REPRESENTATION OF NUMBERS BY QUATERNARY QUADRATIC FORMS

Arpita Kar

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Mathematics and Statistics

Department of Mathematics and Statistics
Queen's University
July, 2016

Acknowledgement

First of all, I would like to thank my parents for their unconditional support.

I also wish to express sincere gratitude to my supervisor, Professor Ram Murty for his utmost encouragement and guidance during my Master's study. I am also grateful to Professor Francesco Cellarosi and Professor Mike Roth for agreeing to serve on my examination committee. I also thank them for their careful reading of this report and for giving me corrections and suggestions. Needless to say, any error that remains is solely mine.

Last but not the least, I would like to thank all my lovely friends for being the essence of my life in this department.

Abstract

The interest in representing numbers as a sum of squares of non-negative integers is very old and has led to several celebrated results.

A classical result of Fermat from 1640 asserts that any prime $p \equiv 1 (\mathrm{mod}\ 4)$ is a sum of two squares of integers. Fermat also conjectured that each $n \in \mathbb{N}$ can be written as a sum of triangular numbers where triangular numbers are those integers of the form

$$t_x = \frac{x(x+1)}{2},$$

$x \in \mathbb{Z}$. An equivalent version of this conjecture states that $8n + 3$ is a sum of three squares (of odd integers). This was solved by Legendre and Gauss when they proved that any positive integer n can be written as a sum of three squares of integers iff $n \neq 4^i(8k + 7)$ for any non-negative integers i and k.

Based on some work of Euler, in 1722, Lagrange showed that every natural number is a sum of four squares of integers. In connection with Lagrange's theorem, Ramanujan raised the problem of determining all the positive integers a, b, c, d such that every natural number n is representable in the form $ax^2 + by^2 + cz^2 + du^2$. He proved that there exists 55 such quadruples (a, b, c, d) with $1 \leq a \leq b \leq c \leq d$. A proof of this fact will be outlined in Chapter 2. Motivated by Ramanujan's work, L. Panaitopol proved in 2005 that for a, b, c positive integers with $a \leq b \leq c$, every odd natural number can be written in the form $ax^2 + by^2 + cz^2$ with $x, y, z \in \mathbb{Z}$ iff the vector (a, b, c) is $(1, 1, 2)$ or $(1, 2, 3)$ or $(1, 2, 4)$. See **[15]**.

While we can ask about which integers can be represented by a given quadratic form, it is also interesting to ask in how many ways a certain integer m can be represented as that quadratic form. This will be one of our themes in this thesis.

Diophantus concerned himself with several problems of this type more than eighteen hundred years ago but it was only towards the end of the seventeenth century that notable advances were made and valid proofs published. For a positive integer k, let $r_k(n)$ denote the number of representations of the non-negative integer n as a sum of k squares of integers, that is, $r_k(n)$ is the number of solutions of the Diopantine equation

$$x_1^2 + \cdots x_k^2 = n \ (x_i \in \mathbb{Z}, 1 \leq i \leq k). \tag{0.1}$$

We observe that $r_2(1) = 4$. For $k = 2$, Euler proved that (0.1) is solvable iff each prime divisor p of n, for which $p \equiv 3 (\text{mod } 4)$ occurs in n to an even power. Later the formula

$$r_2(n) = 4\{ \sum_{\substack{d|n \\ d \equiv 1(4)}} 1 - \sum_{\substack{d|n \\ d \equiv 3(4)}} 1\}$$

was established independently by Gauss using arithmetic of $\mathbb{Z}[i]$ and by Jacobi using elliptic functions. By similar methods, using theta functions Jacobi found formulas for $r_4(n), r_6(n), r_8(n)$ (see for eg. pg.244 of [**16**]).

Liouville found formulas for the number of ways of representing an integer as $x^2 + y^2 + 2z^2 + 2u^2$, $x^2 + y^2 + z^2 + 2u^2$, $x^2 + 2y^2 + 2z^2 + 2u^2$ (see [**11**] and [**12**]).

In 2015, using modular forms, Ayse Alaca and Jamiah Alanazi determined explicit formulas for the number of representations of a positive integer n by quaternary quadratic forms with coefficients $1, 2, 7$ or 14. See [**2**].

The method employed by Ramanujan in his paper is elementary. We discuss this in Chapter 2. What would be desirable are explicit formulas for the number of such representations for each of the 55 tuples. In principle, this can be done using the theory of modular forms. After discussing preliminaries in Chapter 3, we will sketch a general strategy for this goal in Chapter 4. To illustrate how one applies this strategy, we will consider the case $(1, 1, 1, 3)$ in Chapter 5. That is, we determine the number of ways to express any integer n as $x^2 + y^2 + z^2 + 3u^2$. As far as we know, this has not been derived before and so we assume that this is the new result of this thesis.

Contents

CHAPTER 1

SUM OF THREE SQUARES

In this chapter, we will study which numbers can be written as a sum of three squares. We follow Ankeny [**1**] who gave an elementary presentation. We first review basic facts relevant to our discussion.

1.1. Jacobi Symbol

DEFINITION 1. *Fix a prime p. Then for any integer a, the Legendre symbol is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue (mod } p\text{)} \\ -1 & \text{if } a \text{ is a quadratic nonresidue (mod } p\text{)} \\ 0 & \text{if } p|a. \end{cases}$$

LEMMA 1. *Let p be a prime and $a \neq 0$. Then $x^2 \equiv a(\text{mod } p)$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$.*

PROOF. For the proof of the forward direction, suppose that $x^2 \equiv a(\text{mod } p)$ has a solution. Let x_0 be this solution, i.e., $x_0^2 \equiv a(\text{mod } p)$. But then,

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1(\text{mod } p).$$

The last congruence follows from Fermat's Little Theorem.

Conversely, note that $a \not\equiv 0(\text{mod } p)$. So $a(\text{mod } p)$ can be viewed as an element of $(\mathbb{Z}/p\mathbb{Z})^*$, the units of $(\mathbb{Z}/p\mathbb{Z})$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group, there exists some generator g such that $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. So, $a = g^k$, where $1 \leq k \leq p-1$. From our hypothesis,

$$a^{(p-1)/2} \equiv g^{k(p-1)/2} \equiv 1(\text{mod } p).$$

Because the order of g is $(p-1)$, $(p-1)|k\dfrac{(p-1)}{2}$. But this implies that $2|k$. So, $k = 2k'$. Hence we can write $a(\text{mod } p)$ as

$$a \equiv g^k \equiv g^{2k'} \equiv (g^{k'})^2 \,(\text{mod } p).$$

Hence, a is a square mod p, completing the proof. □

THEOREM 1. *For a prime p,*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \ (mod\ p).$$

PROOF. If $p|a$, the conclusion is trivial. So, suppose p does not divide a. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. We can factor this statement as

$$a^{p-1} - 1 \equiv (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Thus, $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. We will consider each case separately.

If $a^{(p-1)/2} \equiv 1 \pmod{p}$, then by the previous lemma, there exists a solution to the equation $x^2 \equiv a \pmod{p}$. But that would mean that

$$\left(\frac{a}{p}\right) = 1.$$

Otherwise if $a^{(p-1)/2} \equiv -1 \pmod{p}$, then by the previous lemma, there is no solution to the equation $x^2 \equiv a \pmod{p}$. But that would mean that

$$\left(\frac{a}{p}\right) = -1.$$

Hence we conclude that

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

□

THEOREM 2.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

PROOF. We will use Theorem (1) to prove this result, Thus,

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

Similarly,

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

and

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

But then,

$$\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Thus,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

But because the Legendre symbol only takes on the values ± 1, we can rewrite this statement as

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

which is what we wanted to show. □

Now in the next theorem, we will state some more properties of the Legendre symbol. (For a proof, see pg. 82, 83 of [**8**]).

THEOREM 3. *For all odd primes p,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

i.e.

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

Also,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Now, we state the famous Law of Quadratic Reciprocity which can be proved using properties of the Legendre symbol and Gauss sums (For a proof, see pg. 87 of [**8**]).

THEOREM 4. *(Law of Quadratic Reciprocity) Let p and q be odd primes. Then,*

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

DEFINITION 2. *Let b be a positive odd integer, and suppose that $b = b_1 \cdots b_l$, a product of (not necessarily distinct) primes. For an integer a relatively prime to b, the Jacobi symbol $\left(\frac{a}{b}\right)$ is defined to be the product*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b_1}\right) \cdots \left(\frac{a}{b_l}\right)$$

where $\left(\frac{a}{b_i}\right)$, $i = 1, 2, \cdots l$ denotes the Legendre symbol. If $b = 1$, $\left(\frac{a}{b}\right) = 1$.

We now state some properties of the Jacobi symbol (For a proof, refer to [**8**]).

THEOREM 5. *(Properties of the Jacobi symbol)*

(1) If b is a prime, the Jacobi symbol $\left(\frac{a}{b}\right)$ is the Legendre symbol $\left(\frac{a}{b}\right)$.

(2) If $\left(\frac{a}{b}\right) = -1$, then a is not a quadratic residue (mod b). The converse need not hold if b is not a prime.

(3) $\left(\frac{aa'}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)\left(\frac{a'}{b}\right)\left(\frac{a'}{b'}\right)$ if aa' and bb' are relatively prime.

(4) $\left(\frac{a^2}{b}\right) = \left(\frac{a}{b^2}\right) = 1$ if a and b are relatively prime.

(5) $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} = 1$ if $b \equiv 1$ (mod 4) and $= -1$ if $b \equiv -1$ (mod 4).

(6) $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8} = 1$ if $b \equiv \pm 1$ (mod 8) and $= -1$ if $b \equiv \pm 3$ (mod 8).

(7) If a and b are relatively prime odd positive integers, then

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

1.2. Minkowski's Theorem and Sum of two squares

A subset $C \subset \mathbb{R}^n$ is convex if $\forall x, y \in C$, we have

$$\lambda x + (1-\lambda)y \in C \text{ for } 0 \leq \lambda \leq 1.$$

We say C is symmetric if $x \in C \implies -x \in C$.

We say C is bounded if it is contained in some sphere of finite radius.

We define the volume of a domain $C \subseteq \mathbb{R}^n$ to be

$$\text{vol}(C) = \int_C \chi(x)dx$$

where $\chi(x)$ is the characteristic function of C:

$$\chi(x) = \begin{cases} 1 & \text{if } x \in C \\ 0 & \text{if } x \notin C \end{cases}$$

LEMMA 2. *(Siegel) Let C be a symmetric, bounded domain in $\mathbb{R}^n$. If vol$(C) > 1$, then there are two distinct points $P, Q \in C$ such that $P - Q$ is a lattice point.*

PROOF. Let $\phi(x) = 1$ or 0 according as $x \in C$ or not. Then the set

$$\psi(x) = \sum_{\gamma \in \mathbb{Z}^n} \phi(x + \gamma).$$

Clearly, $\psi(x)$ is bounded and integrable. Thus

$$\begin{aligned}
\int_{\mathbb{R}^n/\mathbb{Z}^n} \psi(x)dx &= \int_{\mathbb{R}^n/\mathbb{Z}^n} \sum_{\gamma \in \mathbb{Z}^n} \phi(x + \gamma)dx \\
&= \sum_{\gamma \in \mathbb{Z}^n} \int_{\mathbb{R}^n/\mathbb{Z}^n} \phi(x + \gamma)dx \\
&= \sum_{\gamma \in \mathbb{Z}^n} \int_{\gamma + \mathbb{R}^n/\mathbb{Z}^n} \phi(x)dx \\
&= \int_{\mathbb{R}^n} \phi(x)dx \\
&= \text{vol}(C) > 1.
\end{aligned}$$

Since $\psi(x)$ takes only integer values, we must have $\psi(x) \geq 2$ for some x. Therefore, there are two distinct points $P + \gamma$, $P + \gamma'$ in C so their difference is a lattice point. □

LEMMA 3. *If C is any convex, bounded, symmetric domain of volume $> 2^n$, then C contains a lattice point.*

PROOF. By lemma 2, the bounded symmetric domain $\frac{1}{2}C$ contains two distinct points $\frac{1}{2}P$ and $\frac{1}{2}Q$ such that $\frac{1}{2}P - \frac{1}{2}Q$ is a lattice point, because

$$\text{vol } (\frac{1}{2}C) = \frac{\text{vol } C}{2^n} > 1.$$

Since C is convex,

$$0 \neq \gamma = \frac{1}{2}P - \frac{1}{2}Q \in C$$

as $P, Q \in C$. This is a non-zero lattice point in C.

□

THEOREM 6. *(Minkowski's Theorem on lattice points in convex symmetric bodies) Let C be a bounded, symmetric , convex domain in $\mathbb{R}^n$. Let $a_1, \cdots, a_n$ be linearly independent vectors in $\mathbb{R}^n$. Let A be the $n \times n$ matrix whose rows are the a_i's. If*

$$vol\ (C) > 2^n |det\ A|,$$

then there exists rational integers $x_1, \cdots, x_n$ (not all zero) such that

$$x_1 a_1 + \cdots + x_n a_n \in\ C.$$

PROOF. Consider the set D of all $(x_1, \cdots, x_n) \in \mathbb{R}^n$ such that

$$x_1 a_1 + \cdots + x_n a_n \in C.$$

It is easily seen that D is bounded, symmetric, and convex because C is. Moreover, $D = A^{-1}C$ so that by linear algebra,

$$\text{vol}\,(D) = \text{vol}\,(C)(|\det A|)^{-1}.$$

Thus, by lemma 3, if vol $(D) > 2^n$, then D contains a lattice point $(x_1, \cdots, x_n) \neq 0$ such that $x_1 a_1 + \cdots + x_n a_n \in C$. But vol $(D) > 2^n$ is equivalent to

$$\text{vol}\,(D) > 2^n |\det A|,$$

which is what we desired. □

LEMMA 4. *If p is a positive prime, then there is an element $x \in \mathbb{F}_p$ such that $x^2 \equiv -1$ (mod p) if and only if either $p = 2$ or $p \equiv 1$ (mod 4).*

PROOF. If $p = 2$, then $1 \equiv -1 \pmod 2$, so $1^2 = 1 \equiv -1 \pmod 2$. Hence we can take $x = 1$. Conversely, if $1 \equiv -1$ (mod p), we can see that $p = 2$ since $1 = ap - 1$ for some integer a which implies $ap = 2$.

Wilson's Theorem gives

$$(p-1)! \equiv -1 \pmod p.$$

We can pair up k and $(p-k)$ in the product above so that

$$k(p-k) \equiv -k^2 \pmod p$$

which implies

$$(-1)^{(p-1)/2}(\frac{p-1}{2})!^2 \equiv -1 \pmod p.$$

Thus if $p \equiv 1 \pmod 4$, there is an $x \in \mathbb{F}_p$ such that $x^2 \equiv -1 \pmod p$. The converse follows from Fermat's little theorem:

$$1 \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$$

so that $(p-1)/2$ is even i.e. $p \equiv 1 \pmod 4$.

□

THEOREM 7. *(Sum of two squares) Let p be a prime such that $p \equiv 1$ (mod 4). Then, p can be written as sum of two squares.*

PROOF. Consider the set

$$S = \{m \in \mathbb{N} : pm = A^2 + B^2, A, B \in \mathbb{Z}\}.$$

First we note by lemma (4), $S \neq \emptyset$. Let m_0 be the smallest non-zero element in S.i.e.

$$m_0 p = x^2 + y^2,$$

for some $x, y \in \mathbb{Z}$.
We want to show that $1 \in S$. By contradiction let us assume that $m_0 \geq 2$. Let

$$x \equiv x_0 \pmod{m_0}$$

and

$$y \equiv y_0 \pmod{m_0}$$

where

$$|x_0| \leq \frac{m_0}{2} \text{ and } |y_0| \leq \frac{m_0}{2}.$$

This can be done by choosing residue classes modulo m_0 as $\{-m_0/2, -m_0/2+1, \cdots, m_0/2\}$.
Thus, we have

$$x^2 + y^2 \equiv x_0^2 + y_0^2 \pmod{m_0}.$$

Let $m_1 \in \mathbb{Z}$ be such that

$$m_1 m_0 = x_0^2 + y_0^2.$$

Then,

$$\begin{aligned} m_0^2 m_1 p &= (x^2 + y^2)(x_0^2 + y_0^2) && (1.1) \\ &= (xx_0 + yy_0)^2 + (xy_0 - x_0 y)^2 && (1.2) \end{aligned}$$

But

$$m_0 | xx_0 + yy_0$$

and

$$m_0 | xy_0 - x_0 y.$$

Thus dividing (1.1) by m_0^2, we get

$$m_1 p = \left(\frac{xx_0 + yy_0}{m_0}\right)^2 + \left(\frac{xy_0 - x_0 y}{m_0}\right)^2 \quad (1.3)$$

On the other hand we have that

$$\begin{aligned} m_1 m_0 &= x_0^2 + y_0^2 \\ &\leq \frac{m_0^2}{4} + \leq \frac{m_0^2}{4} \\ &= \frac{m_0^2}{2} \end{aligned}$$

which implies that

$$m_1 < \frac{m_0}{2}.$$

Also, $m_1 \neq 0$. That is because that would contradict the fact that $m_0 \neq 0$. Now, by (1.3), pm_1 can be written as sum of two squares and that contradicts the minimality of m_0. That proves the theorem.

□

1.3. Sum of Three Squares

In this section, we summarise a proof due to Ankeny **[1]** of the following theorem.

THEOREM 8. *If n is a positive integer not of the form $4^\lambda(8\mu + 7)$, then n is the sum of three squares.*

PROOF. Without loss of generality, we can assume that n is square free. Also, we can assume that n when considered modulo 8, leaves remainder 1, 2, 3, 5 and 6. First we consider the case when $n \equiv 3 \pmod 8$.

Since n is square free and congruent to 3 modulo 8, let

$$n = p_1 \cdots p_r$$

where p_j's are odd primes. Also consider a positive prime q which satisfies the following conditions:

$$\left(\frac{-2q}{p_j}\right) = 1,\ j = 1, 2, \cdots, r, \tag{1.4}$$

$$q \equiv 1 \pmod 4 \tag{1.5}$$

where $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol. Equations (1.4) and (1.5) are equivalent to requiring that q lies in certain residue classes modulo $4n$ (all relatively prime to $4n$), such a q does exist by Dirichlet's Theorem on primes in arithmetic progressions.

Now,

$$\begin{aligned}
1 &= \prod_{j=1}^{r} \left(\frac{-2q}{p_j}\right) \\
&= \prod_{j=1}^{r} \left(\frac{-2}{p_j}\right)\left(\frac{q}{p_j}\right) \text{ (by Theorem (2))} \\
&= \left(\frac{-2q}{n}\right) \prod_{j=1}^{r} \left(\frac{p_j}{q}\right) \text{ (by Definition (2) and Theorem (4))} \\
&= \left(\frac{-2}{n}\right)\left(\frac{n}{q}\right) \text{ (by Theorem (2))} \\
&= \left(\frac{-2}{n}\right)\left(\frac{-n}{q}\right) \text{ (since } n \equiv 3 \text{ (mod 8))} \\
&= \left(\frac{-n}{q}\right) \text{ (by Theorem (3))}.
\end{aligned}$$

Thus we get that

$$\left(\frac{-n}{q}\right) = 1.$$

Thus there exists an odd integer b such that

$$b^2 \equiv -n(\text{ mod } q).$$

i.e. for some integer h_1,

$$b^2 - 4h_1 = -n. \tag{1.6}$$

Modulo 4,equation (1.6) gives

$$1 - h_1 \equiv 1 \text{ (mod 4)},$$

i.e. for some integer h,

$$h_1 = 4h$$

and

$$b^2 - 4qh = -n. \tag{1.7}$$

Equation (1.4) implies that there exists an integer t such that

$$t^2 = -\frac{1}{2q} \text{ (mod } n). \tag{1.8}$$

Now consider the following figure

$$R^2 + S^2 + T^2 < 2n \tag{1.9}$$

where

$$R = 2tqx + tby + nz, \tag{1.10}$$

$$S = \sqrt{2q}x + \frac{b}{\sqrt{2q}}y, \tag{1.11}$$

$$T = \frac{\sqrt{n}}{\sqrt{2q}}y. \tag{1.12}$$

In the $(R, S, T)-$ space, equation (1.9) defines a convex symmetric body of volume $\frac{4}{3}\pi(2n)^{3/2} = \frac{1}{3}(2n)^{3/2}$ since the figure has radius $\sqrt{2n}$. The determinant of the transformation given by equations (1.10), (1.11) and (1.12) is

$$\begin{vmatrix} 2tq & tb & n \\ \sqrt{2q} & \frac{b}{\sqrt{2q}} & 0 \\ 0 & \frac{\sqrt{n}}{\sqrt{2q}} & 0 \end{vmatrix} \tag{1.13}$$

which equals $n^{3/2}$. Thus, (1.9) defines a convex symmetric body of volume $\frac{1}{3}(2n)^{3/2}$ in the $(x, y, z)-$ space. Clearly, $\frac{1}{3}(2n)^{3/2} > 8$.

Hence, applying Theorem 6, we get that there exists integer values of x, y, z (not all zero) which satisfy (1.9), (1.10), (1.11) and (1.12). Let those integer values be x_1, y_1, z_1 and the corresponding values of R, S, T be R_1, S_1, T_1 respectively.

By applying equations (1.10), (1.11), and (1.12), we get that

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= R_1^2 + (\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1)^2 + (\frac{\sqrt{n}}{\sqrt{2q}})^2 && (1.14) \\ &= R_1^2 + \frac{1}{2q}(2qx_1 + by_1)^2 + \frac{n}{2q}y_1^2 && (1.15) \\ &= R_1^2 + 2(qx_1^2 + bx_1y_1 + hy_1^2). && (1.16) \end{aligned}$$

Let $v = qx_1^2 + bx_1y_1 + hy_1^2$. Also, by choice of t in (1.8), we have the following,

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= (2tqx_1 + tby_1 + nz_1)^2 + (\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1)^2 + (\frac{\sqrt{n}}{\sqrt{2q}}y_1)^2 && (1.17) \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{2q}(2qx_1 + by_1)^2 && (1.18) \\ &\equiv 0 \pmod{n}. && (1.19) \end{aligned}$$

Thus the above gives that $R_1^2 + 2v < 2n$ and $n | R_1^2 + 2v$. Also since the transformation given by (1.10), (1.11), (1.12) is non-degenerate and not all of x_1, y_1, z_1 are zero, $R_1^2 +$

$2v \neq 0$. Hence,

$$R_1^2 + 2v = n. \tag{1.20}$$

Let p be an odd prime which divides v exactly to an odd power.

Now we consider two cases :

Case 1 : $p \nmid n$

By (1.20), we have that

$$\left(\frac{n}{p}\right) = 1. \tag{1.21}$$

Also, since $v = qx_1^2 + bx_1y_1 + hy_1^2$,

$$4qv = (2qx_1 + by_1)^2 + ny_1^2. \tag{1.22}$$

If $p|q$, then by (1.7),

$$\left(\frac{-n}{p}\right) = 1.$$

If $p \nmid q$, then by (1.22),

$$\left(\frac{-n}{p}\right) = 1.$$

Thus in either case

$$\left(\frac{-n}{p}\right) = 1.$$

which combined with (1.21), gives

$$\left(\frac{-1}{p}\right) = 1 \text{ or } p \equiv 1 \pmod 4.$$

Case 2 : $p \mid n$

By (1.20) and since $v = qx_1^2 + bx_1y_1 + hy_1^2$, we get that

$$R_1^2 + \frac{1}{2q}((2qx_1 + by_1)^2 + ny_1^2) = n \tag{1.23}$$

which implies that $p|R_1$ and $p|(2qx_1 + b_1)$ and thus dividing both sides of (1.23) by p, we get

$$\frac{1}{2q}\frac{n}{p}y_1^2 = \frac{n}{p} \pmod p.$$

i.e.

$$y_1^2 = 2q \pmod p.$$

i.e.

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

which combined with (1.4), yields

$$\left(\frac{-1}{p}\right) = 1 \text{ or } p \equiv 1 \pmod 4.$$

Thus in both cases, we get that $p \equiv 1 \pmod 4$.i.e. all odd primes which divide v exactly to an odd power are congruent to 1 modulo 4, which implies that $2v$ is the sum of two squares by Theorem 7. Thus by (1.20), n is the sum of three squares. That proves the theorem for the case when $n \equiv 3 \pmod 8$.

Now for the case when $m \equiv 1, 2, 5 \text{ or } 6 \pmod 8$, the same proof as above goes through with a few alterations as follows :

Consider a positive prime q which satisfies the following conditions :

$$\left(\frac{-q}{p_j}\right) = 1,\ j = 1, 2, \cdots, r, \tag{1.24}$$

$$q \equiv 1 \pmod 4 \tag{1.25}$$

and if n is even, choose $n = 2n_1$,

$$\left(\frac{-2}{q}\right) = (-1)^{(n_1-1)/2},$$

$$t^2 \equiv -\frac{1}{q} \pmod{p_j},$$

t odd,

$$b^2 - qh = -n,$$

and

$$R = tqx + tby + nz, \tag{1.26}$$

$$S = \sqrt{q}x + \frac{b}{\sqrt{q}}y, \tag{1.27}$$

$$T = \frac{\sqrt{n}}{\sqrt{q}}y. \tag{1.28}$$

With these changes, the proof in the other cases also follows.

□

CHAPTER 2

SUMMARY OF RAMANUJAN'S PAPER

In this chapter, we give a summary of Ramanujan's paper "On the expression of numbers of the form $ax^2 + by^2 + cz^2 + du^2$" where he found 55 positive 4-tuples (a, b, c, d) such that any positive number can be written as $ax^2 + by^2 + cz^2 + du^2$ for those 4-tuples. He used the process of elimination first to get the 55 possible 4-tuples (a, b, c, d) such that any positive number can be written as $ax^2 + by^2 + cz^2 + du^2$. Here is his argument.

Without loss of generality, we can assume $a \leq b \leq c \leq d$.
Note $a = 1$ otherwise 1 cannot be expressed as $ax^2 + by^2 + cz^2 + du^2$. This is because the least value of $ax^2 + by^2 + cz^2 + du^2$ would be ax^2 when $y = z = u = 0$ for any value of b, c, d and if $a > 1$, then 1 can never be expressed as $ax^2 + by^2 + cz^2 + du^2$ for any value of a. Thus $a = 1$. So, we have to find values of b, c, d such that any positive integer can be written as $x^2 + by^2 + cz^2 + du^2$.
If $b > 2$, then $c, d \geq 3$ and 2 cannot be expressed in this form because setting $z = u = 0$, we will have $x^2 + by^2 = 2$. The only solutions to this are :

(1) $x = 1, y = 1, b = 1$
(2) $x = 0, y = 1, b = 2$.

Thus, $1 \leq b \leq 2$. So, there are two cases we need to consider :
Case 1: Values of (c, d) such that any positive integer can be written as $x^2 + y^2 + cz^2 + du^2$.
Case 2: Values of (c, d) such that any positive integer can be written as $x^2 + 2y^2 + cz^2 + du^2$.

Case 1. If $c > 3$,, then 3 cannot be expressed in this form because for any value of d, taking $u = 0$, we will have $x^2 + y^2 + cz^2 = 3$.
The only solutions to this are

(1) $x = 0, y = 0, z = 1, c = 3$.
(2) $x = 1, y = 1, z = 1, c = 1$.

(3) $x = 1, y = 0, z = 1, c = 2$.

Thus, $1 \leq c \leq 3$.

So, there are three subcases of this Case 1 that we need to consider.

Case 1 a. Values of d such that any positive integer can be written as $x^2 + y^2 + z^2 + du^2$.

If $d > 7$, then 7 cannot be written as $x^2 + y^2 + z^2 + du^2$. Thus $1 \leq d \leq 7$.

Case 1 b. Values of d such that any positive integer can be written as $x^2 + y^2 + 2z^2 + du^2$.

If $d > 14$, then 14 cannot be written as $x^2 + y^2 + 2z^2 + du^2$. Thus $2 \leq d \leq 14$.

Case 1 c. Values of d such that any positive integer can be written as $x^2 + y^2 + 3z^2 + du^2$.

If $d > 6$, then 6 cannot be written as $x^2 + y^2 + 3z^2 + du^2$. Thus $3 \leq d \leq 6$.

Case 2. If $c > 5$, then 5 cannot be expressed in this form because since $c \leq d$, for any value of d, taking $u = 0$, we will have $x^2 + 2y^2 + cu^2 = 5$.

The only solutions to this are:

(1) $x = 0, y = 0, u = 0, c = 5$.

(2) $x = 0, y = 1, u = 1, c = 3$.

(3) $x = 1, y = 0, u = 1, c = 4$.

(4) $x = 1, y = 1, u = 1, c = 2$.

Thus $2 \leq c \leq 5$. So, there are four subcases of this Case 2 that we need to consider.

Case 2 a. Values of d such that any positive integer can be written as $x^2 + 2y^2 + 2z^2 + du^2$. If $d > 7$, then 7 cannot be written as $x^2 + 2y^2 + 2z^2 + du^2$. Thus $2 \leq d \leq 7$.

Case 2 b. Values of d such that any positive integer can be written as $x^2 + 2y^2 + 3z^2 + du^2$. If $d > 10$, then 10 cannot be written as $x^2 + 2y^2 + 3z^2 + du^2$. Thus $3 \leq d \leq 10$.

Case 2 c. Values of d such that any positive integer can be written as $x^2 + 2y^2 + 4z^2 + du^2$. If $d > 14$, then 14 cannot be written as $x^2 + 2y^2 + 4z^2 + du^2$. Thus $4 \leq d \leq 14$.

Case 2 d. Values of d such that any positive integer can be written as $x^2 + 2y^2 + 5z^2 + du^2$. If $d > 10$, then 10 cannot be written as $x^2 + 2y^2 + 5z^2 + du^2$. Thus $5 \leq d \leq 10$.

That leaves the following 55 $4-$tuples listed in the next page.

Next, Ramanujan uses the following result about ternary quadratic forms.

THEOREM 9. *The necessary and sufficient condition that a number cannot be expressed as*

$$x^2 + y^2 + z^2,$$

$(1,1,1,1)$	$(1,2,3,5)$	$(1,2,4,8)$	$(1,1,1,2)$	$(1,2,4,5)$	$(1,2,5,8)$	$(1,1,2,2)$	$(1,2,5,5)$
$(1,1,2,9)$	$(1,2,2,2)$	$(1,1,1,6)$	$(1,2,3,9)$	$(1,1,1,3)$	$(1,1,2,6)$	$(1,2,4,9)$	$(1,1,2,3)$
$(1,2,2,6)$	$(1,2,5,9)$	$(1,2,2,3)$	$(1,1,3,6)$	$(1,1,2,10)$	$(1,1,3,3)$	$(1,2,3,6)$	$(1,2,3,10)$
$(1,2,3,3)$	$(1,2,4,6)$	$(1,2,4,10)$	$(1,1,1,4)$	$(1,2,5,6)$	$(1,2,5,10)$	$(1,1,2,4)$	$(1,1,1,7)$
$(1,1,2,11)$	$(1,2,2,4)$	$(1,1,2,7)$	$(1,2,4,11)$	$(1,1,3,4)$	$(1,2,2,7)$	$(1,1,2,12)$	$(1,2,3,4)$
$(1,2,3,7)$	$(1,2,4,12)$	$(1,2,4,4)$	$(1,2,4,7)$	$(1,1,2,13)$	$(1,1,1,5)$	$(1,2,5,7)$	$(1,2,4,13)$
$(1,1,2,5)$	$(1,1,2,8)$	$(1,1,2,14)$	$(1,2,2,5)$	$(1,2,3,8)$	$(1,2,4,14)$	$(1,1,3,5)$	

Table 1: Table of 55 tuples

$$x^2+y^2+2z^2,$$
$$x^2+y^2+3z^2,$$
$$x^2+2y^2+2z^2,$$
$$x^2+2y^2+3z^2,$$
$$x^2+2y^2+4z^2,$$
$$x^2+2y^2+5z^2,$$

is that it should be of the form

$$4^\lambda(8\mu+7),$$
$$4^\lambda(16\mu+14),$$
$$9^\lambda(9\mu+6),$$
$$4^\lambda(8\mu+7),$$
$$4^\lambda(16\mu+10),$$
$$4^\lambda(16\mu+14),$$
$$25^\lambda(25\mu+10) \text{ or } 25^\lambda(25\mu+10)$$

respectively.

PROOF. Consider the first case of the theorem. Suppose an integer can be written as sum of three squares. Now we know that any integer can be written as $4k$ or $8k+1$ for some k. Now considering the different residues that the three squares leave, it can be seen that the sum of the three squares is never congruent to 7 modulo 8. The other direction of the theorem follows from Theorem 8. The other cases can be done similarly. □

Now let us consider Case 1a as before.

We have to show that any integer N can be expressed as $N = x^2 + y^2 + z^2 + du^2$, $1 \leq d \leq 7$. If N is not of the form $4^\lambda(8\mu + 7)$, then N can be written as $x^2 + y^2 + z^2$ by Theorem 9. So we take $u = 0$ for $1 \leq d \leq 7$. Then those N can be written as $x^2 + y^2 + z^2 + du^2$.
Let N be of the form $4^\lambda(8\mu + 7)$.

When $d = 1, 2, 4, 5, 6$, taking $u = 2^\lambda$, we get that

$$N - du^2 = 4^\lambda(8\mu + 7 - d)$$

which is not of the form $4^\lambda(8\mu + 7)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + z^2$, that is

$$N = x^2 + y^2 + z^2 + du^2.$$

When $d = 3$ and $\mu = 0$, taking $u = 2^\lambda$, we get that,

$$N - du^2 = 4^{\lambda+1}$$

which is not of the form $4^\lambda(8\mu + 7)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + z^2$, that is

$$N = x^2 + y^2 + z^2 + du^2.$$

When $d = 3$ and $\mu \geq 1$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(8\mu - 5)$$

which is not of the form $4^\lambda(8\mu + 7)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + z^2$, that is

$$N = x^2 + y^2 + z^2 + du^2.$$

When $d = 7$ and $\mu = 0, 1, 2$, taking $u = 2^\lambda$. we get that,

$$N - du^2 = 0, (2 \times 4^{\lambda+1}), 4^{\lambda+2}$$

none of which is of the form $4^\lambda(8\mu + 7)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + z^2$, that is

$$N = x^2 + y^2 + z^2 + du^2.$$

When $d = 7$ and $\mu \geq 3$, taking $u = 2^{\lambda+1}$. we get that,

$$N - du^2 = 4^\lambda(8\mu - 21)$$

which is not of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+z^2$, that is

$$N = x^2+y^2+z^2+du^2.$$

Thus, in any of these cases N can be written as $x^2+y^2+z^2+du^2$ for $1 \leq d \leq 7$.

Consider Case 1b as before.

We have to show that any integer N can be expressed as $N = x^2+y^2+2z^2+du^2$, $2 \leq d \leq 14$.

If N is not of the form $4^\lambda(16\mu+14)$, then N can be written as $x^2+y^2+2z^2$ by Theorem 9. So we take $u = 0$ for $2 \leq d \leq 14$ and N of that form. Then N can be written as $x^2+y^2+2z^2+du^2$.

Let N be of the form $4^\lambda(16\mu+14)$.

When $d = 2,3,...,9,11,12,13$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 4^\lambda(16\mu+14-d)$$

which is not of the form $4^\lambda(16\mu+14)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+2z^2$, that is

$$N = x^2+y^2+2z^2+du^2.$$

When $d = 10$ and $\mu = 0$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 4^{\lambda+1}$$

which is not of the form $4^\lambda(16\mu+14)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+2z^2$, that is

$$N = x^2+y^2+2z^2+du^2.$$

When $d = 10$ and $\mu \geq 1$, taking $u = 2^{\lambda+1}$, we get that ,

$$N-du^2 = 4^\lambda(16\mu+4)$$

which is not of the form $4^\lambda(16\mu+14)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+2z^2$, that is

$$N = x^2+y^2+2z^2+du^2.$$

When $d = 14$ and $\mu = 0,1$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 0,4^{\lambda+2}$$

none of which is of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + 2z^2$, that is

$$N = x^2 + y^2 + 2z^2 + du^2.$$

When $d = 14$ and $\mu \geq 2$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(16\mu - 10)$$

which is not of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + 2z^2$, that is

$$N = x^2 + y^2 + 2z^2 + du^2.$$

Thus, in any of these cases N can be written as $x^2 + y^2 + 2z^2 + du^2$ for $2 \leq d \leq 14$.

Now we consider Case 1c as before.

We have to show that any integer N can be expressed as $N = x^2 + y^2 + 3z^2 + du^2$, $3 \leq d \leq 6$.

If N is not of the form $9^\lambda(9\mu + 6)$, then N can be written as $x^2 + y^2 + 3z^2$ by Theorem 9. So we take $u = 0$ for $3 \leq d \leq 6$. Then N can be written as $x^2 + y^2 + 3z^2 + du^2$.
Let N be of the form $9^\lambda(9\mu + 6)$.

When $d = 4, 5$, taking $u = 3^\lambda$, we get that,

$$N - du^2 = 9^\lambda(9\mu + 6 - d)$$

which is not of the form $9^\lambda(9\mu + 6)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + 3z^2$, that is

$$N = x^2 + y^2 + 3z^2 + du^2.$$

When $d = 3$ and $\mu = 0$, taking $u = 3^\lambda$, we get that,

$$N - du^2 = 9^{\lambda+1}$$

which is not of the form $9^\lambda(9\mu + 6)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + y^2 + 3z^2$, that is

$$N = x^2 + y^2 + 3z^2 + du^2.$$

When $d = 3$ and $\mu \geq 1$, taking $u = 3^\lambda$, we get that,

$$N - du^2 = 9^\lambda(9\mu + 3)$$

which is not of the form $9^\lambda(9\mu+6)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+3z^2$, that is

$$N = x^2+y^2+3z^2+du^2.$$

When $d=6$ and $\mu \geq 0$, taking $u=3^\lambda$, we get that,

$$N-du^2 = 9^{\lambda+1}\mu$$

which is not of the form $9^\lambda(9\mu+6)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+y^2+3z^2$, that is

$$N = x^2+y^2+3z^2+du^2.$$

Thus, in any of these cases N can be written as $x^2+y^2+3z^2+du^2$ for $3 \leq d \leq 6$.

Consider Case 2a as before.

We have to show that any integer N can be expressed as $N = x^2+2y^2+2z^2+du^2$, $2 \leq d \leq 7$.

If N is not of the form $4^\lambda(8\mu+7)$, then N can be written as $x^2+2y^2+2z^2$ by Theorem 9. So we take $u=0$ for $2 \leq d \leq 7$. Then N can be written as $x^2+2y^2+2z^2+du^2$. Let N be of the form $4^\lambda(8\mu+7)$.

When $d=2,4,5,6$, taking $u=2^\lambda$, we get that,

$$N-du^2 = 4^\lambda(8\mu+7-d)$$

which is not of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+2z^2$, that is

$$N = x^2+2y^2+2z^2+du^2.$$

When $d=3$ and $\mu=0$, taking $u=2^\lambda$, we get that,

$$N-du^2 = 4^{\lambda+1}$$

which is not of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+2z^2$, that is

$$N = x^2+2y^2+2z^2+du^2.$$

When $d=3$ and $\mu \geq 1$, taking $u=2^{\lambda+1}$, we get that,

$$N-du^2 = 4^\lambda(8\mu-5)$$

which is not of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+2z^2$, that is

$$N = x^2+2y^2+2z^2+du^2.$$

When $d=7$ and $\mu = 0,1,2$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 0, (2\times 4^{\lambda+1}), 4^{\lambda+2}$$

none of which is of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+2z^2$, that is

$$N = x^2+2y^2+2z^2+du^2.$$

When $d=7$ and $\mu \geq 3$, taking $u = 2^{\lambda+1}$, we get that,

$$N-du^2 = 4^\lambda(8\mu-21)$$

which is not of the form $4^\lambda(8\mu+7)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+2z^2$, that is

$$N = x^2+2y^2+2z^2+du^2.$$

Thus, in any of these cases N can be written as $x^2+2y^2+2z^2+du^2$ for $2 \leq d \leq 7$.

Consider Case 2b as before.

We have to show that any integer N can be expressed as $N = x^2+2y^2+3z^2+du^2$, $3 \leq d \leq 10$.

If N is not of the form $4^\lambda(16\mu+10)$, then N can be written as $x^2+2y^2+3z^2$ by Theorem 9. So we take $u=0$ for $3 \leq d \leq 10$. Then N can be written as $x^2+2y^2+3z^2+du^2$. Let N be of the form $4^\lambda(16\mu+10)$.

When $d = 3,4,5,7,8,9$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 4^\lambda(16\mu+10-d)$$

which is not of the form $4^\lambda(16\mu+10)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+3z^2$, that is

$$N = x^2+2y^2+3z^2+du^2.$$

When $d=6$ and $\mu = 0$, taking $u = 2^\lambda$, we get that,

$$N-du^2 = 4^{\lambda+1}$$

which is not of the form $4^\lambda(16\mu+10)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+3z^2$, that is

$$N = x^2+2y^2+3z^2+du^2.$$

When $d=6$ and $\mu \geq 1$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(16\mu-14)$$

which is not of the form $4^\lambda(16\mu+10)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+3z^2$, that is

$$N = x^2+2y^2+3z^2+du^2.$$

When $d=10$ and $\mu = 0,1,2$, taking $u = 2^\lambda$, we get that,

$$N - du^2 = 0, 4^{\lambda+2}, (2\times 4^{\lambda+2})$$

none of which is of the form $4^\lambda(16\mu+10)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+3z^2$, that is

$$N = x^2+2y^2+3z^2+du^2.$$

When $d=10$ and $\mu \geq 3$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(16\mu+14)$$

which is not of the form $4^\lambda(16\mu+10)$. So, by Theorem 9, $N-du^2$ can be written as $x^2+2y^2+3z^2$, that is

$$N = x^2+2y^2+3z^2+du^2.$$

Thus, in any of these cases N can be written as $x^2+2y^2+3z^2+du^2$ for $3 \leq d \leq 10$.

Consider Case 2c as before.

We have to show that any integer N can be expressed as $N = x^2+2y^2+4z^2+du^2$, $4 \leq d \leq 14$.

If N is not of the form $4^\lambda(16\mu+14)$, then N can be written as $x^2+2y^2+4z^2$ by Theorem 9. So we take $u=0$ for $4 \leq d \leq 14$. Then N can be written as $x^2+2y^2+4z^2+du^2$.

Let N be of the form $4^\lambda(16\mu+14)$.

When $d = 4, 5, 6, 7, 8, 9, 11, 12, 13$, taking $u = 2^\lambda$, we get that,

$$N - du^2 = 4^\lambda(16\mu + 14 - d)$$

which is not of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + 2y^2 + 4z^2$, that is

$$N = x^2 + 2y^2 + 4z^2 + du^2.$$

When $d = 10$ and $\mu = 0$, taking $u = 2^\lambda$, we get that,

$$N - du^2 = 4^{\lambda+1}$$

which is not of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + 2y^2 + 4z^2$, that is

$$N = x^2 + 2y^2 + 4z^2 + du^2.$$

When $d = 10$ and $\mu \geq 1$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(16\mu - 6)$$

which is not of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + 2y^2 + 4z^2$, that is

$$N = x^2 + 2y^2 + 4z^2 + du^2.$$

When $d = 14$ and $\mu = 0, 1, 2$, taking $u = 2^\lambda$, we get that,

$$N - du^2 = 0, 4^{\lambda+2}, (2 \times 4^{\lambda+2})$$

none of which is of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + 2y^2 + 4z^2$, that is

$$N = x^2 + 2y^2 + 4z^2 + du^2.$$

When $d = 14$ and $\mu \geq 3$, taking $u = 2^{\lambda+1}$, we get that,

$$N - du^2 = 4^\lambda(16\mu - 14)$$

which is not of the form $4^\lambda(16\mu + 14)$. So, by Theorem 9, $N - du^2$ can be written as $x^2 + 2y^2 + 4z^2$, that is

$$N = x^2 + 2y^2 + 4z^2 + du^2.$$

Thus, in any of these cases N can be written as $x^2 + 2y^2 + 4z^2 + du^2$ for $4 \leq d \leq 14$.

Similarly, Case 2d can also be considered as before.

Thus we have succeeded in summarising the fact that any integer can be expressed as $ax^2 + by^2 + cz^2 + du^2$ for the 55 4-tuples shown in the table earlier.

REMARK 1. *A form is said to be universal if it represents every positive integer. If a form is not universal, then its truant is defined to be the smallest positive integer not represented by it.*
In 1993, *Conway and Schneeberger announced the following remarkable result:*

THEOREM 10 (The Fifteen Theorem). *If a positive-definite quadratic form having integer matrix represents every positive integer upto* 15, *then it represents every positive integer.*

The original proof of this theorem was never published, perhaps because several of the cases involved rather intricate arguments. But in [**3**], *Manjul Bhargava gives a very simple proof of the* 15*-theorem and derives the complete list of universal quaternaries. In fact in the remarks section of the paper, Bhargava proves the following theorem:*

THEOREM 11. *If a positive definite quadratic form having integer matrix represents the nine critical numbers* $1, 2, 3, 5, 6, 7, 10, 14$, *and* 15, *then it represents every positive integer. (Equivalently, the truant of any non-universal form must be one of these nine numbers).*

However, he also proves this another slight strengthened version of the fifteen theorem which shows that the number 15 *is really special:*

THEOREM 12. *If a positive definite quadratic form having integer matrix represents every number below* 15, *then it represents every number above* 15.

This result leads to Ramanujan's assertion to be corrected slightly that there are 54, *not* 55 *universal diagonal quaternary quadratic forms. This is because the form* $x^2 + 2y^2 + 5z^2 + 5u^2$ *is not universal as it does not represent 15.*

CHAPTER 3

PRELIMINARIES ON MODULAR FORMS

In this chapter, we give a short review of the basic theory of modular forms. We refer the reader to **[5]**, **[9]**, **[10]**, **[13]**, **[14]**, **[16]**, **[17]** and **[18]** for further details.

3.1. The Modular Group

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

is called the (full) modular group and it plays a pivotal role in the theory of modular forms. It is generated by $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

For each natural number N, the principal congruence subgroup of level N denotes $\Gamma(N)$ is the group

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

In particular, $\Gamma(1) = SL_2(\mathbb{Z})$. $\Gamma(N)$ is a normal subgroup of $SL_2(\mathbb{Z})$ of finite index. In particular,

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} (1 - \frac{1}{p^2})$$

where $[A : B]$ denotes the index of B in A.

A subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is called a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some N. Since $\Gamma(N)$ is of finite index in $SL_2(\mathbb{Z})$, it follows that any congruence subgroup is also of finite index in $SL_2(\mathbb{Z})$. In the theory of modular forms, congruence subgroups will play a dominant role. If Γ is a congruence subgroup, the smallest N such that $\Gamma(N) \subset \Gamma$ is called the level of Γ.

The Hecke subgroups are denoted $\Gamma_0(N)$ and defined by

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N) \right\}.$$

It is easy to see that this is a group. Clearly, $\Gamma(N) \subset \Gamma_0(N)$ and so these are congruence subgroups.

Consider the map

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$$

given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d(\text{mod } N).$$

It is clearly a surjective homomorphism. This is because if we consider $d \in (\mathbb{Z}/N\mathbb{Z})^*$, then $\gcd(d, N) = 1$. So, $\exists\ a, b \in \mathbb{Z}$, such that $ad - Nb = 1$. So, $\begin{bmatrix} a & b \\ N & d \end{bmatrix}$ maps to d. The kernel denoted by $\Gamma_1(N)$ is given by

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \text{ (mod } N), d \equiv 1 \text{ (mod } N) \right\}.$$

Thus we have

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}).$$

3.2. The Upper Half Plane

Let $\mathfrak{H}$ denote the upper half plane,

$$\mathfrak{H} = \{z \in \mathbb{C} : \text{Im } (z) > 0\}$$

viewed as open subset of $\mathbb{C}$ with usual topology. We define an action of the group

$$GL_2^+(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc > 0 \right\}$$

on $\mathfrak{H}$ via the formula

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az + b}{cz + d}.$$

It can be shown that this indeed defines an action of $GL_2^+(\mathbb{R})$ on $\mathfrak{H}$. The transformations

$$z \to \frac{az + b}{cz + d}$$

are called fractional linear transformations or Mobius transformations.

DEFINITION 3. *Let G be a group and X a topological space. Then for the $G-$action on X, two elements $x, y \in X$ are called* ***G-equivalent*** *if there is a $g \in G$ such that $gx = y$.*

DEFINITION 4. *If Γ is a subgroup of $SL_2(\mathbb{Z})$ and $\mathcal{F} \subset \mathfrak{H}$ is a closed set with connected interior, we say that $\mathcal{F}$ is a fundamental domain for Γ if*

- *any $z \in \mathfrak{H}$ is $\Gamma-$equivalent to a point in $\mathcal{F}$.*
- *no two interior points of $\mathcal{F}$ are $\Gamma-$equivalent.*
- *the boundary of $\mathcal{F}$ is a finite union of smooth curves.*

Let $\mathcal{F} = \{z \in \mathfrak{H} : |\mathrm{Re}(z)| \leq \frac{1}{2}, |z| \geq 1\}$. Then $\mathcal{F}$ is a fundamental domain for the action of $SL_2(\mathbb{Z})$ on $\mathfrak{H}$. We now define the extended upper half plane $\mathfrak{H}^*$ as

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{i\infty\},$$

that is, $\mathfrak{H}^*$ is obtained by adjoining all the rational numbers and $i\infty$ called the cusps (which should be visualised as adding the point at infinity far up the positive imaginary axis and all the rational numbers on the real axis). It is easy to see that $SL_2(\mathbb{Z})$ permutes the cusps transitively when it acts on $\mathfrak{H}^*$ via the formula

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az+b}{cz+d} \text{ for } z \in \mathfrak{H}.$$

For cusps $\mathbb{Q} \cup i\infty$, we identify $i\infty$ with $\frac{1}{0}$ and define

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{r}{s} = \frac{ar+bs}{cr+ds}.$$

We extend the usual topology on $\mathfrak{H}$ to $\mathfrak{H} \cup \{i\infty\}$ as follows. First, a fundamental system of open neighbourhoods of $i\infty$ is $N_C = \{z \in \mathbb{H} : \mathrm{Im}(z) > C\} \cup \{i\infty\}$ for any $C > 0$. Note that if we map $\mathfrak{H}$ to the punctured open unit disc by sending

$$z \mapsto q = e^{2\pi i z}$$

and if we agree to take the point $\{i\infty\} \in \mathfrak{H}^*$ to the origin under this map, then N_C is the inverse image of the open disc of radius $e^{-2\pi C}$ centered at the origin and we have defined our topology on $\mathfrak{H} \cup \{i\infty\}$ so as to make $z \mapsto q = e^{2\pi i z}$ continuous.

The change of variables from z to q plays a basic role in the theory of modular functions. We use it to define an analytic structure on $\mathfrak{H} \cup \{i\infty\}$. In other words, given

a function on $\mathfrak{H}$, we say that it is meromorphic at $i\infty$ if it can be expressed as a power series in the variable q having at most finitely many negative terms, that is, it has a Fourier expansion of the form

$$f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n z} = \sum_{n\in\mathbb{Z}} a_n q^n$$

in which $a_n = 0$ for $n \ll 0$.
We say that $f(z)$ is holomorphic at $i\infty$ if $a_n = 0$ for all negative n and we say that $f(z)$ vanishes at $i\infty$ if $a_0 = 0$. More generally, if $f(z)$ has period N, then we use the map

$$z \mapsto q_N = e^{2\pi i z/N}$$

to map $\mathfrak{H} \cup \{i\infty\}$ to the open unit disc. We can then express $f(z)$ as a series in q_N, and say that it is meromorphic at $i\infty$ if $a_n = 0$ for $n \ll 0$.

Next, for a cusp $a/c \in \mathbb{Q} \subset \mathfrak{H}^*$, we define a fundamental system of open neighbourhoods by completing a, c to a matrix $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and using α to transport the N_C to discs which are tangent to the real axis at a/c. In other words, with this topology, to say that a sequence z_j approaches a/c means that $\alpha^{-1} z_j$ approaches $i\infty$.

3.3. Modular forms for $SL_2(\mathbb{Z})$

DEFINITION 5. *Let $f(z)$ be a meromorphic function on the upper half plane $\mathfrak{H}$ and let k be an integer. Suppose that $f(z)$ satisfies the relation*

$$f(\gamma z) = (cz + d)^k f(z), \forall \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}).$$

In particular, for elements $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$,

$$f(z+1) = f(z)$$

and

$$f(-\frac{1}{z}) = (-z)^k f(z).$$

Also suppose $f(z)$ is meromorphic at infinity, that is, the Fourier series

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q^n, q = e^{2\pi i z}$$

has at most finitely many non-zero a_n with $n < 0$. Then $f(z)$ is called a modular function of weight k for $SL_2(\mathbb{Z})$. If, in addition, $f(z)$ is actually holomorphic on $\mathfrak{H}$ and at infinity (i.e. $a_n = 0\ \forall n < 0$), then $f(z)$ is called a modular form of weight k for $SL_2(\mathbb{Z})$. The set of such functions is denoted $M_k(SL_2(\mathbb{Z}))$. If we further have $a_0 = 0$, i.e. the modular form vanishes at infinity, then $f(z)$ is called a cusp form of weight k for $SL_2(\mathbb{Z})$. The set of such functions is denoted $S_k(SL_2(\mathbb{Z}))$. Finally, the expansion $f(z) = \sum_{n\in\mathbb{Z}} a_n q^n$ is called its q-expansion.

Remark :

- If k is odd, there are no non-zero modular functions of weight k for Γ. If I denotes the identity matrix of $SL_2(\mathbb{Z})$, then for a modular function f, we have $f((-I)z) = (-1)^k f(z)$. Since k is odd, this implies that $f(z) = -f(z)$. Thus, $f = 0$.
- The conditions for a function to be a modular form are preserved under addition and scalar multiplication, that is, the set of modular functions, forms and cusp forms of some fixed weight are complex vector spaces. In addition, the product of a modular function (form) of weight k_1 and modular function (form) of weight k_2 is a modular function (form) of weight $k_1 + k_2$ and the quotient of a modular function (form) of weight k_1 by a non-zero modular function (form) of weight k_2 is a modular function of weight $k_1 - k_2$. In particular, the set of modular functions of weight 0 is a field.

3.4. Eisenstein Series

Let k be an even integer greater than 2. For $z \in \mathfrak{H}$, we define

$$G_k(z) = {\sum_{m,n}}' \frac{1}{(mz+n)^k}$$

where the sum is over pairs of integers m, n not both zero.

Because k is at least 4, $G_k(z)$ is absolutely convergent and uniformly convergent in any compact subset of $\mathfrak{H}$. Hence $G_k(z)$ is a holomorphic function on $\mathfrak{H}$. It is also obvious that $G_k(z) = G_k(z+1)$ and that the Fourier expansion for $G_k(z)$ has no negative terms because $G_k(z)$ approaches a finite limit as $z \to i\infty$:

$$\lim_{z\to i\infty} {\sum_{m,n}}' \frac{1}{(mz+n)^k} = \sum_{n\neq 0} \frac{1}{n^k} = 2\zeta(k).$$

Finally we can also check that

$$z^{-k}G_k(-\frac{1}{z}) = \sum_{m,n}{}' \frac{1}{(-m+nz)^k} = G_k(z).$$

Thus we have proved the following proposition.

LEMMA 5. $G_k \in M_k(SL_2(\mathbb{Z}))$.

We now compute the $q-$expansion coefficients for G_k. It turns out that these coefficients are essentially the arithmetic functions,

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}.$$

LEMMA 6. *Let k be an even integer greater than 2, and let $z \in \mathfrak{H}$. Then the modular form $G_k(z)$ defined earlier has $q-$expansion*

$$G_k(z) = 2\zeta(k)(1 - \frac{2k}{B_k}) \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

where $q = e^{2\pi iz}$, and the Bernoulli numbers B_k are defined by setting

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

Because of this proposition, we could define the "normalised Eisenstein series" as

$$E_k(z) = \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n.$$

An alternate way of defining the normalised Eisenstein series is to sum only over relatively prime pairs m, n, that is,

$$E_k(z) = \frac{1}{2} \sum_{(m,n)=1} \frac{1}{(-m+nz)^k}.$$

Thus, $E_k(z)$ is defined so as to have rational $q-$expansion coefficients. Here are some examples :

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n;$$

$$E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n;$$

$$E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n)q^n;$$

$$E_{10}(z) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n)q^n;$$

$$E_{12}(z) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n;$$

$$E_{14}(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n.$$

Thus, in fact, we have the following result.

LEMMA 7. *For every even $k \geq 4$, $E_k(z)$ is a modular form of weight k for the full modular group $SL_2(\mathbb{Z})$ satisfying $E_k(i\infty) = 1$.*

THEOREM 13. $\forall k \geq 4$, $M_k(SL_2(\mathbb{Z})) = \mathbb{C}E_k \oplus S_k(SL_2(\mathbb{Z}))$.

PROOF. Let $f \in M_k(SL_2(\mathbb{Z}))$. Let $\lambda = f(i\infty)$ denote the constant term in the Fourier expansion. Then clearly,

$$f = \lambda E_k + (f - \lambda E_k)$$

where $(f - \lambda E_k) \in S_k(SL_2(\mathbb{Z}))$ since it vanishes at cusp $i\infty$. Thus the result follows. □

We see that we get Eisenstein series for every even weight greater than 2. It turns out that the normalised Eisenstein series E_2 is not a modular form. We use the same definition as for other E_k, except that the double sum when $k = 2$ is not absolutely convergent, so we need to take care of the order of summation. Thus we define

$$E_2(z) = \frac{1}{2\zeta(2)}\sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty}{}' \frac{1}{(mz+n)^2}$$

where the primed summation means that $n \neq 0$ if $m = 0$. A small computation gives that

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n$$

where $q = e^{2\pi iz}$ and $\sigma_1(n) = \sum_{d|n} d$. For a proof see, **[14]**.

3.5. Modular Forms for Congruence Subgroups

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ of level N. We saw that $\mathfrak{H}^*$ is the extended upper half plane :

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{i\infty\}.$$

Modular forms for congruence subgroups are holomorphic functions $f(z) : \mathfrak{H} \to \mathbb{C}$ for which

$$f(\gamma z) = (cz+d)^k f(z), \forall \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma. \tag{3.1}$$

The punctured fundamental neighbourhood

$$U_C = \{z \in \mathfrak{H} : \text{Im}\,(z) > C\}$$

of $i\infty$ is mapped via $z \mapsto e^{2\pi iz/N}$ onto the punctured disc centered at zero, of radius $e^{-2\pi C/N}$.We might write $q^{1/N} = e^{-2\pi C/N}$ for a typical point on the punctured disc.

Let h be the least positive integer such that $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \Gamma$. Since Γ is of level N, we have $h \leq N$. For any function satisfying (3.1), we have $f(z+h) = f(z)$. Hence we have a well-defined map, which we also call f, from the unit disc to $\mathbb{C}$:

$$q^{1/h} \mapsto f(z)$$

where $z \in \mathfrak{H}$ is any point such that $q^{1/h} = e^{2\pi iz/h}$. If $f(z) : \mathfrak{H} \to \mathbb{C}$ is holomorphic, then $f(q^{1/h})$ will be holomorphic on the punctured unit disc and hence will have a Laurent expansion centered at $q^{1/h} = 0$,

$$f(q^{1/h}) = \sum_{n=-\infty}^{\infty} a_n q^{n/h}.$$

We call

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi izn/h}$$

a Fourier series at $i\infty$. More generally, for any $\gamma = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z})$, the function

$$(f|\gamma)(z) = (tz+u)^{-k} f(\frac{rz+s}{tz+u})$$

will be holomorphic on $\mathfrak{H}$ and will be modular under $\gamma^{-1}\Gamma\gamma$. Since $\Gamma(N)$ is normal in $SL_2(\mathbb{Z})$, the group $\gamma^{-1}\Gamma\gamma$ will also be a level N congruence subgroup. Thus we let h be the least positive integer such that $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \gamma^{-1}\Gamma\gamma$ so that $f|\gamma$ will be $h-$ periodic:

$$(f|\gamma)(z+h) = (f|\gamma)(z).$$

As before, we consider the holomorphic function on the unit disc given by

$$q^{1/h} \mapsto (f|\gamma)(z)$$

where $z \in \mathfrak{H}$ is any point such that $q^{1/h} = e^{2\pi iz/h}$. Now $(f|\gamma)$ will have a Laurent expansion

$$(f|\gamma)(q^{1/h}) = \sum_{n=-\infty}^{\infty} b_n q^{n/h}$$

centered at $q^{1/h} = 0$. We say that

$$(f|\gamma)(z) = \sum_{n=-\infty}^{\infty} b_n e^{2\pi izn/h}$$

is a Fourier expansion of f at $\gamma(i\infty)$.

When $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \notin \Gamma$, it is possible that there is some $\begin{bmatrix} -1 & h' \\ 0 & -1 \end{bmatrix} \in \gamma^{-1}\Gamma\gamma$ with $h' \geq 1$ but $\begin{bmatrix} 1 & h' \\ 0 & 1 \end{bmatrix} \notin \gamma^{-1}\Gamma\gamma$. In this case, $h = 2h'$. The theory of Riemann surfaces suggests that the Laurent series for $f|\gamma$ be considered as an expansion in terms of $q^{1/h'}$ rather than $q^{1/h}$. This leads to the possibility of half-integer orders at these so-called irregular cusps. Therefore, we define the width of the cusp $\gamma(i\infty)$ to be the least positive integer h' such that at least one of

$$\begin{bmatrix} 1 & h' \\ 0 & 1 \end{bmatrix} \in \gamma^{-1}\Gamma\gamma$$

or

$$\begin{bmatrix} -1 & h' \\ 0 & -1 \end{bmatrix} \in \gamma^{-1}\Gamma\gamma$$

holds and the expansion of $f|\gamma$ is written as

$$(f|\gamma)(z) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi izn/h'}.$$

Then the order of f at $\gamma(i\infty)$ is defined as

$$\nu_{\gamma(i\infty)}(f) := \inf\{n \in \frac{1}{2}\mathbb{Z} : c_n \neq 0\}.$$

If $-\infty < \nu_{\gamma(i\infty)}(f) < 0$, then f is said to be meromorphic at $\gamma(i\infty)$ with a pole of order $|\nu_{\gamma(i\infty)}(f)|$. If $\nu_{\gamma(i\infty)}(f) \geq 0$, then f is said to be holomorphic at $\gamma(i\infty)$. If $\nu_{\gamma(i\infty)}(f) > 0$, then f is said to vanish at $\gamma(i\infty)$ and has a zero of order $\nu_{\gamma(i\infty)}(f)$.

A modular form of weight k for Γ is a holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ satisfying

$$f(\gamma z) = (cz + d)^k f(z), \forall \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma. \tag{3.2}$$

which is holomorphic at every cusp. We denote by $M_k(\Gamma)$ the $\mathbb{C}-$vector space of modular forms of weight k for Γ. If $f \in M_k(\Gamma)$ is such that f vanishes at all the cusps, we say that f is a cusp form of weight k for Γ and $S_k(\Gamma)$ denotes the $\mathbb{C}-$vector space of such forms.

Let $k \geq 3$ and N a natural number. Let $g \in (\mathbb{Z}/N\mathbb{Z})^2$. We define the Eisenstein series

$$G_{k,g}(z) = \sum_{(m,n)\equiv g(\text{mod } N)}{}' \frac{1}{(mz+n)^k}, z \in \mathfrak{H}$$

where the summation is over all integers m, n satisfying the congruence condition $(m,n) \equiv g(\text{mod } N)$ and the dash on the summation means we exclude $(m,n) = (0,0)$. For any $\gamma \in SL_2(\mathbb{Z})$, it can be shown that $G_{k,g} \in M_k(\Gamma(N))$. Note that if k is odd and $2g \equiv (0,0)(\text{mod } N)$, then $G_{k,g} = 0$ since $G_{k,g} = (-1)^k G_{k,-g}$ and $g \equiv -g \text{ (mod } N)$.

If we let $g = (a_1, a_2) \in (\mathbb{Z}/N\mathbb{Z})^2$, then we can get the $q-$expansion of $G_{k,g}(z)$ which is given as follows:

$$G_{k,g}(z) = b_{k,g}(0) + \sum_{n=1}^{\infty} b_{k,g}(n) e^{2\pi i n z/N}$$

where the Fourier coefficients $b_{k,g}(n)$ are given as follows :

$$b_{k,g}(0) = \begin{cases} 0 & \text{if } a_1 \not\equiv 0(\text{mod } N) \\ \sum_{m\equiv a_2(\text{mod } N)} m^{-k} & \text{if } a_1 \equiv 0(\text{mod } N) \end{cases}$$

and

$$b_{k,g}(n) = \frac{(-2\pi i)^k}{N^k(k-1)!} \sum_{\substack{d|n \\ n/d\equiv a_1(\text{mod } N)}} d^{k-1}(\text{sgn } d) e^{2\pi i a_2 d/N}$$

where the summation is over all divisors of n (positive and negative) and

$$\text{sgn } d = \begin{cases} +1 & \text{if } d > 0 \\ -1 & \text{if } d < 0 \end{cases}$$

It can be shown that if

$$E_{2,N}(z) := E_2(z) - NE_2(Nz),$$

then $E_{2,N} \in M_2(\Gamma_0(N))$.

3.6. The Valence and Dimension Formulas

Given a meromorphic function $f : \mathfrak{H} \to \mathbb{C}$, not identically zero, and $z_0 \in \mathfrak{H}$, there is a unique integer n such that $\frac{f(z)}{(z-z_0)^n}$ is holomorphic and non-zero at z_0. We say n is the order of f at z_0 and denote it by $\nu_{z_0}(f)$. If f is holomorphic, then $\nu_{z_0}(f)$ is the order of the zero of f at z_0.

If f is a modular form of weight k for the full modular group, then $\nu_{z_o}(f)$ depends only on the orbit of z_0 under $SL_2(\mathbb{Z})$ so we need only study $\nu_z(f)$ for z in the fundamental domain of $SL_2(\mathbb{Z})$. $\nu_{i\infty}(f)$ is defined to be the order of the zero at $q = 0$ in the $q-$ expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

i.e. $\nu_{i\infty}(f)$ is the smallest value of n such that $a_n \neq 0$.

Note that $f \in M_k(SL_2(\mathbb{Z}))$ has only finite number of zeroes in the standard fundamental domain $\mathcal{F}$ because f being holomorphic on $\mathfrak{H}$ implies that the zeroes are isolated. Moreover, for some $c > 0$, the region $\{z \in \mathcal{F} : \text{Im } (z) > c\} \cup \{i\infty\}$, being a fundamental neighbourhood of $i\infty$, contains no zero of f except possibly $i\infty$. All other zeroes are contained in the compact region $\{z \in \mathcal{F} : \text{Im } (z) \leq c\}$ and this number is finite.

We now state the valence and dimension formulas. For a proof, see **[14]**.

THEOREM 14. *(The valence formula for $SL_2(\mathbb{Z})$) Let f be a modular form, not identically zero, of weight k for the full modular group $SL_2(\mathbb{Z})$. Then*

$$\nu_{i\infty}(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_{\rho^2}(f) + \sum_{\substack{z \neq i,\rho^2 \\ z \in \mathcal{F}}}{}' \nu_z(f) = \frac{k}{12},$$

where the primed summation excludes points with $Re(z) = \frac{1}{2}$ and points with both $|z| = 1$ and $Re(z) > 0$. Here $i = \sqrt{-1}$ and $\rho = e^{\frac{2\pi i}{3}}$.

THEOREM 15. *(The dimension formula for $SL_2(\mathbb{Z})$) For $k \geq 0$,*

$$dim\ M_k(SL_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 (mod\ 12) \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 (mod\ 12) \end{cases}$$

and for $k \geq 4$,

$$dim\ S_k(SL_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 (mod\ 12) \\ \lfloor \frac{k}{12} \rfloor & \text{if } k \not\equiv 2 (mod\ 12) \end{cases}$$

One can also derive analogs of the valence and dimension formula for any congruence subgroup Γ of $SL_2(\mathbb{Z})$. The general method used to derive these formulas is via the Riemann-Roch theorem, so we will content ourselves by merely stating the results.

We first need to define elliptic points. A point $z \in \mathfrak{H}$ is called an elliptic point for Γ if $\{\pm I\}\Gamma_z$ is strictly larger than $\{\pm\}$, where $\Gamma_z = \{\gamma \in \Gamma : \gamma z = z\}$ is the stabiliser subgroup of z. In other words, z is an elliptic point for Γ if and only if $\{\pm I\}\Gamma_z \neq \{\pm I\}$. We define the order of an elliptic point to be $|\frac{\{\pm I\}\Gamma_z}{\{\pm I\}}|$.

THEOREM 16. *(The valence formula for congruence subgroup) Let* Γ *be a congruence subgroup of* $SL_2(\mathbb{Z})$ *and* $0 \neq f \in M_k(\Gamma)$. *Then*

$$\sum_{z \in \Gamma \backslash \mathfrak{H}^*} \frac{\nu_z(f)}{|\Gamma_z|} = \frac{k}{2}(\frac{\epsilon_2}{2} + \frac{2\epsilon_3}{3} + \epsilon_\infty + 2g - 2),$$

where the sum is over $\Gamma-$ *equivalence classes of* $z \in \mathfrak{H}^*$, $\nu_z(f)$ *denotes the order of* f *at* z, Γ_z *is the stabiliser of* z *in* $\frac{\{\pm I\}\Gamma_z}{\{\pm I\}}$, g *is the genus of* $\Gamma \setminus \mathfrak{H}^*$, ϵ_2 *is the number of elliptic points of order* 2 *in the fundamental domain for* Γ, ϵ_3 *is the number of elliptic points of order* 3 *in the fundamental domain for* Γ, *and* ϵ_∞ *is the number of* $\Gamma-$*inequivalent cusps in the fundamental domain for* Γ.

This analogously gives the dimension formula for congruence subgroup.

THEOREM 17. *(The dimension formula for congruence subgroup) Let* Γ *be a congruence subgroup of* $SL_2(\mathbb{Z})$ *and* k *an non-negative integer. Then*

$$dim\ M_k(\Gamma) = \begin{cases} (k-1)(g-1) + [\frac{k}{4}]\epsilon_2 + [\frac{k}{3}]\epsilon_3 + \frac{k}{2}\epsilon_\infty & \text{if } k \geq 2 \\ 1 & \text{if } k = 0 \end{cases}$$

and

$$dim\ S_k(\Gamma) = \begin{cases} dim\ M_k(\Gamma) - \epsilon_\infty & \text{if } k \geq 4 \\ g & \text{if } k = 2 \\ 0 & \text{if } k = 0 \end{cases}$$

where g, ϵ_2, ϵ_3, ϵ_∞ *are as in the previous theorem.*

THEOREM 18. *(Sturm's Bound) Let* Γ *be a congruence subgroup and* $f \in M_k(\Gamma)$. *Let* $r_1, \cdots, r_t$ *be the* $\Gamma-$ *inequivalent cusps of* Γ. *If*

$$\sum_{i=1}^{t} \nu_{r_i}(f) > \frac{k[SL_2(\mathbb{Z}) : \{\pm I\}\Gamma]}{12},$$

then $f = 0$.

COROLLARY 1. *For any congruence subgroup* Γ *of* $SL_2(\mathbb{Z})$,

$$dim\ M_k(\Gamma) \leq \frac{k}{12}[SL_2(\mathbb{Z}) : \{\pm I\}\Gamma] + 1.$$

3.7. The Eta Function

For $z \in \mathfrak{H}$, we define the Dedekind $\eta-$ function by

$$\eta(z) = e^{2\pi iz/24} \prod_{n=1}^{\infty} (1 - e^{2\pi inz}).$$

THEOREM 19. *For* $z \in \mathfrak{H}$,

$$\eta(-\frac{1}{z}) = \sqrt{\frac{z}{i}}\eta(z),$$

where the square root is the branch with non-negative real part.

PROOF. The product defining $\eta(z)$ clearly converges to a non-zero value for any $z \in \mathfrak{H}$ and thus defines a holomorphic function on $\mathfrak{H}$. Taking the logarithmic derivative, we get

$$\frac{\eta'(z)}{\eta(z)} = \frac{\pi i}{12}(1 - 24\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}),$$

where $q = e^{2\pi iz}$. The right hand side is clearly $\pi i E_2(z)/12$ since

$$\frac{q^n}{1-q^n} = \sum_{m=1}^{\infty} q^{mn}$$

and

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n,$$

where $q = e^{2\pi iz}$ and $\sigma_1(n) = \sum_{d|n} d$. Therefore replacing z by $-\frac{1}{z}$, we get

$$\frac{\eta'(-\frac{1}{z})}{\eta(-\frac{1}{z})} = \frac{\pi i}{12} E_2(-\frac{1}{z}).$$

Now it can be shown easily that

$$E_2(-\frac{1}{z}) = z^2 E_2(z) + \frac{6z}{\pi i}.$$

So, we obtain,

$$\frac{\eta'(-\frac{1}{z})}{\eta(-\frac{1}{z})}.\frac{1}{z^2} = \frac{\pi i E_2(z)}{12} + \frac{1}{2z}$$

so that

$$\frac{\eta'(-\frac{1}{z})}{\eta(-\frac{1}{z})}.\frac{1}{z^2} = \frac{\eta'(z)}{\eta(z)} + \frac{1}{2z}.$$

But the right hand side is now clearly the logarithmic derivative of $\sqrt{z}\eta(z)$. Therefore, $\eta(-\frac{1}{z}) = \lambda\sqrt{z}\eta(z)$ for some constant λ. Putting $z = i$ shows that $\lambda = \frac{1}{\sqrt{i}}$. Finally since $z \in \mathfrak{H}$, it is clear that $\frac{\sqrt{z}}{\sqrt{i}} = \sqrt{\frac{z}{i}}$.

□

3.8. Nebentypus

A Dirichlet character of modulus N is a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*.$$

This implies that $\chi(1) = 1$.

Let χ be a Dirichlet character of modulus N. For each $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$, we define $\psi(\gamma) = \chi(d)$. Then it can be shown that $\psi(\gamma_1\gamma_2) = \psi(\gamma_1)\psi(\gamma_2)$.

The set of Dirichlet characters of modulus N forms a group of order $\phi(N)$ under multiplication, where ϕ denotes the Euler function.

THEOREM 20. $\sum_\chi \chi(d) = \begin{cases} \phi(N) & \text{if } d \equiv 1 \text{ (mod } N). \\ 0 & \text{otherwise} \end{cases}$

where the sum is over all Dirichlet characters modulo N.

PROOF. If $d = 1$, the result is clear since the set of Dirichlet characters modulo N forms a group of order $\phi(N)$. Therefore suppose $d \not\equiv 1 \pmod N$. Then there is a character ψ such that $\psi(d) \neq 1$. Thus

$$T = \sum_\chi \chi(d) = \sum_\chi (\chi\psi)(d) = \psi(d)T$$

because as χ ranges over all Dirichlet characters, so does $\chi\psi$. Hence $T = 0$ since $\psi(d) \neq 1$.

□

THEOREM 21. *If $\chi \neq 1$ is a Dirichlet character modulo N, then*

$$\sum_{a \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(a) = 0.$$

PROOF. Since χ is not trivial, there is a $b \neq 1$ such that $\chi(b) \neq 1$ with $(b, N) = 1$. Then,

$$S = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(a) = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(ab) = \chi(b)S$$

because as a ranges over co-prime residue classes, so does ab. Therefore $S = 0$ since $\chi(b) \neq 1$.

□

For any Dirichlet character χ modulo N, we define the following vector subspace of $M_k(\Gamma_1(N))$:

$$M_k(\Gamma_0(N), \chi) := \left\{ f \in M_k(\Gamma_1(N)) : f|\gamma = \chi(d)f,\ \forall \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \right\}.$$

In other words, for a Dirichlet character χ modulo N, a holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is a modular form of weight k and nebentypus χ for $\Gamma_0(N)$ if

- $f|\gamma = \chi(d)f\ \forall \gamma \in \Gamma_0(N)$,
- $f|\xi(z) = \sum_{n=0}^{\infty} a_{\xi,n} q_N^n\ \forall \xi \in SL_2(\mathbb{Z}), q_N = e^{2\pi i z/N}$.

If $a_{\xi,0} = 0\ \forall \xi \in SL_2(\mathbb{Z})$, then f is called a cusp form of weight k and nebentypus χ for $\Gamma_0(N)$. We denote by $S_k(\Gamma_0(N), \chi)$ the subspace of $M_k(\Gamma_0(N), \chi)$ consisting of these forms. The complement of $S_k(\Gamma_0(N), \chi)$ in $M_k(\Gamma_0(N), \chi)$ is the Eisenstein subspace and denoted $E_k(\Gamma_0(N), \chi)$. An element of the Eisenstein subspace is called the Eisenstein series of weight k and nebentypus χ for $\Gamma_0(N)$. In particular, if χ is the trivial character, then $M_k(\Gamma_0(N), \chi) = M_k(\Gamma_0(N))$.

CHAPTER 4

THE SUM OF FOUR SQUARES AND VARIATIONS

In this chapter, we first outline a proof of Jacobi's four square theorem using modular forms and then sketch a general method for determining an explicit formula for the number of ways of expressing any positive integer as a special value of a given quaternary quadratic form, with positive integer coefficients.

4.1. Jacobi's Four Square Theorem

Let $\theta(z)$ denote Ramanujan's theta function defined by

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 z}$$

for $z \in \mathfrak{H}$

The Dedekind eta function $\eta(z)$ is the holomorphic function defined on the upper half plane $\mathfrak{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$ by

$$\eta(z) = e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}).$$

If we take $q = q(z) = e^{2\pi i z}$ with $z \in \mathfrak{H}$ and so $|q| < 1$, we get

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

For $a, b, c, d \in \mathbb{N}, n \in \mathbb{N}_0$, we define

$$N(a, b, c, d; n) = |\{(x, y, z, w) \in \mathbb{Z}^4 : n = ax^2 + by^2 + cz^2 + dw^2\}|$$

Now it is easy to see that for $q \in \mathbb{C}$, writing $q = e^{2\pi i z}$, we have

$$\sum_{n=1}^{\infty} N(a, b, c, d; n) q^n = \theta(az)\theta(bz)\theta(cz)\theta(dz),$$

where we define $N(a, b, c, d; 0) = 1$.

DEFINITION 6. *An **eta quotient** is defined to be the finite product of the form*

$$f(z) = \prod_{\delta} \eta^{r_\delta}(\delta z)$$

where δ runs through a finite set of positive integers and r_δ are non-zero integers.

The infinite product representation of $\theta(z)$ is given by the eta quotient

$$\theta(z) = \frac{\eta^5(2z)}{\eta^2(z)\eta^2(4z)}.$$

This can be proved easily by substituting $x = 1$ in Jacobi's triple product identity for $|q| < 1$ given by

$$\prod_{n=0}^{\infty}(1-q^{2n+2})(1+q^{2n+1}x)(1+\frac{q^{2n+1}}{x}) = \sum_{n=-\infty}^{\infty} q^{n^2}x^n.$$

For a proof, see page 81 of **[14]**. If we are interested in $N(1,1,1,1;n)$, we need to consider $\theta^4(z)$.

THEOREM 22. *If*

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 z},$$

then

$$\theta(\frac{z}{4z+1}) = \sqrt{4z+1}\theta(z),$$

where the branch of the square root is the principal branch (whose image is contained in the right half plane).

PROOF. We saw that $\theta(z)$ can be written as

$$\theta(z) = \frac{\eta^5(2z)}{\eta^2(z)\eta^2(4z)}$$

and from section 3.7, we have that

$$\eta(-\frac{1}{z}) = \sqrt{\frac{z}{i}}\eta(z).$$

It is immediate from the definition that

$$\eta(z+1) = e^{\frac{\pi i}{12}}\eta(z).$$

Now,

$$\begin{aligned}\eta(\tfrac{4z}{4z+1}) &= \eta(-\tfrac{1}{4z+1}+1)\\ &= e^{\frac{\pi i}{12}}\eta(-\tfrac{1}{4z+1})\\ &= e^{\frac{\pi i}{12}}\sqrt{\tfrac{4z+1}{i}}\eta(4z+1)\\ &= e^{\frac{\pi i}{6}}\sqrt{\tfrac{4z+1}{i}}\eta(4z).\end{aligned}$$

Also,

$$\begin{aligned}\eta(\tfrac{2z}{4z+1}) &= \eta(-(-\tfrac{1}{2z}-2)^{-1})\\ &= \sqrt{i\tfrac{4z+1}{2z}}\eta(-\tfrac{1}{2z}-2)\\ &= e^{\frac{-\pi i}{6}}\sqrt{i\tfrac{4z+1}{2z}}\eta(-\tfrac{1}{2z})\\ &= e^{\frac{-\pi i}{6}}\sqrt{i\tfrac{4z+1}{2z}}\sqrt{\tfrac{2z}{i}}\eta(2z).\end{aligned}$$

Finally,

$$\begin{aligned}\eta(\tfrac{z}{4z+1}) &= \eta(-(-\tfrac{1}{z}-4)^{-1})\\ &= \sqrt{i\tfrac{4z+1}{z}}\eta(-\tfrac{1}{z}-4)\\ &= e^{\frac{-\pi i}{3}}\sqrt{i\tfrac{4z+1}{z}}\eta(-\tfrac{1}{z})\\ &= e^{\frac{-\pi i}{3}}\sqrt{i\tfrac{4z+1}{z}}\sqrt{\tfrac{z}{i}}\eta(z).\end{aligned}$$

Putting everything together gives

$$\theta(\tfrac{z}{4z+1}) = \sqrt{4z+1}\theta(z).$$

□

THEOREM 23. $\theta^4 \in M_2(\Gamma_0(4))$.

PROOF. Using the previous theorem, we get

$$\theta^4(\frac{z}{4z+1}) = (4z+1)^2\theta^4(z).$$

Since $\theta^4(z+1) = \theta^4(z)$ and since $\Gamma_0(4)$ is generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$ and $-I$, we deduce that $\theta^4 \in M_2(\Gamma_0(4))$. □

THEOREM 24. *dim* $M_2(\Gamma_0(4)) = 2$ *and* $\{E_{2,2}, E_{2,4}\}$ *is a basis for* $M_2(\Gamma_0(4))$.

PROOF. Using Corollary 2.1,

$$\dim M_2(\Gamma_0(4)) \leq 2.$$

Now, $E_{2,2}$ and $E_{2,4} \in M_2(\Gamma_0(4))$. It is easy to check that

$$E_{2,2} = -1 - 24q + \cdots$$

$$E_{2,4} = -3 - 24q + \cdots$$

Clearly these elements are linearly independent over $\mathbb{C}$. □

THEOREM 25. *(Jacobi) With* $N(a,b,c,d;n)$ *as defined above,*

$$N(1,1,1,1;n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d.$$

PROOF. We have $\theta^4 \in M_2(\Gamma_0(4))$. So, writing θ^4 in terms of the basis elements, we have

$$\theta^4 = aE_{2,2} + bE_{2,4}.$$

A quick calculation comparing coefficients of $q-$expansions of both sides of this equation leads to

$$\theta^4 = -\frac{1}{3}E_{2,4},$$

which leads to the formula

$$N(1,1,1,1;n) = 8(\sigma(n) - 4\sigma(n/4)),$$

where $\sigma(n/4) = 0$ if $4 \nmid n$. If $4|n$, we write $n = 4n_1$ and $4\sigma(n_1)$ is the sum of the divisors d of n with $4|d$. That leads to the desired formula.

□

4.2. Sketch of the General Method

For $q \in \mathbb{C}$ and $z \in \mathfrak{H}$, writing $q = e^{2\pi iz}$, we have

$$\sum_{n=0}^{\infty} N(a,b,c,d;n)q^n = \theta(az)\theta(bz)\theta(cz)\theta(dz),$$

where $N(a,b,c,d;0) = 1$.
Since $\theta(z)$ has the following infinite product expansion

$$\theta(z) = \frac{\eta^5(2z)}{\eta^2(z)\eta^2(4z)},$$

we see that $\sum_{n=0}^{\infty} N(a,b,c,d;n)q^n$ is given by a certain eta quotient.

We will now use the following theorem to determine if certain eta quotients are modular forms. For a proof, see pg.99 of **[9]**

THEOREM 26. *(Ligozat's Criteria) Let $f(z)$ be an eta quotient given by*

$$f(z) = \prod_{\delta} \eta^{r_\delta}(\delta z)$$

where δ runs through a finite set of positive integers and r_δ are non-zero integers and there existsa positive integer N which satisfy the following conditions :

(L1) $\sum_{\delta|N} \delta \cdot r_\delta \equiv 0 \ (mod\ 24)$

(L2) $\sum_{\delta|N} \frac{N}{\delta} \cdot r_\delta \equiv 0 \ (mod\ 24)$

(L3) for each $d|N$, $\sum_{\delta|N} \frac{gcd(d,\delta)^2 \cdot r_\delta}{\delta} \geq 0$.

Then, $f(z) \in M_k(\Gamma_0(N), \chi)$ *where the character* $\chi(m)$ *is given by*

$$\left(\frac{(-1)^k s}{m}\right)$$

with weight $k = \frac{1}{2}\sum_{\delta|N} r_\delta$ *and* $s = \prod_{\delta|N} \delta^{r_\delta}$.

If (L3) is replaced by

(L4) for each $d|N$, $\sum_{\delta|N} \frac{gcd(d,\delta)^2 \cdot r_\delta}{\delta} > 0$,

then $f(z) \in S_k(\Gamma_0(N), \chi)$ *where the character* $\chi(m)$ *is given by*

$$\left(\frac{(-1)^k s}{m}\right)$$

with weight $k = \frac{1}{2}\sum_{\delta|N} r_\delta$ *and* $s = \prod_{\delta|N} \delta^{r_\delta}$.

Fix a positive integer N. Let ϵ be a Dirichlet character modulo N. To find the set of canonical generators for the group $(\mathbb{Z}/N\mathbb{Z})^*$, write $N = \prod_{i=0}^{n} p_i^{e_i}$ where $p_0 < p_1 < \cdots < p_n$ are the prime divisors of N. Each factor $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is a cyclic group $C_i = \langle g_i \rangle$, except if $p_0 = 2$ and $e_0 \geq 3$, in which case $(\mathbb{Z}/p_0^{e_0}\mathbb{Z})^*$ is a product of the cyclic group $C_0 = \langle -1 \rangle$ of order 2 with the cyclic subgroup $C_1 = \langle 5 \rangle$. In all cases we have

$$(\mathbb{Z}/N\mathbb{Z})^* \cong \prod_{0 \leq i \leq n} C_i.$$

For i such that $p_i > 2$, choose the generator g_i of C_i to be the element of $\{2, 3, \cdots, p_i^{e_i} - 1\}$ that is smallest and generates Finally use the Chinese Remainder Theorem to lift each g_i to an element in $(\mathbb{Z}/N\mathbb{Z})^*$, also denoted g_i, that is modulo each $p_j^{e_j}$ for $j \neq i$. Now we will describe how one can compute the conductor of a character. As a reference for these facts, see page 70 of **[19]**.

The following is the algorithm for computing the order of a Dirichlet character.

ALGORITHM 1. *(Order of Character) This algorithm computes the order of a Dirichlet character* ϵ *modulo* N.

- *Compute the order* r_i *of each* $\epsilon(g_i)$*, for each minimal generator* g_i *of* $(\mathbb{Z}/N\mathbb{Z})^*$. *The order of* $\epsilon(g_i)$ *is a divisor of* $n = |(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*|$ *so we can compute its order by considering the divisors of* n.
- *Compute and output the least common multiple of the integers* r_i.

The next algorithm factors a character ϵ as a product of "local" characters.

ALGORITHM 2. *(Factorisation of Character)Given a Dirichlet character* ϵ *modulo* N, *with* $N = \prod_{i=0}^{n} p_i^{e_i}$, *this algorithm finds Dirichlet characters* ϵ_i *modulo* $p_i^{e_i}$, *such that for all* $a \in (\mathbb{Z}/N\mathbb{Z})^*$,*we have* $\epsilon(a) = \prod \epsilon_i(a \pmod{p_i^{e_i}})$. *If* $2|N$, *the steps are as follows:*

- *Let* g_i *be the minimal generators of* $(\mathbb{Z}/N\mathbb{Z})^*$, *so* ϵ *is given by a list* $[\epsilon(g_0), \cdots, \epsilon(g_n)]$
- *For* $i = 2, \cdots, n$, *let* ϵ_i *be the character modulo* $p_i^{e_i}$ *defined by the singleton list* $[\epsilon(g_i)]$.
- *Let* ϵ_1 *be the character modulo* 2^{e_1} *defined by the list* $[\epsilon(g_0), \epsilon(g_1)]$ *of length* 2. *Output the* ϵ_i *and terminate.*

If $2 \not| N$*, then omit the third step and include all i in the second step.*

DEFINITION 7. *(Conductor) The conductor of a Dirichlet character* ϵ *modulo* N *is the smallest positive divisor* $c|N$ *such that there is a character* ϵ' *modulo* c *for which* $\epsilon(a) = \epsilon'(a)$ *for all* $a \in \mathbb{Z}$ *with* $(a, N) = 1$*. A Dirichlet character is primitive if its modulus equals its conductor. The character* ϵ' *associated to* ϵ *with modulus equal to the conductor of* ϵ *is called the primitive character associated to* ϵ*.*

ALGORITHM 3. *(Conductor)The following algorithm computes the conductor of Dirichlet character modulo* N*.*

1. *[Factor Conductor] Find characters* χ_i *whose product is* χ*.*
2. *[Computing order] Compute order* r_i *for each* χ_i*.*
3. *[Conductor of factors] For each i, either set* c_i *to be* 1 *if* χ_i *is the trivial character or set* $c_i = p_i^{ord_{p_i}(r_i)+1}$*, where* $ord_p(n)$ *denotes the largest power of p that divides n.*
4. *[Finished] compute product of the* c_i*.*

Once we have computed the conductor of the character, we can use it to compute the dimension of the space $M_k(\Gamma_0(N), \chi)$.

The following theorem gives the formulae to compute the dimensions of $E_k(\Gamma_0(N), \chi)$ and $S_k(\Gamma_0(N), \chi)$. See page 98 of **[19]**.

THEOREM 27.

$$\dim S_k(\Gamma_0(N), \chi) - \dim M_{2-k}(\Gamma_0(N), \chi) = \frac{k-1}{12}\mu_0(N) - 1/2\prod_{p|N}\lambda(p, N, \nu_p(c)) + \gamma_4(k)\sum_{x \in A_4(N)}\chi(x) + \gamma_3(k)\sum_{x \in A_3(N)}\chi(x) \quad (4.1)$$

where

$$\mu_0(N) = \prod_{p|N}(p^{\nu_p(N)} + p^{\nu_p(N)-1})$$

and

$$A_4(N) = \{x \in \mathbb{Z}/n\mathbb{Z} : x^2 + 1 = 0\}$$

and

$$A_3(N) = \{x \in \mathbb{Z}/n\mathbb{Z} : x^2 + x + 1 = 0\}$$

and

$$\gamma_4(k) = \begin{cases} -1/4 & \text{if } k \equiv 2 \ (mod\ 4) \\ 1/4 & \text{if } k \equiv 0 \ (\ mod\ 4) \\ 0 & \text{if } k \text{ odd.} \end{cases}$$

and

$$\gamma_3(k) = \begin{cases} -1/3 & \text{if } k \equiv 2 \ (mod\ 3) \\ 1/3 & \text{if } k \equiv 0 \ (mod\ 3) \\ 0 & \text{if } k \equiv 1 \ (mod\ 3.) \end{cases}$$

and for $p|N$, let $r = \nu_p(N)$. Then,

$$\lambda(p, N, \nu_p(c)) = \begin{cases} p^{r/2} + p^{r/2-1} & \text{if } 2 \cdot \nu_p(c) \leq r, 2|r \\ 2 \cdot p^{(r-1)/2} & \text{if } 2 \cdot \nu_p(c) \leq r, 2 \nmid r \\ 2 \cdot p^{r-\nu_p(c)} & \text{if } 2 \cdot \nu_p(c) > r \end{cases}$$

Also,

$$dim\ E_k(\Gamma_0(N), \chi) = dim\ M_k(\Gamma_0(N), \chi) - dim\ S_k(\Gamma_0(N), \chi)$$

where

$$\begin{aligned} \dim M_k(\Gamma_0(N), \chi) = -(\frac{1-k}{12}\mu_0(N) - 1/2 \prod_{p|N} \lambda(p, N, \nu_p(c)) \\ + \gamma_4(2-k) \sum_{x \in A_4(N)} \chi(x) + \gamma_3(2-k) \sum_{x \in A_3(N)} \chi(x)) \end{aligned} \quad (4.2)$$

Note: Here c denotes the conductor of χ.

Let χ and ψ be primitive Dirichlet characters with conductors L and R respectively. Let

$$E_{k,\chi,\psi}(z) = c_0 + \sum_{m \geq 1} (\sum_{n|m} \psi(n)\chi(m/n)n^{k-1}) e^{2\pi imz} \quad (4.3)$$

where

$$c_0 = \begin{cases} 0 & \text{if } L > 1 \\ -\frac{B_{k,\psi}}{2k} & \text{if } L = 1 \end{cases}$$

When $\chi = \psi = 1$, $k \geq 4$, then $E_{k,\chi,\psi} = E_k$.

THEOREM 28. *Let $t > 0$ be an integer and χ, ψ be as above, and let k be a positive integer such that $\chi(-1)\psi(-1) = (-1)^k$. Except when $k = 2$ and $\chi = \psi = 1$, the power series $E_{k,\chi,\psi}(tz)$ defines an element of $M_k(RLt, \chi/\psi)$. If $\chi = \psi = 1, k = 2, t > 1$, and $E_2(z) = E_{k,\chi,\psi}(z)$, then $E_2(z) - tE_2(tz)$ is a modular form in $M_2(\Gamma_0(t))$.*

THEOREM 29. *The Eisenstein series in $M_k(\Gamma_0(N), \epsilon)$ coming from the previous theorem with $RLt|N$ and $\chi/\psi = \epsilon$ form a basis for $E_k(\Gamma_0(N), \epsilon)$.*

Once we have a basis for $E_k(\Gamma_0(N), \chi)$, one can compute a basis of $S_k(\Gamma_0(N), \chi)$ using Ligozat's criteria and combining the two, get a basis for $M_k(\Gamma_0(N), \chi)$. This is because it is known that

$$M_k(\Gamma_0(N), \chi) = S_k(\Gamma_0(N), \chi) \oplus E_k(\Gamma_0(N), \chi).$$

See **[19]**. Thus we can write $\sum_{n=0}^{\infty} N(a, b, c, d; n)q^n$ in terms of the basis elements. Finally comparing coefficients of q^n on both sides, we can derive an explicit formula for $N(a, b, c, d; n)$.

CHAPTER 5

COMPUTING THE NUMBER OF REPRESENTATIONS OF AN INTEGER AS $x^2 + y^2 + z^2 + 3u^2$

For $a, b, c, d \in \mathbb{N}, n \in \mathbb{N}_0$, we defined

$$N(a, b, c, d; n) = |\{(x, y, z, w) \in \mathbb{Z}^4 : n = ax^2 + by^2 + cz^2 + dw^2\}|$$

In Chapter 2, we saw 54 4−tuples (a, b, c, d) so that there exists $(x, y, z, w) \in \mathbb{Z}^4$ such that any positive integer can be written as $ax^2 + by^2 + cz^2 + dw^2$. We are interested in determining explicit formula for the number of representations of a positive integer n by quaternary quadratic forms with coefficients being one of those 55 4−tuples.
Out of those 55 4−tuples, formulas for a few are known. The following formula

$$N(1, 1, 1, 1; n) = 8\sigma(n) - 32\sigma(n/4)$$

where $\sigma(n) = \sum_{m|n} m$ is due to Jacobi. We outlined a proof of this in the previous chapter. The formula

$$N(1, 1, 2, 2; n) = 4\sigma(n) - 4\sigma(n/2) + 8\sigma(n/4) - 32\sigma(n/8)$$

was stated by Liouville. Similarly, formulas for $N(1, 1, 1, 2; n)$ and $N(1, 2, 2, 2; n)$ were also stated by Liouville. See **[11]** and **[12]**.

In this chapter, we will determine a similar formula for $N(1, 1, 1, 3; n)$ using the theory of modular forms developed in Chapter 3 and 4.
We are interested in $N(1, 1, 1, 3; n)$; thus we need to consider $f(z) = \theta^3(z)\theta(3z)$.

THEOREM 30. *$f(z) = \theta^3(z)\theta(3z) \in M_2(\Gamma_0(12), \chi)$ for $\chi(d) = (\frac{2^4 \cdot 3}{d})$.*

PROOF. Using the infinite product representation for $\theta(z)$, we get that

$$\theta^3(z)\theta(3z) = \frac{\eta^{15}(2z)\eta^5(6z)}{\eta^6(z)\eta^6(4z)\eta^2(3z)\eta^2(12z)}.$$

Now, using Ligozat's Criteria for $N = 12$ and $f(z) = \theta^3(z)\theta(3z)$, we get that

$$f(z) \in M_2(\Gamma_0(12), \chi)$$

for $\chi(d) = (\frac{2^4 \cdot 3}{d})$.

□

Now our goal is to find a basis for $M_2(\Gamma_0(12), \chi)$ so that we can write $f(z) = \theta^3(z)\theta(3z)$ in terms of the basis elements.

5.1. Computing Dimension of $M_2(\Gamma_0(12), \chi)$

To apply the formula mentioned in Chapter 4, we first need to compute the conductor of χ. Firstly, we see that $\chi(d) = (\frac{2^4 \cdot 3}{d})$ is a character modulo 12.

d	0	1	2	3	4	5	6	7	8	9	10	11
$\chi(d)$	0	1	0	0	0	-1	0	-1	0	0	0	1

Table 2: Table for values of χ.

To factorise χ, we do the following:

First we note that

$$(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/2^2\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*.$$

Since $(\mathbb{Z}/4\mathbb{Z})^*$ is generated by $\{1,3\}$ and $(\mathbb{Z}/3\mathbb{Z})^*$ is generated by $\{1,2\}$, the minimal generators for $(\mathbb{Z}/12\mathbb{Z})^*$ are x_1 and x_2 such that x_1 is the lift of $(1,2) \in (\mathbb{Z}/2^2\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$ and x_2 is the lift of $(3,1) \in (\mathbb{Z}/2^2\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$ respectively to $(\mathbb{Z}/12\mathbb{Z})^*$. Using the Chinese remainder Theorem, we get that $x_1 = 5$ and $x_2 = 7$.
Now we use the algorithm from Chapter 4 and note that $\chi(5) = -1$ has order 2 in $(\mathbb{Z}/3\mathbb{Z})^*$ and $\chi(7) = -1$ has order 2 in $(\mathbb{Z}/4\mathbb{Z})^*$.
Thus,
$c_1 = 2^{ord_2(2)+1} = 4$
$c_2 = 3^{ord_3(2)+1} = 3$.

Thus we get that the conductor of χ is 12.

$$\mu_0(12) = 12.$$

$$\lambda(2, 12, \nu_2(12)) = 2.$$

$$\lambda(3, 12, \nu_3(12)) = 2.$$

$$A_4(12) = \emptyset.$$

$$A_3(12) = \emptyset.$$

Since $\dim M_0(\Gamma_0(12), \chi) = 0$, applying the formulas for dimension, we get that

$$\dim S_2(\Gamma_0(12), \chi) = 0$$

and

$$\dim E_2(\Gamma_0(12), \chi) = 4.$$

Thus,

$$\dim M_2(\Gamma_0(12), \chi) = 4.$$

5.2. Computing a Basis for $M_2(\Gamma_0(N), \chi)$

We will use the machinery developed in Chapter 4 to construct a basis for $E_2(\Gamma_0(12), \chi)$.

Since $|(\mathbb{Z}/12\mathbb{Z})^*| = 4$, there are 4 Dirichlet characters of modulus 12 over $\mathbb{R}$. Also since we know that $\{5, 7\}$is the set of minimal generators for $(\mathbb{Z}/12\mathbb{Z})^*$, the Dirichlet characters modulo 12 are given by $\epsilon_1 = \chi$, ϵ_2, ϵ_3 and ϵ_4 which are defined as follows :

- $\epsilon_1(5) = -1, \epsilon_1(7) = -1$
- $\epsilon_2(5) = 1, \epsilon_2(7) = 1$
- $\epsilon_3(5) = -1, \epsilon_3(7) = 1$
- $\epsilon_4(5) = 1, \epsilon_4(7) = -1$

Evaluating the conductors of these characters as before, we get that ϵ_2, ϵ_3, ϵ_4 has conductors $1, 3, 4$ respectively. Thus, $\epsilon_2, \epsilon_3, \epsilon_4$ are primitive Dirichlet characters modulo $1, 3, 4$ respectively.

THEOREM 31. *Let χ and ψ be Dirichlet characters. For $n \in \mathbb{N}$, we define $\sigma_{\chi,\psi}(n)$ by*

$$\sigma_{\chi,\psi}(n) = \sum_{1 \leq m, m|N} \psi(m)\chi(n/m)m.$$

For $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ as defined earlier, we define the following power series :

$$E_{\epsilon_1,\epsilon_2}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_1,\epsilon_2}(n)e^{2\pi inz},$$

$$E_{\epsilon_2,\epsilon_1}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_2,\epsilon_1}(n)e^{2\pi inz},$$

$$E_{\epsilon_4,\epsilon_3}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_4,\epsilon_3}(n)e^{2\pi inz},$$

$$E_{\epsilon_3,\epsilon_4}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_3,\epsilon_4}(n) e^{2\pi i n z}.$$

Then these forms $E_{\epsilon_1,\epsilon_2}(z)$, $E_{\epsilon_2,\epsilon_1}(z)$, $E_{\epsilon_3,\epsilon_4}(z)$ and $E_{\epsilon_4,\epsilon_3}(z)$ form a basis for $E_2(\Gamma_0(12),\chi)$ for $\chi(d) = (\frac{2^4.3}{d})$.

PROOF. First, write $q = e^{2\pi i z}$. Then, we consider the following 4 cases :

Case 1: For $\chi = \frac{\epsilon_1}{\epsilon_2}$. $R = 1, L = 12, t = 1, k = 2$,

$$\begin{aligned} E_{2,\epsilon_1,\epsilon_2}(z) &= c_0 + \sum_{m\geq 1} (\sum_{n|m} \epsilon_2(n)\epsilon_1(m/n)n) q^m \\ &= q + 2q^2 + 3q^3 + 4q^4 + \cdots \end{aligned}$$

Case 2: For $\chi = \frac{\epsilon_2}{\epsilon_1}$. $R = 12, L = 1, t = 1, k = 2$,

$$\begin{aligned} E_{2,\epsilon_2,\epsilon_1}(z) &= c_0 + \sum_{m\geq 1} (\sum_{n|m} \epsilon_1(n)\epsilon_2(m/n)n) q^m \\ &= -1 + q + q^2 + q^3 + q^4 + \cdots \end{aligned}$$

Case 3: For $\chi = \frac{\epsilon_4}{\epsilon_3}$. $R = 3, L = 4, t = 1, k = 2$,

$$\begin{aligned} E_{2,\epsilon_4,\epsilon_3}(z) &= c_0 + \sum_{m\geq 1} (\sum_{n|m} \epsilon_3(n)\epsilon_4(m/n)n) q^m \\ &= q - 2q^2 - q^3 + 4q^4 + \cdots \end{aligned}$$

Case 4: For $\chi = \frac{\epsilon_3}{\epsilon_4}$. $R = 4, L = 3, t = 1, k = 2$,

$$\begin{aligned} E_{2,\epsilon_3,\epsilon_4}(z) &= c_0 + \sum_{m\geq 1} (\sum_{n|m} \epsilon_4(n)\epsilon_3(m/n)n) q^m \\ &= q - q^2 - 3q^3 + q^4 + \cdots \end{aligned}$$

Then using Theorem 26, theses four forms form a basis for $E_2(\Gamma_0(12),\chi)$ for $\chi(d) = (\frac{2^4.3}{d})$. □

COROLLARY 2. *Let χ and ψ be Dirichlet characters. For $z \in \mathfrak{H}$, write $q = e^{2\pi i z}$. For $n \in \mathbb{N}$, we define $\sigma_{\chi,\psi}(n)$ by*

$$\sigma_{\chi,\psi}(n) = \sum_{1\leq m, m|n} \psi(m)\chi(n/m)m.$$

For $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ as defined earlier, we define the following power series:

$$E_{\epsilon_1,\epsilon_2}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_1,\epsilon_2}(n) e^{2\pi i n z},$$

$$E_{\epsilon_2,\epsilon_1}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_2,\epsilon_1}(n) e^{2\pi i n z},$$
$$E_{\epsilon_4,\epsilon_3}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_4,\epsilon_3}(n) e^{2\pi i n z},$$
$$E_{\epsilon_3,\epsilon_4}(z) = \sum_{n=1}^{\infty} \sigma_{\epsilon_3,\epsilon_4}(n) e^{2\pi i n z}.$$

Then these forms form a basis for $M_2(\Gamma_0(12), \chi)$ for $\chi(d) = (\frac{2^4.3}{d})$.

PROOF. Since

$$\dim S_2(\Gamma_0(12), \chi) = 0,$$

and

$$M_k(\Gamma_0(N), \chi) = E_k(\Gamma_0(N), \chi) \oplus S_k(\Gamma_0(N), \chi),$$

we have that

$$\dim M_2(\Gamma_0(12), \chi) = \dim E_2(\Gamma_0(12), \chi) = 4.$$

Thus using the previous theorem, the result follows. □

5.3. Computing $N(1,1,1,3;n)$

THEOREM 32. $f(z) = \theta^3(z)\theta(3z) = 6E_{\epsilon_1,\epsilon_2}(z) - E_{\epsilon_2,\epsilon_1}(z) - 2E_{\epsilon_4,\epsilon_3}(z) + 3E_{\epsilon_3,\epsilon_4}(z)$.

PROOF.

$$\begin{aligned} f(z) &= \theta^3(z)\theta(3z) \\ &= (\sum_{n=-\infty}^{\infty} e^{2\pi i n^2 z})^3 (\sum_{n=-\infty}^{\infty} e^{2\pi i 3n^2 z}) \\ &= (1 + 2\sum_{n\geq 1} e^{2\pi i n^2 z})^3 (1 + 2\sum_{n\geq 1} e^{2\pi i 3n^2 z}). \end{aligned}$$

Say this is equal to

$$aE_{\epsilon_1,\epsilon_2}(z) + bE_{\epsilon_2,\epsilon_1}(z) + cE_{\epsilon_4,\epsilon_3}(z) + dE_{\epsilon_3,\epsilon_4}(z)$$

Then writing $q = e^{2\pi i z}$ and from the proof of Theorem 28, comparing coefficients of q^0, q^1, q^2 and q^3 on both sides of the equality, we get that,

$$-b = 1 \implies b = -1,$$

$$a + b + c + d = 6,$$

$$2a + b - 2c - d = 12,$$

$$3a + b - c - 3d = 10.$$

Solving for a, b, c, d using these equations we get that $a = 6$, $b = -1$, $c = -2$ and $d = 3$ which proves the theorem.

□

COROLLARY 3.

$$N(1,1,1,3;n) = 6\sigma_{\epsilon_1,\epsilon_2}(n) - \sigma_{\epsilon_2,\epsilon_1}(n) - 2\sigma_{\epsilon_4,\epsilon_3}(n) + 3\sigma_{\epsilon_3,\epsilon_4}(n).$$

PROOF. Since for $q = e^{2\pi iz}$, we have

$$\sum_{N=1}^{\infty} N(1,1,1,3;n)q^n = \theta(z)^3\theta(3z)$$

and using Theorem 29, we have

$$\theta^3(z)\theta(3z) = 6E_{\epsilon_1,\epsilon_2}(z) - E_{\epsilon_2,\epsilon_1}(z) - 2E_{\epsilon_4,\epsilon_3}(z) + 3E_{\epsilon_3,\epsilon_4}(z),$$

the result follows. □

Now, let us illustrate in an example that the formula indeed works. Consider the case when $n = 10$. Let us try to compute $N(1,1,1,3;10)$.

$$\begin{aligned}\sigma_{\epsilon_1,\epsilon_2}(10) &= \epsilon_2(1)\epsilon_1(10)\cdot 1 + \epsilon_2(2)\epsilon_1(5)\cdot 2 + \epsilon_2(5)\epsilon_1(2)\cdot 5 + \epsilon_2(10)\epsilon_1(1)\cdot 10\\ &= 8.\end{aligned}$$

$$\begin{aligned}\sigma_{\epsilon_2,\epsilon_1}(10) &= \epsilon_1(1)\epsilon_2(10)\cdot 1 + \epsilon_1(2)\epsilon_2(5)\cdot 2 + \epsilon_1(5)\epsilon_2(2)\cdot 5 + \epsilon_1(10)\epsilon_2(1)\cdot 10\\ &= -4.\end{aligned}$$

$$\begin{aligned}\sigma_{\epsilon_4,\epsilon_3}(10) &= \epsilon_3(1)\epsilon_4(10)\cdot 1 + \epsilon_3(2)\epsilon_4(5)\cdot 2 + \epsilon_3(5)\epsilon_4(2)\cdot 5 + \epsilon_3(10)\epsilon_4(1)\cdot 10\\ &= 8.\end{aligned}$$

$$\begin{aligned}\sigma_{\epsilon_3,\epsilon_4}(10) &= \epsilon_4(1)\epsilon_3(10)\cdot 1 + \epsilon_4(2)\epsilon_3(5)\cdot 2 + \epsilon_4(5)\epsilon_3(2)\cdot 5 + \epsilon_4(10)\epsilon_3(1)\cdot 10\\ &= -4.\end{aligned}$$

Then, by Theorem 31,

$$\begin{aligned}N(1,1,1,3;10) &= (6\cdot 8) - (-4) - (2\cdot 8) + (3\cdot(-4))\\ &= 24.\end{aligned}$$

Now let us explicitly write down the representations of 10 as $x^2 + y^2 + z^2 + 3u^2$. Firstly, note that $u = 0$. This is because u cannot be greater than equal to 2. If $u = 1$, then 7 must be written as a sum of three squares which is not possible. Thus, the possibilities are $(x, y, z, u) = (0, 1, 3, 0)$, $(x, y, z, u) = (0, -1, 3, 0)$, $(x, y, z, u) = (0, 1, -3, 0)$ and $(x, y, z, u) = (0, -1, -3, 0)$. But also, since u remains fixed, the values of x, y, z can be permuted in 3! ways. Thus, total number of representations of 10 as $x^2 + y^2 + z^2 + 3u^2$ is $4 \cdot (3!)$ which equals 24 which is what we got using Theorem 31.

5.4. Conclusion and Further Work

In this thesis we have determined formulae for the number of representations of positive integers by quaternary quadratic forms by using a modular form approach. We have sketched a general method which can be employed to find the number of ways in which an integer can be written as $ax^2 + by^2 + cz^2 + du^2$. Then, we have illustrated it in the case when $a = 1, b = 1, c = 1, d = 3$. It would be natural to use this general method to compute the number of representations of an integer as $ax^2 + by^2 + cz^2 + du^2$ where (a, b, c, d) is any of the 55-tuples computed by Ramanujan. That would require some tedious work but we believe it can be done.

Finally, it would also be interesting to extend this work to find the number of representations of positive integers by quadratic forms with 5 or more variables. These questions will comprise the theme of future work.

Bibliography

[1] N. C. Ankeny, Sum of Three Squares, Proceedings of the American Mathematical Society Vol. 8, No. 2 (Apr., 1957), pp. 316-319.

[2] Ayse Alaca, Jamilah Alanazi, Representation By Quaternary Quadratic Forms whose coefficients are 1, 2, 7 or 14, accepted in Integers Journal, 2016.

[3] Bhargava, Manjul, On the Conway-Schneeberger fifteen theorem. (English summary) Quadratic forms and their applications (Dublin, 1999), 27–37, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[4] Conway, J. H. Universal Quadratic Forms and the Fifteen Theorem,(English summary) Quadratic forms and their applications (Dublin, 1999), 23–26, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000. 11E25 (11E20 11H55).

[5] F. Diamond and J. Shurman, A First Course in Modular Forms, Graduate Text in Mathematics 228, Springer-Verlag, 2004.

[6] B. Gordon and D. Sinor, Multiplicative properties of η-products, Lecture Notes in Math, vol.1395 Springer-Verlag, New York (1989), 173-200.

[7] G. H. Hardy, P. V. Seshu Aiyar, B. M. Wilson, Collected Papers of Srinivasa Ramanujan, Chelsea Publishing Company, New York, 1962.

[8] Jody Esmonde, M. Ram Murty, Problems in Algebraic Number Theory, Springer, New York 1991.

[9] L. J. P. Kilford, Modular Forms, A classical and computational introduction, Imperial College Press, London, 2008.

[10] Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1984.

[11] J. Liouville, Sur les deux formes $x^2 + y^2 + 2(z^2 + t^2)$, J. Pures Appl. Math. 5(1860), 269-272.

[12] J. Liouville, Sur les deux formes $x^2 + y^2 + z^2 + 2t^2$, $x^2 + 2(y^2 + z^2 + t^2)$, J. Pures Appl. Math. 6(1861), 225-230.

[13] T. Miyake, Modular Forms, Springer Monographs in Mathematics. SpringerVerlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[14] M. Ram Murty, Michael Dewar, Hester Graves, Problems in the Theory of Modular Forms, IMSc Lecture Notes No.1, Hindustan Book Agency, 2015.

[15] L. Panaitopol, On the representation of natural numbers as sums of squares, Amer. Math. Monthly 112 (2005), 168–171.

[16] Robert A. Rankin, Modular Forms and Functions, Cambridge University Press, Cambridge 1977.

[17] Serge Lang, Introduction to Modular Forms, Springer-Verlag Berlin Heidelberg 1976.

[18] J. P. Serre, A course in arithmetic, Springer-Verlag, New York, 1973.

[19] William Stein, Modular Forms, a Computational Approach, Graduate Studies in Mathematics, American Math Society, Volume 79, Rhode Island, 2007.