le bc$ with equality possible only if $b=-1, c=-1$.

$|y_1| \le \sqrt{|ac|}$ ie) $y_1^2 \le |ac|$ with equality possible only if $a=1, c=-1$.

$|z_1| \le \sqrt{|ab|}$, ie) $z_1^2 \le |ab|$ with equality possible only if $a=1, b=-1$.

Unless $b=-1, c=-1$

$ax_1^2+by_1^2+cz_1^2 < ax_1^2 < abc$

Since $y_1^2 < -ac$ & $b<0 \Rightarrow by_1^2 > -abc$

$\therefore z_1^2 < -ab$ & $c < 0 \Rightarrow cz_1^2 > -abc$

$ax_1^2 + by_1^2 + cz_1^2 \geq by_1^2 + cz_1^2$

$ax_1^2 + by_1^2 + cz_1^2 > -abc - abc$

$= -2abc$

Thus, we have

$-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc.$

Since x_1, y_1, z_1 is a solution of ②, ①

implies that $ax_1^2 + by_1^2 + cz_1^2 \equiv 0 \pmod{abc}$

Since $ax_1^2 + by_1^2 + cz_1^2 = 0$ (or) $-abc$ unless

$b = c = -1$

If $ax_1^2 + by_1^2 + cz_1^2 = 0$ then x_1, y_1, z_1 is

the required solution of $ax^2 + by^2 + cz^2 = 0$

Suppose $ax_1^2 + by_1^2 + cz_1^2 = -abc$

put $x_2 = -by_1 + x_1z_1$, $y_2 = ax_1 + y_1z_1$

$z_2 = z_1^2 + ab$

we verify that $ax_2^2 + by_2^2 + cz_2^2 = 0$.

For $a(-by_1 + x_1z_1)^2 + b(ax_1 + y_1z_1)^2 + c(z_1^2 + ab)^2$

$= (ab^2y_1^2 + x_1^2z_1^2 - 2bx_1y_1z_1) + b(a^2x_1^2 + y_1^2z_1^2 + 2ax_1y_1z_1)$

$+ c(z_1^2 + ab)^2$

$= ab(by_1^2 + ax_1^2) + z_1^2(ax_1^2 + by_1^2) + c(z_1^2 + ab)^2$

$= (ax_1^2 + by_1^2)(z_1^2 + ab) + c(z_1^2 + ab)^2.$

$= (z_1^2 + ab)\left[ax_1^2 + by_1^2 + c(z_1^2 + ab)\right]$

$= (z_1^2 + ab)\left[ax_1^2 + by_1^2 + cz_1^2 + abc\right]$

$= 0. \quad \left[\because ax_1^2 + by_1^2 + cz_1^2 = -abc\right]$

$ax_2^2 + by_2^2 + cz_2^2 = 0.$

$\therefore x_2, y_2, z_2$ is a soln of $ax^2 + by^2 + cz^2 = 0.$