Representation of Quadratic Forms: A Tool for Coding and Cryptography

Ms.Chetna
Dept. of Mathematics, M.M. Modi College, Patiala, Punjab, India

Abstract
Number theory has a rich historical background. It is one of the purest areas of mathematics because of the attraction for the representation of integers. For a long time, the study of number theory was the area of pure mathematics without practical applications.It has many applications in the area of geometry, probability theory, quantum mechanics and quantum field theory. The number of representations by any quadratic form depends mostly on the solution given by that particular form.The results of the present paper can be used in coding theory to code and decode information and signals for security management. Application of representation of quadratic forms in Cryptography is just one of the practical applications in computer systems.

Keywords
Number Theory, Quadratic Forms, Coding, Cryptography, Computer System

I. Introduction

Number theory has a rich historical background. It was one of the purest areas of mathematicsbecause of the attraction for the representation of integers. For a long time, the study of number theory was the area of pure mathematics without practical applications.Representations by the quadratic forms are one of the main branches of mathematics. It has many applications in the area of geometry, probability theory, quantum mechanics and quantum field theory. According to the results given by Duke [6], Dickson [5], Alaca [1] and Alaca andWilliams [2], Chetna et al. [4], we have seen that number of representations by any quadratic form depends mostly on the solution given by that particular form. Keeping in view the results the following theorem is being proved. In the following theorem we are particularly considering the case when the prime number is odd. For elementary results, we follow Burton [3] and Niven [7].

Theorem:- Let p is an odd prime, where $\frac{p^u}{z}, u \geq 0$. Let us consider the diagonal form in n variables:

$$f(\alpha_1, \dots\dots\dots, \alpha_n) = \sum_{j=1}^{n} a_j p_j^s \alpha_j^2 (mod p f^{u_s+1}) \qquad (1)$$

where the number of variables $n_1+\cdots+n_s = n$ with their determinants $d_1,\dots\dots\dots,d_s$ are relatively prime to p and $a_1,\dots\dots\dots,a_i$ are the integers which are prime to p for the given $\in_1 \geq 0,\dots\dots\dots,\in_i \geq 0$.

Let $p^{s_1} \setminus \beta_1, \dots\dots\dots, p^{s_i} \setminus \beta_i$ and if $\beta_1 \equiv \cdots \equiv \beta_i \equiv 0(mod p^i)$ hold, then we must have $\beta_i = 0, v_i = \infty, \gamma = \min(u + v_i + e_i)$ where $0 \leq e_1 \leq \cdots \leq e_s$ are pair wise disjoint variables. From here we can implies that if $\beta_1 \equiv \cdots \equiv \beta_i \equiv 0(mod p^i)$ hold, then we have $\gamma=\infty$. Further let B=b(t) be an integer which is determined according to the conditions given below:

$$b(t) = \begin{cases} 0 & if\, t \leq e_1 \leq 2u \\ b\, if\, e_b + 2u < t < e_{b+1} + 2u \\ s & if\, e_s + 2u < t \end{cases} \qquad (2)$$

Then,

1. if $w < 2u + e_1, w < \gamma$, then (3)

$$\mu(p) = 0$$

2. if $\gamma \leq w, \gamma \leq 2u + e_1$, then

$$\mu(p) = p^{-ni+\gamma} \qquad (4)$$

3. if $2u + e_1 < \gamma \leq w$, then

$$\mu(p) = p^{-(n-2)n+s_1+}$$

$$\left(\sum_t (p-1)p^{-ni+t-1-1/2\sum_{n=1}^{b(t)} n_i(t-e_i-2u)}\right)\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2 \sum_{n=1}^{b(t)} n_i(t-e_i)^2}\right) \qquad (5)$$

4. if $2u + e_1 \leq w < \gamma$, then

$$\mu(p) = p^{-(n-2)n+s_1} +$$

$$+\left(\sum_t (p-1)p^{-ni+t-1-1/2\sum_{n=1}^{b(t)} n_i(t-e_i-2u)}\right)\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{n=1}^{b(t)} n_i(t-e_i)^2}\right)$$

$$+\begin{cases} -p^{w-nu-\frac{1}{2}\sum_{n=1}^{b(w+1)} n_i(w+1-e_i-2u)}\left(\prod_{i=1}^{b(w+1)}\left(\frac{d_i}{p}\right)^{w+1-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{n=1}^{b(w+1)} n_i(w+1-e_i)^2}\right), \\ \qquad if \sum_{n=1}^{b(w+1)} n_i(w+1-e_i) \equiv 0(mod2) \\ \left(\frac{-m_1}{p}\right)p^{w-nu-\frac{1}{2}\sum_{i=1}^{b(w+1)} n_i(w+1-e_i-2u)}\left(\prod_{i=1}^{b(w+1)}\left(\frac{d_i}{p}\right)^{w+1-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2(1+\sum_{i=1}^{b(w+1)} n_i(w+1-e_i)^2)}\right) \\ \qquad if \sum_{n=1}^{b(w+1)} n_i(w+1-e_i) \equiv 1(mod2) \end{cases} \quad (6)$$

Proof: - By Chetna et al. [4],we have

$$G'_{p^u,\beta_1,.....,\beta_n}(gf,\mathrm{p^t}) = \begin{cases} p^{-nu}G'(gp^{2u}f,p^t)e^{2\pi i\frac{gf(\beta_1,.....,\beta_n)}{p^t}} if t \leq \gamma \\ 0, \qquad if t > \gamma \end{cases}$$

Therefore

$$A(p^t) = \begin{cases} p^{-n(t+u)}\sum_{g(modp^t)} G'(gp^{2u}f,p^t)e^{2\pi i\frac{gf(\beta_1,.....,\beta_n)}{p^t}} if t \leq \gamma \\ 0, \qquad if t > \gamma \end{cases} \quad (7)$$

For $t \leq \gamma$, we have

$$A(p^t) = p^{-nu-\frac{1}{2}\sum_{i=1}^{b(t)} n_i(t-e_i-2u)}\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{i=1}^{b(t)} n_i(t-e_i)^2}\right)\left(\sum_{g(modp^t)}\frac{g}{p}^{\sum_{i=1}^{b(t)} n_i(t-e_i)} e^{-2\pi i\frac{gp^w m_1}{p^t}}\right) \quad (8)$$

Therefore for $t \geq 1$ the formula (7) and (8) are given by

$$A(p^t) = \begin{cases} 0, if t > \gamma, or if t > w+1 or if t < w+1 \text{ and } \sum_{i=1}^{b(t)} n_i(t-e_i) \equiv 1(mod2) \\ (p-1)p^{t-1-nu-\frac{1}{2}\sum_{i=1}^{b(t)} n_i(t-e_i-2u)}\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{i=1}^{b(t)} n_i(t-e_i)^2}\right), \\ \qquad if t \leq \gamma, t < w+1 \ \sum_{i=1}^{b(t)} n_i(t-e_i) \equiv 0(mod2) \\ \left(-p^{t-1-nu-\frac{1}{2}\sum_{i=1}^{b(t)} n_i(t-e_i-2u)}\right)\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{i=1}^{b(t)} n_i(t-e_i)^2}\right) \\ \qquad if t \leq \gamma, t < w+1 \ \sum_{i=1}^{b(t)} n_i(t-e_i) \equiv 0(mod2) \\ \left(\frac{-m_1}{p}\right)p^{t-\frac{1}{2}-nu-\frac{1}{2}\sum_{i=1}^{b(t)} n_i(t-e_i-2u)}\left(\prod_{i=1}^{b(t)}\left(\frac{d_i}{p}\right)^{t-e_i}\right)\left(i^{\left(\frac{p-1}{2}\right)^2\sum_{i=1}^{b(t)} n_i(t-e_i)^2}\right), \\ \qquad if t \leq \gamma, t < w+1 \ \sum_{i=1}^{b(t)} n_i(t-e_i) \equiv 0(mod2) \end{cases} \quad (9)$$

In particular, when $t \leq \gamma, t \leq 2u + e_1$

$$A(p^t) = \begin{cases} (p-1)p^{t-1-nu}, & if\, t < w+1 \\ -p^{t-1-nu} if\, t = w+1 \end{cases} \quad (10)$$

By using the formula (9), we are able to obtain the value for $\mu(p)$

1. On taking into consideration the case $w \leq \gamma$, $w \leq 2u + e_1$ and by using (9) and (10), we have got the formula (3)

$$\mu(p) = \sum_{t=0}^{\infty} A(p^t) = \sum_{t=0}^{w+1} A(p^t) = \frac{1}{p^{nu}}\left\{1 + \sum_{t=0}^{w}(p-1)p^{t-1} - p^w\right\} = 0$$

2. When we consider $\gamma \leq w$, $\gamma \leq 2u + e_1$, we obtain the formula (4)

$$\mu(p) = \sum_{t=0}^{\infty} A(p^t) = \sum_{t=0}^{\gamma} A(p^t)$$

$$= \frac{1}{p^{nu}}\left\{1 + \sum_{t=0}^{\gamma}(p-1)p^{t-1}\right\}$$

$$= p^{-nu+\gamma}$$

3. On taking $2u + e_1 < \gamma \leq w$, we obtain the formula (5)

$$\mu(p) = \sum_{t=0}^{\infty} A(p^t) = \sum_{t=0}^{2u+e_1} A(p^t) + \sum_{t=2u+e_1+1}^{\gamma} A(p^t)$$

$$= p^{-(n-2)u+e_1} + \sum_{2u+e_1 < t \leq w} A(p^t)$$

4. When we take $2u + e_1 < w \leq \gamma$, we obtain the formula (6)

$$\mu(p) = \sum_{t=0}^{\infty} A(p^t) = \sum_{t=0}^{2u+e_1} A(p^t) + \sum_{t=2u+e_1+1}^{w+1} A(p^t)$$

$$= p^{-(n-2)u+e_1} + \sum_{2u+e_1 < t \leq w} A(p^t) + A(p^{w+1})$$

which proves the result.

Thus, the above theorem concludes that if an odd prime p is not divided by z, then we can say that $u = 0$, $v_i = \infty (i = 1, \ldots\ldots, n)$, $\gamma = \infty$, $m = p^w m_1$, where m_1 is prime to p. Moreover, we also observe that if we take $z = 1$, then there is no need to assume that the diagonal form f is congruent to $(mod\, p^{e_s+1})$. The above given theorem gives the representation of quadratic form for the variables equals to or greater than 4. The results can be used in coding theory to code and decode information and signals for security management. Application of representation of quadratic forms in Cryptography is just one of the practical applications in computer systems.

References

[1] AlacaAyse, Representations by quaternary quadratic forms whose coefficients are 1, 3 and 9, ActaArith., 136, pp. 151-166, 2009.

[2] AlacaAyse, Williams Kenneth S.,"On the Quaternary Forms $x^2 + y^2 + 2z^2 + 3t^2$, $x^2 + 2y^2 + 2z^2 + 6t^2$, $2x^2 + 3y^2 + 6z^2 + 6t^2$ and $x^2 + 3y^2 + 3z^2 + 6t^2$, International J. of Number Theory Vol. 8, No. 7, pp. 1661-1686, 2012.

[3] Burton David M.,"Elementary Number Theory", 6th Ed., Tata McGraw-Hill, 2010.

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

[5] Dickson L.E., Integers represented by positive ternary quadratic forms, Bull. Amer. Math. Soc. 33, pp. 63-70, 1927.

[6] Duke William, Some old problems and new results about quadratic forms, Notices Amer. Math. Soc. 44, No. 2, pp. 193–195, 1997.

[7] Niven, Zuckerman, Montgomery,"An Introduction to the Theory of Numbers", 5th Ed., Wiley India Pvt. Ltd., 2010.

Ms.Chetna, M.Sc (Mathematics), M.Phil, is presently working as Assistant Professor in the Department of Mathematics at M.M. Modi College, Patiala, Punjab, INDIA. She has more than 14 years of rich experience of teaching and research. She has one book and 05 research papers published to her credit. Her doctoral research is focused on finding the advanced solutions of Quadratic Forms.