REPRESENTATION OF NUMBERS DIVISIBLE BY A SUFFICIENTLY LARGE SQUARE

MS. CHETNA, DR. HARDEEP SINGH

Abstract: The present paper examines the concept of the representation of integers, say m, by positive ternary quadratic forms $f(x_1, x_2, x_3)$ over the field of integers. In particular, it is proved that every sufficiently large integer is represented by integral positive ternary quadratic form of odd mutually simple invariants, if it satisfies the necessary generating conditions as well as the certain additional conditions related to the method of proof. The first part of the paper deals with some general results and the second part show the representation of numbers divisible by a sufficiently large square.

Keywords: Ternary Quadratic Forms, Representation, Invariants, Characters.

Introduction: Let $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ (1) is the primitive positive ternary quadratic form over the field of integers with odd determinant $\delta, a_{ij}(i, j = 1,2,3)$ are the integers, $a_{ij} = a_{ji}, \det(a_{ij}) = \delta, \gcd(a_{ij}) = 1$. Let $F(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a'_{ij}x_ix_j$ is the ternary quadratic form algebraically similar to the form$f$, where a'_{ij} is a cofactor of the element a_{ij} in the matrix $(a_{ij}), i, j = 1,2,3$. Let d is a divisor of this form such that$f = dF$, where $F$is a primitive form which is mutually primitive to the form f. Then $\delta = d^2k$, where k is an integer and $[d, k]$ is called the invariant of the form f. By Shimura [12] if there is a form $f_1$equivalent to the form f, then

$f_1 \equiv \alpha_1x_1^2 + \alpha_2p^ux_2^2 + \alpha_3p^{u+v}x_3^2(mod p^t)$ (2)

where$\alpha_1, \alpha_2, \alpha_3$ are the integers which are relatively prime to p. Let f be the form with invariants $[d, k], F$ be the certain mutual primitive form. If p be a prime number, then there is an integer m relatively prime to p represent by the form f then the quantity $\mu_p(f) = \left(\frac{m}{p}\right)$ is called the character of f modulo$p$ and set of characters

$\left\{\mu_{p_1}(f), \dots \dots \dots, \mu_{p_{n_1}}(f); \mu_{q_1}(F), \dots \dots \dots, \mu_{q_{n_2}}(F)\right\}$ (3)

is called complete set of characters of the form In all these definitions we assume that f is the primitive integral positive quadratic form with odd determinant. Let $f$and $F$are mutually primitive forms. Also we can say that representation of $f(x_1, x_2, x_3) = m$ and $F(X_1, X_2, X_3) = M$ are called simultaneous if $x_1X_1 + x_2X_2 + x_3X_3 = 0$ (4)

Let f and F are mutually primitive quadratic forms. Let $F(\alpha_1, \alpha_2, \alpha_3) = m$, where number m represented by form F is the submission of the combination of the binary form $\theta(x, y) = f(a_1x + b_1y, a_2x + b_2y, a_3x + b_3y)$ from theform f,if$\begin{cases} a_2b_3 - a_3b_2 = \alpha_1 \\ a_3b_1 - a_1b_3 = \alpha_2 \\ a_1b_2 - a_2b_1 = \alpha_3 \end{cases}$ (5)

For the above definitions and the following results we referred the work of Burton [3], Serre [11], Shimura [12].

Result 1.1: Let $\theta(x, y) = v(px^2 + 2qxy + ry^2)$ be a positive integral binary quadratic form with determinant δ and a divisor $v(w)$ where $w = \gcd(p, q, r), w = w_1w_2$, where $w_1$is square free. Then the number of representations by$\theta(x, y) = f(a_1x + b_1y, a_2x + b_2y, a_3x + b_3y)$ (8)

with respect to positive integral ternary quadratic form f with the additional condition that v divide $\gcd(a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1)$ (9)

are$< \rho_1(\gamma(\delta))^4w_2^{\frac{1}{2}}\left(\gcd(\frac{\delta}{v^2}, v\right)^{\frac{1}{2}}$ (10)

where the constant $\rho_1 > 0$ depends only on the determinant of the form$f$.The next observation can be obtained by using classical results from the arithmetic of quadratic forms (Hahn [6], Elman [5]). However, here we are giving the independent elementary proof.

Result 1.2: Let $f(x_1, x_2, x_3)$ is the integral primitive ternary quadratic form with odd invariant $[d, k]$. Let $d = rd_1$, where $r$is an integer relatively prime to d_1k and let us assume that for every prime number p included in the form of the class r, we have$\left(\frac{-\Delta f}{p}\right) = 1$ (11)

then there exist integers $c_{ij}(i, j = 1,2,3)$, satisfying the equality

$f(x_1, x_2, x_3) = (\sum_{i=1}^{3} c_{1i}x_i, \sum_{i=1}^{3} c_{2i}x_i, \sum_{i=1}^{3} c_{3i}x_i)$ (12)

where$f$ is the ternary form over the field of integers with invariants$[d_1, k], \det(c_{ij}) = r$.

Proof: We now transform the form f into an equivalent form f_1 given as$f_1 = \begin{pmatrix} dka'_{11} & dka'_{12} & dka'_{13} \\ dka'_{21} & da'_{22} & da'_{23} \\ dka'_{31} & da'_{32} & da'_{33} \end{pmatrix}$ (13)

where$a'_{ij} = a'_{ji}$ are the integers. Hence by the condition (11). We can say that there are relatively prime integers $n_{11} and\, n_{21}$ satisfying the equation$(dka'_{11})n_{11}^2 + 2(dka'_{12})n_{11}n_{21} + (dka'_{22})n_{21}^2 \equiv 0(mod r^2)$ (14)

By (13) and (14) therefore, we have$f_2(y_1, y_2, y_3) = \theta(ry_1, y_2, y_3)$ (15)

whereθ is an integral form with invariants $[d_1, k]$. Equation (15) is equivalent to (12), which proves the remark.

Result 1.3: Let F is a positive integral quadratic form with odd co-prime invariants $[d, k]$, f be a mutual primitive form of it and m is a positive integer which is relatively prime to $2dk$, for which the congruence$x_0^2 + \Delta f(x_1, x_2, x_3) \equiv m(mod 2^3 d^2 k)$ (16)

is solvable.

Then$r(\Theta_\mathrm{F}, \mathrm{m}) =$

$$(2^3)\left(\frac{1}{\mathrm{k}^2}\prod_{\frac{\mathrm{k}}{\mathrm{p}}}\frac{1}{1-\frac{1}{\mathrm{p}^2}}\right)\left(\frac{1}{\mathrm{d}}\prod_{\frac{\mathrm{d}}{\mathrm{p}}}\frac{1}{1-\frac{\frac{-\Delta \mathrm{f}}{\mathrm{p}}}{\mathrm{p}}}\right)\left(\mathrm{m}\prod_{\frac{\mathrm{m}}{\mathrm{p}}}\left(1-\frac{1}{\mathrm{p}}\right)\right)+$$

$$0\left(\mathrm{m}^{\frac{3}{4}+\varepsilon}\right)(17)$$

where the constants in O depends only on d, k and arbitrary $\in> 0$ (Kitaoke [8]). Now further by using the result 1.3 we can prove the next result.

Result 1.4: Let F is a positive integral quadratic form with odd co-prime invariants $[d, k]$, let f is a mutual primitive form of it and m is a positive integer relatively prime to $2dk$ for which the congruence (18) holds. Let r and h be positive integers with the condition rhdivides m, all of which are m multipliers included in the form of class r and $\frac{r}{h}$. Let Φ is defined as the class of primitive Hermitian $(mod\, h)$ and R is the primitive Hermitian of norm r.We denote $r(, \Theta_\mathrm{F}, \mathrm{m}, \Phi, \mathrm{R})$ be the number primitive integer m by hermitian M in Θ_F with the condition $M \in \Phi, \frac{\mathrm{M}}{\mathrm{R}}$ (18)

if for some $\theta > 0, r^{38} = O\left(\left(\frac{rm}{h}\right)^{\frac{1}{40}-\theta}\right)$ (19)

then we have

$$r(, \Theta_\mathrm{F}, \mathrm{m}, \Phi, \mathrm{R}) \sim (2^3)\left(\frac{1}{\mathrm{k}^2}\prod_{\frac{\mathrm{k}}{\mathrm{p}}}\frac{2}{1-\frac{1}{\mathrm{p}^2}}\right)\left(\frac{1}{\mathrm{d}}\prod_{\frac{\mathrm{d}}{\mathrm{p}}}\frac{1}{1-\frac{\frac{-\Delta \mathrm{f}}{\mathrm{p}}}{\mathrm{p}}}\right)\left(\frac{\mathrm{m}}{\mathrm{rh}}\frac{1}{\prod_{\frac{\mathrm{r}}{\mathrm{p}}}\left(1-\frac{1}{\mathrm{p}}\right)}\right) \quad (20)$$

where the constants in the equation (20) depend only on d, k & θ.

Proof: By Timothy [13], we can show that if M_1a primitive Hermition of norms is $m_1 = \frac{mg}{h_1} = \frac{mrg}{h}$ and if it satisfies the conditions$M_1 B \equiv 0(mod rg)(21)$

Then $M = M_1 B^{-1} A$ (22)

is also a primitive Hermitian of norm m satisfying the conditions (18) and conversely if M satisfies (18), then M_1 satisfies the condition (21). Thus equation (22) establishes a one-to-one correspondence between primitive Hermitian M_1 of norm m_1 with the condition (21) and primitive Hermitian M of norm m with the condition (18). Let us suppose that $r(, \Theta_\mathrm{F}, \mathrm{m}, \mathrm{B}, \mathrm{R}')$ be the number of representations of such Hermitian M_1, then we can find an asymptotic formula for the number of primitive Hermitian of norms m with the condition (18) lying in a given area and elliptical region belonging to a given class $(mod h)$, where h is relatively prime to $2m$.

On the representation of numbers divisible by a sufficiently large square: Since Ono, Soundararajan [10] and Oliver Robert J. Lemke [9] has focused on the problem of determining ternary quadratic forms which represent every locally represented integer. Assuming the Generalized Riemann Hypothesis they showed that one can effectively find representations by ternary forms with small determinants. They also mentioned that there are always local obstructions in the representations by ternary forms. This motivates us to prove the following theorem which also improves the result of Kane [7].

Theorem 2.1: Let $f(x_1, x_2, x_3)$ is a primitive positive quadratic form over the field of integers with invariants $[d, k]$ which are relatively odd co-prime. Let m is an integer for which there is the primitive congruence$f(x_1, x_2, x_3) \equiv \mathrm{m}(\mathrm{mod}\ 2^3\mathrm{dkm})$ (23)

Then there exists an integer $s_0$depending only on d and k if m is divisible by the square of the integer$s$ where s is greater then s_0 and relatively prime to $2dk$, then the number ⍰ is primitively represented by the form greater than $x_8 g(-km)(24)$.

Proof: Let $q_1 \ldots\ldots\ldots q_t$ are the different powers of prime numbers such that $q = \max(q_1 \ldots\ldots\ldots q_k)$. Then either $t \geq \sqrt{\log s_0}$ and $q \geq t \geq \sqrt{\log s_0}$ or

$t < \sqrt{\log s_0}$ and q$\geq s_0^{\frac{1}{t}} > e^{\sqrt{\log s_0}}$.With the increase in the value of $s_0$the value of $min\left\{\sqrt{\log s_0}\,, e^{\sqrt{\log s_0}}\right\}$ increases upto infinity, and the number s can be replaced by the number q. Let us suppose that $s = \pi^{\varepsilon}$. Moreover, we can assume that either π is bounded by a constant depending only on $d$and k, or s is a prime number. Since the number $\frac{m}{s^2}$satisfies the congruence conditions of f and f has a primitive solution therefore by (23), we have $f(x_1, x_2, x_3) \equiv \frac{m}{s^2}(\text{mod } 2^3\text{dkm})$.Thus for such forms of f there exists form f_1, the number of primitive representations of $\frac{m}{s^2}$ by the form f_1 is greater than $x_1 g\left(-\frac{km}{s^2}\right)$ (Shimura[12]), where $x_1 > 0$is a constant depending only on dk. we get $f_1 f_1(x_1, x_2, x_3) = \frac{1}{r^2} f(\sum_{i=1}^{3} c_{1i}x_i\,, \sum_{i=1}^{3} c_{2i}x_i \sum_{i=1}^{3} c_{3i}x_i)$ (25)

Here $c_{ij}(i, j = 1,2,3)$are integers with $\det(c_{ij}) = r^3$ where integer r relatively prime to $2dk$ depends only on d, k *and* γ. By Chan [4] and Alladi et al. [1] we can also assume the number r simply from s, for otherwise we can find a substitution which has the same properties with the denominator r' which is prime to r since s be a degree of prime number, then we get s simply from r'. So, we can get the number r simply from s. Since each of the form is greater than $x_1 c\left(-\frac{km}{s^2}\right)$ so the primitive representations are$\frac{m}{s^2} = f_1(x_1, x_2, x_3)$ (26)

By the equality (25) we can say that$\frac{mr^2}{s^2} = f(\sum_{i=1}^{3} c_{1i}x_i\,, \sum_{i=1}^{3} c_{2i}x_i \sum_{i=1}^{3} c_{3i}x_i)$ (27)

as the number $\frac{mr^2}{s^2}$ is represented by the form f. Let h be the divisor of this representation. Then h divides r^2. Thus it is obvious that different representations by (26) correspond to different representation by (27). Since r depends only on d, k and γ then there are representations greater than $x_2 g\left(-\frac{km}{s^2}\right)$ of the number $\frac{mr^2}{s^2}$ by the form f with the same divisor h and here $x_2 > 0$ is a constant depends only on d, k and γ. In other words, there is a primitive representation greater than $x_2 g\left(-\frac{km}{s^2}\right)$ of the number $\frac{mr^2}{s^2 g^2}$ by the form f. Since we get r simply from s and as h divides r^2 therefore on setting the values as $r_1 = \frac{r}{\gcd(r,h)}, r_2 = \frac{g}{\gcd(r,h)}$, we have $\frac{mr^2}{s^2 g^2} = m_1 r_1^2, m_1(r_2 s)^2 = m$, where m_1 is an integer, r_1 and r_2 are co-prime integers with the conditions that $r_1$divides r and r_2 divide r^3. Thus we have primitive representations of $m_1 r_1^2 > x_2 g\left(-\frac{km}{s^2}\right)$by the form f. Let F be the mutual primitive form of f with the invariant $[d, k]$. Consider the Hermitian algebra $\mathcal{H}_F$. As indicated above, this algebra has primitive vectors $L = x_1 i_1 + x_2 i_2 + x_3 i_3 > x_2 g\left(-\frac{km}{s^2}\right)$which has norm $m_1 r_1^2$. Since the number $r_1$co-prime with $2dk$ is a quadratic residue $(mod\ k)$ and k are odd numbers, then the congruence $x_0^2 + kf(x_1, x_2, x_3) \equiv r_1(mod\ 2^3 d^2 k^4)$ gives the primitive solution. Therefore for given m we have $\gamma \geq \gamma_0(d, k)$ and there is a primitive Hermitian R_1 of norm r_1. Now we prove that for sufficiently large $s_0 = s_0(d, k)$ and for each vector L there exist the primitive norm $km_1 r_1^2$ which is greater than $x_3 s$ for Q of norm $kr_2 s$. Firstly let the Hermition primitive B on $(mod\ kr_1 r_2 \pi)$ be$\begin{cases} ksr_1 \equiv N(B)(mod\ 2^3 d^2 k^4 \cdot ksr_2 \cdot k^4 r_1^2 r_2^2 \pi^2) \\ divisor\ B'LB(mod\ 2dk^2 r_1 r_2 \pi) = k \\ LB \equiv 0(mod\ R_1) \end{cases}$ (28)

Since $2^3 d^2, k^9, r_1^2$ and $r_2^3 s\pi^2$ are relatively prime pair-wise, and L be a primitive vector, so in order to prove the required result firstly it is sufficient to prove the existence of B_1 with the condition $kr_2 s \equiv N(B_1)(mod\ 2^3 d^2)$ (29)

Secondly, the existence of B_2 primitive $(mod\ k)$ with the condition$\begin{cases} kr_2 s \equiv N(B_2)(mod\ k^9) \\ divisor\ B'_2 LB_2(mod\ k^2) = k \end{cases}$ (30)

Thirdly, the existence of B_3 with the condition $\begin{cases} kr_2 s \equiv N(B_3)(mod\ r_1^2) \\ LB_3 \equiv 0(mod\ R_1) \end{cases}$ (31)

Fourth, the existence of B_4 with the condition$\begin{cases} kr_2 s \equiv N(B_4)(mod\ r_2^3 s\pi^2) \\ B'_4 LB_4\ primitive\ (mod\ r_2 \pi) \end{cases}$ (32)

The existence of a Hermitian B_1 by (29) where $kr_2 s$ and $2d$ are relatively co-prime follows directly from the well-known theorems on Quadratic congruence (Burton [3]). We show that there is a primitive Hermitian $B_2(mod\ k)$ with the condition (30). Let us assume that $F \equiv c_1 z_1^2 + kc_2 z_2^2 + kc_3 z_3^2 (mod\ k^9)$ where d and k are relatively co-prime and integers c_1, c_2, c_3 are prime to k, let us suppose $L = x_1 i_1 + x_2 i_2 + x_3 i_3$ and there exist integers b_2 and b_3 such that (Burton [3])$r_2 s \equiv c_1 c_3 b_2^2 + c_1 c_2 b_3^2 (mod\ k^8)$ (33)

Since $r_2 s$ and k are relatively prime so the first and second condition of (30) immediately follows from the primitiveness of L and by comparing (33). The existence of Hermitian B_3 with the condition (31) hold (kitaoka [8]).. Finally, we prove the existence of Hermitian B_4 with the condition (32). In order to prove this firstly we show that there is a Hermitian B_4^1 for which $\begin{cases} N(B_4^1) \equiv 0(modr_2s) \\ B'^1_4LB_4^1 \ primitive \ (modr_2\varepsilon) \end{cases}$ (34)

Indeed, let p is a prime divisor of r_2s and p^n divides r_2s. Then there exist D such that$\begin{cases} N(D) \equiv 0(mod\ p) \\ D'LD \ primitive \ (mod\ p) \end{cases}$ (35)

Therefore, there exist D with the condition (35) (Kitaoka [8]). Then by the induction on t we consider $C \equiv D(mod\ p)$ such that$N(C) \equiv 0(mod\ p^t)$.Therefore we can find a Hermitian $B_4^{(1)}$ with the condition (34). We choose Hermitian $B_4^{(2)} \equiv B_4^{(1)}(mod\ sr_2)$ such that $N(B_4^{(2)}) \equiv r_2su(mod\ sr_2^3\pi^2)$where the integer u is relativly prime to $r_2\pi$. Finally, we select $B_4^{(3)}$ and then $B_4 = B_4^{(2)}B_4^{(3)}$ satisfy the condition (32). So we found a primitive Hermitian $B(mod\ kr_1r_2\pi)$ from the terms (28). Next we now distinguish two cases. (1) Let $s = \pi^\varepsilon$ and π is bounded by a constant depending only on $d$and k. Then by Shimura[12] for sufficiently large integer $s_0 > x_3s$ there exist primitive Hermitian Q of norm kr_2s for which$Q \equiv B(mod\ k^2r_1r_2\pi)$ (36)

By (28) and (36) there exists a primitive vector $\frac{1}{k}Q'LQ$ and $LQ \equiv 0(mod\ R_1)$. (2)Let$s = \pi$ is a prime number. Then by (Shimura[12]) for a sufficiently large integer $s_0 > x_3s$ there exist primitive Hermitian Q with norm kr_2s for which$Q \equiv B(mod\ k^2r_1r_2)$ (37)

Therefore, for sufficiently large number $s_0 > x_3s$ there exist primitive Hermitian Q with norm kr_2s which in addition to (37) gives the condition$Q'LQ\ primitive\ (mod\ s)$ (38)

By (28), (37) and (38) there are a primitive vector $\frac{1}{k}Q'LQ$and $LQ \equiv 0(mod\ R_1)$. Hence we get primitive representations of the number m greater than $x_8g(-km)$ by the form f.

References:

1. AlladiKrishnaswami , Bhargava Manjul, Savitt David; (Editors), *Quadratic and Higher Degree Forms (Developments in Mathematics),* Springer, (2013).
2. Bhargava Manjul, *Higher composition laws I: A new view on Gauss composition and quadratic generalizations,* Annals of Mathematics, 159 (2004), 223–250.
3. Burton David M., *Elementary Number Theory,* 6th Ed., Tata McGraw-Hill, 2010.
4. Chan W K , Representations of Integral Quadratic Polynomials , 2012.
5. Elman, R. and Lam, T.Y. *Quadratic forms under algebraic extensions.* Math. Ann. 219, (1976), 21-42.
6. Hahn Alexander J., Quadratic Forms over Z from Diophantus to the 290 Theorem, Advances in Applied Clifford Algebras, 18 (2008), 670–676.
7. Kane Ben; *Representations of integers by ternary quadratic forms,* Int. J. of Number Theory, 06, 1, (2010), 127.
8. Kitaoka Yoshiyuki, *Arithmetic of quadratic forms,* Cambridge University Press (1999).
9. Lemke Oliver Robert J., *Representation by ternary quadratic forms,* Bulletin of the London Mathematical Society, 46, No. 6 (2014), 1240-1247.
10. Ono Ken and Soundararajan K., Integers Represented by Ternary Quadratic Forms, Centre de RecherchesMathematique; CRM Proceedings and Lecture Notes Volume 19, 1999.
11. Serre Jean-Pierre, A Course in Arithmetic, Springer-Verlag New York, Inc. 1973.
12. Shimura Goro, Arithmetic of quadratic forms, Springer-Verlag New York, Inc. 2010.
13. Timothy O'Meara, Introduction to Quadratic Forms. Springer-Verlag, 1963, Reprinted in the Classics of Mathematics Series, Springer-Verlag, 2000.

***

Ms. Chetna/Department of Mathematics/ M.M. Modi College/
Patiala/ Punjab/ dhiraj.pbiuniv@gmail.com
Dr. Hardeep Singh/Department of Mathematics/
Government Mahindra College/ Patiala/ Punjab