Unit - V

Some Diophantine Equations:

The Equation $ax + by = c$.

Any linear equation in two variables having integral co-efficients can be put in the form.

$$ax + by = c \quad \text{---} \quad (1)$$

where a, b & c are given integers.

We consider the problem of identifying all solution of this equation in which x & y are integers.

If $a = b = c = 0$;

Then every pair (x, y) of integer is a solution of (1).

where as if $a = b = 0$ & $c \neq 0$.

Then (1) has no solution.

Now suppose that atleast one of a & b is non zero. and

Let $g = g.c.d\ (a, b)$.

If $g \nmid c$.

Then (1) has no solution.

Suppose that the pairs (x_1, y_1) (x, y) are integral solutions of (1).

By subtracting, we find that,

$$a(x - x_1) + b(y - y_1) = 0.$$

we divide through by g and rearrange to see that,

$$(a/g)(x - x_1) = (b/g)(y_1 - y).$$

ie) a/g divides the product $(b/g)(y_1 - y)$.

But $(a/g, b/g) = 1$.

It follows that a/g divides $y_1 - y$. ie) $ka/g = y_1 - y$ for some

we find that $x - x_1 = kb/g$.

Ex:

Find all solutions of $999x - 49y = 5000$.

Soln:

By the division algorithm.

we observe that,

$$999 = 20 \cdot 49 + 19 \quad \text{— (4)}$$

This suggests writing the equation in the form $19x - 49(y - 20x) = 5000$ — (2)

putting, $x' = x$,

$$y' = -20x + y.$$

we find that the original equation is expressed by the condition

$$19x' - 49y' = 5000 \quad \text{— (3)}$$

This is simpler because the co-efficient are smaller.

Since $49 = 2 \cdot 19 + 11$.

We write this equation as

$$19(x' - 2y') - 11y' = 5000. \quad \text{—(4)}$$

i.e. $$19x'' - 11y'' = 5000. \quad \text{—(5)}$$

where $x'' = x' - 2y'$ &

$y'' = y'$.

Since $19 = 2 \cdot 11 - 3$.

we write this equation as

$$-3x'' - 11(-2x'' + y'') = 5000 \quad \text{—(6)}$$

i.e. $$-3x^{(3)} - 11y^{(3)} = 5000 \quad \text{—(7)}$$

where $x^{(3)} = x''$ &

$y^{(3)} = -2x'' + y''$.

As $11 = 4 \cdot 3 - 1$

we write the equation as

$$-3(x^{(3)} + 4y^{(3)}) + y^{(3)} = 5000$$

i.e. $$-3x^{(4)} + y^{(4)} = 5000. \quad \text{—(9)}$$

where $x^{(4)} = x^{(3)} + 4y^{(3)}$ & —(10)

$y^{(4)} = y^{(3)}$.

Making the further change of variables

$x^{(5)} = x^{(4)}$, $y^{(5)} = -3x^{(4)} + y^{(4)}$. —(11)

We see that the original equation is equivalent to the equation

$$y^{(5)} = 5000.$$

Here the value of $y^{(5)}$ is a fixed integer, & $x^{(5)}$ is an arbitrary integer.

Since the pairs of integers (x, y) are in 1-1 correspondence with pairs of integers $(x^{(5)}, y^{(5)})$.

It follows that the original equation has infinitely many solutions in integers.

To express x & y explicitly in terms of $x^{(5)}$ & $y^{(5)}$.

we first determine n & y in terms of n' & y'.

Then in terms of n'' & y'' and so on.

These transformation can be developed at the original equation is being simplified.

we start by writing,

$$999n - 49y = 5000$$

$$n = n,$$

$$y = y \quad \text{—— (2)}$$

Then we rewrite these equations in the form.

(2) $\Rightarrow 19n - 49(-20n + y) = 5000$

$$n = n$$

adding & subtracting $20n'$

$$20n' + (-20n + y) = y$$

i.e.

(3) $\Rightarrow 19n' - 49y' = 5000$ put $n = n'$, $y = -20n + y'$

$$n' = n$$

$$20n' + y' = y \quad \text{—— (3)}$$

we rewrite this as,

(4) $\Rightarrow 19(n' - 2y') - 11y' = 5000$

adding & subtracting $2y'$

$$n' - 2y' + 2y' = n \qquad \text{put } \therefore n = n' - 2y'$$

$$20(n' - 2y') + 41y' = y$$

$\Rightarrow 20n' - 40y' + 41y' = y$

$20n' + y' = y$

i.e.

(5) $\Rightarrow 19n'' - 11y'' = 5000$

$$n'' + 2y'' = n \quad \text{—— (4)} \qquad \because n' = n' - 2y'$$

$$20n'' + 41y'' = y$$

We rewrite this as,

(6) $\Rightarrow -3n'' - 11(-2n'' + y'') = 5000$

$$5n'' + 2(-2n'' + y'') = n$$

$5n'' - 4n'' + 2y'' = n \Rightarrow n'' + 2y'' = n$

$$102n'' + 41(-2n'' + y'') = y$$

$102n'' - 82n'' + 41y'' = y \Rightarrow 20n'' + 41y'' = y$

i.e.

(7) $\Rightarrow -3n^{(3)} - 11y^{(3)} = 5000$

$$5n^{(3)} + 2y^{(3)} = n \quad \text{—— (5)} \qquad \therefore n'' = n^{(3)}$$

$$102n^{(3)} + 41y^{(3)} = y \qquad y^{(3)} = -2n'' + y'$$

we rewrite this as

$$-3(x^{(3)} + 4y^{(3)}) + y^{(3)} = 5000 \quad \text{—} \textcircled{5}$$

$$5(x^{(3)} + 4y^{(3)}) - 18y^{(3)} = x$$

$$102(x^{(3)} + 4y^{(3)}) - 367y^{(3)} = y$$

ii) $\Rightarrow -3x^{(4)} + y^{(4)} = 5000$

$$5x^{(4)} - 18y^{(4)} = x \quad \text{—} \textcircled{6}$$

$$102x^{(4)} - 367y^{(4)} = y.$$

$x^{(4)} = x^{(3)} + 4y^{(3)}$

$y^{(3)} = y^{(4)}$

we rewritten as

$\textcircled{5} \Rightarrow -(3x^{(4)} + y^{(4)}) = 5000$

$$-49x^{(4)} - 18(-3x^{(4)} + y^{(4)}) = x$$

$$-999x^{(4)} - 367(-3x^{(4)} + y^{(4)}) = y.$$

iii) $\textcircled{11} \Rightarrow y^{(5)} = 5000$

$$-49x^{(5)} - 18y^{(5)} = x \quad \text{—} \textcircled{7}$$

$$-999x^{(5)} - 367y^{(5)} = y \quad \text{—} \textcircled{8}$$

$x^{(5)} = x^{(4)}$

$y^{(5)} = -3x^{(4)} + y^{(4)}$

Inserting this value of $y^{(5)}$, and writing k in place of $x^{(5)}$.

we conclude that the solutions of the proposed equation are given by

Solving, $y^{(5)} = 5000$, $x^{(5)} = k$

$\textcircled{A} \Rightarrow -49k - 18(5000) = x$

$\textcircled{B} \Rightarrow -999k - 367(5000) = y$

$\textcircled{A} \Rightarrow x = -49k - 90000$

$\textcircled{B} \Rightarrow y = -999k - 1835000.$ — ©

This parameterization of the solutions is not unique.

For eg, we could set

$$k = -1837 - m$$

in which case the equations above would become. put $k = -1837 - m$ value sets in ©

$$x = 49m + 13$$

$$y = 999m + 163.$$

$x = -49(-1837-m) - 90000$

$y = -999(-1837-m) - 1835000$

$x = 90013 + 49m - 90000$

$y = 1835163 + 999m - 1835000$

$x = 49m + 13$

$y = 999m + 163$

Eg:- Find all integers x & y such that

$$147x + 258y = 369.$$

Soln:-

we write,

$$147x + 258y = 369$$

	147	258	369				
	1	0					
	0	1					
→	147	111	369		36	111	369
	1	-1	$C_2 \to C_2 - C_1$ →		2	-1	$C_1 \to C_1$
	0	1			-1	1	
→	36	3	369		0	3	369
	2	-7	$C_2 \to C_2 - 3C_1$ →		86	-7	$C_1 \to C_1$
	-1	4			-49	4	

Let the variables that are implicit in this last array be called u & v.

36	2	-
36	-84	45
(+)	(+)	—
0	86	-

Since $3v = 369$.

we deduce that $v = 123$.

and that the full set of solutions is given by taking

$$x = 86u - 861$$

$$y = -49u + 492.$$

The variables u & v were obtained from the original variables x & y by a homogeneous change of co-ordinates.

We may deduce the size of the constant term in our answer by introduction introducing an inhomogeneous change of variables.

For eg, if we put $u = t + 10$

Then we find that

$$x = 86t - 1,$$

$$y = -49t + 2.$$

Eg:-

Find all solutions of the simultaneous congruences

$$3x + 3z \equiv 1 \pmod{5}$$

$$4x - y + z \equiv 3 \pmod{5}.$$

Soln:-

We construct an array of co-efficients as before.

Using operation (C1).

we add the third column to both columns 1 & 2.

$$\begin{matrix} 3 & 0 & 3 & 1 \\ 4 & -1 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{matrix} \rightarrow \begin{matrix} 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{matrix}$$

Using (R1), we multiply the second row by 2 and add the result to the first row.

Then we interchange the first & third columns and the first and second rows.

$$\begin{matrix} 1 & 3 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{matrix} \xrightarrow{R_1 \to 2R_2 + R_1} \begin{matrix} 1 & 0 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 1 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{matrix}$$

Next we multiply the third column by 2. and add the result to the second column and then interchange the second and third columns.

$$\begin{matrix} 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 1 & \\ 0 & 1 & 0 & \\ 1 & 3 & 1 & \end{matrix} \xrightarrow{C_2 \to 2C_3 + C_2} \begin{matrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 2 & \\ 0 & 0 & 1 & \\ 0 & 1 & 2 & \\ 1 & 1 & 3 & \end{matrix} \pmod 5$$

Thus we arrive at a new system of congruences, in variables t, u, v, say.

we see that

$$t \equiv 3 \pmod 5$$

$$u \equiv 2 \pmod 5$$

while v can take any value $\pmod 5$

Thus the given system has five solutions given by,

$$x \equiv 0 + u + 2v \equiv 2 + 2v \pmod 5$$

$$y \equiv 0 + 0 + v \equiv v \pmod 5$$

$$z \equiv t + u + 3v \equiv 3 + 2 + 3v \equiv 5 + 3v$$

$$\equiv 0 + 3v \pmod 5$$

$$\equiv 3v \pmod 5$$

In general, the system of simultaneous congruences.

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod q$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod q$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \equiv b_m \pmod q$$

has a solutions $\pmod q$ iff,

$$\text{g.c.d}(a_j, q) \mid b_j' \qquad (1 \le j \le r)$$

$$b_j' \equiv 0 \pmod q \qquad (r < j \le m)$$

Pythagorean Triangles :

We wish to solve the equation $x^2 + y^2 = z^2$ in the integers.

The two most familiar solutions are 3, 4, 5 & 5, 12, 13.

We refer to such a triple of the integers as a pythagorean triple or a pythagorean triangle.

Since in geometric terms x & y are the legs of a right triangle with hypotenuse z.

In view of the algebraic identity

$$(r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2 \quad \text{— (1)}$$

we may obtain an infinity of pythagorean triangles by taking,

$$\left.\begin{aligned} x &= r^2 - s^2 \\ y &= 2rs \\ z &= r^2 + s^2 \end{aligned}\right\} \quad \text{— (2)}$$

where r & s take integral values with $r > s > 0$.

Here, remarkably, we S.T all pythagorean triangles arise in this way.

Since the equation under consideration is homogeneous, if x, y, z is a pythagorean triple, then so also is kx, ky, kz for any the integer k.

For ex. The pythagorean triangle 3, 4, 5 gives 6, 8, 10 and also 60, 80, 100.

Thus any given pythagorean triangle gives rise to an infinite family of similar triangles.

To initiate our analysis, we identify in this family the smallest triangle.

Suppose that x, y & z are given the integers for which $x^2 + y^2 = z^2$.

Let d be a common divisor of x & y.

Then $d^2 \mid n^2$ & $d^2 \mid y^2$; and

Hence $d^2 \mid (n^2 + y^2)$

i.e) $d^2 \mid z^2$

By unique factorization, It follow that $d \mid z$.

Indeed by further arguments of this sort, we discover that any common factor of two of the numbers n, y, z must divide the third.

i.e) $(n, y) = (y, z) = (z, n) = (n, y, z)$

Let g denote this common value, and put $n_1 = n/g$, $y_1 = y/g$, $z_1 = z/g$

Then n_1, y_1, z_1 is a pythagorean triple with $(n_1, y_1) = 1$.

We call such a triple primitive, since it is not a multiple of a smaller triple.

Thus we see that all pythagorean triangles similar to the given triangle n, y, z are multiples of n_1, y_1, z_1.

Lemma:

If u & v are relatively prime two integers whose product uv is a perfect square, then u & v are both perfect squares.

proof

Let p be a prime that divides u, and

Let α be the exact power of p in u. (In symbols, $p^\alpha \| u$).

Since u & v are relatively prime, p does not divide v, and

Hence $p^\alpha \| uv$.

But uv is a perfect square, so α must be even.

Since this holds for all primes p dividing u,

It follows that u is a perfect square.

Similarly v must be a perfect square.

If x, y, z is a primitive pythagorean triple with x & z are odd, and y even,

Then $z-x$ & $z+x$ are both even.

Accordingly, we divide by 4 & write our equation as.

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

Any common divisor of the two factors on the left divides both their sum z and their difference x.

Since $(x, z) = 1$.

It follows that the two factors on the left have no common factor.

We deduce that

$$(z+x)/2 = r^2.$$

$$(z-x)/2 = s^2 \quad \&$$

$$y/2 = rs$$

for some the integers r, s.

We also see that $(r, s) = 1$. and that $r > s$.

Also, since z is odd, r & s are of opposite parity (one is even, the other odd).

On solving for x, y, & z in terms of r & s,

we obtain the equations

$$x = r^2 - s^2$$

$$y = 2rs$$

$$z = r^2 + s^2 \quad \text{already noted.}$$

Thus we have the following result.

Theorem:

The the prime solutions of $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$, where r & s are arbitrary integers of opposite parity with $r > s > 0$ & $(r, s) = 1$.

Assorted Examples:

Theorem:

The equation $15x^2 - 7y^2 = 9$, has no solution in integers.

proof

Since the first and third members are divisible by 3.

It follows that $3 | 7y^2$

and Hence $3 | y$.

Thus the second and third members are divisible by 9.

So that $9 | 15x^2$, & hence $3 | x$.

put $x_1 = x/3$, $y_1 = y/3$.

So that $15x_1^2 - 7y_1^2 = 1$.

This has no solution as a congruence (mod 3).

Hence proved.

Let $p(x_1, \dots x_n)$ be a homogeneous polynomial of degree d with integral co-efficients.

Then the Diophantine equation.

$$p(x_1, \dots, x_n) = 0 \quad \text{— (1)}$$

has the trivial solution §

$$x_1 = x_2 = \dots = x_n = 0.$$

If $(x_1, \dots x_n)$ is a non trivial solution.

Then we may set

$g = g.c.d\ (x_1, \dots x_n)$. and

divide the equation by g^d, to obtai

a primitive solution, one for which the variables are relatively prime.

In general we cannot guarantee that such variables will be pairwise relatively prime.

Theorem:

The equation $x^3 + 2y^3 + 4z^3 = 9w^3$ has no non-trivial solution.

proof

We S.T the congruence

$x^3 + 2y^3 + 4z^3 = 9w^3 \pmod{27}$

has no solution for which

$g.c.d\ (x, y, z, w, 3) = 1$.

We note that for any integer a,

$a^3 \equiv 0$ or $\pm 1 \pmod 9$.

Thus $x^3 + 2y^3 + 4z^3 \equiv 0 \pmod 9$.

$\Rightarrow x \equiv y \equiv z \equiv 0 \pmod 3$.

But then $x^3 + 2y^3 + 4z^3 \equiv 0 \pmod{27}$.

So that $3 \mid w^3$.

Hence $3 \mid w$.

This contradicts the assumption that $g.c.d\ (x, y, z, w, 3) = 1$.

Hence proved.

Theorem:

The equation $y^2 = x^3 + 7$ has no solution in integers.

proof

If x is even then the equation is impossible as a congruence $\pmod 4$.

This in any solution, x must be odd, and hence y must be even.

If then follows that $x \equiv 1 \pmod 4$.

Since the left side of the equation is non-ve.

we deduce that $x \geq -1$.

We rewrite the equation in the form $y^2 + 1 = (x+2)(x^2 - 2x + 4)$

Here the left side is odd, and w.k.t every prime factor of the left side is $\equiv 1 \pmod 4$.

Hence every the divisor of the left side is $\equiv 1 \pmod 4$.

On the other hand, the right side has the the divisor $n+2 \equiv 3 \pmod 4$.

Thus these two expressions cannot be equal.

In the argument just completed, we discover an inconsistency $\pmod q$ for some prime $q \equiv 3 \pmod 4$ which divides $n+2$.

This q is not fixed, but is instead a function of the hypothetical solution n, y.

Theorem:

The Diophantine equation $n^4 + n^3 + n^2 + n + 1 = y^2$ has the integral solutions $(-1, 1), (0, 1), (3, 11)$ and no others.

proof.

put $f(n) = 4n^4 + 4n^3 + 4n^2 + 4n + 4$

Then $f(n) = (2n^2 + n)^2 + 3(n + 2/3)^2 + 8/3$

It follows that

$f(n) > (2n^2 + n)^2$ $\forall$ real n.

On the other hand,

$f(n) = (2n^2 + n + 1)^2 - (n+1)(n-3)$.

Hence the last term is the except for those real numbers n in the interval

$I = [-1, 3]$.

ie) $f(n) < (2n^2 + n + 1)^2$

provided that $n \notin I$.

Thus we see that if n is an integer $n \notin I$.

Then $f(n)$ lies between two consecutive perfect square.

Namely, $(2n^2+n)^2 < (2n^2+n+1)^2$.

Hence $f(n)$ cannot be a perfect square, except possibly for those integers $n \in I$, we examine individually.

Hence proved.

Theorem:-

The equation $x^4 + y^4 = z^2$ has no solution in the integers.

proof:

The secret is that one should not consider the given equation in isolation but rather in tandem with a second equation.

$$a^2 + 4b^4 = c^4 \quad \text{---} \quad (1)$$

we S.T if the given equation

$$x^4 + y^4 = z^2 \quad \text{---} \quad (2)$$

has a solution in the integers

Then so does this second equation and conversely if

solution in the integers.

Then so does (2).

On closer examination, we discover that if we start with a solution of (2). use it to construct a solution of (1). and

Then use that solution to construct a solution of (2).

Then we do not obtain the original solution of (2) that we started with.

Instead, the new solution is smaller, in the sense that z is smaller.

This always us to derive a contradiction.

Since we may assume that ever initial solution is minimal.

This is Fermat's method of descent.

Let x, y, z be arbitrary the integers that satisfy ②.

Set $g = g.c.d\,(x, y)$.

Since g^4 divide the left side of ②. It follows that $g^2 | z$.

putting $x_1 = x/g \quad y_1 = y/g$,

$$z_1 = z/g^2$$

we see that x_1, y_1, z_1 are the integer that satisfy ② and that have the further property that x_1 & y_1 are relatively prime.

Thus x_1^2, y_1^2, z_1^2 is a primitive pythagorean triple.

By interchanging x_1 & y_1, if necessary, we may arrange that x_1 is odd and y_1 is even.

Then I relatively prime the integers r & s,

$$x_1^2 = r^2 - s^2 \quad \text{—— ③}$$

$$y_1^2 = 2rs \quad \text{—— ④}$$

$$z_1^2 = r^2 + s^2 \quad \text{—— ⑤}$$

Here r & s are of opposite parity, and to determine which one is odd,

we observe from ③ that s, x_1, r is a primitive pythagorean triple.

Hence r is odd and s is even.

In view ④, we may with $u = r$ & $v = 2s$.

Thus I opposite integers b & c I $r = c^2, \quad s = 2b^2$

Taking $a = x_1$.

we see from ③ that a, b, c is a solution of ① in the integers

Moreover, using ⑤ we see that

$$c \leq c^4 = r^2 < r^2 + s^2 = z_1 \leq z \quad \text{— ⑥}$$

Now suppose that a, b, c are the integers that satisfy ①.

put $h = g.c.d(b, c)$.

Then $h^4 \mid a^2$ & Hence $h^2 \mid a$.

putting $a_1 = a/h^2$, $b_1 = b/h$

$c_1 = c/h$.

we find that a_1, b_1, c_1 are the integers satisfying ① which have the further property that b_1 & c_1 are relatively prime.

Thus $a_1, 2b_1^2, c_1^2$ constitute a primitive pythagorean triple.

Then ∃ relatively prime integers r', s' of opposite parity ∋

$$a_1 = r'^2 - s'^2 \quad \text{—— ⑦}$$

$$b_1^2 = r's' \quad \text{—— ⑧}$$

$$c_1^2 = r'^2 + s'^2 \quad \text{—— ⑨}$$

Then by ⑧.

we see that ∃ the integers x' and y' ∋ $r' = x'^2$, $s' = y'^2$.

Setting $z' = c_1$.

we conclude by ⑨ that x', y', z' is a solution of ② in the integers.

Here $z' \leq c$ & hence by ⑥.

we see that $z' < z$.

Thus the set of values of z arising in the integers contains a least element.

It follows that the set of such z is empty.

i.e) ② has no solution in the integers.

Hence proved.

Fermat's last Theorem, or Fermat's big theorem:-

This is one of Fermat's most famous results.

From it we see that at once that the equation

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

has no solutions in the integers.

Fermat's asserted, more generally, that if n is an integer, $n > 2$, then the equation

$$x^n + y^n = z^n$$

has no solutions in the integers.

This proposition, though still a conjecture for many values of n, is known as Fermat's last thm or Fermat's big thm. as contrasted with Fermat's little thm.

We treat the case $n = 3$ using simple ideas in algebraic number theory.

Simultaneous Linear Equation:

Let $a_1, a_2 \cdots a_n$ be integers not all 0, and suppose we wish to find all solutions in integers of the equation.

$$a_1 x_1 + \cdots + a_n x_n = c$$

We may S.T such solutions exists iff g.c.d $(a_1 \cdots a_n)$ divides c.

The numerical technique exposed in the preceding section also extends easily to larger values of n.

Ex:

Find all solutions in integers of

$$2x + 3y + 4z = 5$$

soln:

We write, $2x + 3y + 4z = 5$

2	3	4	5
1	0	0	
0	1	0	
0	0	1	

$\longrightarrow$

2	1	0	5
1	-1	-2	
0	1	0	
0	0	1	

$$\begin{matrix} 0 & 1 & 0 & 5 \\ 3 & -1 & -2 & \\ -2 & 1 & 0 & \\ 0 & 0 & 1 & \end{matrix}$$

This last array represents simultaneous equation involving 3 new variables say (t, u, v).

The first lines gives the condition $u = 5$.

On substituting this in the lower lines we find that every solutions of the given equation in integer may be expressed in the form.

$$x = 3t - u - 2v$$
$$y = -2t + u + 0$$
$$z = v$$

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

where t & v are integers.

From the nature of the changes of variables made.

w.k.t Triples (x, y, z) of integers satisfying the given equation are in 1-1 correspondence with triples of integers (t, u, v) for which $u = 5$.

Hence each solution of the given equation in integers is given by a unique pair of integers (t, v).

Ex:

Find all solutions in integers of the simultaneous equations

$$20x + 44y + 50z = 10$$
$$17x + 13y + 11z = 19$$

Soln:

Among the coefficients of x, y & z the co-efficients 11 is smallest.

using operation (C1) and the division algorithm, reduce the co-efficients of x & y in the second row (mod 11).

20	44	50	10	−80	−6	50	10
17	13	11	19	−5	2	11	19
1	0	0	→	1	0	0	
0	1	0		0	1	0	
0	0	1		−2	−1	1	

The co-efficients of least absolute value is now in the second row and second column.

We use operation (C1) to reduce the other co-efficients in the second row (mod 2).

	−98	−6	80	10
→	1	2	1	19
	1	0	0	
	3	1	−5	
	−5	−1	6	

There are now two co-efficients of minimal absolute value.

We use the one in the first column as our pivot and use operation (C1) to reduce the other co-efficients in the second row.

	−98	190	178	10
→	1	0	0	19
	1	−2	−1	
	3	−5	−8	
	−5	9	11	

The co-efficients of least non zero absolute value is changed, so we switch to operation (R1) to reduce the co-efficient −98 (mod 1) and then we use (R2) to interchanging the two rows.

	0	190	178	1872
→	1	0	0	19
	1	−2	−1	
	3	−5	−8	
	−5	9	11	

	1	0	0	19
→	0	190	178	1872
	1	−2	−1	
	3	−5	−8	
	−5	9	11	

We now ignore the first row and first column. Among the remaining co-efficients, the one of least non-zero absolute value is 178. We use operation (C1) to reduce the 190 (mod 178), obtaining a remainder 12. Then we use (C1) to reduce 178 (mod 12) obtaining a remainder -2.

$$\begin{matrix} 1 & 0 & 0 & 19 \\ \to\ 0 & 12 & 178 & 1872 \\ 1 & -1 & -1 & \\ 3 & 3 & -8 & \\ -5 & -2 & 11 & \end{matrix} \quad \to \quad \begin{matrix} 1 & 0 & 0 & 19 \\ 0 & 12 & -2 & 1872 \\ 1 & -1 & 14 & \\ 3 & 3 & -53 & \\ -5 & -2 & 41 & \end{matrix}$$

Next we use (C2) reduce 12 (mod 2). Then we use (C4) to interchange the second and third columns, and finally use (C3) to replace -2 by 2.

$$\begin{matrix} 1 & 0 & 0 & 19 \\ \to\ 0 & 0 & -2 & 1872 \\ 1 & 83 & 14 & \\ 3 & -315 & -53 & \\ -5 & 244 & 41 & \end{matrix} \quad \to \quad \begin{matrix} 1 & 0 & 0 & 19 \\ 0 & -2 & 0 & 1872 \\ 1 & -14 & 83 & \\ 3 & 53 & -315 & \\ -5 & -41 & 244 & \end{matrix}$$

Let the variables in our new set of equations be called t, u & v.

The two original equations have been replaced by the two new equations

$$1.t = 19, \quad \& \quad -2.u = 1872.$$

This fixed the values of t & u. Series $1 \mid 19$ & $2 \mid 1872$. These values are integers $t = 19$, $u = 936$. With these values for t & u the bottom three rows above given the equation.

$$n = t - 14u + 83v = 83v - 13085$$

$$y = 3t + 53u - 315v = -315v + 49665$$

$$z = -5t - 41u + 244v = 244v - 38471$$

By making the further change of variable $w = v - 158$ we may adjust the constant terms, so that

$$x = 83w + 29$$

$$y = -315w - 105$$

$$z = 244w + 81$$

As integral solutions of the given equations are in 1-1 correspondence with integral values of w, we have achieved our goal.

19. Suppose that $n>0$, and let $N(n)$ denote the number of solutions of the congruence $S^2=(-1)(\text{mod}\, n)$. Then prove that $r(n)=4N(n)$, and $R(n)=\sum r(n/d^2)$ where the sum is extended over all those positive d for which d^2/n.

20. Find all solutions in integers of the simultaneous equations $20x+44y+50z=10$; $17x+13y+11z=19$.

S.No. 6044 **P 16 MAE 5 C**

(For candidates admitted from 2016–2017 onwards)

M.Sc. DEGREE EXAMINATION, APRIL 2019.

Mathematics – *Elective*

ALGEBRAIC NUMBER THEORY

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20)

Answer ALL questions.

1. State Division Algorithm.

2. Let $f(x)=x^2+x+7$. Find all roots of the congruence $f(x)=0(\text{mod}\, 15)$.

3. State Hensel's lemma.

4. Define : Order of modulo m.

5. Define : Quadratic non-residue modulo m.

6. Define : Legendre symbol $\left(\frac{a}{p}\right)$.

7. Define : class number of d.

8. State Mobius inversion formula.

9. Write down the three row operations to alter the coefficients of the equation.

10. Define : Unimodular matrix.

SECTION B — (5 × 5 = 25)

Answer ALL the questions.

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

Or

(b) Prove that the product of any K consecutive integers is divisible by $K!$.

12. (a) Show that 1763 is composite.

Or

(b) Solve : $x^2 + x + 47 \equiv 0 \pmod{7^3}$.

13. (a) The order of an element of a finite group G is a division of the order of the group. If the order of the group is denoted by n, then prove that $a^n = e$ for every element a in the group.

Or

(b) State and prove Gauss lemma.

14. (a) Show that an odd prime p can be written in the form $p = x^2 - 2y^2$ if and only if $p \equiv \pm 1 \pmod 8$.

Or

(b) Prove that for every positive integer n, $\sum_{d/n} \varphi(d) = n$.

15. (a) Find all solutions in integers of $2x + 3y + 4z = 5$.

Or

(b) Prove that the equation $x^3 + 2y^3 + 4z^3 = 9W^3$ has no non trivial solution.

SECTION C — (3 × 10 = 30)

Answer any THREE questions.

16. State and prove the Chinese remainder theorem.

17. If p is an odd and g is a primitive root modulo p^2 then prove that g is a primitive root modulo p^α for $\alpha = 3, 4, 5\ldots$

18. If p and q are distinct odd primes, then prove that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$.