https://doi.org/10.15415/mjis.2018.62009

Representation of Integers by Form $f(x_1, x_2, x_3)$ Over The Field $\Delta_{f,m}$

CHETNA[1*]

[1] P.G. Department of Mathematics, M.M. Modi College, Patiala, Punjab

[1,*]**Email: chetna.modicollege@gmail.com**

Received: February 4, 2018| Revised: February 16, 2018???| Accepted: February 21, 2018

Published online: March 01, 2018

Abstract This paper deals with the representation by the quadratic form in three variables with odd prime invariants. In this paper a primitive quadratic form over the field of integers with odd invariants is considered and another form mutually primitive to it especially for the case $m \to \infty$ and the field $\Delta_{f,m}$ does not change its form. Then it is proved that the number of representations by form is greater than the number of classes of integral primitive binary quadratic forms.

Keywords: Quadratic Form, Binary Form, Representations, Primes, Odd Invariants.

1. INTRODUCTION

Quadratic forms are homogeneous quadratic polynomials in n variables. In the cases of one, two, and three variables they are called unary, binary, and ternary. The theory of quadratic forms and methods used in the study of quadratic forms depend to the large extent on the nature of the coefficients, which may be real or complex numbers, rational numbers, or integers. It is quite a problem to portray the integer solutions to a quadratic form in several variables. The other problem is to find out which integers are represented by a particular quadratic form Chetna and singh [3].

Chan *et al.* [2] in their paper explained that if *h* is an integer and *A, B, C* are Hermitian where *A* is primitive (mod h). If $AB \equiv 0(mod\, h)$ and $AC \equiv 0(\mathrm{mod}\, h)$, then $BC \equiv 0(mod\, h)$. They also explained that if h = h_1h_2 is an integer where $h_1 \le x_1$ and the integer h_2 prime to det *f* and let *t* be divisor of *A* and $t_1 = \gcd(t, h_2) \le x_2$. Then the number of divisors of Hermitian *A* with norm *h* is bounded above by a constant depending only on x_1 and x_2. Oliver [10] in his paper has focused on the problem of determining when a quadratic form represents every positive integer. He explained that for the quadratic forms in three variables there are always limitations to represent all integers over any field, but then question arise which local integer is represented by this quadratic form. Chetna *et al.* [4] explained the connection between representations of numbers by the quadratic form and solubility of the quadratic form. Further Chetna and Singh [6] gave the representations over the field of p-adic numbers. Further Chetna [7] explained that number of representations by any quadratic form depends mostly on the solution given by that particular form and proved the result that can be used in coding theory to code and decode information and signals for security management.Representation theory plays very important role in the field of mathematics. In the paper (Chetna and Singh [5]), the general hypothesis given by Riemann is considered and found the number of integers represented by forms in three variables with small determinants. This paper deals with the representation by the quadratic form in three variables with odd prime invariants. The following lemmas are used to obtain the desired result.

1.1 Lemma 1[9]: Let *f* be a positive quadratic form in three variables over the field of integers with the determinant δ and let equations are

$$l + L_i = V_i K_i \quad i = 1, \ldots., n \tag{1}$$

where l is an integer, $L_1, \ldots\ldots\ldots, L_n$ are the integral forms with norms m, $K_1, \ldots\ldots\ldots, K_n$ are the proper integral of norm k prime to $2\delta, V_1, \ldots\ldots\ldots, V_n$ are the integral of norm v prime to k. Let the inequalities be (a) $n > x_1 m^{\frac{1}{2}-\in}$, (b) $x_2 m^{\sigma-\in} \le k \le x_3 m^{\sigma+\in}$, (c) $\gcd(m,k) < x_4 m^{\in}$ where $0 < \sigma \le \frac{1}{2}$ are the real numbers and for $x_i > 0, i = 1,2,3,4$ there exist constant $\in > 0$, where $\in$ is an arbitrary real number. Then, the number w among distinct integrals $K_1, \ldots\ldots\ldots, K_n$ is given by $w > x_{\in} m^{\sigma-3\in}$ where $x_{\in} > 0$ constant depending only on $\in, u, x_1, x_2, x_3, x_4$.

1.2 Lemma 2[9]: Let *f* is the positive integral quadratic form in three variables of determinant δ and let the equations be $l + L_i = V_i K_i, (i = 1, \ldots\ldots\ldots, n)$ where l is an integer, $L_1, \ldots\ldots\ldots, L_n$ are the different primitive integrals forms with norms m, $K_1, \ldots\ldots\ldots, K_n$ are the integral forms with norms k prime to 2δ, $V_1, \ldots\ldots\ldots, V_n$ are the integral forms with norm v prime to k. Let $m = m_1 m_2$, where m_1 be square of an integer and m_2 be square-free and $m_1 < x_{17} e^{\sigma_{17}\frac{\sqrt{logm}}{\log(logm)}}$. Let the inequalities

$$n > x_{18} m^{\frac{1}{2}} e^{-\sigma_{18}\frac{\sqrt{logm}}{\log(logm)}} \tag{2}$$

$$x_{19} m^{\mu} e^{-\sigma_{19}\frac{\sqrt{logm}}{\log(logm)}} \le k \le x_{20} m^{\mu} e^{\sigma_{20}\frac{\sqrt{logm}}{\log(logm)}} \tag{3}$$

$$\gcd(m,k) < x_{21} e^{\sigma_{21}\frac{\sqrt{logm}}{\log(logm)}} \tag{4}$$

where μ be a real number, $0 < \mu \le \frac{3}{8}, x_{17}, x_{18}, x_{19} > 0, x_{20} x_{21} x_{22} \sigma_{17} \sigma_{18} \sigma_{19} \sigma_{20} \sigma_{21} \sigma_{22}$ are constants that depend only on δ. Suppose that for different $K_1, \ldots\ldots\ldots, K_n$ there exist distinct w, then $w > x m^{\mu} e^{-\sigma\frac{\sqrt{logm}}{\log(logm)}}$ where $\sigma, x > 0$ are the constants that depend only on δ.

2. REPRESENTATIONS OF INTEGERS BY INTEGRAL FORM $f(x_1, x_2, x_3)$ WHEN $m \to \infty$ AND $\Delta_{f,m}$ RETAINS ITS FORM

Now by using the above lemmas the following theorem gives on the representation by positive quadratic form in three variables with odd prime invariants when $m \to \infty$.

2.1 Theorem: Let $f = f(x_1, x_2, x_3)$ be a positive integral primitive quadratic form in three variables with odd invariant $[d,k]$, $F = F(x_1, x_2, x_3)$ is mutual primitive form with the invariant $[d,k]$. We consider the form $\mathcal{H}_F$. Let r_1 and r_2 are the positive integers and $r = r_1 r_2 > 1$ is prime to $2dk$ and consider A_1 and A_2 be the form with conditions $N(A_1) = 0(mod\, r_1), N(A_1) = 0(mod\, r_1)$ where the form $A_2 A_1$ are primitive over $(mod\ r)$. Let the numbers *m, l, h* of the form L_0 in the field $\Delta_{f,m}$ on the surface of the form in three variables $f(x_1, x_2, x_3)$ with $\gamma > 0$ satisfy the conditions of the theorem. We denote $r_{h,L_0}(\Delta_{f,m}, r_1, A_1, r_2, A_2, l)$ the number of integer for primitive form L with norms km along with the conditions

$$L \equiv L_0(mod\, h), (l+L) A_1 \equiv 0(mod\, r_1), A_1(l+L) \equiv 0(modr_2) \tag{5}$$

Then, if $m \to \infty$ and $\Delta_{f,m}$ retains its form, then

$$r_{h,L_0}(\Delta_{f,m}, r_1, A_1, r_2, A_2, l) > xg(-km) \tag{6}$$

where $x > 0$ is the constant depending only on *k, d, r, h, y* over the field $\Delta_{f,m}$.

2.1.1 Proof: Let us suppose that $s = r^t$. By (Chetna and Singh [5]), we can say that $t = t\,(d, k)$ is the number of primitive form L with norms kms^2 is less than $x_1 g\left(-kms^2\right)$, where $x_1 > 0$ the constant depends only on d and k. Among these forms there are $g' > x_2 g\left(-kms^2\right)$ equivalent to each other, where the constant $x_2 > 0$ depends only on d and k. Let us consider

$$L_1, \ldots\ldots\ldots, L_{g'}, g' > x_2 g\left(-kms^2\right) \tag{7}$$

We show that for sufficiently large m, where $m > m'$ a set of $(d,\ k)$ in (7) can be chosen such that $g > x_3 g\left(-kms^2\right)$ for primitive forms $L_1, \ldots\ldots\ldots, L_n$ with norms kms^2 and have the equations $sl' + L_i = V_i M_i, \left(i = 1, \ldots\ldots\ldots, n, g > x_3 g\left(-kms^2\right)\right)$, where $M_1, \ldots\ldots\ldots, M_g$ are the integral forms with norms $r^w, V_1, \ldots\ldots\ldots, V_g$ are the integral forms with norms v prime to r and for integer w following inequality occurs $x_4 m^{\mu} \le r^w < m^{\mu}$, where μ is the real number such that $0 < x_5 \le \mu \le \frac{2}{2}$ and the constants $x_3 > 0, x_4 > 0,$ and $x_5 > 0$ depend only on $d,\ k$. Here, we assume that the number m is so large such that $m \ge m'^{(1)}(d,k)$ and for $w > 0$ the integer l' satisfies the congruence $l' \equiv l(mod\, r)$. Let $a = \left[\frac{1}{x_2}\right] + 1$ is a positive integer depending only on d,k. Then, by (Burton (1)) we have $g' > \frac{g\left(-kms^2\right)}{a}$.

We define an integer e for the inequalities

$$\frac{1}{r} m^{\frac{1}{8a}} \le r^e < m^{\frac{1}{8a}} \tag{8}$$

and consider integers, $z_0 = r^{2ae}, z_1 = r^{(2a+1)e}, \ldots\ldots\ldots, z_y = r^{(2a+a)e} = r^{3ae}$. Since the number m is so large such that $m \ge m'^{(2)}(d,k,r)$, therefore by (Kane [8]),we have $ea > t$. For each z_i we consider an integer l_i satisfying the following conditions:

$$\gcd\left(\frac{\left(sl_i\right)^2 + kms^2}{z_i}, r\right) = 1, \left(i = 1, \ldots\ldots\ldots, y\right) \tag{9}$$

and by the lemma we can find $z_i \le z_a = r^{3ae} < m^{\frac{3}{8}}, u_i > \frac{m}{z_a} > m^{\frac{5}{8}}, z_i \le u_i\,(i = 0, \ldots\ldots, a)$. Now, consider the primitive classes of positive binary quadratic forms with the determinant kms^2, where $\Phi_j \Theta_\lambda\,(j = 1,\ldots\ldots\ldots, g'; \lambda = 0,1,\ldots\ldots\ldots, a)$. Therefore, by (Niven et al.[9]) there exist fixed pair (λ_0, δ_0) for which we have

$$> \frac{x_2}{(a+1)^2}\, g\left(-kms^2\right) \tag{10}$$

with the condition

$$\Phi_i^{-1}\Phi_j = \Theta_{\lambda_0}\Theta_{\delta_0}^{-1} \tag{11}$$

where $\Phi_i^{-1}\Phi_j$ is the class by the pair (L_i, L_j). By (9) in this class, there is a binary quadratic form (v, sl', r^2) where v relatively prime to r and l' satisfies the equation (3) and $w = e(\lambda_0 - \delta_0)$. Let c be a four-dimensional $(x_0^2 + kf)$ corner in the field. Then by (Chetna and Singh [5]), we have

$$\frac{c}{2\pi^2} = \frac{\gamma''}{4\pi}$$

is the form in the field Ω_W depending only on the form in the region $\Delta''_{f,m}$ and it depends on W and finally on the form in the field $\Delta_{f,m}$. Consider A with condition that $AL \equiv L_0 A, N(A) \equiv r^a \,(mod\, h)$. We choose a primitive form S with norms r^z where z is a constant depending only on *d, k, h, y* in the field $\Delta_{f,m}$ such that $S = RS_{xu}R\ldots\ldots\ldots RS_{1u}R\ldots\ldots\ldots RS_{11}$ for any i and j $(1 \le i \le n, 1 \le j \le u)$. If L is a primitive form with norm km in the field Ψ_i with $L^{(j)}(mod\, h)$, then

$$\begin{cases} \left(S_{ij}R\ldots\ldots\ldots RS_{11}\right)L\left(S_{ij}R\ldots\ldots\ldots RS_{11}\right)^{-1} \in \Delta_{f,m} \\ \left(S_{ij}R\ldots\ldots\ldots RS_{11}\right)L \equiv L_0\left(S_{ij}R\ldots\ldots\ldots RS_{11}\right)(mod\, h) \end{cases} \tag{13}$$

Firstly, consider the form S_{11} with norm $r^{a_1 - 1}$ where a_1 is bounded above by a constant depending only *d, k, h, y* in the field $\Delta_{f,m}$ for which the product RS_{11} is primitive and if a primitive form L with norm km in Ψ_1

with $L^{(1)}(mod\, h)$, then $\begin{cases} S_{11}LS_{11}^{-1} \in \Delta_{f,m} \\ S_{11}L \equiv L_0 S_{11}(mod\, h) \end{cases}$. Now, we choose the number $a_1 = a_1(d,k,h,\Delta_{f,m})$ so large such that there exist a primitive form T_1 with norms r^{a_1} with the following properties: (a) R divides T_1, (b) T_1 belongs to $\Lambda_{L^{(1)}}^{(a_1-1)}$,$(c)T$ belongs to Λ_{W_1}. Let us suppose that $T_1 = RS_{11}$, where S_{11} is a primitive form, then

$$\begin{cases} (S_{12}RS_{11})L(S_{12}RS_{11})^{-1} \in \Delta_{f,m} \\ (S_{12}RS_{11})L \equiv L_0(S_{12}RS_{11})(mod\, h) \end{cases}$$

Since we know that if there is an uncritical integer r over the algebra $\mathcal{H}_F$ and R, M are primitive (mod r) where $N(R) = r$ and r divides $N(M)$. Then there is a hermitian X_0 such that $M(X_0) \equiv 0(mod\, R)$ and X_0R' is primitive (*mod r*). If a hermitian X satisfies the congruence $M(X) \equiv 0(mod\, R)$ then there is an integer X such that $X \equiv uX_0(mod\, R)$. Therefore we have for some positive integer z' depending only on *d, k* and *r* there exist integral primitive form R_1 and R_2 with the conditions by Burton[1]

$$R_1A_1 \equiv 0(mod\, r_1), A_2R_2 \equiv 0(mod\, r_2), N(R_1) = r_1^{z'}, N(R_2) = r_2^{z'} \qquad (14)$$

We show that the form $R = R_1R_2$ with norms $r_1^{z'}r_1^{z'} = r^{z'}$ is primitive. Indeed, if for some prime we have $R_1R_2 \equiv 0(mod\, p)$ then there are three possibilities:

a) If gcd (p, r_2) = 1 and then $R_1 \equiv 0(mod\, p)$, but it contradicts to the existence of R_1.
b) If gcd (p, r_1) = 1 and then $R_2 \equiv 0(mod\, p)$, which also leads to the contradiction.
c) If $p \setminus \gcd(r_1, r_2)$ such that $R_1R_2 \equiv 0(mod\, p)$, $R_1A_1 \equiv 0(mod\, r_1)$, $A_2R_2 \equiv 0(mod\, r_2)$

then we get

$$R'_2\, A_1 \equiv 0(mod\, r_1), A'_1\, R_2 \equiv 0(mod\, r_2), A_2A_1 \equiv 0(mod\, p)$$

which also leads to the contradiction.
Thus $R = R_1R_2$ is a primitive form with conditions (12). Now, we choose an integer $l' = l(mod\, r)$ such that

$$l'^2 + km \equiv 0\left(mod\, r^k\right) \tag{15}$$

This is possible with respect to (84). Let $\Delta'_{f,m} = R_2^{-1}\Delta_{f,m}R_2$ be the result in the field $\Delta_{f,m}$ by using form R_2 with $\Delta'_{f,m}$ which is congruent to $\Delta_{f,m}$. Since $\overline{C^{(\tau)}}L' \equiv 0\left(mod\, s\right)$, then (Shimura [7])

$$L' \equiv 0\left(mod\, s\right), L' = sL'' \tag{16}$$

where L'' is the form with norm km. Thus, the set of primitive form L with norm kms^2 through (13) and (14) mapped into a set of primitive form L'' with norm km. Each form corresponds to L'' be less than equal to x_{13}. So we get value greater than $x_{15}g(-km)$ and the equation

$$L_i'' \equiv L^{(\xi_0)}\left(mod\, h\right) \tag{17}$$

is equal to $g_3 > x_{16}g\left(-km\right)$, where the constant $x_{16} > 0$ depending only on k, d, h, y over the field $\Delta_{f,m}$. Consider the form

$$L'_0 = R_2^{-1(mod\, h)}L_0R_2\left(mod\, h\right)$$

Then, there exists $> xg\ (-km)$ a primitive integral form L' with norm km along the condition

$$L' \equiv L_0'\left(mod\, h\right), \frac{l' + L'}{R_1R_2} \tag{18}$$

Each such form L' has one-to-one correspondence with primitive form $L = R_2LR_2^{-1}$ with norms km with the condition

$$L \equiv L_0\left(mod\, h\right), \frac{l' + L'}{R_1} \tag{19}$$

Now consider $S = S_2RS_1$ where $S_1 = S_{\xi_0\xi_0'}R\ldots\ldots\ldots RS_{11}$ and on combining (16) & (17), we deduce that

$$r_{h,L_0}\left(\Delta_{f,m}, R, l\right) > x_{16}g\left(-km\right)$$

for primitive integral form L_i''', which follows the proof.

3. REFERENCES

[1] Burton David M.(2010), Elementary Number Theory, 6th Ed., Tata McGraw-Hill.

[2] Chan, Wai Kiu and Oh, Byeong-Kweon, Class numbers of ternary quadratic forms, Journal of number theory (Orlando, Fla: Elsevier), **135** (2014).

[3] Chetna and Singh H., Representations by quadratic forms: a review of significant developments, International Journal of Education and applied research (IJEAR), **5(2),** July - Dec 2015.

[4] Chetna, Singh G. and Singh H., Linkage between the integral representation of the elements by quadratic forms and their solutions, Mathematical Sciences International Research Journal, **4(1),** 2015.

[5] Chetna and Singh H., Representation of numbers divisible by sufficiently large squares, Engineering Sciences International Research Journal, **3(2),** 2015.

[6] Chetna and Singh H., Representation by quadratic forms over field of the p-adic numbers, International Journal of Computer Science and Technology, **7(1),** 2016.

[7] Chetna Representation of Quadratic Forms: A Tool for Coding and Cryptography IJECT **8(2),** April - June (2017).

[8]]Kane Ben, Representations of integers by ternary quadratic forms, Int. J. Number Theory, **6(1),** 2010.

[9] Niven, Zuckerman and Montgomery (2010), An Introduction to the Theory of Numbers, 5th Ed., Wiley India Pvt. Ltd.

[10] Oliver Robert J. Lemke, Representation by ternary quadratic forms. Bulletin of the London Mathematical Society **46,** (2014).