Applications of Modular Forms

Essay submitted for the Examination in Part III
of the Mathematical Tripos, 2003.

David S Freeman

Emmanuel College, Cambridge

dsf27@cam.ac.uk

15 May 2003

I declare that this essay, "Applications of Modular Forms," is work done as part of the Mathematical Tripos Part III Examination for the year 2003. It is the result of my own work, and except where stated otherwise, it includes nothing that was performed in collaboration. No part of this essay has been submitted for a degree or any such qualification.

David S Freeman
Emmanuel College

15 May 2003

Applications of Modular Forms

David S Freeman
Emmanuel College
dsf27@cam.ac.uk

15 May 2003

1 Introduction

In the same volume of Diophantus in which he scribbled the enigmatic comment that became known as the Last Theorem, Pierre Fermat also wrote,

> I have discovered a most beautiful theorem...every number is a square or the sum of two, three or four squares... The theorem is based on the most diverse and abstruse mysteries of numbers, but I am not able to include the proof here...[1]

More than a hundred years later, in 1770, Lagrange gave the proof that Fermat omitted, showing that any natural number can be expressed as the sum of four squares. Given this result, a natural question to ask is how many ways a given number can be represented by a sum of four squares. This problem was solved by Jacobi in 1829, who gave a concise formula for the number of representations.

If we denote by $r_s(n)$ the number of representations of n as a sum of s squares, then Jacobi's formula gives $r_4(n)$. Subsequent mathematicians adapted Jacobi's result to sums of other numbers of squares and by 1907 had given formulae for $s = 3$ and every even integer through 12. In 1916, Ramanujan observed that it is possible to compute a very good approximation to $r_s(n)$ that holds for all s. The main goal of this essay is to explain and prove this assertion, which takes the form of the following theorem.

[1] Cit. and trans. in [N, p. 3]

Theorem 1. *For any nonnegative integer n and positive integer s, let $r_s(n)$ be the number of solutions in the integers to the equation*

$$x_1^2 + \ldots + x_s^2 = n.$$

Then for $s \geq 4$,

$$r_s(n) = \delta_s(n) + h_s(n),$$

where $\delta_s(n) = O\left(n^{s/2-1}\right)$ and $h_s(n) = O\left(n^{s/4}\right)$.

In particular, $\delta_s(n)$ is a very good approximation to $r_s(n)$ for large n. For general s the formulae for $\delta_s(n)$ and $h_s(n)$ are hard to work with, but we can simplify them in a few specific cases. When s is a multiple of 4 we can compute a simple formula for $\delta_s(n)$ in terms the divisors of n, and when s is 4 or 8 the term $h_s(n)$ is identically zero. Combining these results gives us explicit formulae for the number of representations of n as a sum of four or eight squares.

Theorem 2. *Let $r_s(n)$ be defined as in Theorem 1. Then*

$$r_4(n) = \begin{cases} 8\sum\limits_{d|n} d & \text{for } n \text{ odd} \\ 24\sum\limits_{\substack{d|n \\ d \text{ odd}}} d & \text{for } n \text{ even,} \end{cases}$$

and

$$r_8(n) = 16\sum_{d|n}(-1)^{n-d}d^3.$$

Jacobi proved the formula for $r_4(n)$ using theta functions, which are a type of modular form. The proof of the more general theorem builds on the same ideas and relies on the theory of modular forms. In Section 2 we show that the number of ways a number can be represented as the sum of s squares is given by the Fourier coefficients of a certain theta function, and we demonstrate that this function is in fact a modular form. In Section 3, we use a type of modular form called Eisenstein series to derive an explicit formula for the portion of the theta function that does not vanish on all cusps. After this is done what remains of the original theta function is a cusp form. In Section 4, we show that the Fourier coefficients of this cusp form are not too large, so that in the limit as n goes to infinity the contribution of the cusp form is negligible. We also discuss methods of improving the bound on $h_s(n)$

in Theorem 1, which involves estimating the Fourier coefficients of a type of cusp form called Poincaré series.

One might ask whether Theorem 1 generalises to sums of cubes and higher powers. The answer is yes, but the functions involved are not modular forms, and thus a completely different method of proof is necessary. The "circle method" devised by Hardy and Littlewood in the early 1920s provides the machinery to compute an asymptotic formula for sums of higher powers that is analogous to Theorem 1. In Section 5 we describe how this method gives the result for sums of kth powers and we show that the more general theorem agrees with Theorem 1 when $k = 2$. Unfortunately, the Hardy-Littlewood method does not allow us to compute any formulae analogous to those in Theorem 2.

2 Theta Functions

Our approach to counting representations of sums of squares begins by examining the properties of theta functions. The exposition in this section (loosely) follows that of Sarnak [S2, §1.3]. Further details, especially with regard to Proposition 2.4, can be found in [I, §10]. Iwaniec treats a very general class of theta functions; where necessary we have specialised his results to the cases in which we are interested.

We begin by defining the n-dimensional analogue of the classical theta function.

Definition. *Let $\mathbb{H}$ denote the upper half-plane of $\mathbb{C}$. For any positive integer n, let*

$$\theta_n(z) = \sum_{\mathbf{m}\in\mathbb{Z}^n} e^{\pi i|\mathbf{m}|^2 z} \tag{2.1}$$

for any $z \in \mathbb{H}$.

This series converges absolutely for all $z \in \mathbb{H}$. It is clear from the definition that $\theta_n(2z)$ has a Fourier series,

$$\theta_n(2z) = \sum_{m=-\infty}^{\infty} a_m e^{2\pi i m z}. \tag{2.2}$$

Since each vector in $\mathbb{Z}^n$ of length $\sqrt{m}$ contributes 1 to a_m, the series (2.2) has the property the Fourier coefficients a_m are exactly the number of representations of m as the sum of n squares. If we let $\Theta_n(z) = \theta_n(2z)$ and show that

$\Theta_n(z)$ is a modular form for a certain congruence subgroup of $SL_2(\mathbb{Z})$, then we can use the theory of modular forms to analyse the Fourier coefficients a_m.

The key property of modular forms is how they transform under the action of subgroups of $SL_2(\mathbb{Z})$. For example, a modular form $f(z)$ of weight k (k a positive even integer) for $SL_2(\mathbb{Z})$ transforms as

$$f(\gamma z) = (cz+d)^k f(z) \tag{2.3}$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. We therefore wish to discover transformation properties of the functions $\theta_n(z)$, with the goal of showing that these functions are modular forms. We first observe that

$$\theta_n(z) = \theta_1(z)^n. \tag{2.4}$$

This observation allows us to focus our attention on the transformation properties of $\theta_1(z)$. The simplest of these properties is clear from the definition:

$$\theta_1(z+2) = \theta_1(z). \tag{2.5}$$

Next we use the Poisson summation formula to derive a slightly more complicated transformation property. The formula is as follows.

Result 2.1 (Poisson summation formula; cf. [I, §1.1]). *Let $f : \mathbb{R} \to \mathbb{C}$ be a C^∞ function, and let*

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x y} dx.$$

Suppose that for any $N \geq 0$, $|f(x)|$ and $|\hat{f}(x)|$ are both less than $C \cdot |x|^{-N}$ for some C (depending on N). Then

$$\sum_{m=-\infty}^{\infty} f(m) = \sum_{m=-\infty}^{\infty} \hat{f}(m).$$

We will also need the Fourier transform of the Gaussian function.

Lemma 2.2. *For $x \in \mathbb{R}$ and fixed constants $c \in \mathbb{R}$ and $\alpha \in \mathbb{C} \setminus \{0\}$, let $f(x) = e^{-\pi\alpha(x+c)^2}$ and define $\hat{f}(y)$ as in Result 2.1. Then*

$$\hat{f}(y) = \frac{1}{\sqrt{\alpha}} e^{2\pi i c y - \pi y^2/\alpha}.$$

(Here and throughout this essay, $\sqrt{\cdot}$ denotes the principal branch of the square root, with $\arg\sqrt{z} \in (-\pi/2, \pi/2]$. For k a half integer, we define $z^k = (\sqrt{z})^{2k}$.)

Proof. Körner [Kö, Lemma 50.2] computes

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} e^{-i\zeta t}e^{-t^2/2}dt = e^{-\zeta^2/2}.$$

Making the changes of variable $t = (x+c)\sqrt{2\pi\alpha}$, $\zeta = y\sqrt{2\pi/\alpha}$ gives the result. □

We combine these two results to deduce a transformation property of the theta function.

Proposition 2.3.

$$\theta_1(-1/z) = \sqrt{-iz}\theta_1(z).$$

Proof. Let $\alpha = i/z$ and $c = 0$ in Lemma 2.2. Then we have

$$\begin{aligned} f(x) &= e^{-i\pi x^2/z} \\ \hat{f}(x) &= \sqrt{\frac{z}{i}}e^{i\pi x^2 z}, \end{aligned}$$

and thus by the definition of θ_n (equation (2.1)) and the Poisson summation formula (Result 2.1), we have

$$\theta_1(-1/z) = \sum_{x=-\infty}^{\infty} f(x) = \sum_{x=-\infty}^{\infty} \hat{f}(x) = \sqrt{-iz}\theta_1(z).$$

□

In principle, equation (2.5) and Proposition 2.3 allow us to compute the transformation of θ_1 under the group $\Gamma_\theta \subset SL_2(\mathbb{Z})$ generated by $\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$. However, the computations are bulky, and we desire a more explicit formula. If we consider the action of the slightly smaller group $\Gamma(2) \subset \Gamma_\theta$,[2] where

$$\Gamma_2 = \left\{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix}1&0\\0&1\end{pmatrix} \pmod 2\right\},$$

then we may derive the following transformation property:

[2]Gunning [G, §5] shows that $[SL_2(\mathbb{Z}) : \Gamma_\theta] = 3$ and $[\Gamma_\theta : \Gamma(2)] = 2$.

Proposition 2.4. *Let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(2)$ *(i.e.* $a \equiv d \equiv 1 \pmod 2$ *and* $b \equiv c \equiv 0 \pmod 2$*). Then*

$$\theta_n(\gamma z) = \left(\frac{2c}{d}\right)^n \epsilon_d^{-n}\,(cz+d)^{n/2}\,\theta_n(z),$$

where $\left(\frac{c}{d}\right)$ *is the Jacobi-Legendre quadratic residue symbol for positive odd* d *(see [W]) extended to all odd* d *by*

$$\begin{aligned} \left(\frac{c}{d}\right) &= \frac{c}{|c|}\left(\frac{c}{-d}\right) \text{ if } c \neq 0, \\ \left(\frac{0}{d}\right) &= \begin{cases} 1 & \text{if } d = \pm 1 \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

and

$$\epsilon_q = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ i & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. To simplify notation, we define $e(z) = e^{2\pi i z}$. We start by using $ad - bc = 1$ to rewrite γz as

$$\gamma z = \frac{az+b}{cz+d} = \left(\frac{a}{c} - \frac{1}{c(cz+d)}\right).$$

Then we have

$$\theta_1(\gamma z) = \sum_{m=-\infty}^{\infty} e\left(\frac{m^2}{2}\left(\frac{a}{c} - \frac{1}{c(cz+d)}\right)\right). \tag{2.6}$$

Since $c \equiv 0 \pmod 2$,

$$e\left(\frac{a(m+cx)^2}{2c}\right) = e\left(\frac{am^2}{2c} + amx + \frac{acx^2}{2}\right) = e\left(\frac{am^2}{2c}\right)$$

for any $x \in \mathbb{Z}$, and thus $e(\frac{am^2}{2c})$ depends only on m modulo c. We can therefore rewrite (2.6) as

$$\begin{aligned} \theta_1(\gamma z) &= \sum_{g \pmod c}\left(e\left(\frac{ag^2}{2c}\right)\sum_{\substack{m\in\mathbb{Z} \\ m\equiv g \pmod c}} e\left(\frac{m^2}{2}\left(\frac{-1}{c(cz+d)}\right)\right)\right) \\ &= \sum_{g \pmod c}\left(e\left(\frac{ag^2}{2c}\right)\sum_{m\in\mathbb{Z}} e\left(\frac{1}{2}\left(\frac{g}{c}+m\right)^2\left(\frac{-c}{cz+d}\right)\right)\right). \end{aligned}$$

We can apply the Poisson summation formula (Result 2.1) to replace the term in the inner sum by its Fourier transform (see Lemma 2.2), which gives

$$\theta_1(\gamma z) = \sum_{g \pmod c} \left(e\left(\frac{ag^2}{2c}\right) \sum_{m\in\mathbb{Z}} \sqrt{\frac{cz+d}{ic}} e\left(\frac{m^2}{2}\left(\frac{cz+d}{c}\right) + \frac{gm}{c}\right)\right).$$

Splitting m into its congruence classes modulo c, we obtain

$$\theta_1(z) = \sqrt{\frac{cz+d}{ic}} \sum_{g \pmod c} \sum_{l \pmod c} e\left(\frac{ag^2}{2c} + \frac{gl}{c} + \frac{dl^2}{2c}\right) \sum_{m\in\mathbb{Z}} e\left(\frac{1}{2} z m^2\right).$$

Since $(c,d) = 1$, we can substitute $l' = l - dg$ and still be summing over all congruence classes modulo c. Making this substitution (and applying $ad - bc = 1$) gives

$$\begin{aligned}\theta_1(\gamma z) &= \sqrt{\frac{cz+d}{ic}}\theta_1(z) \sum_{g \pmod c} \sum_{l' \pmod c} e\left(\frac{ag^2}{2c} + bgl + \frac{1}{2}bdl^2\right) \\ &= \sqrt{\frac{cz+d}{ic}}\theta_1(z) \sum_{g \pmod c} e\left(\frac{ag^2}{2c}\right),\end{aligned}$$

since all of the variables are integers and $b \equiv 0 \pmod 2$. Again since $(c,d) = 1$, we can make the substitution $g = dx$ and still be summing over all congruence classes modulo c. Thus the term $ag^2/2c$ becomes $ad^2x^2/2c = bdx^2/2 + dx^2/2c$. Since $b \equiv 0 \pmod 2$, we have

$$\theta_1(\gamma z) = \sqrt{\frac{cz+d}{ic}}\theta_1(z) \sum_{x \pmod c} e\left(\frac{dx^2}{2c}\right). \tag{2.7}$$

The sum in this equation is a Gauss sum; to evaluate it, we wish to use the following formula:

Result 2.5 ([I, Lemma 4.8]). *Let p, q be integers with $(2p, q) = 1$ and $q \geq 0$. Then*

$$\sum_{t \pmod q} e\left(\frac{pt^2}{q}\right) = \left(\frac{p}{q}\right)\epsilon_q\sqrt{q},$$

where $\left(\frac{p}{q}\right)$ and ϵ_q are defined as in Proposition 2.4.

The sum in equation (2.7) does not satisfy the hypotheses of the Result 2.5, so we must manipulate the expression a bit. The key observation at this stage is that we now have two ways of using equation (2.7) to evaluate the expression $\theta_1(\gamma(-1/z))$, namely, substituting $-1/z$ for z and applying Proposition 2.3, and substituting $\gamma' = \gamma \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} b & -a \\ d & -c \end{smallmatrix}\right)$ for γ. Making these substitutions gives the following identity:

$$\begin{aligned} \sqrt{\frac{dz-c}{id}}\theta_1(z)g(-c,d) &= \sqrt{\frac{-c/z+d}{ic}}\theta_1(-1/z)g(d,c) \\ &= \sqrt{\frac{c-dz}{c}}\theta_1(z)g(d,c), \end{aligned}$$

where

$$g(p,q) = \sum_{x \pmod q} e\left(\frac{px^2}{2q}\right).$$

It follows that

$$g(d,c) = \sqrt{\frac{ic}{d}}\overline{g(c,d)}.$$

By assumption, d is an odd integer, so we may substitute $2x$ for x in the expression for g on the right hand side, which gives

$$g(d,c) = \sqrt{\frac{ic}{d}} \sum_{x \pmod d} e\left(\frac{-2xct^2}{d}\right). \tag{2.8}$$

The right hand side of equation (2.8) satisfies the hypotheses of Lemma 2.5, so we conclude that

$$g(d,c) = \sqrt{ic}\left(\frac{2c}{d}\right)\overline{\epsilon_d}.$$

Substituting this expression into equation (2.7) gives

$$\theta_1(\gamma z) = \sqrt{cz+d}\left(\frac{2c}{d}\right)\epsilon_d^{-1}.$$

Taking the nth power of both sides proves the proposition (cf. equation (2.4)). □

As we observed above, the function whose Fourier coefficients count representations as sums of squares is not $\theta_n(z)$ but rather $\Theta_n(z)$, which we defined to be equal to $\theta_n(2z)$. We may deduce the transformation property of $\Theta_n(z)$ from Proposition 2.4.

Corollary 2.6. *Let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4)$ *(i.e.* $c \equiv 0 \pmod 4$*). Then*

$$\Theta_n(\gamma z) = \left(\frac{c}{d}\right)^n \epsilon_d^{-n} (cz+d)^{n/2}\, \Theta_n(z). \tag{2.9}$$

Proof. By definition of $\Theta_n(z)$,

$$\Theta_n(\gamma z) = \theta_n(2\gamma z) = \theta_n\left(\frac{a(2z)+2b}{(c/2)(2z)+d}\right) = \theta_n\left(\gamma'(2z)\right),$$

where $\gamma' = \left(\begin{smallmatrix} a & 2b \\ c/2 & d \end{smallmatrix}\right)$. Since $4|c$, $\gamma' \in \Gamma(2)$, and we may apply Proposition 2.4 to deduce the result. □

Note that for n divisible by 4, Corollary 2.6 gives

$$\Theta_n(\gamma z) = (cz+d)^{n/2}\Theta_n(z),$$

which is the familiar transformation property for modular forms of even weight (cf. equation (2.3)).

A function that satisfies the transformation property given in equation (2.9) for a subgroup $\Gamma \subset \Gamma_0(4)$ is said to be a *modular function of weight $n/2$ for Γ*. However, this transformation property is not enough to make $\Theta_n(z)$ a modular form; we also need to examine the function's behaviour at the cusps of $\Gamma_0(4)$.

A modular form of even weight for $SL_2(\mathbb{Z})$ is said to be *holomorphic at ∞* if it has a Fourier expansion $\sum a_n e^{2\pi i n z}$ and $a_n = 0$ for all $n < 0$. In a more general congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ there may be multiple cusps, each corresponding to an equivalence class of $s \in \mathbb{Q} \cup \{\infty\}$ under the action of Γ. To define holomorphicity at a cusp other than infinity, we make a change of variables that moves the cusp to infinity and divide out by the automorphy factor.

Definition. *Let $\Gamma \subset SL_2(\mathbb{Z})$, and let $f : \mathbb{H} \to \mathbb{C}$ be a modular function of weight k for Γ. Given $s \in \mathbb{Q} \cup \{\infty\}$, choose $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Q})$ such that $s = \delta(\infty)$. Let $w = \delta^{-1}z$ be the* local variable at s *and define $f\,|[\delta]_k : \mathbb{H} \to \mathbb{C}$ (read "f hit by delta") by*

$$f\,|[\delta]_k\,(w) = f(\delta w)(cw+d)^{-k}.$$

We say f is holomorphic at the cusp s *if there is some positive integer M such that*

$$f\,|[\delta]_k\,(w) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n w/M},$$

and $a_n = 0$ for all $n < 0$. The coefficient $a_0 = f\,|[\delta]_k\,(\infty)$ is the value of f at the cusp s.

In general, the coefficients in the Fourier expansion, and therefore the values at the cusps, will depend on the choice of local variable w. Actions of successive changes of variable behave nicely (see for example [K, Proposition III.16]), but we will not need such results. Our aim now is to show that the function $\Theta_n(z)$ is holomorphic at the cusps of $\Gamma_0(4)$. To do so we need to find out what these cusps are; it turns out that there are three equivalence classes.

Lemma 2.7. *Let $s \in \mathbb{Q}$. Write $s = p/q$, where $(p,q) = 1$. Then s is $\Gamma_0(4)$-equivalent to one of the following:*

1. *∞, if $4|q$;*
2. *0, if q is odd; or*
3. *$1/2$, if $q \equiv 2 \pmod 4$.*

Moreover, no two of ∞, 0, and $1/2$ are $\Gamma_0(4)$-equivalent.

Proof. Since $(p,q) = 1$, we may choose integers a, b such that $ap + bq = 1$.

1. Suppose $4|q$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ -q & p \end{smallmatrix}\right)$. Then $\gamma \in \Gamma_0(4)$ and $\gamma(p/q) = \infty$.
2. Suppose q is odd. By replacing a with $a+kq$ and b with $b-kp$ (for some k) if necessary, we may assume that $a \equiv 0 \pmod 4$. Let $\gamma = \left(\begin{smallmatrix} q & -p \\ a & b \end{smallmatrix}\right)$. Then $\gamma \in \Gamma_0(4)$ and $\gamma(p/q) = 0$.
3. Suppose $q \equiv 2 \pmod 4$. Then a is odd. By replacing a with $a+q$ and b with $b-p$ if necessary, we may assume $a \equiv 1 \pmod 4$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ 2a-q & p+2b \end{smallmatrix}\right)$. Then $\gamma \in \Gamma_0(4)$ and $\gamma(p/q) = 1/2$.

It remains to show that ∞, 0, and $1/2$ are all inequivalent. Any matrix $\gamma \in SL_2(\mathbb{Z})$ that takes p/q to ∞ must be of the form $\gamma = \left(\begin{smallmatrix} a & b \\ -q & p \end{smallmatrix}\right)$, so if 4 does not divide q then $\gamma \notin \Gamma_0(4)$; thus 0 $(= 0/1)$ and $1/2$ are not equivalent to ∞. Similarly, any $\gamma \in SL_2(\mathbb{Z})$ that takes p/q to 0 is of the form $\gamma = \left(\begin{smallmatrix} q & -p \\ a & b \end{smallmatrix}\right)$, so if q is even then a must be odd and thus $\gamma \notin \Gamma_0(4)$. We conclude that $1/2$ is not equivalent to 0. □

We can now show that $\Theta_n(z)$ is holomorphic at all three cusps, and in fact calculate its value at each. We will use these values in Section 3 to express theta series in terms of Eisenstein series.

Proposition 2.8. *For any positive integer n, $\Theta_n(z)$ is holomorphic at all cusps of $\Gamma_0(4)$. Furthermore, the values at the cusps are*

1. $\Theta_n(\infty) = 1$,

2. $\Theta_n \Big| \left[\begin{pmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix}\right]_{n/2} (\infty) = i^{-n/2}$, *and*

3. $\Theta_n \Big| \left[\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\right]_{n/2} (\infty) = 0$.

Proof. By Lemma 2.7, it suffices to show that $\Theta_n(z)$ is holomorphic at ∞, 0, and 1/2, and by equation (2.4) we need only consider $\Theta_1(z)$. It is clear from the definition that $\Theta_1(z)$ is holomorphic at ∞, since

$$\Theta_1(z) = \sum_{m=-\infty}^{\infty} e^{2\pi i m^2 z} = 1 + 2\sum_{m=1}^{\infty} e^{2\pi i m^2 z}.$$

The constant term is 1, so

$$\Theta_1(\infty) = \Theta_n(\infty) = 1.$$

Let $\delta = \begin{pmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix}$, and note that $\delta(\infty) = 0$. Then in the local variable at zero,

$$\begin{aligned} \Theta_1 \Big| [\delta]_{1/2} (w) &= (2w)^{-1/2}\Theta_1\left(-\frac{1}{4w}\right) \\ &= (2w)^{-1/2}\theta_1\left(-\frac{1}{2w}\right). \end{aligned}$$

Applying Proposition 2.3 gives

$$\Theta_1 \Big| [\delta]_{1/2} (w) = \sqrt{-i}\,\theta_1(2w) = \sqrt{-i}\,\Theta_1(w).$$

Applying the definition as we did above at infinity, we see that Θ_1 is holomorphic at zero and

$$\Theta_1 \Big| [\delta]_{1/2} (\infty) = i^{-1/2}.$$

Taking the nth power gives

$$\Theta_n \Big| [\delta]_{n/2} (\infty) = i^{-n/2}.$$

To evaluate $\Theta_n(z)$ at the cusp 1/2 we will need the following lemma.

Lemma 2.9. $\theta_1(z-1) = 2\theta_1(4z) - \theta_1(z)$.

Proof. From the definition,

$$\begin{aligned}
\theta_1(z-1) &= \sum_{m=-\infty}^{\infty} e^{\pi i m^2 z} e^{-\pi i m^2} \\
&= \sum_{m \text{ even}} e^{\pi i m^2 z} - \sum_{m \text{ odd}} e^{\pi i m^2 z} \\
&= 2 \sum_{m \text{ even}} e^{\pi i m^2 z} - \sum_{m=-\infty}^{\infty} e^{\pi i m^2 z} \\
&= 2\, \theta_1(4z) - \theta_1(z).
\end{aligned}$$

□

Now let $\delta = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$, and note that $\delta(\infty) = \frac{1}{2}$. Then

$$\begin{aligned}
\Theta_1 \Big| [\delta]_{1/2}(w) &= (2w+1)^{-1/2} \Theta_1\left(\frac{w}{2w+1}\right) \\
&= (2w+1)^{-1/2} \theta_1\left(\frac{2w}{2w+1}\right).
\end{aligned}$$

Applying Proposition 2.3, Lemma 2.9, and Proposition 2.3 again gives

$$\begin{aligned}
\Theta_1 \Big| [\delta]_{1/2}(w) &= (2w+1)^{-1/2} \sqrt{-i\left(-1-\frac{1}{2w}\right)}\, \theta_1\left(-1-\frac{1}{2w}\right) \\
&= \sqrt{\frac{i}{2w}} \left(2\, \theta_1\left(-\frac{2}{w}\right) - \theta_1\left(-\frac{1}{2w}\right)\right) \\
&= \sqrt{\frac{i}{2w}} \left(2\sqrt{-\frac{iw}{2}}\, \theta_1\left(\frac{w}{2}\right) - \sqrt{-2iw}\, \theta_1(2w)\right) \\
&= \Theta_1(w/4) - \Theta_1(w). \qquad (2.10)
\end{aligned}$$

From this last expression we see that $\Theta_1(z)$ is holomorphic at $1/2$. The leading coefficients cancel, giving

$$\Theta_1 \Big| [\delta]_{1/2}(\infty) = \Theta_n \Big| [\delta]_{n/2}(\infty) = 0.$$

□

We have now shown that $\Theta_n(z)$ is a modular form of weight $n/2$ for $\Gamma_0(4)$ according to the following definition:

Definition. *Let n be a positive integer, and let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4)$ *(i.e. $ad - bc = 1$ and $4|c$). Define the* automorphy factor $j(\gamma, z)$ *by*

$$j(\gamma, z) = \left(\frac{c}{d}\right) \epsilon_d^{-1} \sqrt{cz + d}, \qquad (2.11)$$

where $\left(\frac{c}{d}\right)$ *and* ϵ_d *are defined as in Proposition 2.4. Let k be half a positive integer. Then a* modular form $f(z)$ of weight k for $\Gamma_0(4)$ *is a holomorphic function* $f : \mathbb{H} \to \mathbb{C}$ *satisfying*

1. $f(\gamma z) = j(\gamma, z)^{2k} f(z)$ *for any* $\gamma \in \Gamma_0(4)$,
2. $f(z)$ *is holomorphic at each cusp of* $\Gamma_0(4)$.

If f is a modular form that vanishes at all cusps of $\Gamma_0(4)$, then f is a a cusp form.

Since $\left(\frac{c}{d}\right) \epsilon_d$ is a fourth root of unity, when k is an even integer this definition agrees with the usual definition of modular forms of even weight for a congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$. This definition in the same form can be used to define modular forms for half-integer weight for any subgroup $\Gamma \subset \Gamma_0(4)$ of finite index. For half-integer weight forms for a general discrete subgroup $\Gamma \subset SL_2(\mathbb{R})$, the factor $\left(\frac{c}{d}\right) \epsilon_d$ is replaced by a more general "multiplier system"; for details, see [I].

It is clear from the definition that the space of modular forms of weight k for $\Gamma_0(4)$ is a vector space over $\mathbb{C}$. In fact, this space is finite dimensional.

Proposition 2.10. *Let $\mathcal{M}_k(\Gamma_0(4))$ denote the space of modular forms of weight k for $\Gamma_0(4)$. Then* $\dim(\mathcal{M}_k(\Gamma_0(4))) < \infty$.

Proof. We first observe that given k and l, for $f \in \mathcal{M}_k(\Gamma_0(4))$ and $g \in \mathcal{M}_l(\Gamma_0(4))$, $fg \in \mathcal{M}_{k+l}(\Gamma_0(4))$. Choose some nonzero $f_0 \in \mathcal{M}_k(\Gamma_0(4))$. Then the map $f \mapsto (f_0)^{23} f$ is an injection from $\mathcal{M}_k(\Gamma_0(4))$ into $\mathcal{M}_{24k}(\Gamma_0(4))$. Since k is a half integer it therefore suffices to show the result for $12|k$.

Let $q = e^{2\pi i z}$, and define

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

It is well known (see e.g. [S2, Appendix 1.1]) that Δ is a modular form of weight 12 for $SL_2(\mathbb{Z})$, and thus also for any congruence subgroup $\Gamma \subset$

$SL_2(\mathbb{Z})$. It is clear from the definition that Δ vanishes at ∞, and thus Δ is a cusp form for any $\Gamma \subset SL_2(\mathbb{Z})$. In addition, Δ is nonzero everywhere on $\mathbb{H}$.

Suppose $12|k$, and let f be a modular form of weight k for $\Gamma_0(4)$. For each cusp s of $\Gamma_0(4)$, choose $\delta \in SL_2(\mathbb{Q})$ such that $\delta s = \infty$, and let the Fourier expansion of f at the cusp s be

$$f \left|[\delta]_k\right. (w) = a_n(s) e^{2\pi i n w}.$$

Suppose that for each s, $a_n(s) = 0$ for all $n < h_s k/12$, where h_s is the order of the zero of Δ at the cusp s. Then the function $f \cdot \Delta^{-k/12}$ is holomorphic on $\mathbb{H}$ and at all cusps, and therefore

$$f \cdot \Delta^{-k/12} \in \mathcal{M}_0(\Gamma_0(4)) = \mathbb{C},$$

so $f = c \cdot \Delta^{k/12}$ for some $c \in \mathbb{C}$. Let $N = \sum_s h_s$ and define a linear map $\psi : \mathcal{M}_k(\Gamma_0(4)) \to \mathbb{C}^N$ that sends a modular form f to the vector consisting of its first $h_s k/12$ Fourier coefficients at each cusp. Then $\ker(\psi) = \mathbb{C} \cdot \Delta^{k/12}$, and we conclude that

$$\begin{aligned} \dim(\mathcal{M}_k(\Gamma_0(4))) &\leq 1 + \frac{k}{12} \sum_s h_s \\ &< \infty. \end{aligned} \tag{2.12}$$

□

For even $k \geq 2$, one can use the Riemann-Roch Theorem (see [Mi, Theorem 4.9]) to calculate an explicit formula for the dimension of the space of modular forms of weight k. We will need this result to prove the explicit formulae in Theorem 2. (In the specific cases we consider the dimension can be computed by more elementary means; see Proposition 3.10 below.) To prove the order of magnitude estimates in Theorem 1, all we need is that the space of modular forms is finite dimensional.

3 Eisenstein Series

An important example of modular forms of half-integer weight is the set of Eisenstein series. Eisenstein series are always non-cuspidal modular forms (i.e. the constant term in the Fourier expansion is nonzero), and it turns out that they span the space of non-cuspidal modular forms. This is useful for our application to representations of integers as sums of squares because (as we will see in Section 4 below) the Fourier coefficients of cusp forms are of strictly smaller order than those for Eisenstein series, and thus the Fourier coefficients of the theta function are dominated by those for the Eisenstein series.

In this section we define the Eisenstein series for $\Gamma_0(4)$, show they are modular forms with appropriate behaviour at each cusp of $\Gamma_0(4)$, and calculate their Fourier coefficients. The formulae simplify nicely for the series of even integer weight, while for the other series we can deduce only an order of magnitude estimate. Our exposition of the Eisenstein series and demonstration of their properties follows that of Sarnak [S2, §1.4], while the calculation of the Fourier coefficients follows Koblitz [K, §III.3 and IV.2].

We begin by recalling the standard definition of Eisenstein series for even integer weight k:

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k},$$

where $\zeta(k)$ is the Riemann zeta function. We may rewrite this sum (see [K, §III.2]) as

$$E_k(z) = \sum_{\substack{m\geq 0 \\ (m,n)=1}} \frac{1}{(mz+n)^k},$$

and note that this is a sum of $j(\gamma,z)^{-2k}$ over matrices γ of the form $\left(\begin{smallmatrix} * & * \\ m & n \end{smallmatrix}\right)$. We interpret this set of matrices as coset representatives of $\Gamma_\infty\backslash SL_2(\mathbb{Z})$, where $\Gamma_\infty = \left\{\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right), j \in \mathbb{Z}\right\}$ is the stabiliser of ∞ in $SL_2(\mathbb{Z})$. We are now prepared to generalise the definition.

Definition. *Let $k > 2$ be a half integer, and $s \in \mathbb{Q} \cup \{\infty\}$. Choose $\delta \in SL_2(\mathbb{Q})$ such that $\delta s = \infty$. The* Eisenstein series of weight k at the cusp s for $\Gamma_0(4)$ *is*

$$E_k^{(s)}(\delta z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} j(\gamma,\delta z)^{-2k},$$

where the automorphy factor j is defined by equation (2.11).

If we choose coset representatives for $\Gamma_\infty\backslash\Gamma_0(4)$ of the form $\left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right)$ with $4|c$ and keep only one of each pair $\{(c,d),(-c,-d)\}$, then we may write the series at infinity as

$$E_k^{(\infty)}(z) = \sum_{\substack{4|c,\ d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} (cz+d)^{-k}. \tag{3.1}$$

The series $E_k^{(\infty)}$ converges absolutely for $k > 2$ since

$$\left|E_k^{(\infty)}(z)\right| \leq \sum_{\substack{4|c,\ d>0 \\ (c,d)=1}} |cz+d|^{-k} \leq \sum_{\substack{c,d\in\mathbb{Z} \\ (c,d)\neq(0,0)}} |cz+d|^{-k},$$

and the last sum converges absolutely for $k > 2$. By the same reasoning, $E_k^{(s)}$ converges absolutely for $k > 2$ and any $s \in \mathbb{Q}$.

It is straightforward to check that the Eisenstein series satisfy the transformation property of modular forms. We require a simple lemma.

Lemma 3.1. *The automorphy factor $j(\gamma, z)$ satisfies*

$$j(\alpha\beta, z) = j(\alpha, \beta z) \cdot j(\beta, z)$$

for any $\alpha, \beta \in \Gamma_0(4)$.

Proof. For any function f we have

$$\frac{f(\alpha\beta z)}{f(z)} = \frac{f(\alpha\beta z)}{f(\beta z)} \cdot \frac{f(\beta z)}{f(z)}$$

Using $\Theta_1(z)$ as our function f and applying the transformation property in Corollary 2.6 gives the result. □

We use this lemma to show that each Eisenstein series transforms like a modular form.

Proposition 3.2. *Let k be a half integer greater than 2, let $s \in \mathbb{Q} \cup \{\infty\}$, and choose $\delta \in SL_2(\mathbb{Z})$ such that $\delta s = \infty$. Then for any $\eta \in \Gamma_0(4)$,*

$$E_k^{(s)}(\eta\delta z) = j(\eta, \delta z)^{2k} E_k^{(s)}(\delta z).$$

Proof. By the definition,

$$E_k^{(s)}(\eta\delta z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} j(\gamma, \eta\delta z)^{-2k},$$

and by Lemma 3.1,

$$E_k^{(s)}(\eta\delta z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} \left(\frac{j(\eta,\delta z)}{j(\gamma\eta,\delta z)}\right)^{2k}.$$

However, right multiplication by η just permutes the cosets of $\Gamma_\infty\backslash\Gamma_0(4)$, which does not change the value of the sum since we have absolute convergence. We may therefore rewrite the sum as

$$E_k^{(s)}(\eta\delta z) = j(\eta,\delta z)^{2k} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} (j(\gamma,\delta z))^{-2k},$$

giving the result. □

The above result shows that for a given choice of local variable $w = \delta z$, the Eisenstein series at two equivalent cusps s, s' are identical, so we can refer to "the Eisenstein series at s," meaning the series at all cusps that are $\Gamma_0(4)$-equivalent to s. We now investigate the behaviour at the cusps of the Eisenstein series, which will allow us to rewrite the theta function in terms of Eisenstein series and cusp forms.

Proposition 3.3. *Let $w = \delta z$ be a local variable at a cusp s of $\Gamma_0(4)$, and let $E_k^{(s)}(w)$ be the Eisenstein series of weight k ($k > 2$ a half integer) at s. Then $E_k^{(s)}(\infty) = 1$, and $E_k^{(s)}(s') = 0$ for any cusp s' not $\Gamma_0(4)$-equivalent to s.*

Proof. We carry out the calculations for the series at infinity; those for the other series are identical.

The only term in the sum defining the Eisenstein series that does not go to zero as z goes to infinity is that corresponding to the identity in $\Gamma_\infty\backslash\Gamma_0(4)$, or $(c,d) = (0,1)$ in the notation of equation (3.1). Splitting this term out of the sum gives

$$E_k^{(\infty)}(z) = 1 + \sum_{\substack{c>0,4|c \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k}\,(cz+d)^{-k}.$$

Taking absolute values and adding terms where we have omitted values of c and d gives

$$\left|E_k^{(\infty)}(z) - 1\right| \leq 2\sum_{c=1}^{\infty}\sum_{d=1}^{\infty} |cz+d|^{-k}.$$

Let $z = iy$ for $y \in \mathbb{R}, y > 0$. By comparison with a double integral in the variables c and d, we see that for $k > 2$ there is some constant $C > 0$ such that
$$\left| E_k^{(\infty)}(iy) - 1 \right| \leq \frac{C}{y^{k-2}}.$$
As y goes to infinity the right hand side goes to zero, so $E_k^{(\infty)}(\infty) = 1$.

For the cusp at zero, we use $\delta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to change to the local variable $w = -1/z$:

$$\begin{aligned} E_k^{(\infty)} \left|[\delta]_k \right. (w) &= w^{-k} E_k^{(\infty)}(-1/w) \\ &= \sum_{\substack{4|c,\ d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} \left(dw + c\right)^{-k}. \end{aligned}$$

Since d is odd, all the terms go to zero as w goes to infinity. We thus have

$$\left| E_k^{(\infty)} \left|[\delta]_k \right. (w) \right| \leq 2 \sum_{c=0}^{\infty} \sum_{d=1}^{\infty} \left| dw + c \right|^{-k},$$

and since $k > 2$, as w goes to infinity this sum goes to zero by the same reasoning as above.

Finally, using $\delta = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ to change to the local variable at $\frac{1}{2}$ gives

$$\begin{aligned} E_k^{(\infty)} \left|[\delta]_k \right. (w) &= (2w+1)^{-k} E_k^{(\infty)} \left(\frac{w}{2w+1}\right) \\ &= \sum_{\substack{4|c,\ d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} \left((c+2d)w + d\right)^{-k}. \end{aligned}$$

Since $(c, d) = 1$, all terms go to zero as w goes to infinity, and thus the sum goes to zero by the same reasoning as in the previous two cases. □

Taken together, Propositions 3.2 and 3.3 imply that the Eisenstein series are modular forms. Furthermore, since each series is nonzero at a different cusp, we can write any modular form as a linear combination of Eisenstein series plus a form that vanishes at all cusps. We now carry out this calculation for $\Theta_n(z)$. To simplify notation, we will assume that the Eisenstein series at zero is defined in the variable $w = -1/4z$, and we will denote by $E_k^{(0)}(z)$ the function $E_k^{(0)} \left| \left[\begin{pmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix} \right]_k \right. (z)$.

Corollary 3.4. *For any positive integer $n > 4$,*

$$\Theta_n(z) = E_{n/2}^{(\infty)}(z) + i^{-n/2} E_{n/2}^{(0)}(z) + F_{n/2}(z),$$

where $F_{n/2}(z)$ is a cusp form of weight $n/2$ for $\Gamma_0(4)$.

Proof. By Propositions 2.8 and 3.3, the function

$$F_{n/2}(z) = \Theta_n(z) - E_{n/2}^{(\infty)}(z) - i^{-n/2} E_{n/2}^{(0)}(z)$$

vanishes on all three cusps of $\Gamma_0(4)$. By linearity of modular forms, $F_{n/2}(z)$ is a modular form of weight $n/2$, and thus a cusp form. □

We now wish to calculate the Fourier coefficients of the non-cuspidal part of $\Theta_n(z)$. In general, the Legendre symbol and ϵ_d in the definition of the Eisenstein series makes it impossible to compute a simple expression; however, we can make an order-of-magnitude estimate. We compute the coefficients for each of the two Eisenstein series separately.

Proposition 3.5. *Let $E_k^{(\infty)}(z)$ and $E_k^{(0)}(z)$ be the Eisenstein series of weight $k > 2$ at ∞ and 0, respectively, for $\Gamma_0(4)$. Then*

$$\begin{aligned} E_k^{(\infty)}(z) &= 1 + \sum_{l=1}^{\infty} a_l e^{2\pi i l z}, \\ E_k^{(0)}(z) &= \sum_{l=1}^{\infty} b_l e^{2\pi i l z}, \end{aligned}$$

where

$$a_l = \frac{(-2\pi i)^k}{(k-1)!} l^{k-1} \sum_{\substack{n>0 \\ 4|n}} n^{-k} \sum_{\substack{0\le j<n \\ (j,n)=1}} \left(\frac{n}{j}\right)^{-2k} \epsilon_j^{2k} e^{2\pi i l j/n}, \tag{3.2}$$

$$b_l = \frac{(-\pi i)^k}{(k-1)!} l^{k-1} \sum_{n>0 \text{ odd}} n^{-k} \epsilon_n^{2k} \sum_{\substack{0\le j<n \\ (j,n)=1}} \left(\frac{j}{n}\right)^{-2k} e^{-2\pi i l j/n}. \tag{3.3}$$

Proof. From the definition of the Eisenstein series (choosing the pair of $\{(c,d),(-c,-d)\}$ with $c > 0$), we have

$$E_k^{(\infty)}(z) = 1 + \sum_{\substack{4|c,\ c>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} (cz+d)^{-k}. \tag{3.4}$$

Since the sum is absolutely convergent for $k > 2$, we may group terms for a given c by the value of d modulo c:

$$E_k^{(\infty)}(z) = 1 + \sum_{\substack{c>0 \\ 4|c}} \sum_{\substack{0 \le j < c \\ (j,c)=1}} \sum_{h=-\infty}^{\infty} \left(\frac{c}{j+ch}\right)^{-2k} \epsilon_{j+ch}^{2k} (cz + j + ch)^{-k}.$$

We now observe that since c is divisible by 4, ϵ_{j+ch} and $\left(\frac{c}{j+ch}\right)$ are independent of h. (For the latter we appeal to the multiplicative and reciprocity properties of the Jacobi symbol, which can be found in [W].) We now have

$$E_k^{(\infty)}(z) = 1 + \sum_{\substack{c>0 \\ 4|c}} c^{-k} \sum_{\substack{0 \le j < c \\ (j,c)=1}} \left(\frac{c}{j}\right)^{-2k} \epsilon_j^{2k} \sum_{h=-\infty}^{\infty} \left(z + \frac{j}{c} + h\right)^{-k}.$$

To evaluate the innermost sum, we use to a formula that can be derived from the series expansion of the cotangent:

Result 3.6 ([I, eq. (1.46)]). *For $z \in \mathbb{H}$ and $k \ge 2$ an integer,*

$$\sum_{a=-\infty}^{\infty} (z+a)^{-k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i l z}.$$

Applying this result to expression for $E_k^{(\infty)}(z)$ gives

$$E_k^{(\infty)}(z) = 1 + \sum_{\substack{c>0 \\ 4|c}} c^{-k} \sum_{\substack{0 \le j < c \\ (j,c)=1}} \left(\frac{c}{j}\right)^{-2k} \epsilon_j^{2k} \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i l z} e^{2\pi i l j/c}.$$

Bringing the constant and the factor $l^{k-1} e^{2\pi i l z}$ to the outside and replacing c with n gives the result.

To begin the analogous computation for the Eisenstein series at zero, recall that we defined the series in the variable $w = -1/4z$:

$$E_k^{(0)}(w) = \sum_{\substack{4|c, d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} (cw + d)^{-k}.$$

Hitting with $\delta = \left(\begin{smallmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{smallmatrix}\right)$ to change back to the variable z (i.e. the local variable at infinity) gives

$$\begin{aligned} E_k^{(0)}(z) &= (2z)^{-k} \sum_{\substack{4|c,d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} \left(-\frac{c}{4z}+d\right)^{-k} \\ &= 2^{-k} \sum_{\substack{4|c,d>0 \\ (c,d)=1}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^{2k} \left(dz-\frac{c}{4}\right)^{-k}. \end{aligned}$$

We now let $c = 4m$ and note that $(4m, d) = 1$ if and only if d is odd and $(m, d) = 1$. Furthermore, since $\left(\frac{4}{d}\right) = 1$ for all d, $\left(\frac{c}{d}\right) = \left(\frac{m}{d}\right)$. We thus have

$$E_k^{(0)}(z) = 2^{-k} \sum_{\substack{d>0 \text{ odd} \\ (m,d)=1}} \left(\frac{m}{d}\right)^{-2k} \epsilon_d^{2k} (dz-m)^{-k}. \tag{3.5}$$

As above, we group terms, this time for each d grouping by the value of m modulo d,

$$\begin{aligned} E_k^{(0)}(z) &= 2^{-k} \sum_{d>0 \text{ odd}} \epsilon_d^{2k} \sum_{\substack{0\le j<d \\ (j,d)=1}} \sum_{h=-\infty}^{\infty} \left(\frac{j+dh}{d}\right)^{-2k} \epsilon_d^{2k} (dz-j+dh)^{-k} \\ &= 2^{-k} \sum_{d>0 \text{ odd}} d^{-k}\epsilon_d^{2k} \sum_{\substack{0\le j<d \\ (j,d)=1}} \left(\frac{j}{d}\right)^{-2k} \sum_{h=-\infty}^{\infty} \left(z-\frac{j}{d}+h\right)^{-k}. \end{aligned}$$

Applying Result 3.6 gives

$$E_k^{(0)}(z) = 2^{-k} \sum_{d>0 \text{ odd}} d^{-k}\epsilon_d^{2k} \sum_{\substack{0\le j<d \\ (j,d)=1}} \left(\frac{j}{d}\right)^{-2k} \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i l z} e^{-2\pi i l j/d}.$$

Bringing the constant and the factor $l^{k-1}e^{2\pi i l z}$ to the outside and replacing d with n gives the result. □

We now wish to bound the growth of the Fourier coefficients that we have just calculated, so that we may get an order of magnitude estimate for $\Theta_n(z)$. This task is a straightforward corollary of the above result.

Corollary 3.7. *Let a_l and b_l be defined as in Proposition 3.5 above. Then for $k > 2$ there exist positive real numbers C_a, C_b such that for any $l > 0$,*

$$\begin{aligned} |a_l| &\le C_a l^{k-1} \\ |b_l| &\le C_b l^{k-1} \end{aligned}$$

Proof. The innermost sum in the expression for a_l in (3.2) has absolute value less than n, since each term has absolute value 1 and there are fewer than n terms. Thus

$$|a_l| \leq \frac{(2\pi)^k}{(k-1)!} l^{k-1} \sum_{n=1}^{\infty} n^{1-k}.$$

The sum converges for $k > 2$, giving the result. The proof for b_l is analogous. □

The formulae in Proposition 3.5 are in general the most explicit we can calculate for a_l and b_l. However, when k is an even integer, the Legendre symbols and ϵ_d all drop out, so we can simplify the result further.

Proposition 3.8. *Let a_l and b_l be defined as in Proposition 3.5. Then for $k > 2$ an even integer,*

$$\begin{aligned} a_l &= \frac{-2k}{(2^k-1)B_k} \sum_{\substack{d \mid l \\ l/d \text{ even}}} (-1)^d d^{k-1} \\ b_l &= \frac{-2k}{(2^k-1)B_k} \sum_{\substack{d \mid l \\ l/d \text{ odd}}} d^{k-1} \end{aligned}$$

where B_k are the Bernoulli numbers*, defined as the coefficients in the power series*

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}. \tag{3.6}$$

Proof. For the coefficients a_l, we begin with equation (3.4). We note that since k is an even integer, $\left(\frac{m}{d}\right)^{-2k} = \epsilon_d^{2k} = 1$. Evaluating at $z/2$ and letting $c' = c/2$ gives

$$E_k^{(\infty)}\left(\frac{z}{2}\right) = 1 + \sum_{\substack{c'>0 \text{ even} \\ (c',d)=1}} (c'z + d)^{-k}.$$

We wish to sum over all pairs (c', d) with c' even, not just over relatively prime pairs, so we multiply and divide by the sum over all odd j of j^{-k}:

$$\begin{aligned} E_k^{(\infty)}\left(\frac{z}{2}\right) &= 1 + \left(\sum_{j>0 \text{ odd}} j^{-k}\right)^{-1} \sum_{j>0 \text{ odd}} \sum_{c'>0 \text{ even}} \sum_{\substack{d=-\infty \\ (c',d)=1}}^{\infty} (jc'z + jd)^{-k} \\ &= 1 + \frac{2^{-k}}{\zeta(k) - 2^{-k}\zeta(k)} \sum_{n>0 \text{ even}} \sum_{m=-\infty}^{\infty} \left(\frac{nz-1}{2} + m\right)^{-k}, \end{aligned} \tag{3.7}$$

where in the last sum we have let $m = (jd+1)/2$ and $n = jc'$. We now apply Result 3.6 to deduce

$$E_k^{(\infty)}\left(\frac{z}{2}\right) = 1 + \left(\frac{1}{\zeta(k)(2^k-1)}\right)\left(\frac{(2\pi i)^k}{(k-1)!}\right)\sum_{n>0 \text{ even}}\sum_{d=1}^{\infty} d^{k-1}e^{\pi i n d z}e^{-\pi i d}.$$

To rewrite the constant in front of the sum, we use the fact (see [I, eq. (1.42)]) that for $k \geq 2$ an even integer,

$$B_k = -\frac{2k!}{(2\pi i)^k}\zeta(k), \tag{3.8}$$

where B_k are the Bernoulli numbers. From this formula we deduce that

$$\left(\frac{1}{\zeta(k)(2^k-1)}\right)\left(\frac{(2\pi i)^k}{(k-1)!}\right) = \frac{-2k}{(2^k-1)B_k}.$$

Replacing $z/2$ with z and letting $l = nd$ gives the result.

For the coefficients b_l, we begin with equation (3.5) and again note that since k is an even integer, $\left(\frac{m}{d}\right)^{-2k} = \epsilon_d^{2k} = 1$. This time, we wish to sum over all pairs (m, d) with d odd. We again multiply and divide by the sum over all odd j of j^{-k}:

$$\begin{aligned} E_k^{(0)}(z) &= 2^{-k}\left(\sum_{j>0 \text{ odd}} j^{-k}\right)^{-1}\sum_{j>0 \text{ odd}}\sum_{d>0 \text{ odd}}\sum_{\substack{m=-\infty \\ (m,d)=1}}^{\infty}(jdz - jm)^{-k} \\ &= \frac{2^{-k}}{\zeta(k) - 2^{-k}\zeta(k)}\sum_{n>0 \text{ odd}}\sum_{m'=-\infty}^{\infty}(nz - m')^{-k}, \end{aligned} \tag{3.9}$$

where in the last sum we have let $n = jd$ and $m' = jm$. We now apply Result 3.6 to deduce

$$E_k^{(0)}(z) = \left(\frac{1}{\zeta(k)(2^k-1)}\right)\left(\frac{(2\pi i)^k}{(k-1)!}\right)\sum_{n>0 \text{ odd}}\sum_{d=1}^{\infty} d^{k-1}e^{2\pi i n d z}.$$

Applying equation (3.8) shows that the constant is equal to $\frac{-2k}{(2^k-1)B_k}$. Letting $l = nd$ gives the result. □

The above results on Eisenstein series are valid for any half-integer weight $k > 2$. For $k = 2$ the series converge only conditionally, so some extra complications arise. There are two ways to approach the convergence problems.

The first (see [K, §III.2]) is to define the Eisenstein series of weight 2 in the usual manner, in which case the sums converge conditionally but do not satisfy the right transformation rule. For the series at the cusp s in the local variable w, we have

$$E_2^{(s)}(\gamma w) = (cw+d)^2 E_2^{(s)}(w) + \phi_s(w),$$

where ϕ_s is the "error term." It turns out that the error term is simple enough so that given any two Eisenstein series, there is some linear combination for which the error terms cancel, and thus this linear combination is a (non-cuspidal) modular form of weight 2 for $\Gamma_0(4)$.

The other way to deal with Eisenstein series of weight 2 (see [S2, Remark 1.4.4]) is to introduce the function

$$E_2^{(s)}(w,t) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} (cw+d)^{-2} \left|cw+d\right|^{-2t}$$

and take the limit as t goes to zero. This limit exists and transforms correctly but is not quite holomorphic. However, the non-holomorphic part is a single term in the Fourier expansion, so we may take any linear combination that annihilates the non-holomorphic part, which leaves (as above) a two-dimensional space of modular forms of weight 2 that are not cusp forms.

To extend Corollary 3.4 to the case $n = 4$, we require the function $E_2^{(\infty)}(z) - E_2^{(0)}(z)$ to be a modular form of weight 2 for $\Gamma_0(4)$. Fortunately, this is the case.

Proposition 3.9. *Let*

$$E_2^{\theta}(z) = E_2^{(\infty)}(z) - E_2^{(0)}(z).$$

Then $E_2^\theta(z)$ is a modular form of weight 2 for $\Gamma_0(4)$.

Proof. From equations (3.7) and (3.9), we have

$$\begin{aligned} E_2^\theta(z) &= 1 + \frac{2}{\pi^2} \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \left(\frac{1}{\left(2nz - \frac{1}{2} + m\right)^2} - \frac{1}{\left((2n-1)z+m\right)^2} \right) \quad (3.10) \\ &= 1 + \frac{2}{\pi^2} \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \frac{(1-4n)z^2 + (2n-2m)z + (m-\frac{1}{4})}{\left(2nz - \frac{1}{2} + m\right)^2 \left((2n+1)z+m\right)^2}. \end{aligned}$$

Taking absolute values term by term gives

$$\left|E_2^\theta(z)\right| \le \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \frac{A\left|m\right| + Bn + C}{\left(4n^2 \left|z\right|^2 + 4mn \operatorname{Re}(z) + m^2\right)^2},$$

for some positive constants A, B, C (depending on z). (Note that we have absorbed the non-quadratic terms in the denominator into the constants.) It is clear from equation (3.10) that $E_2^\theta(z+1) = E_2^\theta(z)$, so we may assume without loss of generality that $|\mathrm{Re}(z)| \leq 1/2$. Applying this fact gives

$$\left|E_2^\theta(z)\right| \leq 2\max\left(|z|^2, |z|^{-2}\right)\sum_{n=1}^{\infty}\sum_{m=0}^{\infty}\frac{Am+Bn+C}{(4n^2-2mn+m^2)^2}.$$

If we make the substitution $u = n$, $v = m - n$, then

$$\begin{aligned}\left|E_2^\theta(z)\right| &\leq \sum_{u=1}^{\infty}\sum_{v=-\infty}^{\infty}\frac{A'u+B'|v|+C'}{(3u^2+v^2)^2}\\ &\leq 2\sum_{u=1}^{\infty}\sum_{v=0}^{\infty}\frac{A'u+B'v+C'}{(u^2+v^2)^2}.\end{aligned}$$

If we absorb the constant C' into the other two constants and use the fact that since A', B', u, v are all nonnegative,

$$\frac{A'u+B'v}{\sqrt{u^2+v^2}} \geq \min\left(A', B'\right),$$

then we have

$$\left|E_2^\theta(z)\right| \leq \sum_{u=1}^{\infty}\sum_{v=0}^{\infty}\frac{D}{(u^2+v^2)^{3/2}}$$

for some positive constant D. This last sum converges by comparison with the integral

$$\iint\limits_R \frac{dx\ dy}{(x^2+y^2)^{3/2}} = \pi\int_\epsilon^\infty \frac{dr}{r^2},$$

where R is the half-plane $y > 0$ minus a disc around the origin of radius ϵ.

Since the sum (3.10) converges absolutely for all z, $E_2^\theta(z)$ is holomorphic on $\mathbb{H}$, and checking holomorphicity at the cusps is straightforward. To show the transformation property, we use the definition of Eisenstein series to write

$$E_2^\theta(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} j(\gamma,z)^{-4} - z^{-2}j\left(\gamma, -\frac{1}{z}\right)^{-4}.$$

Since the sum is absolutely convergent, we may apply the same reasoning as in the proof of Proposition 3.2 to deduce that for $\eta = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_0(4)$, $E_2^\theta(\eta z) = (cz+d)^2 E_2^\theta(z)$. □

Now that we have absolute convergence in the Eisenstein series of weight 2, we may extend the formulae in Propositions 3.5 and 3.8 to the case $k = 2$. The calculations are for the most part identical, and we omit the details; for a full treatment see [Mu, §I.15].

In general the cusp form $F_{n/2}(z)$ in Corollary 3.4 is nontrivial; however, it vanishes for certain small values of n, and the theta series is exactly equal to the sum of the two Eisenstein series.

Proposition 3.10. *For $n = 4$ or 8, the cusp form $F_{n/2}(z)$ defined in Corollary 3.4 is identically equal to zero.*

We give two different proofs. The first is computational, and the second uses some more powerful results about Riemann surfaces to describe the result in terms of dimensions of vector spaces.

Proof No. 1. The first proof requires a result about the number of zeroes of a modular function f for $\Gamma_0(4)$, which may be proved by integrating the logarithmic derivative of f around the boundary of a fundamental domain for $\Gamma_0(4)$. (Milne [Mi, Prop. 4.12] uses the Riemann-Roch Theorem to prove the result in greater generality, but we do not need this stronger version.)

Result 3.11 ([K, §III.3, Problem 17]). *Let $f(z)$ be a nonzero modular function of weight k ($k \geq 0$ an even integer) for $\Gamma_0(4)$. Let F be a fundamental domain for $\Gamma_0(4)$, including the three cusps, and for $p \in F$ denote by $v_p(f)$ the order of the zero or pole of $f(z)$ at the point p. Then*

$$\sum_{p \in F} v_p(f) = \frac{k}{2}.$$

Since $\Theta_4(z)$ is a modular form (of weight 2), it has no poles in any fundamental domain F. Furthermore, we have from equation (2.10),

$$\Theta_4 \left|[\delta]_2\right. (w) = a_1 e^{2\pi i w} + \text{higher powers of } e^{2\pi i w},$$

where $\delta = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$. Thus $\Theta_4(z)$ has a zero of order 1 at the cusp $1/2$, and by Result 3.11 it has no other zeroes. It follows that $\Theta_8(z) = \Theta_4(z)^2$ has a zero of order 2 at the cusp $1/2$ and no other zeroes or poles.

Proposition 3.8 (extended to weight 2 via Proposition 3.9) gives an explicit formula for the Fourier coefficients of the modular form $E^{(\infty)}_{n/2}(z) + i^{n/2} E^{(0)}_{n/2}(z)$ for $n = 4$ or 8. One can easily compute that the first four coefficients a_m do in fact give the number of representations of m as the sum of four or eight squares. Thus in both cases the function

$$\Theta_n(z) - E_{n/2}^{(\infty)}(z) - i^{n/2} E_{n/2}^{(0)}(z)$$

has a zero of order four at ∞. Since $\Theta_n(z)$ has at zero of order $n/4$ at $1/2$ and no other zeroes, the function

$$\psi(z) = 1 - \frac{E_{n/2}^{(\infty)}(z) - i^{n/2} E_{n/2}^{(0)}(z)}{\Theta_n(z)}$$

has a zero of order four at ∞, a pole of order $n/4$ at $1/2$, and no other poles. Since $\psi(z)$ is a modular function of weight zero and has fewer poles than zeroes, by Result 3.11 it is identically equal to zero. We conclude that

$$\Theta_n(z) = E_{n/2}^{(\infty)}(z) + i^{n/2} E_{n/2}^{(0)}(z),$$

and the cusp form $F_{n/2}(z)$ is identically equal to zero. □

Proof No. 2. Milne [Mi] uses the Riemann-Roch Theorem and the correspondence between modular forms of weight k and $k/2$-fold differential forms to derive the following dimension formula:

Result 3.12 ([Mi, Theorem 4.9]). *Let $k \geq 2$ be an even integer, and $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup. If $\mathcal{M}_k(\Gamma)$ is the space of modular forms of weight k for $\Gamma \subset SL_2(\mathbb{Z})$, then*

$$\dim(\mathcal{M}_k(\Gamma)) = (k-1)(g-1) + \frac{1}{2}\nu_\infty k + \sum_p \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_p}\right)\right\rfloor,$$

where g is the genus of $\Gamma\backslash\mathbb{H}^*$, ν_∞ is the number of inequivalent cusps of Γ, the sum is over elliptic points p of Γ, e_p is the order of the stabiliser of p, and $\lfloor x \rfloor$ is the greatest integer function.

For the group $\Gamma_0(4)$, Milne computes [Mi, Example 2.23] that the genus g is zero, and there are no elliptic points.[3] Since $\Gamma_0(4)$ has three cusps, we have for k even,

$$\dim(\mathcal{M}_k(\Gamma_0(4))) = 1 + \frac{k}{2}. \tag{3.11}$$

For $k = 2$ the space of non-cusp forms is two-dimensional (cf. discussion before Proposition 3.9), and therefore it is equal to the entire space $\mathcal{M}_2(\Gamma_0(4))$. For $k > 2$ the three Eisenstein series are linearly independent non-cusp forms, and thus for $k = 4$ they span the entire space $\mathcal{M}_4(\Gamma_0(4))$. Thus for $n = 4$ or 8 the cusp form $F_{n/2}(z)$ must be identically zero. □

[3]Actually, the computation is carried out for $\Gamma(2)$, which is conjugate to $\Gamma_0(4)$.

The second proof of Proposition 3.10 leads to an interesting observation: From Result 3.11 we see that that the zeroes of the weight-12 modular form Δ have total order 6, and therefore equation (3.11) implies that the upper bound (2.12) that we computed for the dimension of $\mathcal{M}_k(\Gamma_0(4))$ when $12|k$ is in fact an equality.

We now have all the ingredients necessary to give the formulae for the number of representations of an integer n as the sum of 4 or 8 squares.

Proof of Theorem 2. By definition, the number $r_s(n)$ is the nth Fourier coefficient of the function $\Theta_s(z)$. By Proposition 2.8 and Corollary 2.6, $\Theta_s(z)$ is a modular form of weight $s/2$ for $\Gamma_0(4)$. By Corollary 3.4 (using Proposition 3.9 to extend to weight 2),

$$\Theta_s(z) = E^{(\infty)}_{s/2}(z) + i^{-s/2}E^{(0)}_{s/2}(z) + F_{s/2}(z),$$

where $F_{s/2}(z)$ is a cusp form. By Proposition 3.10, $F_{s/2}(z)$ is identically zero for $s = 4$ or 8. The Fourier coefficients a_n of $\Theta_s(z)$ may therefore be calculated from Proposition 3.8.

For $s = 4$, Proposition 3.8 (extended to weight 2 and using equation (3.6) to compute $B_2 = 1/6$) gives

$$a_n = 8\left(\sum_{\substack{d|n \\ n/d \text{ odd}}} d - \sum_{\substack{d|n \\ n/d \text{ even}}} (-1)^d d\right).$$

If n is odd, the second sum is zero. If $n = 2^a m$ for odd m, then each divisor d of m corresponds to divisors $2^a d, 2^{a-1}d, \ldots, 2d, d$ of n. The contribution to the sum is thus $8d(2^a - 2^{a-1} - \ldots - 2 + 1) = 24d$. We conclude that

$$a_n = \begin{cases} 8\sum_{d|n} d & \text{for } n \text{ odd} \\ 24\sum_{\substack{d|n \\ d \text{ odd}}} d & \text{for } n \text{ even.} \end{cases}$$

For $s = 8$, Proposition 3.8 (using equation (3.6) to compute $B_4 = -1/30$) gives

$$a_n = 16\left(\sum_{\substack{d|n \\ n/d \text{ odd}}} d^3 - \sum_{\substack{d|n \\ n/d \text{ even}}} (-1)^d d^3\right).$$

We note that in the first sum $n-d$ is even, and in the second sum $n-2d$ is even, so we may multiply by $(-1)^{n-d}$ and $(-1)^{n-2d}$ respectively to conclude

$$a_n = 16\sum_{d|n}(-1)^{n-d}d^3.$$

□

4 Fourier Coefficients of Cusp Forms

Corollary 3.4 gives an expression for the theta function as a sum of Eisenstein series and cusp forms, and Propositions 3.5 and 3.8 give formulae for the Fourier coefficients of the Eisenstein series. For these formulae to be useful in calculating the number of representations as sums of squares, we must show that the Fourier coefficients of cusp forms are not too large. There are results of varying depth and generality for this problem, but it turns out that the simplest bound is enough for our purposes, since for $k > 2$ it is strictly smaller than the bound for the Eisenstein series derived in Corollary 3.7.

Our discussion of the Poincaré series follows that of Sarnak [S2, §1.5]; Iwaniec [I, §3] treats the topic in greater generality. Our treatment of Kloosterman sums and bounds for the Fourier coefficients of cusp forms roughly follows that of Iwaniec [I, §4-5].

Proposition 4.1. *Suppose*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

is a cusp form of weight k for $\Gamma_0(4)$. Then there exists some positive constant C such that

$$|a_n| \le C \cdot n^{k/2}.$$

Proof. Since $\mathrm{Im}(\gamma z) = \mathrm{Im}(z)/|cz+d|^2$ for any $\gamma \in SL_2(\mathbb{R})$ and $f(z)$ is a modular form of weight k, the function $F(z) = |f(z)|\,\mathrm{Im}(z)^{k/2}$ is $\Gamma_0(4)$-invariant. Since $f(z)$ decays exponentially at the cusps, $F(z)$ is bounded on all of $\mathbb{H}$; say $|F(z)| \le M$.

For the Fourier coefficient a_n, we have

$$a_n = \int_{iy}^{1+iy} e^{-2\pi i n z} f(z)\,dz,$$

where $z = x + iy$. Thus

$$|a_n| \le e^{2\pi ny} \int_0^1 |f(x+iy)|\, dx \le M e^{2\pi ny} y^{-k/2}.$$

Setting $y = 1/n$ gives the result. □

We now have all of the necessary tools to prove Theorem 1.

Proof of Theorem 1. By definition, the number $r_s(n)$ is the nth Fourier coefficient of the function $\Theta_s(z)$. By Proposition 2.8 and Corollary 2.6, $\Theta_s(z)$ is a modular form of weight $s/2$ for $\Gamma_0(4)$. By Corollary 3.4 (and its extension to weight 2 in Proposition 3.9), for $s \ge 4$,

$$\Theta_s(z) = E_{s/2}^{(\infty)}(z) + i^{-s/2} E_{s/2}^{(0)}(z) + F_{s/2}(z),$$

where $F_{s/2}(z)$ is a cusp form. By Corollary 3.7, the nth Fourier coefficients of $E_{s/2}^{(\infty)}(z)$ and $E_{s/2}^{(0)}(z)$ are $O\left(n^{s/2-1}\right)$, and by Proposition 4.1, the nth Fourier coefficient of $F_{s/2}(z)$ is $O(n^{s/4})$. □

Note that for $s = 4$, Theorem 1 splits $r_4(n)$ into two terms that are both $O(n)$, which is not particularly useful; however, by Proposition 3.10 the term corresponding to the cusp form vanishes. For $s > 4$, the term corresponding to the Eisenstein series dominates, and Propositions 3.5 and 3.8 give formulae for $r_s(n)$ with error no more than a constant times $n^{s/4}$.

4.1 Poincaré Series

The bound in Proposition 4.1, though it is strong enough to prove Theorem 1, is not the best possible, and we devote the remainder of the section to improving the bound. These improvements provide only marginal gain when counting representations as sums of five or more squares, and by Proposition 3.10 they are not necessary for counting sums of four squares. However, an improvement on Proposition 4.1 is essential to get a nontrivial estimate of representations by more general quadratic forms in four variables, since the cusp forms that vanish for sums of squares may not do so in the general case.

We begin by showing that the space of cusp forms is spanned by a set of forms called *Poincaré series*. The construction of the Poincaré series is very similar to the construction of the Eisenstein series.

Definition. *Let* m *be a nonnegative integer and* $k > 2$ *be a half integer. For* $s \in \mathbb{Q} \cup \{\infty\}$*, choose* $\delta \in SL_2(\mathbb{Q})$ *such that* $\delta s = \infty$*. The* mth Poincaré series of weight k at the cusp s for $\Gamma_0(4)$ *is*

$$P^{(s)}_{m,k}(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j(\gamma, \delta z)^{-2k} e^{2\pi i m \gamma \delta z},$$

where the automorphy factor j *is defined by equation (2.11).*

To see that the series is well-defined, note first that for $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\gamma_2 = \left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right)$ in the same coset of Γ_∞, $\gamma_1 \delta z - \gamma_2 \delta z = \gamma_3 \delta z$, where $\gamma_3 = \left(\begin{smallmatrix} a-a' & b-b' \\ c & d \end{smallmatrix}\right)$ is a nonzero matrix with determinant zero. Since all entries are integers and $(c, d) = 1$, $\gamma_3 = \left(\begin{smallmatrix} rc & rd \\ c & d \end{smallmatrix}\right)$ for some integer r. Thus $e\left(m\gamma_3\delta z\right) = e\left(rm\right) = 1$, and $e\left(m\gamma_1\delta z\right) = e\left(m\gamma_2\delta z\right)$.

Note that for $m = 0$ the Poincaré series are the Eisenstein series. Each term of a Poincaré series has absolute value less than or equal to the corresponding term in the Eisenstein series, so each series converges absolutely for $k > 2$ and all m. (As with the Eisenstein series, we may extend to the case $k = 2$ via careful summation, but we will not need this result.) That the Poincaré series are of any interest at all is due to the following result:

Proposition 4.2. *For* $m \geq 1$*,* $k > 2$*, and any* $s \in \mathbb{Q} \cup \{\infty\}$*, the* m*th Poincaré series of weight* k *at the cusp* s *for* $\Gamma_0(4)$ *is a cusp form.*

Proof. By the same reasoning as in the proof of Proposition 3.2, for $\eta \in \Gamma_0(4)$,

$$P^{(s)}_{m,k}(\eta\delta z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} \left(\frac{j(\eta, \delta z)}{j(\gamma\eta, \delta z)}\right)^{-2k} e^{2\pi i m \gamma \eta \delta z},$$

and since right multiplication by η merely permutes the cosets of $\Gamma_\infty \backslash \Gamma_0(4)$, we find

$$P^{(s)}_{m,k}(\eta\delta z) = j(\eta, \delta z)^{2k} P^{(s)}_{m,k}(\delta z). \tag{4.1}$$

We now calculate the values at the cusps for the Poincaré series at infinity; the calculations for the other series are identical. Let s be a cusp of $\Gamma_0(4)$, and $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Q})$ such that $\delta(\infty) = s$. Let $w = \delta^{-1} z$ be the local variable at the cusp s. Then

$$P^{(\infty)}_{m,k} \left|[\delta]_k\right. (w) = (cw + d)^{-k} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j(\gamma, \delta^{-1} w)^{-2k} e^{2\pi i m \gamma \delta^{-1} w}.$$

For any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$, let $j'(\gamma, z) = |cz+d|^{1/2}$. Taking absolute values of the Poincaré series term by term, we have

$$\left| P^{(\infty)}_{m,k} \left|[\delta]_k\right. (w) \right| \leq j'(\delta, w)^{-2k} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j'(\gamma, \delta^{-1} w)^{-2k} e^{-2\pi m \sigma(\gamma)},$$

where $\sigma(\gamma) = \mathrm{Im}(\gamma \delta^{-1} w)$. A simple computation shows that for any matrices α, β,

$$j'(\alpha\beta z) = j'(\alpha, \beta(z)) \cdot j'(\beta, z).$$

Applying this relation gives

$$\left| P^{(\infty)}_{m,k} \left|[\delta]_k\right. (w) \right| \leq \left(\frac{j'(\delta, w)}{j'(\delta^{-1}, w)} \right)^{-2k} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j'(\gamma\delta^{-1}, w)^{-2k} e^{-2\pi m \sigma(\gamma)}$$

$$\leq \left(\frac{j'(\delta, w)}{j'(\delta^{-1}, w)} \right)^{-2k} \left(e^{-2\pi m \sigma(\gamma_0)} + \sum_{\substack{\gamma \in \Gamma_\infty \backslash \Gamma_0(4) \\ \gamma\delta^{-1} \neq I}} j'(\gamma\delta^{-1}, w)^{-2k} \right),$$

where in the second line we have split out the term (if any) corresponding to a γ_0 such that $\gamma_0 \delta^{-1} \in \Gamma_\infty$. If we let $w = iy$, all the terms inside the summation go to zero as w goes to infinity, so by the same reasoning as in the proof of Proposition 3.3, the sum is bounded by Cy^{-k+2} for some constant C. Furthermore, the coefficient $j'(\delta, iy)/j'(\delta^{-1}, iy)$ is equal to 1, so we have

$$\left| P^{(\infty)}_{m,k} \left|[\delta]_k\right. (w) \right| \leq e^{-2\pi m \sigma(\gamma_0)} + \frac{C}{y^{k-2}}.$$

The second term clearly goes to zero as y goes to infinity, and since $\gamma_0 \delta^{-1}$ is in the stabiliser of infinity, the first term also goes to zero as y goes to infinity.

Carrying out the above calculation for each Poincaré series, we conclude that $P^{(s)}_{m,k}$ is holomorphic at all cusps of $\Gamma_0(4)$, and furthermore, that its value at every cusp is zero. This result and the transformation property (4.1) imply that all of the Poincaré series are cusp forms. $\square$

Next we show that the Poincaré series span the space of all cusp forms. To do this we use the *Petersson inner product* $\langle \cdot, \cdot \rangle$ on $S_k(\Gamma_0(4))$, the space of cusp forms of weight k for $\Gamma_0(4)$. This inner product is defined by

$$\langle f, g \rangle = \int_{\Gamma_0(4) \backslash \mathbb{H}} y^k f(z) \overline{g(z)} \frac{dx\, dy}{y^2}$$

for $f, g \in S_k(\Gamma_0(4))$. The integral is well-defined because for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$ we have

$$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im}(z)}{|cz+d|^2},$$

and thus the function $y^k f(z)\overline{g(z)}$ and the differential $y^{-2}dx\,dy$ are $\Gamma_0(4)$-invariant. The integral converges (absolutely) since f and g are cusp forms and therefore decay exponentially as y goes to infinity. It is clear from the definition that this is indeed an inner product: it is bilinear, $\langle f, g\rangle = \overline{\langle g, f\rangle}$, and $\langle f, f\rangle$ is a nonnegative real number that is equal to zero if and only if f is identically zero. We now use this inner product to compute the projection of an arbitrary cusp form f onto the Poincaré series.

Lemma 4.3. *Let $k > 2$ be a half integer, and let $P_{m,k}^{(\infty)}(z)$ be the mth Poincaré series of weight k at infinity for $\Gamma_0(4)$. Suppose $f \in S_k(\Gamma_0(4))$ such that*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Then

$$\left\langle f, P_{m,k}^{(\infty)} \right\rangle = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}} a_m.$$

Proof. From the definition of the Petersson inner product and of the Poincaré series,

$$\begin{aligned}
\left\langle f, P_{m,k}^{(\infty)} \right\rangle &= \int\limits_{\Gamma_0(4)\backslash\mathbb{H}} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} f(z)\overline{j(\gamma,z)}^{-2k} e^{-2\pi i m \overline{\gamma z}} y^k \frac{dx\,dy}{y^2} \\
&= \int\limits_{\Gamma_\infty\backslash\mathbb{H}} f(z) e^{-2\pi i m \overline{z}} y^k \frac{dx\,dy}{y^2} \\
&= \sum_{n=1}^{\infty} \int_0^\infty \int_0^1 a_n e^{2\pi i (nz - m\overline{z})} y^k \frac{dx\,dy}{y^2},
\end{aligned}$$

where the absolute convergence of the sum and the integral have allowed us to interchange the order of summation and integration. The only term that does not vanish identically is $n = m$; in that case, using $z - \overline{z} = 2iy$ and the definition of the Gamma function gives

$$\int_0^\infty \int_0^1 e^{-4\pi m y} y^{k-2} dx\,dy = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}},$$

from which the result follows immediately. □

From this lemma, we deduce that all cusp forms are linear combinations of Poincaré series.

Proposition 4.4. *For $k > 2$ a half integer, the space of cusp forms $S_k(\Gamma_0(4))$ is spanned by the Poincaré series $P_{m,k}^{(\infty)}$ for $m \in \mathbb{N}$.*

Proof. Let $V \subset S_k(\Gamma_0(4))$ be the linear subspace spanned by the $P_{m,k}^{(\infty)}$. By Proposition 2.10, $S_k(\Gamma_0(4))$ is finite dimensional, and therefore if there is some nonzero $f \in S_k(\Gamma_0(4)) \setminus V$, then there is some nonzero g orthogonal to V. By Lemma 4.3, the Fourier coefficients of any such g all vanish, and thus g is identically zero, a contradiction. □

Note that we have not used any special property of the cusp at infinity, and therefore Proposition 4.4 also holds for the Poincaré series at any cusp s. There are many open questions about Poincaré series which stem naturally from the above results, including:

- What are the linear relations between the various Poincaré series?
- Construct a basis of $S_k(\Gamma_0(4))$ consisting of Poincaré series.
- Which of the Poincaré series do not vanish identically?

For a summary of some of the known results to these questions, see [I, §3.3].

4.2 Kloosterman Sums

Since the space of cusp forms $S_k(\Gamma_0(4))$ is finite-dimensional, Proposition 4.4 reduces the problem of bounding the Fourier coefficients of cusp forms to the same problem for Poincaré series. We now show that this problem in turn comes down to estimating certain exponential sums called *Kloosterman sums* which arise in the Fourier expansion of the Poincaré series. In the remainder of the section, we outline various methods for estimating Kloosterman sums, each of which improves the estimate in Proposition 4.1. The discussion that follows will not be as rigorous as that above; for more details see [S2] and [I].

Proposition 4.5. *Let $P_{k,m}(z)$ be the mth Poincaré series at infinity of weight $k > 2$ for $\Gamma_0(4)$. Then $P_{k,m}(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, with*

$$a_n = \delta_{mn} + 2\pi i^{-k} \left(\frac{n}{m}\right)^{\frac{k-1}{2}} \sum_{\substack{4|c \\ c>0}} c^{-1} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right) S(m,n,c),$$

where $J_\nu(x)$ is the Bessel function of order ν defined by

$$J_\nu(z) = \sum_{j=0}^{\infty} \frac{(-1)^j}{j!\Gamma(j+1+\nu)} \left(\frac{x}{2}\right)^{\nu+2j},$$

and $S(m,n,c)$ is the Kloosterman sum

$$S(m,n,c) = \sum_{ad\equiv 1 \pmod{c}} \left(\frac{c}{d}\right)^{2k} \epsilon_d^{-2k} e\left(\frac{ma+nd}{c}\right). \tag{4.2}$$

Proof. From the definition of the Poincaré series, we have

$$\begin{aligned} P_{k,m}(z) &= e(mz) + \sum_{\substack{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)/\Gamma_\infty \\ \gamma\neq 1}} \sum_{\tau\in\Gamma_\infty} j(\gamma\tau,z)^{-2k} e(m\gamma\tau z) \\ &= e(mz) + \sum_{\substack{\gamma=\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma_0(4)/\Gamma_\infty \\ c\neq 0}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^k \sum_{n\in\mathbb{Z}} \\ &\qquad (c(z+n)+d)^{-k} e\left(\frac{ma}{c} - \frac{m}{c(c(z+n)+d)}\right), \end{aligned}$$

where we have used $ad - bc = 1$ to write

$$\gamma\tau z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} z = \frac{a}{c} - \frac{1}{c(c(z+n)+d)z}.$$

Applying the Poisson summation formula (Result 2.1) gives

$$\begin{aligned} P_{k,m}(z) &= e(mz) + \sum_{\substack{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)/\Gamma_\infty \\ c\neq 0}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^k \sum_{n\in\mathbb{Z}} \\ &\qquad \int_{-\infty}^{\infty} (c(z+v)+d)^{-k} e\left(\frac{ma}{c} - \frac{m}{c(c(z+v)+d)} - nv\right) dv, \end{aligned}$$

and making the substitution $u = z + v + d/c$ gives

$$\begin{aligned} P_{k,m}(z) &= e(mz) + \sum_{\substack{4|c \\ c>0}} \sum_{ad\equiv 1 \pmod{c}} \left(\frac{c}{d}\right)^{-2k} \epsilon_d^k \sum_{n\in\mathbb{Z}} \\ &\qquad e\left(nz + \frac{ma+nd}{c}\right) \int_{-\infty+iy}^{\infty+iy} (cu)^{-k} e\left(-\frac{m}{c^2 u} - nu\right) du. \end{aligned}$$

By Cauchy's theorem, the integral does not depend on y, and thus for $n \leq 0$ letting y go to infinity shows that the integral vanishes. For $n > 0$, the integral evaluates to

$$\frac{2\pi}{i^k c} \left(\frac{n}{m}\right)^{\frac{k-1}{2}} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right),$$

so if we define the Kloosterman sum $S(m,n,c)$ by equation (4.2), then we have

$$P_{k,m}(z) = e(mz) + \frac{2\pi}{i^k}\sum_{n=1}^{\infty}\left(\frac{n}{m}\right)^{\frac{k-1}{2}} e(nz) \sum_{\substack{4|c \\ c>0}} c^{-1} S(m,n,c) J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right),$$

which proves the proposition. □

Since there is a well-known bound for the Bessel function, estimating the Fourier coefficients of cusp forms becomes a matter of estimating the Kloosterman sums. We focus on the case where the weight k is an even integer, in which case the Legendre symbol and ϵ_d drop out, and we have the so-called "classical" Kloosterman sum

$$S(m,n,c) = \sum_{ad \equiv 1 \pmod{c}} e\left(\frac{ma+nd}{c}\right).$$

We note that the sum $S(m,n,c)$ is a real number since for each pair (a,d) with $ad \equiv 1 \pmod{c}$, $(-a,-d)$ is a different pair with the same property.

The Kloosterman sums satisfy some basic properties which simplify calculations. If $(a,c) = 1$ we have

$$S(am,n,c) = S(m,an,c), \tag{4.3}$$

and if $(c_1, c_2) = 1$ we have

$$S(m,n,c_1c_2) = S\left(m, \overline{c_2}^2 n, c_1\right) S\left(m, \overline{c_1}^2 n, c_2\right), \tag{4.4}$$

where $\overline{c_1}$ and $\overline{c_2}$ are multiplicative inverses of c_1 and c_2 modulo c_2 and c_1, respectively. This multiplicativity property allows us to restrict our attention to the sum $S(m,n,p)$ where p is a prime. We will need the following lemma, which bounds the number of distinct prime divisors of an integer c.

Lemma 4.6. *For n a positive integer, let $\omega(n)$ be the number of distinct prime divisors of n. Then for any $\epsilon > 0$, there exists some $C > 0$ such that for all n,*

$$\omega(n) \leq \epsilon \log n + C.$$

Proof. Since the sequence of primes is strictly increasing, given any $a > 1$ there exists some $r > 0$ such that for any positive integer m, the product of the first m primes is greater than ra^m, and therefore any integer less than ra^m has at most m distinct prime factors. If we substitute $n = ra^m$, then n has at most $(\log n - \log r)/\log a$ distinct prime factors. Substituting $a = e^{1/\epsilon}$ gives the result. □

Lemma 4.6 and the multiplicativity property (4.4) allow us to translate a bound on the Kloosterman sums $S(m, n, p^\alpha)$ into a bound on all Kloosterman sums $S(m, n, c)$.

Proposition 4.7. *Suppose that for p prime and α a positive integer, the Kloosterman sum defined in (4.2) (with k a positive even integer) satisfies*

$$S(m, n, p^\alpha) \leq C \cdot p^{\sigma\alpha}$$

for some $\sigma \in [0, 1)$ and some positive constant C. Then the nth Fourier coefficient of the mth Poincaré series of weight k for $\Gamma_0(4)$ satisfies

$$|a_n| \leq C' \cdot n^{\frac{k-1}{2}+\frac{\sigma}{2}+\epsilon}$$

for some positive constant C' and any $\epsilon > 0$.

Proof. By the multiplicativity property of Kloosterman sums (4.4),

$$S(m, n, c) = C^{\omega(c)} c^\sigma,$$

where $\omega(c)$ is the number of distinct prime divisors of c. By Lemma 4.6, there exists a constant D such that $\omega(c) \leq \epsilon \log c + D$, and thus $|S(m, n, c)| \leq D' \cdot c^{\sigma+\epsilon}$ for some D'.

The bound for the Bessel function is

$$J_\nu(x) \leq R \cdot \min\left(x^\nu, \frac{1}{\sqrt{x}}\right),$$

for some positive R, which gives $J_\nu(x) \leq R \cdot x^\delta$ for any $\delta \in [-1/2, \nu]$. Setting $\nu = k - 1$ and $\delta = \sigma + 2\epsilon$, (where we have chosen ϵ so that $\sigma + 2\epsilon < k - 1$), we have from Proposition 4.5,

$$|a_n| \leq R\left(\frac{n}{m}\right)^{\frac{k-1}{2}} \sum_{\substack{4|c \\ c>0}} \left(4\pi\sqrt{mn}\right)^{\sigma+2\epsilon} c^{-1-\epsilon}.$$

The sum converges for any $\epsilon > 0$, and thus for any given m and n we have the result. □

For $\alpha \geq 2$ and p an odd prime, the Kloosterman sum $S(m, n, p^\alpha)$ can be evaluated explicitly for certain values of m and n; see [I, §4] for details. The result is that for p a prime and $\alpha \geq 2$ an integer,

$$|S(m, n, p^\alpha)| \leq 2p^{\alpha/2} \tag{4.5}$$

for any m and n.

The Kloosterman sum $S(m, n, p)$ cannot be evaluated explicitly in the same manner, and the work on estimating Kloosterman sums primarily involves improving the estimate on this sum. Kloosterman himself calculated a nontrivial estimate using "power-moments" defined by

$$V_\ell(p) = \sum_{\substack{a \pmod p \\ a \neq 0}} S(a, 1, p)^\ell. \tag{4.6}$$

For $\ell = 4$, one can compute (see [I, §4.4])

$$V_4(p) = 2p^3 - 3p^2 - p - 1.$$

Dropping all but the term $a \equiv mn \pmod p$ in equation (4.6) gives

$$S(mn, 1, p)^4 \leq V_4(p) \leq 2p^3,$$

and applying the property (4.3) gives

$$|S(m, n, p)| \leq 2p^{3/4}$$

if $(p, n) = 1$. If $p|n$ then

$$S(m, n, p) = \begin{cases} -1 & \text{if } (p, m) = 1 \\ p - 1 & \text{if } (p, m) \neq 1. \end{cases}$$

Since there are only a finite number of such p they may be absorbed into the constant, giving

$$|S(m, n, p)| \leq C \cdot p^{3/4}$$

for all p. With this result and the bound (4.5), we may take $\sigma = 3/4$ in Proposition 4.7, which gives

$$|a_n| = O\left(n^{\frac{k}{2} - \frac{1}{8} + \epsilon}\right).$$

In 1948, A. Weil proved the Riemann hypothesis for curves over finite fields, from which he deduced the so-called "Weil bound,"

$$|S(m, n, p)| \leq 2p^{1/2}. \tag{4.7}$$

This bound and equation (4.5) give $\sigma = 1/2$ in Proposition 4.7, and thus

$$|a_n| = O\left(n^{\frac{k}{2}-\frac{1}{4}+\epsilon}\right).$$

Weil's proof of the bound (4.7) is quite deep; Iwaniec [I, §5.2] gives an elementary proof of the same bound by estimating sums of Kloosterman sums.

Finally, we note that for even weights k, the best possible bound for a_n is given by the "Ramanujan conjecture,"

$$|a_n| = O\left(n^{\frac{k}{2}-\frac{1}{2}+\epsilon}\right).$$

This conjecture was proven in 1974 by P. Deligne.

If the weight k is odd or half an odd integer, the calculations are more subtle but the idea is the same. One use multiplicative properties of the Kloosterman sums (in this case also called "Salié sums") to reduce the problem to estimating $S(m, n, p^\alpha)$ for p prime. The crucial estimate (see [I, §4.6]) is again

$$|S(m, n, p)| \leq 2p^{1/2},$$

which gives

$$|a_n| = O\left(n^{\frac{k}{2}-\frac{1}{4}+\epsilon}\right).$$

For general n this is the best bound possible, while for n square-free it can be improved (see [S2, Ch. 4]) to

$$|a_n| = O\left(n^{\frac{k}{2}-\frac{2}{7}+\epsilon}\right).$$

The analogue of the Ramanujan conjecture for half-integer weight k is

$$|a_n| = O\left(n^{\frac{k}{2}-\frac{1}{2}+\epsilon}\right)$$

for n square-free, but unlike the conjecture for even weight k, this result has yet to be proven. The best bounds to date for the function $h_s(n)$ in Theorem 1 are therefore

$$h_s(n) = \begin{cases} O\left(n^{\frac{s}{4}-\frac{1}{4}+\epsilon}\right) & \text{for } s \geq 4,\ n \geq 0 \\ O\left(n^{\frac{s}{4}-\frac{2}{7}+\epsilon}\right) & \text{for } s \geq 4,\ n \geq 0 \text{ square-free} \\ O\left(n^{\frac{s}{4}-\frac{1}{2}+\epsilon}\right) & \text{for } s \geq 4,\ 4|s,\ n \geq 0. \end{cases}$$

5 Sums of Higher Powers

In Sections 2 through 4, we used the theory of modular forms to count representations of integers as sums of squares. A natural question to ask is whether the results and methods generalise to sums of cubes and higher powers. Indeed, there is an analogue of Theorem 1 for sums of an arbitrary power, but the result cannot be derived via modular forms. Instead, one uses the "circle method" devised by Hardy and Littlewood to compute an order-of-magnitude estimate. The main result is:

Theorem 3. *Suppose k and s are integers such that $k \geq 2$ and $s > 2^k$. For n a positive integer, let $r_{k,s}(n)$ be the number of solutions in positive integers to the equation*

$$x_1^k + \ldots + x_s^k = n.$$

Then

$$r_{k,s}(n) = \mathfrak{S}(n)\Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{s/k-1} + h_{s,k}(n),$$

where $\mathfrak{S}(n)$ is an arithmetic function that is bounded above and below by constants depending only on s and k, and $h_{s,k}(n) = O(n^{s/k-1-\epsilon})$ for some $\epsilon > 0$.

As in the case of sums of s squares, the problem comes down to estimating Fourier coefficients of a certain "generating function" raised to the sth power. The generating function in the general case is

$$f_k(z) = \sum_{m=0}^{\infty} e^{2\pi i m^k z}.$$

From this definition, we see that $f_k(z)^s$ has a Fourier series,

$$f_k(z)^s = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

and that the Fourier coefficients a_n are exactly the number of representations $r_{k,s}(n)$. Note that for $k = 2$, $f_k(z)$ is almost the function $\Theta_1(z)$ we considered in Section 2, the only difference being that we are now summing over positive integers only.

One might hope that the function $f_k(z)$ (which converges for $z \in \mathbb{H}$) has transformation properties that allow us to consider it as a modular form. Indeed, we have the relation $f_k(z + 1) = f_k(z)$ for all $z \in \mathbb{H}$. However, to derive the formula for $\Theta_n(-1/z)$ in Proposition 2.3 we used the Poisson summation formula and applied the fact that the Fourier transform of the theta function is another theta function, or, more precisely, that the Fourier transform of a Gaussian is another Gaussian. In the general case, the terms of $f_k(z)$ are not Gaussians, and thus we cannot take a Fourier transform and hope to recover some other form of $f_k(z)$. Our hopes of using the theory of modular forms to estimate the Fourier coefficients of $f_k(z)^s$ are therefore dashed, and we must turn to another method.

The following discussion of the circle method is based closely on that of Nathanson [N, §4-5]. Vaughan [V, §2] and Davenport [D, §2-6] provide similar expositions.

5.1 The Circle Method

The Hardy-Littlewood circle method estimates the Fourier coefficients of $f_k(z)^s$ by computing them directly via integration. Before describing the method, we make a simplification due to Vinogradov, which is to replace the infinite series $f_k(z)$ with a trigonometric polynomial. For any positive integer N, let $P = \lceil N^{1/k} \rceil$, and let

$$p_k(z) = \sum_{m=0}^{P} e\left(m^k z\right).$$

(As before, $e(z) = e^{2\pi i z}$.) Then the first N Fourier coefficients of $p_k(z)^s$ match those of $f_k(z)^s$, and the problem of computing $r_{k,s}(n)$ is reduced to computing Fourier coefficients of $p_k(z)^s$ for sufficiently large N. We thus have

$$r_{k,s}(n) = \int_0^1 p_k(\alpha)^s e(-n\alpha)\, d\alpha, \tag{5.1}$$

which follows from the orthogonality relation,

$$\int_0^1 e(m\alpha)\, e(-n\alpha)\, d\alpha = \delta_{mn}.$$

(Here and throughout the remainder of this section, we implicitly assume that we have fixed a specific n and chosen $N = n$.)

The idea behind the circle method is to divide the interval of integration into two subsets: the "major arcs" $\mathfrak{M}$ and the "minor arcs" $\mathfrak{m}$. The major arcs consist of points α that are near a rational number with small denominator. (The terms "near" and "small" will be made more precise later.) These points give a nontrivial contribution to the integral. As a simple example, consider $\alpha = 1/3$ and $k = 4$. Since

$$e\left(\frac{m^4}{3}\right) = \begin{cases} 1 & \text{if } m \equiv 0 \pmod 3 \\ -\frac{1}{2} + i\frac{\sqrt{3}}{2} & \text{if } m \equiv 1 \text{ or } 2 \pmod 3, \end{cases}$$

$p_4(1/3)$ is roughly equal to $Ni/\sqrt{3}$, so the contribution to the integral is $O(N)$. The minor arcs, on the other hand, consist of points that are not near a rational number with small denominator; these points give a negligible contribution to the integral. For example, if α is irrational, the numbers $\{e\left(n^k\alpha\right) : n \in \mathbb{Z}\}$ are uniformly distributed on the unit circle, and thus for sufficiently large N, the sum as n ranges from 1 to N is very small relative to N.

To construct the major and minor arcs explicitly, we assume $n \geq 2^k$, so $P \geq 2$. Choose $\nu \in (0, 1/5)$, and for every pair of relatively prime integers (q, a) with $1 \leq q \leq P^\nu$ and $0 \leq a \leq q$, define

$$\mathfrak{M}(q,a) = \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{P^{k-v}}\right\},$$

and let

$$\mathfrak{M} = \bigcup_{1 \leq q \leq P^\nu} \bigcup_{\substack{0 \leq a \leq q \\ (q,a)=1}} \mathfrak{M}(q,a).$$

The set $\mathfrak{M}(q,a)$ is called a *major arc* (though it is actually an interval), and $\mathfrak{M}$ is the set of all major arcs. The major arcs thus consist of all $\alpha \in [0,1]$ that are near a rational number with denominator smaller than P^ν. The major arcs are disjoint, for if $\alpha \in \mathfrak{M}(q,a) \cap \mathfrak{M}(q',a')$ and $a/q \neq a'/q'$, then $|aq' - a'q| \geq 1$ and

$$\begin{aligned} \frac{1}{P^{2\nu}} &\leq \frac{1}{qq'} \\ &\leq \left|\frac{a}{q} - \frac{a}{q'}\right| \\ &\leq \left|\alpha - \frac{a}{q}\right| + \left|\alpha - \frac{a'}{q'}\right| \\ &\leq \frac{2}{P^{k-\nu}}, \end{aligned}$$

which is impossible since $P \geq 2$ and $k \geq 2$.

The width of the interval $\mathfrak{M}(q,a)$ is $2P^{\nu-k}$, except when $q=1$, in which case the width is $P^{\nu-k}$. The number of major arcs is

$$\sum_{q=1}^{P^\nu} \varphi(q) \;\leq\; \sum_{q=1}^{P^\nu} q \;=\; \frac{1}{2}P^\nu\left(P^\nu+1\right),$$

and therefore the total measure of the set of major arcs is

$$\mu(\mathfrak{M}) \;\leq\; 2P^{\nu-k}\frac{P^\nu\left(P^\nu+1\right)}{2} \;\leq\; \frac{2}{P^{k-3\nu}}. \tag{5.2}$$

Thus the measure of the major arcs goes to zero as n goes to infinity.

Next, we define the set of *minor arcs* to be

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}.$$

This set is a finite union of (disjoint) open intervals and consists of all $\alpha \in [0,1]$ that are not near a rational number with denominator smaller than P^ν. From (5.2), we see that the measure of the set of minor arcs approaches 1 as n approaches infinity.

We may thus split our expression for $r_{k,s}(n)$ into two terms:

$$r_{k,s}(n) = \int_{\mathfrak{M}} p_k(\alpha)^s e\left(-n\alpha\right) d\alpha + \int_{\mathfrak{m}} p_k(\alpha)^s e\left(-n\alpha\right) d\alpha. \tag{5.3}$$

We will see below that even though the minor arcs comprise the bulk of the unit interval, their contribution to the integral is negligible, and estimating $r_{k,s}(n)$ comes down to estimating the integral over the major arcs.

5.2 The Minor Arcs

When $k=1$, the polynomial

$$p_k(\alpha) = \sum_{m=0}^{P} e\left(m^k\alpha\right)$$

is a geometric series and is thus easy to estimate. For $k>1$, one can use a "forward difference operator" to estimate $p_k(\alpha)$ in terms of sums in which m^k is replaced by a polynomial in m of degree $k-1$. Repeated applications of this argument reduce to the case $k=1$. The rigorous description of this argument follows from a series of lemmas, which we will state but not prove in full detail. For a complete treatment, see [N] or [V].

For any function $f : \mathbb{R} \to \mathbb{R}$, define the *forward difference operator* Δ_d by

$$\Delta_d(f)(x) = f(x+d) - f(x).$$

For $\ell \geq 2$, define the *ℓth iterate* of the forward difference operator,

$$\Delta_{d_\ell,\ldots,d_1} = \Delta_{d_\ell} \circ \Delta_{d_{\ell-1}} \cdots \circ \Delta_{d_1}.$$

The difference operator reduces degrees of polynomials; for example, if we take $f(x)$ to be x^k, then

$$\Delta_{d_\ell,\ldots,d_1}(x^k) = d_1 \cdots d_\ell h_{k-\ell}(x),$$

where $h_{k-\ell}(x)$ is a polynomial in x of degree $k-\ell$ with integer coefficients. If we let $f(x)$ be an arbitrary polynomial of degree k and

$$T(f) = \sum_{x=1}^{Q} e\left(f(x)\right), \tag{5.4}$$

then we may use the difference operator to make the estimate,

$$|T(f)|^{2^j} \leq (2Q)^{2^j - j - 1} \sum_{\substack{d_1,\ldots,d_j \\ |d_i| \leq Q}} \sum_{x \in I} e\left(d_1 \cdots d_j h_{k-j}(x)\right), \tag{5.5}$$

where I consists of integers in a subinterval of $[1, Q]$, and $h_{k-j}(x)$ is a polynomial of degree $k-j$. If we assume that the leading coefficient of $f(x)$ is near a rational number with denominator q, then we may bound the sum in terms of powers of q and Q, which gives the following result:

Lemma 5.1 (Weyl's inequality). *Let $f(x) = \alpha x^k + \ldots$ be a polynomial in x of degree $k \geq 2$ with real coefficients, and suppose*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2},$$

where $q \geq 1$ and $(a, q) = 1$. Let $K = 2^{k-1}$ and $\epsilon \geq 0$, and define $T(f)$ as in (5.4) above. Then there exists some positive constant C (depending on k and ϵ) such that

$$|T(f)| \leq C \cdot Q^{1+\epsilon} \left(q^{-1} + Q^{-1} + Q^{-k} q\right)^{1/K}.$$

Weyl's inequality allows us to bound $p_k(\alpha)$ at any given α in terms of n and the denominator of a rational number near α. However, we wish to bound $p_k(\alpha)$ as it is integrated over all $\alpha \in \mathfrak{m}$. This is accomplished via Hua's lemma.

Lemma 5.2 (Hua's lemma). *For $k \geq 2$ and any $\epsilon > 0$, there exists some positive constant C (depending on k and ϵ) such that*

$$\int_0^1 |p_k(\alpha)|^{2^k} \, d\alpha \leq C \cdot P^{2^k - k + \epsilon}.$$

Proof. The proof proceeds by induction on j for $j = 1, \ldots, k$. The base case $j = 1$ is clear since

$$\int_0^1 |T(\alpha)|^2 \, d\alpha = \sum_{m=1}^{P} \sum_{n=1}^{P} \int_0^1 e\left(\alpha(m^k - n^k)\right) d\alpha = P.$$

Now assume the result holds for some $j \leq k-1$. By equation (5.5), we have

$$|p_k(\alpha)|^{2^j} \leq (2P)^{2^j - j - 1} \sum_{\substack{d_1, \ldots, d_j \\ |d_i| \leq P}} \sum_{x \in I} e\left(\alpha d_1 \cdots d_j h_{k-j}(x)\right),$$

where $h_{k-j}(x)$ is a polynomial of degree $k - j$ with integer coefficients, and I is an interval of consecutive integers contained in $[1, P]$. It follows that

$$|p_k(\alpha)|^{2^j} \leq (2P)^{2^j - j - 1} \sum_d r(d) e\left(\alpha d\right), \tag{5.6}$$

where $r(d)$ is the number of factorisations of d in the form

$$d = d_1 \cdots d_j h_{k-j}(x)$$

with $d_i < P$ and $x \in I$.

Similarly, by writing

$$|p_k(\alpha)|^{2^j} = p_k(\alpha)^{2^{j-1}} p_k(-\alpha)^{2^{j-1}},$$

one obtains

$$|p_k(\alpha)|^{2^j} = \sum_d s(d) e\left(-\alpha d\right), \tag{5.7}$$

where $s(d)$ is the number of representations of d in the form

$$d = \sum_{i=1}^{j-1} y_i^k - \sum_{i=1}^{j-1} x_i^k$$

with $1 \leq x_i, y_i \leq P$. Then

$$\sum_d s(d) = |p_k(0)|^{2^j} = P^{2^j}, \tag{5.8}$$

and by the inductive hypothesis,

$$s(0) = \int_0^1 |p_k(\alpha)|^{2^j} \, d\alpha \le C' \cdot P^{2^j - j + \epsilon} \tag{5.9}$$

for some constant C'. It follows from (5.6) and (5.7) that

$$\begin{aligned}
\int_0^1 |p_k(\alpha)|^{2^{j+1}} \, d\alpha &\le (2P)^{2^j - j - 1} \int_0^1 \sum_d r(d) e(\alpha d) \sum_d s(d) e(-\alpha d) \\
&\le (2P)^{2^j - j - 1} \left(r(0)s(0) + \sum_{d \ne 0} r(d)s(d) \right).
\end{aligned}$$

One can then show that $r(0) = O(P^j)$ and for $d > 0$, $r(d) = O(P^\epsilon)$ for any $\epsilon > 0$. Combining these facts with the bounds (5.8) and (5.9) gives

$$\begin{aligned}
\int_0^1 |p_k(\alpha)|^{2^{j+1}} \, d\alpha &\le C \cdot P^{2^j - j - 1} \left(P^j P^{2^j - j + \epsilon} + P^\epsilon P^{2^j} \right) \\
&\le 2C \cdot P^{2^{j+1} - (j+1) + \epsilon}
\end{aligned}$$

for some constant C, and thus the result holds for $j + 1$. □

Weyl's inequality and Hua's lemma are the two major ingredients in bounding the minor arcs term. In addition, we use a result of Dirichlet that says how closely we may approximate a number by a rational.

Lemma 5.3 (Dirichlet). *Let α and Q be real numbers, $Q \ge 1$. Then there exist relatively prime integers a and q such that $1 \le q \le Q$ and*

$$\left| \alpha - \frac{a}{q} \right| < \frac{1}{qQ}.$$

We now have all the tools necessary to bound the minor arcs term in equation (5.3).

Proposition 5.4. *Let $k \ge 2$ and $s \ge 2^k + 1$. Then there exists $\epsilon > 0$ such that*

$$\int_{\mathfrak{m}} p_k(\alpha)^s e(-n\alpha) \, d\alpha = O\left(n^{\frac{s}{k} - 1 - \epsilon} \right),$$

where the implied constant depends only on k and s.

Proof. We have to save an amount $n^{-1-\epsilon}$ over the trivial estimate $n^{s/k}$. Hua's lemma saves $n^{\epsilon-1}$, and Weyl's inequality saves the rest.

By Dirichlet's theorem (Lemma 5.3) with $Q = P^{k-\nu}$, for any real number α we can find a fraction a/q with $1 \le q \le P^{k-\nu}$ and $(a, q) = 1$ such that

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{qP^{k-\nu}} \le \min\left(\frac{1}{P^{k-\nu}}, \frac{1}{q^2}\right).$$

Since $\alpha \in \mathfrak{m} \subset (P^{\nu-k}, 1 - P^{\nu-k})$, we have $1 \le a \le q - 1$. If $q \le P^{\nu}$, then $\alpha \in \mathfrak{M}(q, a)$, which contradicts our assumption that $\alpha \in \mathfrak{m}$. Thus $q > P^{\nu}$. Applying Weyl's inequality (Lemma 5.1) with $f(x) = \alpha x^k$, we have for any $\epsilon' > 0$,

$$|p_k(\alpha)| \le C \cdot P^{1+\epsilon'}\left(q^{-1} + P^{-1} + P^{-k}q\right)^{1/K} \le C_1 \cdot P^{1+\epsilon'-\nu/K},$$

where $K = 2^k - 1$. With this result and Hua's lemma (Lemma 5.2), we have

$$\begin{aligned}
\left|\int_{\mathfrak{m}} p_k(\alpha)^s e(-n\alpha)\right| d\alpha &\le \sup_{\alpha\in\mathfrak{m}} |p_k(\alpha)|^{s-2^k} \int_0^1 |p_k\alpha|^{2^k} d\alpha \\
&\le \left(C_1 \cdot P^{1+\epsilon'-\nu/K}\right)^{s-2^k}\left(C_2 \cdot P^{2^k-k+\epsilon'}\right) \\
&\le C \cdot P^{s-k+\delta},
\end{aligned}$$

where we have combined the constants into C and set

$$\delta = \frac{\nu}{K}\left(2^k - s\right) + \epsilon'\left(s - 2^k + 1\right).$$

Since $s > 2^k$, we can choose ϵ' sufficiently small so that $\delta < 0$. Letting $\epsilon = -\delta/k$ and using the definition $P = \lceil N^{1/k} \rceil$ gives the result. □

5.3 The Major Arcs

To estimate the major arcs term in equation (5.3), we begin by writing the function $p_k(\alpha)$ on the major arcs as the product of two exponential sums plus a small error term. Bounding these sums and integrating over the major arcs gives us a bound for the major arcs term in terms of an exponential sum called the "singular series," an integral called the "singular integral," and a small error term. Further calculations then show that the singular series is bounded by a constant, and the singular integral is $O\left(n^{s/k-1}\right)$. As in the previous section, we omit many of the details; for a full treatment, see [N] or [V].

We start by introducing the auxiliary functions

$$\begin{aligned} v(\beta) &= \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e\,(m\beta), \\ S(q,a) &= \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right). \end{aligned}$$

Roughly speaking, the function $v(\beta)$ measures the probability that m is a kth power, and $S(q,a)$ measures the distribution of the kth powers modulo q. When α is contained in the major arc $\mathfrak{M}(q,a)$, then $p_k(\alpha)$ is well approximated by the product of these two functions. Specifically,

$$p_k(\alpha) = \left(\frac{S(q,a)}{q}\right) v\left(\alpha - \frac{a}{q}\right) + O\left(P^{2\nu}\right). \tag{5.10}$$

If we write

$$V(\alpha,q,a) = \left(\frac{S(q,a)}{q}\right) v\left(\alpha - \frac{a}{q}\right),$$

then factoring the expression $p_k(\alpha)^s - V(\alpha,q,a)^s$ and applying (5.10) shows that

$$p_k(\alpha)^s - V(\alpha,q,a)^s = O\left(P^{s-1+2\nu}\right).$$

Integrating over the major arcs and applying the estimate for $\mu(\mathfrak{M})$ in (5.2) gives

$$\int_{\mathfrak{M}} |p_k(\alpha)^s - V(\alpha,q,a)^s|\, d\alpha = O\left(P^{s-k-\delta_1}\right)$$

for some $\delta_1 > 0$. Since the integral over all of $\mathfrak{M}$ is equal to the sum of the integrals over the individual arcs $\mathfrak{M}(q,a)$, we see that

$$\int_{\mathfrak{M}} p_k(\alpha)^s e\,(-n\alpha)\, d\alpha = \sum_{1\le p\le P^\nu} \sum_{\substack{0\le a\le q \\ (a,q)=1}} \int_{\mathfrak{M}(q,a)} V(\alpha,q,a)^s e\,(-n\alpha)\, d\alpha + O\left(P^{s-k-\delta_1}\right).$$

Further algebraic manipulation leads to the following result:

Lemma 5.5. *Let*

$$\begin{aligned} \mathfrak{S}(n,Q) &= \sum_{1\le q\le Q} \sum_{\substack{1\le a\le q \\ (a,q)=1}} \left(\frac{S(q,a)}{q}\right)^s e\left(\frac{-na}{q}\right), \\ J^*(n) &= \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e\,(-n\beta)\, d\beta. \end{aligned}$$

Then
$$\int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}(n, P^\nu) J^*(n) + O\left(P^{s-k-\delta_1}\right).$$

Lemma 5.5 tells us that estimating the major arcs term comes down to estimating the sum $\mathfrak{S}(n, P^\nu)$ and the integral $J^*(n)$. The first step in estimating the integral $J^*(n)$ is to show that expanding the range of integration introduces only a small error. Let

$$J(n) = \int_{-1/2}^{1/2} v(\beta)^s e(-n\beta)\, d\beta.$$

The function $J(n)$ is called the *singular integral.* One may use the bound

$$v(\beta) \leq C \cdot \min\left(P, |\beta|^{-1/k}\right)$$

for $|\beta| \leq 1/2$ to show that

$$|J(n) - J^*(n)| = O\left(P^{s-k-\delta_2}\right) \tag{5.11}$$

for some $\delta_2 > 0$. Then by inducting on s and using a computational lemma about the Gamma function, one arrives at the following formula:

$$J(n) = \Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + O\left(N^{\frac{s-1}{k}-1}\right) \tag{5.12}$$

for $s \geq 2$.

To estimate the sum $\mathfrak{S}(N, P^\nu)$, we begin by completing the series to infinity and show that this introduces only a small error. If we let

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} A_n(q),$$

where

$$A_n(q) = \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \left(\frac{S(q,a)}{q}\right)^s e\left(\frac{-na}{q}\right),$$

then there is some $\delta_3 > 0$ such that

$$|\mathfrak{S}(n) - \mathfrak{S}(n, P^\nu)| = O\left(P^{-\delta_3}\right). \tag{5.13}$$

The series $\mathfrak{S}(n)$ is called the *singular series.* We may now apply Weyl's inequality (Lemma 5.1) to make the estimate

$$S(q,a) = O\left(q^{1-\frac{1}{K}+\epsilon}\right),$$

from which we deduce that

$$A_n(q) = O\left(q^{-1-\delta_4}\right) \tag{5.14}$$

for some $\delta_4 > 0$. The singular series $\mathfrak{S}(n)$ thus converges absolutely and uniformly with respect to n. We conclude that there is a constant c_2 (depending only on k and s) such that

$$|\mathfrak{S}(n)| < c_2 \tag{5.15}$$

for all positive integers n.

Bounding the singular series from below is a bit more complicated. The first step is to show that the function $A_n(q)$ is multiplicative; i.e. for q and r relatively prime, $A_n(q)A_n(r) = A_n(qr)$. This property allows us to limit our calculations to the case when q is a power of a prime number. If we define

$$\chi_n(p) = 1 + \sum_{h=1}^{\infty} A_n\left(p^h\right),$$

it is possible to show that

$$\chi_n(p) = \lim_{h\to\infty} \frac{M_n(p^h)}{p^{h(s-1)}}, \tag{5.16}$$

where $M_n(q)$ is the number of solutions to the congruence

$$x_1^k + \cdots + x_s^k \equiv n \pmod{q} \tag{5.17}$$

with the x_i integers in $[1, q]$.

The next step is to expand $\mathfrak{S}(n)$ as an "Euler product,"

$$\mathfrak{S}(n) = \prod_{p \text{ prime}} \chi_n(p). \tag{5.18}$$

From equation (5.16) we deduce that $\mathfrak{S}(n)$ is a positive real number, and from the bound (5.14) it follows that there exists some p_0 such that

$$\frac{1}{2} \le \prod_{p>p_0} \chi_n(p) \le \frac{3}{2}$$

for all $n \ge 1$. It therefore suffices to show that $\chi_n(p)$ is positive for all $p \le p_0$. This result follows from equation (5.16) and the fact that when $q = p^\gamma$, there is always a solution to the congruence (5.17) with the x_i not all divisible by p. We conclude that there is some c_1 such that

$$\mathfrak{S}(n) \ge c_1 > 0 \tag{5.19}$$

for all positive integers n.

We now have all the tools to bound the major arcs term in equation (5.3).

Proposition 5.6. *For $s \geq 2^k + 1$, there exists some $\epsilon > 0$ such that*

$$\int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}(n)\Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + O\left(N^{\frac{s}{k}-1-\epsilon}\right).$$

Proof. By Lemma 5.5,

$$\int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}(n, P^\nu)J^*(n) + O\left(P^{s-k-\delta_1}\right).$$

By equations (5.13) and (5.11), the first term is equal to

$$\left(\mathfrak{S}(n) + O\left(P^{-\delta_3}\right)\right)\left(J(n) + O\left(P^{s-k-\delta_2}\right)\right).$$

By equation (5.12) and the fact that $P = \lceil N^{1/k} \rceil$, $J(n) = O\left(P^{s-k}\right)$. Multiplying out the product and combining error terms yields

$$\int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}(n)J(n) + O\left(P^{s-k-\epsilon'}\right),$$

where we have used the bound (5.15) to incorporate the product of $\mathfrak{S}(n)$ and the error in $J(n)$ into the overall error term. Substituting the formula in equation (5.12) and once more applying the bound (5.15) gives the result. □

5.4 Conclusions

We now combine all of the above results to prove the Hardy-Littlewood asymptotic formula for $r_{k,s}(n)$.

Proof of Theorem 3. From equation (5.1), we have

$$r_{k,s}(n) = \int_0^1 p_k(\alpha)^s e(-n\alpha)\, d\alpha.$$

By construction of the major arcs $\mathfrak{M}$ and the minor arcs $\mathfrak{m}$, this expression splits into two integrals,

$$r_{k,s}(n) = \int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} p_k(\alpha)^s e(-n\alpha)\, d\alpha.$$

By Proposition 5.4,

$$\int_{\mathfrak{m}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = O\left(n^{\frac{s}{k}-1-\epsilon_1}\right),$$

and by Proposition 5.6,

$$\int_{\mathfrak{M}} p_k(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}(n)\Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + O\left(N^{\frac{s}{k}-1-\epsilon_2}\right).$$

Combining the error terms and noting that $\mathfrak{S}(n)$ is bounded above and below by constants depending only on k and s gives the result. □

As a parting remark, we note that when $k = 2$ and $s \geq 5$, Theorem 3 gives

$$r_{2,s}(n) = \delta'_s(n) + h'_s(n), \tag{5.20}$$

where $\delta'_s(n) = O\left(n^{s/2-1}\right)$ and $h'_s(n) = O\left(n^{s/2-1-\epsilon}\right)$. This result is a direct corollary of Theorem 1.

Each of the two treatments of the problem for sums of squares has its advantages. The Hardy-Littlewood circle method allows us to derive both an upper and a lower bound for the function $\delta'_s(n)$ in equation (5.20), so $\delta'_s(n)$ is truly an asymptotic approximation to $r_{k,s}(n)$. With modular forms we did not derive a lower bound, so Theorem 1 allows for the possibility that the so-called "error term" $h_s(n)$ may dominate for some large values of n. On the other hand, the circle method gives a considerably worse bound for the error term $h'_s(n)$ than the $O\left(n^{s/4}\right)$ of Theorem 1. In addition, the circle method can only provide approximations to $r_{k,s}(n)$, and even for the case $k = 2$ we cannot use it to derive any formulae analogous to those in Theorem 2.

References

[D] Davenport, Harold. *Analytic Methods for Diophantine Equations and Diophantine Inequalities.* Ann Arbor: Ann Arbor Publishers, 1962.

[G] Gunning, R.C. *Lectures on Modular forms.* Princeton: Princeton University Press, 1962.

[I] Iwaniec, Henryk. *Topics in Classical Automorphic Forms* (GSM 17). Providence: American Mathematical Society, 1997.

[K] Koblitz, Neal. *Introduction to Elliptic Curves and Modular Forms* (GTM 97). New York: Springer-Verlag, 1984.

[Kö] Körner, T.W. *Fourier Analysis.* Cambridge: Cambridge University Press, 1988.

[Mi] Milne, J.S. *Modular Functions and Modular Forms.* Accessed online: http://www.jmilne.org/math/CourseNotes/math678.html, 24 Apr 2003.

[Mu] Mumford, David. *Tata Lectures on Theta I.* Boston: Birkhäuser, 1983.

[N] Nathanson, Melvyn B. *Additive Number Theory: The Classical Bases* (GTM 164). New York: Springer, 1996.

[S1] Sarnak, Peter. "Kloosterman, quadratic forms and modular forms." *Nieuw Archief voor Wiskunde 5* **1** (2000), 385-389.

[S2] ——. *Some Applications of Modular Forms.* Cambridge: Cambridge University Press, 1990.

[Sch] Scholl, Anthony J. "Modular Forms." Cambridge University, Lent Term 2003.

[V] Vaughan, R.C. *The Hardy-Littlewood method.* Cambridge: Cambridge University Press, 1981.

[W] Weisstein, Eric W. "Jacobi Symbol." Accessed online: http://mathworld.wolfram.com/JacobiSymbol.html, 5 Mar 2003.