IDHAYA COLLEGE FOR WOMEN, KUMBAKONAM.

DEPARTMENT OF MATHEMATICS

CLASS	*: II M.Sc., MATHS*
SUBJECT NAME	*: ALGEBRAIC NUMBER THEORY*
SUBJECT CODE	*: P16MAE5C*
SEM	*: IV*
UNIT	*: V*
FACULTY NAME	*: Mrs.V.JAYAPRIYA*

UNIT – V

5.1 THE EQUATION $ax + by = c$

1. Theorem: Let a, b and c be integers with not both a and b equal to zero, and let $g = g.c.d.(a,b)$. If $g \nmid c$ then the equation $ax + by = c$ has no solutions in integers. If g/c then this equations has infinitely many solutions. If the pair (x_1, y_1) is one integral solution, then all others are of the form $x = x_1 + kb/g,\ y = y_1 - ka/g$ where k is an integer.

Proof : Consider the equation $ax + by = c$.Let us find all the solutions of the equation in which x and y are integers. If $a = b = c = 0$, then the pair (x, y) of integers is a solution of $ax + by = c$, whereas if $a = b = 0$ and $c \neq 0, ax + by = c$ has no solution.

Now suppose that at least one of a and b is nonzero, and let $g = g.c.d.(a,b)$. If $g \nmid c$ then the equation $ax + by = c$ has no solutions. [∵ a|b and a|c inply a|*(bx+cy)* for any integers x and y].

On the other hand by known theorem , there exists integers x_0, y_0 such that $ax_0 + by_0 = g$,and hence if g|c the by n the pair $(cx_0/g\ , cy_0/g)$ is an integral solution of $ax + by = c$. We may find x_0, y_0 by applying Euclidean algorithm. Once a single solution is known, say $ax_1 + by_1 = c$, the other solution are given by taking $x = x_1 + kb/g$, $y = y_1 - ka/g$. Here k is an arbitrary integer. Thus $ax + by = c$ has infinitely many integral solutions if it has one.

Next to show that $ax + by = c$ has no integral solutions beyond the ones we have already found. For suppose that the pairs $(x_1, y_1), (x, y)$ are integral solutions of $ax + by = c$.

By subtracting , we find that $a(x - x_1) + b(y - y_1) = 0$. We divide through by g and rearrange that $(a/g)(x - x_1) = (b/g)(y_1 - y)$

That is,$a\ /\ g$ divides the product $(b/g)(y_1 - y)$. But $(a/g\ , b/g) = 1$. [By theorem, If $d/a\ and\ d/b\ and\ d > 0, then\ \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$. If $(a, b) = g, then\ \left(\frac{a}{g}\ , \frac{b}{g}\right) = 1$ and If $c\ /\ ab$ and $(b, c) = 1\ then\ c/a$.]

It follows that $a\ /\ g$ divides $(y_1 - y)$. That is, $ka/g = (y_1 - y)$ for some integer k. On substituting this in the equation , we have $(x - x_1) = kb/g$.

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

Solution :

By division algorithm, $999 = 20\ .\ 49 + 19$.

Writing the equation in the form $19x - 49(y - 20x) = 5000$.

Putting $x' = x, y' = -20x + y$. The original equation is expressed by the condition $19x' - 49y' = 5000$.

Since $49 = 2\ .\ 19 + 11$,we write this equation as $19(x' - 2y') - 11y' = 5000. (i.e.,) 19x'' - 11y'' = 5000$ where $x'' = x' - 2y'$ and $y'' = y$.

Since $19 = 2\ .\ 11 - 3$, we write this equation as $-3x'' - 11(-2x'' + y'') = 5000$. $(i.e.,) - 3x^{(3)} - 11y^{(3)} = 5000$ where $x^{(3)} = x''$ and $y^{(3)} = (-2x'' + y'')$.

As $11 = 4\ .3 - 1$,we write the equation as $-3\left(x^{(3)} + 4y^{(3)}\right) + y^{(3)} = 5000. (i.e.,) - 3x^{(4)} + y^{(4)} = 5000$. where $x^{(4)} = x^{(3)} + 4y^{(3)}$ and $y^{(4)} = y^{(3)}$.

Making the change of variables $x^{(5)} = x^{(4)}, y^{(5)} = -3x^{(4)} + y^{(4)}$.

The original equation is equivalent to the equation $y^5 = 5000$. The value of $y^{(5)}$ is a fixed integer, and $x^{(5)}$ is an arbitrary integer. Since the pairs (x, y) are in one –to-one correspondence with pairs of integers $(x^{(5)}, y^{(5)})$, it follows that the original equation has infinitely many solution in integers.

To express $xand\ y$ explicitly in terms of $x^{(5)}and\ y^{(5)}$, we first determine $xand\ y$ in terms of $x^{'}and\ y^{'}$, then in terms of $x^{''}$ and $y^{''}$, and so on. These transformations can be developed at the same time the original equation is being simplified. We start by writing

$$\begin{aligned} &999x - 49y = 5000, \\ &x \qquad\qquad = x, \qquad\qquad \dashrightarrow \ (1) \\ &\qquad\quad y = y\ . \end{aligned}$$

Then we rewrite these equations in the form

$$\begin{aligned} &19x - 49(-20 + y) = 5000, \\ &x \qquad\qquad\qquad = x, \qquad\qquad \dashrightarrow \ (2) \\ &20x + (20x + y) \quad = y. \end{aligned}$$

That is,

$$\begin{aligned} &19x' - 49y' = 5000, \\ &x\ ' \qquad\quad = x, \qquad\qquad \dashrightarrow \ (3) \\ &20x^{'} + \quad y' \ = y. \end{aligned}$$

We rewrite this as

$$\begin{aligned} &19(x^{'} - 2y^{'}) - 11y' = 5000, \\ &x - 2y^{'} \qquad + 2y' \ = x, \qquad \dashrightarrow \ (4) \\ &20(x^{'} - 2y^{'}) \ + 41y' \ = y. \end{aligned}$$

That is

$$\begin{aligned} &19x'' - 11y'' = 5000, \\ &x^{''} + 2y'' \quad = x, \qquad\qquad \dashrightarrow \ (5) \\ &20x^{''} + 41y' = y. \end{aligned}$$

We write this as

$$\begin{aligned} &-3x^{''} - 11(-2x^{''} + y^{''}) \ = 5000, \\ &5x^{''} \ + 2(-2x^{''} + y^{''}) \quad = x, \qquad \dashrightarrow \ (6) \\ &102x'' + 41(-2x'' + y'') = y. \end{aligned}$$

That is

$$\begin{aligned} &-3x^{(3)} - 11y^{(3)} \ = 5000, \\ &5x^{(3)} + 2y^{(3)} \quad = x, \qquad\qquad \dashrightarrow \ (7) \end{aligned}$$

$$102x^{(3)} + 41y^{(3)} = y.$$

We write this as

$$\begin{aligned} (-3x^{(4)} + y^{(4)}) &= 5000, \\ -49x^{(4)} - 18(-3x^{(4)} + y^{(4)}) &= x, \qquad \dashrightarrow \ (8) \\ -999x^{(4)} - 367(-3x^{(4)} + y^{(4)}) &= y. \end{aligned}$$

That is

$$\begin{aligned} y^{(5)} &= 5000, \\ -49x^{(5)} - 18\,y^{(5)} &= x, \qquad \dashrightarrow \ (9) \\ 999x^{(5)} - 367y^{(5)} &= y. \end{aligned}$$

Inserting this value of $y^{(5)}$, and writing k in place value of $x^{(5)}$, we conclude that the solutions of the proposed equation are given by taking

$$x = -49k - 9000,$$

$$y = -999k - 1835000$$

This parameterization of the solution is not unique. For example we set $k = -1837 - m$,the above equations become

$$x = 49m + 13$$

$$y = 999m + 163.$$

3. Find all integers x and y such that $\mathbf{147x + 258y = 369}$.

Solution: (Short form of previous problem)

We write

$$\begin{array}{ccc} 147 & 258 & 369 \\ 1 & 0 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 147 & 111 & 369 \\ 1 & -1 & \\ 0 & 1 & \end{array} \rightarrow \begin{array}{ccc} 36 & 111 & 369 \\ 2 & -1 & \\ -1 & 1 & \end{array} \rightarrow$$

$$\begin{array}{ccc} 36 & 3 & 369 \\ 2 & -7 & \\ -1 & 4 & \end{array} \rightarrow \begin{array}{ccc} 0 & 3 & 369 \\ 86 & -7 & \\ -49 & 4 & \end{array}$$

Let the variables that are implicit in this last array be called $u\ and\ v$.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 $u\ and\ v$ were obtained from the original variables $x\ and\ y$ by homogeneous change of coordinates.

We may reduce the size of the constant term by introducing an homogeneous change of variables. For example, if we put $u = t + 10$, then we find $x = 86t - 1, y = -49t + 2$.

5.2 SIMULTANEOUS LINEAR EQUATIONS

4. Find all solutions of integers of $\boldsymbol{2x + 3y + 4z\ = 5.}$

Solution:

We write

$$\begin{array}{cccc} 2 & 3 & 4 & 5 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \rightarrow \begin{array}{cccc} 2 & 1 & 0 & 5 \\ 1 & -1 & -2 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \rightarrow$$

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

This last array represents simultaneous equations involving three new variables , say t, u, v. The first line gives the condition $u = 5$. On substituting this in the lower lines, we find that every solution of the given equation in integers mat be expressed in the form

$$\begin{aligned} x &= 3t - 2v - 5 \\ y &= -2t \qquad + 5 \\ z &= \qquad v \end{aligned}$$

Where t *and* v are integers. We know that the triples (x, y, z) of integers satisfying the given equation are in one-to-one 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 part of integers (t, v).

5. Find all solutions of integers $\boldsymbol{20x + 44y + 50z = 10}$ **,** $\boldsymbol{17x + 13y + 11z = 19}$**.**

Solution:

Among the coefficients of x, y *and* z, the coefficient 11 is smallest. Using operation $(C1)$ and the division algorithm, reduce the coefficients of x *and* y in the second row $(mod 11)$

We write

$$\begin{array}{cccc} 20 & 44 & 50 & 10 \\ 17 & 13 & 11 & \\ 1 & 0 & 1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \rightarrow \begin{array}{cccc} -80 & -6 & 50 & 10 \\ -5 & 2 & 11 & 19 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ -2 & -1 & 1 & \end{array} \rightarrow$$

The coefficient of least absolute value is now in the second row and second column. We use operation $(C1)$ to reduce the other coefficients in the second row $(mod\ 2)$.

$$\begin{array}{cccc} -98 & -6 & 80 & 10 \\ 1 & 2 & 1 & 19 \\ 1 & 0 & 0 & \\ 3 & 1 & -5 & \\ -5 & -1 & 6 & \end{array}$$

There are now two coefficients of minimal absolute value. We use the one in the first column as our pivot and use the operation $(C1)$ to reduce the other coefficients in the second row

$$\begin{array}{cccc} -98 & 190 & 178 & 10 \end{array}$$

$$\begin{array}{cccc} 1 & 0 & 0 & 19 \\ 1 & -2 & -1 & \\ 3 & -5 & -8 & \\ -5 & 9 & 11 & \end{array}$$

The coefficient of least nonzero absolute value is unchanged, so we move to operation $(R1)$ to reduce the coefficient $-98\ (mod 11)$ and then we use $(R2)$ to interchange the two rows.

$$\begin{array}{cccc} 0 & 190 & 178 & 1872 \\ 1 & 0 & 0 & 19 \\ 1 & -2 & -1 & \\ 3 & -5 & -8 & \\ -5 & 9 & 11 & \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 0 & 19 \\ 0 & 190 & 178 & 1872 \\ 1 & -2 & -1 & \\ 3 & -5 & -8 & \\ -5 & 9 & 11 & \end{array} \rightarrow$$

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

$$\begin{array}{cccc} 1 & 0 & 0 & 19 \\ 0 & 12 & 178 & 1872 \\ 1 & -1 & -1 & \\ 3 & 3 & -8 & \\ -5 & -2 & 11 & \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 0 & 19 \\ 0 & 12 & -2 & 1872 \\ 1 & -1 & 14 & \\ 3 & 3 & -53 & \\ -5 & -2 & 41 & \end{array} \rightarrow$$

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

$$\begin{array}{cccc} 1 & 0 & 0 & 19 \\ 0 & 0 & -2 & 1872 \\ 1 & 83 & 14 & \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 0 & 19 \\ 0 & 2 & 0 & 1872 \\ 1 & -14 & 83 & \end{array} \rightarrow$$

$$\begin{array}{ccc} 3 & -315 & -53 \\ -5 & 244 & 41 \end{array} \qquad\qquad \begin{array}{ccc} 3 & 53 & -315 \\ -5 & -41 & 244 \end{array}$$

Let the variables in our new set of equations be called $t, u, and\ v$. The two original equations have been replaced by h two new equations 1 t = 19 and 2 u = 1872. This fixes the values of t and u. Since 1 |19 and 2 |1872 these values are integers: t = 19 and u = 936. With these values for t and u the bottom three rows above give the equations.

$$x = t - 14u + 83v = 83v - 13085$$
$$y = 3t - 53u - 315v = 315v + 49665$$
$$z = -5t - 41u + 244v = 244v - 38471$$

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

$$x = 83w + 29$$
$$y = -315w - 105$$
$$z = 244w + 81$$

6. Find all solutions of the simultaneous congruences

$\boldsymbol{3x + 3z \ \equiv 1(mod\ 5), 4x - 3y + z \equiv 1(mod\ 5).}$

Solution:

We construct an array of coefficients . Using operation $(C1)$,we add the third column to both columns 1 and 2.

$$\begin{array}{cccc} 3 & 0 & 3 & 1 \\ 4 & -1 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \quad \begin{array}{c} \\ \rightarrow \\ \\ \\ \\ \end{array} \quad \begin{array}{cccc} 1 & 3 & 3 & 1 \\ 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{array} \quad \begin{array}{c} \\ \rightarrow \\ \\ \\ \\ \end{array}$$

Using $(R1)$, we multiply the second row by 2 and add the result to the first row. Then we interchange the first and third columns and the first and second rows.

$$\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 1 & \\ 0 & 1 & 0 & \\ 1 & 1 & 1 & \end{array} \rightarrow$$

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

$$\begin{array}{cccc} 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 1 & \\ 0 & 1 & 0 & \\ 1 & 3 & 1 & \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 0 & 1 & 2 & \\ 0 & 0 & 1 & \\ 1 & 1 & 3 & \end{array} \rightarrow$$

Thus we arrive at a new system of congruences, in cariable t, u, v say. We see that $t \equiv 3\ (mod\ 5)$, $u \equiv 2\ (mod\ 5)$. While $v$can take any value $(mod\ 5)$. Thus the given system has five solutions, given by

$$x \equiv u + 2v \ \equiv 2v + 2\ (mod\ 5),$$
$$y \equiv \quad v \quad \equiv v\ \ (mod 5)\ \ ,$$

7. If the system of linear equations

$$\boldsymbol{a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1,}$$

$$\boldsymbol{a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2,} \qquad \longrightarrow (1)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$\boldsymbol{a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m,}$$

has a real solution, and if the system of congruences

$$\boldsymbol{a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1\ (mod\ q)\ ,}$$

$$\boldsymbol{a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \ (mod\ q)}, \qquad \longrightarrow (2)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$\boldsymbol{a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \ (mod\ q)}$$

has a solution for every modulus q, then the equations (1) have an integral solution.

Solution:

Suppose a particular row operation, applied to the $m \times n$ matrix $A,$ gives the matrix $A^{'}$. Let R denote the matrix obtained by applying this same row operation to the $m \times m$ identity matrix $I_{m.}$ Then $A^{'} = RA$. We call such a matrix R an elementary row matrix. Note that the elementary row matrices form a proper subset of the elementary row matrices defined over R.

Similarly, if a particular column operation takes $A\ to\ A^{''}\ and\ I_n\ to\ C$, then $A^{''} = AC$ and we call C an elementary column matrix. Thus the sequence of row and column operations that we have performed in our reduction process may be expressed by matrix multiplication,

$$R_g R_{g-1} \ldots R_2 R_1 A C_1 C_2 \ldots C_{h-1} C_h = D \qquad \longrightarrow (1)$$

Where D is an $m \times n$ diagonal matrix . The matrix V allows us to express the original variables X in terms of our new variables Y is constructed by applying the same column operations to the identity matrix . That is,

$$V = C_1 C_2 \ldots C_{h-1} C_h \qquad \longrightarrow (2)$$

Similarly, the new constant terms B' obtained at the end of the reducyion process are created by applying the row operations to the original set B of constant terms, so that

$$B^{'} = R_g R_{g-1} \ldots R_2 R_1 B \qquad \longrightarrow (3)$$

8. Define Unimodular

Definition: A square matrix U with integral elements is called unimodular if det $(U) = \pm 1$.

9. Theorem: Let U be an be an $m \times m$ matrix with integral elements. Then the following are equivalent:

(i) U is unimodular

(ii) The inverse matrix U^{-1} exists and has integral elements

(iii) U may be expressed as a product of elementary row matrices $U = R_g R_{g-1} \dots R_2 R_1$.

(iv) U may be expressed as a product of elementary column matrices $U = C_1 C_2 \dots C_{h-1} C_h$.

Solution:

(i) $\Rightarrow (\boldsymbol{ii})$

From the definition of adjoint matrix U^{adj} it is evident that if U has integral elements then so does U^{adj} . Since $U^{-1} = \frac{U^{adj}}{\det(U)}$ it follows that U^{-1} has integral elements if det $(U) = \pm 1$.

$(\boldsymbol{ii}) \Longrightarrow (\boldsymbol{i})$

Since $UU^{-1} = I$, it follows that $\det(U)\det(U^{-1}) = \det(I) = 1$. But $\det(U)$ is an integer if U has integral elements,so from (ii) we deduce that both $\det(U)$ and $\det(U^{-1})$ are integers. That is $\det(U)$ divides 1. As the only divisors of 1 are $\pm$ 1. It follows that U is unimodular.

$(\boldsymbol{iii}) \Longrightarrow (\boldsymbol{i})$

We know that the product of two unimodular matrices is again unimodular. Thus $U = R_g R_{g-1} \dots R_2 R_1$. Then U is unimodular.

$(\boldsymbol{i}) \Longrightarrow (\boldsymbol{iii})$

If A is an $m \times n$ matrix with integral elements then there exist elementary row matrices such that $A = R_g R_{g-1} \dots R_2 R_1 T$ $\qquad \longrightarrow (1)$

Where T is an upper – triangular $m \times n$ matrix with integral elements. We proceed as in Gaussian elimination , except the row operations $(R1), (R2) and$ $(R3)$. We apply these row operations to A as follows. In the first column containing nonzero elements, say the first column , we apply the division algorithm and $(R1)$ until only one elemnetin this column is non zero. By means of $(R2)$ we may replace this non zero entry in the first row, By $(R3)$. we may arrange that this element is positive. We now repeat this process on the columns to the right of the one just considered, but we ignore the first row. Thus the second column operated on may have two non zero elements in the first and second rows. Continuing in this manner , we arrive at an upper triangular matrix T. That is $T = R_g R_{g-1} \dots R_2 R_1 A$ for suitable elementary row matrices $R_{i.}$

Hence $A = R_1^{-1} R_2^{-1} \dots R_{g-1}^{-1} R_g^{-1} T$. Since the inverse of an elementary row matrix is again an elementary row matrix. Take $A = U \; in \; (i)$, we deduce that $\det(T) = \pm 1$. But since T is upper-triangular , $\det(T)$ is the product of its diagonal elements. As these diagonal elements are non negative integers, it follows thatr each diagonal element is 1. We may now apply row operation $(R1) \; to \; T$ to clear all entries above diagonal, leaving us with the identity matrix I_m. That is T is the product of elementary row matrices, and hence by (i) , so also is U.

$\boldsymbol{(i) \implies (iv)}$

Alternatively , we observe that R is an elementary row matrix if and only if R' is an elementary column matrix. If U is unimodular then U' is unimodular and by (iii) we deduce that $U = R_g R_{g-1} \dots R_2 R_1$ for suitable elementary row matrices R_i. Hence $U = R_1^t R_2^t \dots R_{g-1}^t R_g^t$, a product of column matrices.

5.3 PYTHAGOREAN TRIANGLES

10. Lemma: If u and v are relatively prime positive integers whose product uv is a perfect square, then u and 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. Since $u \; and \; v$ are relatively prime , p does not divide v, and hence $p^\alpha \parallel uv$. But uv is a perfect square , so 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

11. Theorem : The equation $\boldsymbol{x^3 + 2y^3 + 4z^3 = 9w^3}$ has no non trivial solution.

Proof: We show that the congruence $x^3 + 2y^3 + 4z^3 = 9w^3\ (mod\ 27)$ has no solution for which $g.c.d.(x, y, z, w, 3) = 1.$ We note that for any integer $a, a^3 \equiv 0\ or\ \pm 1\ (mod\ 9).$

Thus $x^3 + 2y^3 + 4z^3 = 9w^3\ (mod\ 9)$ implies that $x \equiv y \equiv z \equiv 0\ (mod\ 3).$ But then $x^3 + 2y^3 + 4z^3 = 9w^3\ (mod\ 27)$, so that $3\ /\ w^3$. Hence $3/w.$ This contradicts the assumptions that $g.c.d.(x, y, z, w, 3) = 1.$

12. Theorem : The Diophantine equation $\boldsymbol{x^4 + x^3 + x^2 + x + 1 = y^2}$ has the integral solutions $\boldsymbol{(–1, 1), (0, 1), (3, 11)}$, and no others.

Proof: Put $f(x) = 4x^4 + 4x^3 + 4x^2 + 4x + 4.$

Since $f(x) = (2x^2 + x)^2 + 3(x + 2/3)^2 + 8/3$, it follows that $f(x) > (2x^2 + x)^2$ for all real x. On the other hand , $f(x) = (2x^2 + x + 1)^2 – (x + 1)(x + 3)$. Here the last term is positive except for those real numbers x in the interval $I = [-1,3]$. That is $f(x) < (2x^2 + x + 1)^2$ provided that $x \notin I$., Then $f(x)$ lies between two consecutive perfect squares, namely $= (2x^2 + x)^2\ and\ (2x^2 + x + 1)^2$.

Hence $f(x)$ cannot be a perfect square , except possibly for those integers $x\epsilon\ I$

. ***************