ALGEBRAIC NUMBER THEORY [P16MAE5C]

M.Sc., MATHEMATICS - APRIL 2019

Subject Incharge : Ms. A. HELEN SHOBANA

Class : II - M.Sc., MATHEMATICS

SECTION - A (10 x 2 = 20)

1) State Division Algorithm:

Given any integers a and b, with a>0, there exist unique integers q and r such that b=qa+r, 0≤r<a. If a∤b, there r satisfies the stronger inequalities 0<r<a.

2) Let $f(x) = x^2+x+7$. Find all the roots of the Congruence $f(x) \equiv 0 \pmod{15}$

Solution:

Given, $x^2+x+7 \equiv 0 \pmod{15}$

Here, $15 = 3^1 \times 5^1$

Let $x = 0, \pm 1, \pm 2$.

Then, $f(x) \equiv 0 \pmod 5$ has no solution

Since $5 \mid 15$.

Therefore $x^2+x+7 \equiv 0 \pmod{15}$ has no solution.

3) State Hensel's lemma:

Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

4) Define : order of a modulo m:

Let m denote a positive integer and a any integer such that $(a, m) = 1$. Let h be the smallest positive integer such that $a^h \equiv 1 \pmod{m}$.

We say that the order of a modulo m is h, or that a belongs to the exponent h modulo m.

5) Define : Quadratic non residue modulo m:

For all a such that $(a, m) = 1$, a is called a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If it has no solution, then a is called a quadratic non-residue modulo m.

6) Define : Legendre symbol (a/p)

If p denotes an odd prime, then the legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue, -1 if a is a quadratic non residue modulo p, and 0 if $p \mid a$.

7) Define : Class number of d:

If d is not a perfect square then the number of equivalence classes of binary quadratic forms of discriminant d is called the class number of d, denoted $H(d)$.

8) State Mobius inversion formula:

If $F(n) = \sum_{d \mid n} f(d)$ for every positive integer n,

then $f(n) = \sum_{d \mid n} \mu(d) F(n/d)$.

9) Write down the three row operations to alter the coefficients of the equations:

(R1) Add an integral multiple m of one equation to another.

(R2) Exchange two equation.

(R3) Multiply both sides of an equation by -1.

10) Define unimodular matrix:

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

SECTION - B (5×5 = 25)

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

Proof:

By the thrm:

If g is the greatest common divisor of b and c, then thre exist Integers x_0 and y_0 Such that $g = (b,c) = bx_0 + cy_0$.

there exist Integers x_0, y_0, x_1, y_1 such that $1 = ax_0 + my_0 = bx_1 + my_1$..

Thus we may write $(ax_0)(bx_1) = (1 - my_0)(1 - my_1) = (1 - my_2)$ where y_2 is defined by the equation $y_2 = y_0 + y_1 - my_0y_1$..

From the equation $abx_0x_1 + my_2 = 1$ we note, by the thrm.

a|b and a|c Imply $a|(bx + cy)$ for any Integers x and y.

that any common divisor of ab and m is a divisor of 1 and hence $(ab, m) = 1$.

Hence proved.

11) b) Prove that the product of any k consecutive integers is divisible by k!.

Proof:

The product as $n(n-1)\ldots(n-k+1)$. If $n \geq k$, then we write this in the form $\binom{n}{k} k!$ and note that $\binom{n}{k}$ is an integer.

By the theorem: 1

Let S be a set containing exactly n elements. For any non-negative integer k, the number of subsets of S containing precisely k elements is $\binom{n}{k}$.

If $0 \leq n < k$, then one of the factors of our product is 0, so the product vanishes.

And it is therefore a multiple of k!

Finally, if $n < 0$, we note that the product may be written,

$$(-1)^k (-n)(-n+1)\cdots(-n+k-1) = (-1)^k \binom{-n+k-1}{k} k!$$

In this the upper member $-n+k-1$ is at least k, So that the theorem I, the binomial Coefficient is an integer.

In this formula for the binomial coefficients is an integer, that we note a symmetry,

$$\binom{n}{k} = \binom{n}{n-k}$$

This is also evident from the combinatorial interpretation.

Since the subsets of A containing k elements are in one-to-one correspondence with the complementary subsets.

$S \setminus A = \{ i \in S : i \notin A \}$ Containing $n-k$ elements.

---

12)a) Show that M_{63} is Composite.

Solution:

By fermet's Congruence, if p is an odd prime number, then $a^{p-1} \equiv 1 \pmod{p}$

If n is an odd prime for which $2^{n-1} \not\equiv 1 \pmod{n}$ then n is composite.

Now, $2^{1763-1} \equiv 1 \pmod{1763}$

$$2^{1762} \equiv 1 \pmod{1763}$$

Here $a^k = 2^{1762}$

$$k = \sum 2^i$$

$$1762 = 2^{10} + 2^9 + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2$$

$$d_j = a^{2^j}.$$

$$2^{2^0} = 2^1 \equiv 2 \pmod{1763}$$

$$2^{2^1} = 2^2 \equiv 4 \pmod{1763}$$

$$2^{2^2} = 2^4 \equiv (2^2)^2 = 4^2 \equiv 16 \pmod{1763}$$

$$2^{2^3} = 2^8 = (2^4)^2 = 16^2 \equiv 256 \pmod{1763}$$

$$2^{2^4} = 2^{16} = (2^8)^2 = 256^2 = 65536$$

$$\equiv 305 \pmod{1763}$$

$$2^{2^5} = 2^{32} = (2^{16})^2 = (305)^2 = 93025$$

$$\equiv 1349 \pmod{1763}$$

$$2^{2^6} = 2^{64} = (2^{32})^2 = (1349)^2 = 1819801$$

$$\equiv 285 \pmod{1763}$$

$2^{2^4} = 2^{128} = (2^{64})^2 = (385)^2 = 148225$

$\equiv 133 \pmod{1763}$

$2^{2^8} = 2^{256} = (2^{128})^2 = (133)^2 = 17689$

$\equiv 59 \pmod{1763}$

$2^{2^9} = 2^{512} = (2^{256})^2 = (59)^2 = 3481$

$\equiv 1718 \pmod{1763}$

$2^{2^{10}} = 2^{1024} = (2^{512})^2 = (1718)^2 = 2951524$

$\equiv 262 \pmod{1763}$

$\therefore 2^{1762} \equiv 262 \cdot 1718 \cdot 133 \cdot 385 \quad 13494 \pmod{1762}$

$\equiv 551 \cdot 133 \quad 385 \quad 13494 \pmod{1762}$

$\equiv 1000 \cdot 385 \cdot 13494 \pmod{1763}$

$\equiv 666 \cdot 1349 \cdot 4 \pmod{1763}$

$\equiv 1067 \cdot 4 \pmod{1763}$

$2^{1762} \equiv 742 \pmod{1763}$

We calculate that $2^{1763} \equiv 742 \pmod{1763}$

and deduce that 1763 is Composite.

Hence proved.

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

Solution:

Let $f(x) = x^2 + x + 47$

$f(1) = 49 \equiv 0 \pmod 7$

$f(2) \not\equiv 0 \pmod 7$

$f(3) \not\equiv 0 \pmod 7$

$f(4) \not\equiv 0 \pmod 7$

$f(5) = 77 \equiv 0 \pmod 7$

$f(6) \not\equiv 0 \pmod 7$

$\therefore x \equiv 1 \pmod 7$ & $x \equiv 5 \pmod 7$ are the only solution of $x^2 + x + 47 \equiv 0 \pmod 7$

Now $f(x) = 2x + 1$

$f'(1) = 3 \not\equiv 0 \pmod 7$

$f'(5) = 11 \not\equiv 0 \pmod 7$

$\therefore$ The roots 1 and 5 are non singular.

Now $a_{j+1} = a_j - f(a_j) \cdot \bar{f}(a_j) \pmod{p^{j+1}} \rightarrow (1)$

Where,

$f'(a)\, \bar{f}'(a) \equiv 1 \pmod p$

$f'(1)\, \bar{f}'(1) \equiv 1 \pmod 7$

Scanned by TapScanner

$$f^{-1}(1) = 5$$

and

$$f'(5)\, f'(\bar{5}) \equiv 1 \pmod{7}$$

$$f'(5) = 2$$

for $j=1$ & $a_1 = 1$

① $\Rightarrow a_2 = a_2 f'(a_1) f'(\bar{a}) \pmod{p^2}$

$\Rightarrow a_2 = 1 - f(1) f'(1) \pmod{7^2}$

$a_2 = 1 - 49(5) \pmod{49}$

$a_2 = -244 \pmod{49}$

$= -48 \pmod{49}$

$= 1 \pmod{49}$

for $j=2$ & $a_2 = 1$.

① $\Rightarrow a_3 = a_2 - f(a_2) f'(\bar{a}) \pmod{p^3}$

$a_3 = 1 - f(1) f'(\bar{1}) \pmod{7^3}$

$a_3 \equiv 1 - (49)(5) \pmod{343}$

$a_3 \equiv -244 \pmod{343}$

$a_3 \equiv 99 \pmod{343}$

Scanned by TapScanner

For $j=1$ x $a_1 = 5$, $a = 5$

$(1) \Rightarrow a_2 \equiv a_1 - f(a_1)\, f'(\bar{a}) \pmod{p^2}$

$a_2 \equiv 5 - f(5)\, f'(\bar{5}) \pmod{7^2}$

$a_2 \equiv 5 - (77)(2) \pmod{49}$

$a_2 \equiv -149 \pmod{49}$

$a_2 \equiv 47 \pmod{49}$

For $j = 2$ and $a_2 = 47$, $a = 5$.

$(1) \Rightarrow a_3 = a_2 - f(a_2)\, f'(\bar{a}) \pmod{p^3}$

$a_3 = 47 - f(47)\, f'(\bar{5}) \pmod{7^3}$

$= 47 - (2303 \times 2) \pmod{343}$

$= -4559 \pmod{343}$

$a_3 \equiv 100 \pmod{343}$

$a_3 \equiv 243 \pmod{343}$

This means 243 is a root of the polynomial.

$f(x) \equiv 0 \pmod{7^3}$

$x^2 + x + 47 \equiv 0 \pmod{7}$

Therefore 99 and 243 are the desired roots.

Hence proved.

Scanned by TapScanner

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

Proof:

Let the element a have order r.

$$e, a, a^2, a^3 \ldots a^{r-1} \quad \rightarrow (1)$$

It is readily seen that (1) are r distinct elements of G. If these r elements do not exhaust the group, there is some other element say b_2.

Then we can prove that,

$$b_2, b_2a, b_2a^2, b_2a^3 \ldots b_2a^{r-1} \rightarrow (2)$$

are r distinct elements, all different from the elements of A.

For in the first place if $b_2a^s = b_2a^t$, then $a^s = a^t$ by the theorem: I

In any group G, $ab = ac$ implies $b = c$, and likewise $ba = ca$ implies $b = c$. If a is any element of a finite group G with identity element e, then there is a unique smallest positive integer r such that $a^r = e$.

And on the other hand, if $b_2 a^s \cdot a^t$, then $b_2 = a^{t-s}$, so that b_2 would be among the powers of a.

If G_1 is not exhausted by the sets A and B, then there is another element b_3 that gives rise to r new elements.

$$b_3,\ b_3a,\ b_3a^2,\ b_3a^3 \ldots\ b_3a^{r-1}.$$

all different from the elements in A and B.

This process of obtaining new elements $b_2, b_3 \ldots$ must terminate since G is finite. So if the last batch of new elements is, say

$$b_k,\ b_k a,\ b_k a^2,\ b_k a^3 \ldots\ b_k a^{r-1}.$$

then the order of the group G is kr and the first part of the theorem is proved.

To prove the second part, we observe that $n = kr$ and $a^r = e$ by the theorem I, hence $a^n = e$

Hence proved.

Scanned by TapScanner

13) b) State and prove the Gauss lemma:

Statement:

For any odd prime p let $(a,p)=1$. Consider the integers $a, 2a, 3a \ldots, \{(p-1)/2\}a$ and their least positive residues modulo p. If n denotes the number of these residues that exceed $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^n$.

Proof:

Let $r_1, r_2 \ldots r_n$ denote the residues that exceed $\frac{p}{2}$.

Let $s_1, s_2 \ldots s_k$ denote the remaining residues.

The r_i and s_i are all distinct, and none is zero.

Furthermore, $n+k = (p-1)/2$.

Now $0 < p - r_i < p/2$, $i = 1, 2 \ldots n$ and the number $p - r_i$ are distinct.

Also no $p - r_i$ is an s_j for if $p - r_i = s_j$ then $r_i \equiv Pa$, $s_j = \sigma a \pmod p$ for some P, σ, $1 \le P \le (p-1)/2$, $1 \le \sigma \le (p-1)/2$, and

$p - Pa \equiv \sigma a \pmod p$.

Since $(a,p)=1$ this implies $a(p+\sigma)\equiv 0$,

$p+\sigma \equiv 0 \pmod{p}$.

Which is impossible:

Thus $p-r_1, p-r_2 \ldots p-r_n, s_1, s_2 \ldots s_k$ are all distinct, are all atleast 1 and less than $p/2$; and they are $n+k = (p-1)/2$ in number.

That is, they are just the integers

$1, 2 \ldots (p-1)/2$ in some order.

Multiplying them together we have,

$$(p-r_1)(p-r_2)\ldots(p-r_n)s_1 s_2 \ldots s_k = 1.2\ldots\frac{p-1}{2}.$$

and then

$$(-r_1)(-r_2)\ldots(-r_n)s_1 s_2 \ldots s_k \equiv 1.2\ldots\frac{p-1}{2} \pmod{p}$$

$$(-1)^n r_1 r_2 \ldots r_n s_1 s_2 \ldots s_k \equiv 1.2\ldots\frac{p-1}{2} \pmod{p}$$

$$(-1)^n a.2a.3a\ldots\frac{p-1}{2}a \equiv 1.2\ldots\frac{p-1}{2} \pmod{p}$$

We can cancel the factors $2, 3 \ldots (p-1)/2$ to obtain $(-1)^n a^{(p-1)/2} \equiv 1 \pmod{p}$. which gives as

$$(-1)^n \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$ By the theorem

Let p be an odd prime. Then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

Hence Proved.

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

Solution:

The quadratic form $f(x,y) = x^2 - 2y^2$ has discriminant $d = 8$ which is not a perfect square.

We first determine all reduced forms of this discriminant.

From this theorem,

Let f be a reduced binary quadratic forms whose discriminant d is not a perfect square. If f is indefinite, then $0 < |a| \leq \frac{1}{2}\sqrt{d}$. If f is positive definite then $0 < a \leq \sqrt{d/3}$. In either case, the number of reduced forms of a given non square discriminant d is finite.

We have $|a| \leq \sqrt{2}$, so that $a = \pm 1$.

From this definition:

Let f be a binary quadratic form whose discriminant d is not a perfect square. we call f reduced if $-|a| < b \leq |a| < |c|$.

we deduce that $b = 0$ or 1.

Scanned by TapScanner

But b and d always have the same parity. So we must have $b=0$. Thus we find that there are precisely two reduced forms of discriminant 8, namely f and $-f$.

Let $M = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}$.

We observe that $\det(M) = 1$, so that $M \in \Gamma$.

Taking this M in this definition,

The quadratic forms $f(x,y) = ax^2 + bxy + y^2$ and $g(x,y) = Ax^2 + Bxy + cy^2$ are equivalent, and we write $f \sim g$, if there is an $M = [m_{ij}] \in \Gamma$ such that $g(x,y) = f(m_{11}x + m_{12}x + m_{22}y)$. In this case we say that M takes f to g.

We find that $f \sim -f$.

Thus $H(8) = 1$.

By this corollary,

Suppose that $d \equiv 0$ or $1 \pmod 4$. If p is an odd prime, then there is a binary quadratic form of discriminant d that represents p, if and only if $p \mid d$ or $\left(\frac{d}{p}\right) = 1$.

Scanned by TapScanner

It follows that p is represented by f if and only $\left(\frac{2}{p}\right) = 1$.

And we obtain the stated result by this quadratic reciprocity.

If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)/2 \cdot \frac{1}{2}(q-1)/2}$$

Hence showed.

---

(4)b Prove that for every positive integer n,

$$\sum_{d|n} \phi(d) = n.$$

Proof:

Let F(n) denote the sum on the left side of the proposed identity.

From this theorem,

If m_1 and m_2 denote two positive, relatively prime integers, then $\phi(m_1, m_2) = \phi(m_1)\phi(m_2)$.

Moreover, if m has the canonical factorization $m = \prod p^{\alpha}$, then $\phi(m) = \prod_{p|m} (p^{\alpha} - p^{\alpha-1}) = m \prod_{p|m} (1 - 1/p)$.

Scanned by TapScanner

We see that $\phi(n)$ is multiplicative.

Thus $F(n)$ is multiplicative, by this theorem,

Let $f(n)$ be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then $F(n)$ is multiplicative.

Since the right side ~~=~~ n, is also a multiplicative function, to establish that $F(n) = n$ for all n it suffices to prove that $F(p^\alpha) = p^\alpha$ for all prime powers p^α.

From this theorem,

The Canonical factorization of n in the form

$$n = 2^\alpha \prod p^\beta \prod q^\gamma$$
$$p \equiv 1(4) \quad q \equiv 3(4)$$

Then n can be expressed as a sum of two squares of integers if and if all the exponents γ are even.

We can see that $\beta > 0$ then, $\phi(p^\beta) = p^\beta - p^{\beta-1}$.

Scanned by TapScanner

Thus,

$$F(p^\alpha) = \sum_{d \mid p^\alpha} \phi(d).$$

$$= \sum_{\beta=0}^{\alpha} \phi(p^\beta)$$

$$= 1 + \sum_{\beta=1}^{\alpha} p^\beta - p^{\beta-1}$$

$$= p^\alpha.$$

Hence proved.

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

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 equation involving three new variables say t, u, v.

Scanned by TapScanner

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

On substitution, this in the lower lines, we find that every solution of the given equation in integers may be expressed in the form,

$$x = 3t - 2v - 5$$

$$y = -2t + 5$$

$$z = v.$$

where t and v are integers.

From the nature of the changes of variables, we know that triples (x, y, z) of integers.

It satisfying the given equation are in one-one correspondence with triples of integers (t, v, u) for which $u = 5$.

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

Scanned by TapScanner

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

Proof:

We show that Congruence $x^3+2y^3+4z^3 \equiv 9w^3 \pmod{27}$ has no solution for which g.c.d $(x,y,z,w,3)=1$.

For any integer a, $a^3 \equiv 0$ or $\pm 1 \pmod 9$.

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

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.

Scanned by TapScanner

SECTION-C.

(6) State and prove the Chinese remainder theorem.

Statement:

Let $m_1, m_2 \ldots m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, a_2 \ldots a_r$ denote any r integers. Then the Congruences,

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r} \rightarrow (1)$$ have common solutions.

If x_0 is one such solution, then an integer x satisfies the congruences (1) if and only if x is of the form $x = x_0 + km$ for some integer k. Here $m = m_1, m_2 \ldots m_r$.

Proof:

Writing $m = m_1, m_2 \ldots m_r$, we see that m/m_j is an integer and that $(m/m_j, m_j) = 1$.

Scanned by TapScanner

Hence by this theorem,

If $(a,m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$

for each j there is an integer b_j such that

$(m/m_j)\, b_j \equiv 1 \pmod{m_j}$.

Clearly $(m/m_j)\, b_j \equiv 0 \pmod{m_i}$ if $i \neq j$.

Put $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$

We consider this number modulo m_i and find that

$$x_0 \equiv \frac{M}{m_i} b_i a_i \equiv a_i \pmod{m_i}$$

Thus x_0 is a solution of the system.

If x_0 and x_1 are two solutions of the system ①, then $x_0 \equiv x_1 \pmod{m_i}$ for $i = 1, 2 \ldots r$.

Hence $x_0 \equiv x_1 \pmod{m}$ by this theorem

$x \equiv y \pmod{m_i}$ for $i = 1, 2 \ldots r$ if and only if

$x \equiv y \pmod{[m_1, m_2 \ldots m_r]}$.

This completes the proof.

Scanned by TapScanner

17) Prove that if p is an odd prime and g is a primitive root modulo p^2, then g is a primitive root modulo p^α for $\alpha = 3, 4, 5 \ldots$

Proof:

Suppose that g is a primitive root $(\text{mod } p^2)$ and that h is the order of g $(\text{mod } p^\alpha)$ where $\alpha > 2$.

From the congruence $g^h \equiv 1 \ (\text{mod } p^\alpha)$ and deduce that $g^h \equiv 1 (\text{mod } p^2)$.

Hence that $\phi(p^2) \mid h$.

By Corollary.

If $(a, m) = 1$, then the order of a modulo m divides $\phi(m)$.

We also know that $h \mid \phi(p^\alpha)$.

Thus $h = p^\beta(p-1)$ for some β ~~along~~ among $\beta = 1, 2 \ldots$ or $\alpha = 1$.

To prove that $\beta = \alpha - 1$, it suffices to show that,

$$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \ (\text{mod } p^\alpha) \rightarrow (A)$$

Scanned by TapScanner

We use induction to show that this holds for all $a \geq 2$.

By hypothesis, the order of $g \pmod{p^2}$ is $\phi(p^2) = p(p-1)$.

Hence $g^{p-1} \not\equiv 1 \pmod{p^2}$ and we have (A) when $\alpha = 2$.

By fermat's congruence, $g^{p-1} \equiv 1 \pmod{p}$, so we may write $g^{p-1} = 1 + b_1 p$ with $p \nmid b_1$.

By the binomial theorem,

$$g^{p(p-1)} = (1 + b_1 p)^p = 1 \cdots \binom{p}{1} b_1 p + \binom{p}{2} b_1^2 p^2 + \cdots$$

Since $p > 2$ by hypothesis, $\binom{p}{2} = p(p-1)/2 \equiv 0 \pmod{p}$.

Hence the above is $\equiv 1 + b_1 p^2 \pmod{p^3}$.

This gives (A) when $\alpha = 3$.

Thus we may write $g^{p(p-1)} = 1 + b_2 p^2 \pmod{p^3}$ with $p \nmid b_2$.

We raise both sides of this to the pth power and repeat this procedure to find that $g^{p^2(p-1)} \equiv 1 + b_2 p^3 \pmod{p^4}$, which gives (A) for $\alpha = 4$.

Scanned by TapScanner

Continuing in this way, we conclude that (A) holds for all $a \geq 2$.

Then the proof is complete.

18) Prove that, if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.$$

Proof:

Let S be the set of all pairs integers (x, y) satisfying $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$.

The set S has $(p-1)(q-1)/4$ members.

Seperate this set into two mutually exclusive subsets S_1 and S_2 accordingly as $qx > py$ or $qx < py$.

There are no pairs (x, y) in S such that $qx = py$.

The set S_1 can be described as the

Scanned by TapScanner

Set of all pairs (x,y) such that $1 \le x \le (p-1)/2$,

$1 \le y < qx/p$.

The number of pairs in S_1 is then seen to be $\sum_{x=1}^{(p-1)/2} [qx/p]$.

Similarly, S_2, consists of the pairs (x,y) Such that $1 \le y \le (q-1)/2$, $1 \le x < py/q$.

And the number of pairs in S_2 is,

$\sum_{y=1}^{(q-1)/2} [py/q]$.

Thus we have,

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{pj}{q}\right] = \frac{p-1}{2}\ \frac{q-1}{2}.$$

and hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}.$$

Hence proved.

Scanned by TapScanner

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

Proof:

Consider any solution $x^2+y^2 = n$, where $n>0$. Of the four points,

$(x,y), (-y,x), (-x,-y), (+y,-x)$, exactly one of them has a first co-ordinate and non-negative second co-ordinate.

Let $P(n)$ denote the number of proper representations $x^2+y^2 = n$ for which $x>0$ and $y>0$.

Then $r(n) = 4P(n)$.

We now prove that $P(n) = N(n)$.

For this first we define a function from the appropriate pairs (x,y) to the appropriate residue classes $s \pmod{n}$.

Second, we show that this function is one to one.

Third, we prove that the function is onto.

To define the function:

Suppose that x and y are integers such that $x^2+y^2 = n$, $x>0$, $y\geq 0$, and $gcd(x,y) = 1$.

Then $g.c.d(x,y) = 1$, so there exists a unique $s \pmod n$ such that $xs \equiv y \pmod n$.

Since $x^2 \equiv -y^2 \pmod n$ on multiplying both side of $x^2 \equiv -y^2 \pmod n$.

we deduce that $s^2 \equiv -1 \pmod n$.

Our function is one to one:

Suppose that for $i = 1, 2$ we have

$n = x_i^2 + y_i^2$, $x_i > 0$, $y_i \geq 0$, $g.c.d(x_i, y_i) = 1$

and $x_i s_i \equiv y_i \pmod n$.

We show that if $s_1 \equiv s_2 \pmod n$, then $x_1 \equiv x_2$ and $y_1 \equiv y_2$.

Suppose that $s_1 \equiv s_2 \pmod{n}$

As $x_1 y_2 s_1 \equiv y_1 y_2 \equiv x_2 y_1 s_2 \pmod{n}$,

it follows that $x_1 y_2 \equiv x_2 y_1 \pmod{n}$.

Since g.c.d $(s_i, n) = 1$.

But $0 < x_i^2 \leq n$, so that $0 < x_i \leq \sqrt{n}$, and

Similarly $0 \leq y_i \leq \sqrt{n}$.

As these two number are congruent modulo n and both lie in the inferval $[0, n)$ we conclude that $x_1 y_2 = x_2 y_1$.

Thus $x_1 | x_2 y_1$.

But g.c.d $(x_1, y_1) = 1$, so it follows that $x_1 | x_2$.

Similarly $x_2 | x_1$.

As the x_i are positive we deduce that $x_1 = x_2$ and hence $y_1 = y_2$.

This completes the proof that our function is one-to-one.

Scanned by TapScanner

Now show that the function is onto:

For each s such that $s^2 \equiv -1 \pmod{n}$, there is a representation $x^2+y^2=n$ for which $x>0$, $y \geq 0$, $(x,y)=1$ and $xs \equiv y \pmod{n}$

Then there is an integer c such that $(2s)^2 - 4nc = -4$.

Thus $g(x,y) = nx^2 + 2sxy + cy^2$ is a positive definite binary quadratic form of discriminant.

Thus there is a matrix $M \in I$ that takes the form $f(x,y) = x^2+y^2$ to the form g.

We see that $m_{11}^2 + m_{21}^2 = n$.

Moreover $g.c.d\ (m_{11}, m_{21}) = 1$.

Since $\det(M) = m_{11}m_{22} - m_{21}m_{12} = 1$

We see that $s = m_{11}m_{12} + m_{21}m_{22}$.

Hence,

$$m_{11}s = m_{11}^2 m_{12} + m_{11}m_{21}m_{22}$$

$$= -m_{21}^2 m_{12} + m_{11}m_{21}m_{22} \pmod{n}$$

(Since $m_{11}^2 \equiv -m_{21}^2 \pmod{n}$)

Scanned by TapScanner

$= -m_{21}^2 m_{12} + m_{21}(1 + m_{21} m_{12})$

(Since $m_{11} m_{22} - m_{21} m_{12} = 1$)

$= m_{21}$.

If in addition $m_{11} > 0$ and $m_{21} \geq 0$, then it suffices to take $x = m_{11}$, $y = m_{21}$.

From the congruences $m_{11} s \equiv m_{21} \pmod{n}$, $s^2 \equiv -1 \pmod{n}$.

we deduce that $(-m_{21}) s \equiv m_{11} \pmod{n}$.

Thus $xs \equiv y \pmod{n}$ in any of these cases.

This completes the proof that $r(n) = 4N(n)$.

To Prove the last assertion of the theorem:

If $x^2 + y^2 = n > 0$ and $d = \gcd(x, y)$.

then $(x/d)^2 + (y/d)^2 = n/d^2$ is a proper representation of n/d^2.

Conversely, if $d > 0$,

$d^2 | n$ and $u^2 + v^2 = n/d^2$ is a proper representation of n/d^2, then $(du)^2 + (dv)^2 = n$ is a representation of n with $g.c.d\ (x, y) = d$.

Scanned by TapScanner

are in one to one correspondence with the proper representations of n/d^2.

20 Find all solutions in integers of the simultaneous equations.

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

Solution:

Among the coefficients of x, y, z the coefficient of 11 is smallest.

Using C_1 operation and the division algorithm, reduce the coefficients of x and 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 coefficient of least absolute value is now in the second row and second column.

Scanned by TapScanner

We use operation C_1 to reduce the other coefficient in second row (mod 2)

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

There are now two coefficient of minimal absoulte value.

We use the one in the first column as our pivot and use operation (C_1) to reduce the other one.

$$\begin{matrix} \to & -98 & 190 & 178 & 10 \\ & 1 & 0 & 0 & 19 \\ & 1 & -2 & -1 & \\ & 3 & -5 & -8 & \\ & -5 & 9 & 11 & \end{matrix}$$

The coefficient of least non zero absolute value is unchanged. So we switch to operation (R_1) to reduce the coefficient -98 (mod

Scanned by TapScanner

and then we use (R2) to interchange the two rows.

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

We ignore the first row and first column. Among the remaining coefficients, the one of least non zero absolute value is 178.

We use operation (C_1) to reduce $190 \pmod{178}$ obtaining a remainder 12.

Then we use (C_1) to reduce $178 \pmod{12}$ obtaining a remainder -2.

$$\begin{matrix} 1 & 0 & 0 & 19 \\ 0 & 12 & 178 & 1872 \\ 1 & -1 & -1 & \\ 3 & 3 & -8 & \\ -5 & -2 & 11 & \end{matrix} \rightarrow \begin{matrix} 1 & 0 & 0 & 19 \\ 0 & 12 & -2 & 1872 \\ 1 & -1 & 14 & \\ 3 & 3 & -53 & \\ -5 & -2 & 91 & \end{matrix}$$

Scanned by TapScanner

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

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

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

The two original equations have been replaced by the two new equations $1.t = 19$ and $2.u = 1872$.

This fixes the values t and u.

Since $1 \mid 19$ and $2 \mid 1872$, these values are integers : $t = 19$, $u = 936$.

Scanned by TapScanner

With these values for t and u, the bottom three rows above the given equations.

$x = t - 14u + 83v = 83v - 13085,$

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

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

By making the futher 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 solution of the given equation. are in one - to - one correspondence with integral values of w.

Hence solved.

Scanned by TapScanner