14b. Theta series, sums of squares

Paul Garrett  garrett@math.umn.edu  http://www.math.umn.edu/~garrett/

[This document is http://www.math.umn.edu/~garrett/m/complex/notes_2020-21/14b_eight_squares.pdf]

1. Holomorphic modular forms for $\Gamma_{\theta}$
2. Holomorphic Eisenstein series for $\Gamma_{\theta}$
3. Divisor formula for $\Gamma_{\theta}$
4. Theta series and Poisson summation
5. Sums of squares
6. Appendix: fundamental domain and generators for $\Gamma_{\theta}$

The first (slightly frivolous) application here is to obtain a formula for the number of ways to express a positive integer as a sum of squares of eight integers. For example, we will prove

$$\text{number of ways to express odd prime } p \text{ as sum of } 8 \text{ squares } = 16(p^3 + 1)$$

This will follow from the fact that the theta series

$$\theta(z) = \sum_{v \in \mathbb{Z}^8} e^{\pi i |v|^2} (\text{with } z \in \mathcal{H})$$

is a holomorphic modular form of weight 4 for the subgroup

$$\Gamma_{\theta} = \Gamma(2) \cup w \Gamma(2) \quad (\text{with } \Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 2 \right\})$$

where $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Further, we use the fact that there are no weight 4 cuspforms for $\Gamma_{\theta}$, from the divisor formula below. We also use the explicit computation of the Fourier coefficients of the two weight 4 Eisenstein series for $\Gamma_{\theta}$.

One early modern study of representability by quadratic forms, by similar methods, was H.D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Proc. London Math. Soc. 25 (1926), 143-173. Kloosterman recognized that more than four variables, especially an even number of variables, is much easier than four or fewer, and gave several references to earlier work.

1. Holomorphic modular forms for $\Gamma_{\theta}$

[1.1] Standard fundamental domain

The appendix proves that the translation $z \to z + 2$ and the inversion $z \to -1/z$ generate $\Gamma_{\theta}$, and there is the standard fundamental domain

$$F = \{ z \in \mathcal{H} : |z| \geq 1, -1 \leq z \leq 1 \}$$

There are two $\Gamma_{\theta}$-inequivalent cusps at the boundary of the standard fundamental domain, $i\infty$ and 1, since $-1$ is identified with +1 by $z \to z + 2$.

[1.2] No odd-weight modular forms for $\Gamma_{\theta}$

Just as for $SL_2(\mathbb{Z})$, there are no (not-identically-zero) odd-weight holomorphic modular forms $f$ for $\Gamma_{\theta}$, since $-1_2 \in \Gamma_{\theta}$, and

$$f(z) = f\left( \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right)(z) = (-1)^k \cdot f(z)$$
[1.3] Fourier expansion at $i\infty$

Similar to $SL_2(\mathbb{Z})$, because of invariance under the translation $z \to z + 2$, holomorphic modular forms for $\Gamma_0$ have Fourier series expansions of the form

$$f(z) = \sum_{n \geq 2} c_n e^{\pi inz}$$

with exponentials $e^{\pi inz}$ rather than $e^{2\pi inz}$ as for $SL_2(\mathbb{Z})$, since the latter contains the translation $z \to z + 1$. That is, the width of the cusp $i\infty$ of $\Gamma_0$ is 2, not 1, as it was for $SL_2(\mathbb{Z})$.

Require that $f$ is bounded as $y \to +\infty$. The Fourier coefficients are obtained by the expected formula, noting that the exponential involving $y$ stays with the constant:

$$\frac{1}{2} \int_{-1}^{1} e^{-\pi inx} f(x + iy) \, dx = \sum_{m} c_m \cdot \frac{1}{2} \int_{-1}^{1} e^{-\pi imx} e^{\pi im(x+iy)} \, dx$$

$$= \sum_{m} c_m \cdot \frac{1}{2} \int_{-1}^{1} e^{-\pi inx} e^{\pi im(x+iy)} \, dx = c_n \cdot e^{-2\pi ny}$$

Thus, the boundedness gives

$$|c_n e^{-2\pi ny}| = \left| \frac{1}{2} \int_{-1}^{1} e^{-\pi inx} f(x + iy) \, dx \right| \leq \int_{-1}^{1} |f(x + iy)| \, dx \ll 1$$

For $n < 0$, letting $y \to +\infty$ proves $c_n = 0$. The order of vanishing of $f$ at $i\infty$ is the lowest index $n_0$ such that $c_{n_0} \neq 0$. This much is parallel to $SL_2(\mathbb{Z})$.

[1.4] Boundedness at the other cusp 1 The details of the proof of the divisor formula below explain, at least with hindsight, that part of the definition of weight $2k$ holomorphic modular form $f$ for $\Gamma_0$ require that, for $g \in SL_2(\mathbb{Z})$ with $g(i\infty) = 1$, as $y \to +\infty$ the value $(f|_{2k}g)(z)$ is bounded.

[1.5] Remark: That is, as it happens, requiring that $f(z)$ itself be bounded as $z \to 1$ inside the standard fundamental region is too strong a condition. By accident, it would exclude some holomorphic Eisenstein series needed for a coherent discussion.

The action of $SL_2(\mathbb{C})$ on complex projective space $\mathbb{C} \cup \{\infty\}$ maps lines-and-circles to lines-and-circles, so any $g \in SL_2(\mathbb{R})$ mapping $i\infty$ to 1 maps regions $\{y > T\}$ to open disks tangent to the real line at 1. For fixed $g$, as $T$ increases, the circles shrink. Thus, in this context, approaching the cusp 1 means to approach within such shrinking circles. In particular, this excludes tangential approach, or any approach other than asymptotically vertical.

[1.6] Fourier expansion at the other cusp 1 Also from the details of the divisor formula the order of vanishing of $f$ at the cusp 1 should be expressed in terms of a Fourier expansion of $f$ at 1. For this, we need to change coordinates on $\mathbb{H}$ so that the isotropy group of 1 in $\Gamma_0$ becomes ordinary translations. That is, we want $g \in SL_2(\mathbb{Z})$ to map 1 to $i\infty$, since for $\gamma(1) = 1$,

$$\gamma^{-1}(i\infty) = \gamma(1) = 1 = g^{-1}(i\infty)$$

gives $(g\gamma^{-1})(i\infty) = i\infty$. The isotropy group of $i\infty$ in $SL_2(\mathbb{R})$ is upper-triangular matrices $P$, so

$$g(\text{isotropy group of 1 in } \Gamma_0)g^{-1} \subset P$$

and, equivalently,

$$\text{isotropy group of 1 in } \Gamma_0 = \Gamma_0 \cap g^{-1}Pg$$
An explicit choice of mapping 1 to \(i\infty\) is easily accomplished by translating and inverting:

\[
1 \rightarrow \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} (1) = 0 \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (0) = i\infty
\]

That is, \(g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\) maps 1 \(\rightarrow\) \(i\infty\). The \textit{translations} in the isotropy group of 1 are \(\Gamma_\theta \cap g^{-1}Ng\), where \(N = \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix}\) is the group of translations in \(SL_2(\mathbb{R})\):

\[
\text{translations in isotropy group of } 1 = \Gamma_\theta \cap \left( \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \right) = \begin{pmatrix} -b + 1 & b \\ -b & b + 1 \end{pmatrix}
\]

The latter is in \(\Gamma_\theta\) if and only if \(b \in \mathbb{Z}\). That is, the \textit{width} of the cusp 1 of \(\Gamma_\theta\) is 1, in contrast to the cusp \(i\infty\) which has width 2 for \(\Gamma_\theta\).

The Fourier expansion at 1 of a modular form \(f\) for \(\Gamma_\theta\) is really the Fourier expansion of \((f|_{2k}g)(z)\) for \(g \in SL_2(\mathbb{Z})\) with \(g(i\infty) = 1\). The determination that the \textit{width} is 1 shows that the expansion will be of the form

\[
(f|_{2k}g)(z) = \sum_{n \in \mathbb{Z}} c_n e^{\pi inz}
\]

The same argument as for \(i\infty\) shows that boundedness implies that the negative-index Fourier coefficients are all 0.

[1.7] \textbf{Hecke’s estimate on Fourier coefficients of cuspforms} Just as for \(SL_2(\mathbb{Z})\), it is straightforward to obtain a useful asymptotic bound on Fourier coefficients of holomorphic cuspforms for \(\Gamma_\theta\). This will be used a little frivolously in obtaining an asymptotic for the number of ways to represent integers as sums of squares, and less frivolously in proving some equidistribution results on spheres.

[1.8] \textbf{Theorem: (Hecke)} For \(f(z) = \sum_{n \geq 1} c_n e^{\pi inz}\) a holomorphic cuspform of weight 2\(k\) for \(\Gamma_\theta\),

\[
c_m = O(n^{\frac{2k}{2}})
\]

\textbf{Proof:} Since \(f\) is bounded as \(y \rightarrow +\infty\),

\[
|c_n \cdot e^{-\pi ny}| = \frac{1}{2} \int_0^2 e^{-\pi inx} f(x + iy) \, dx \leq \frac{1}{2} \int_0^2 |f(x + iy)| \, dx \ll f
\]

This gives a bad preliminary estimate \(|c_n| \ll f e^{\pi n}\), by taking \(y = 1\). As for \(SL_2(\mathbb{Z})\), this gives exponential decay of \(f(x + iy)\) as \(y \rightarrow +\infty\):

\[
|f(x + iy)| \leq \sum_{n \geq 1} |c_n| e^{-\pi ny} \ll_f \sum_{n \geq 1} e^{\pi n} e^{-\pi ny} = \frac{e^{-\pi(y-1)}}{1 - e^{\pi(y-1)}}
\]

A nearly identical discussion applies to \(f\) near the cusp 1, that is, with \(g \in SL_2(\mathbb{Z})\) such that \(g(i\infty) = 1\), the same discussion applies to \((f|_{2k}g)\) near \(i\infty\). Namely,

\[
(f|_{2k}g)(x + iy) \ll_f e^{-2\pi(y-1)} \quad \text{(for } y \gg 1)\]

For example, with

\[
g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}
\]
\[(f|_{2k}g)(x + iy) = z^{-2k} \cdot f(gz) \ll_f e^{-2\pi(y-1)} \ll_f e^{-2\pi(y-1)} \text{ (for } y \gg 2)\]

Since the cusp 1 has width 1, it suffices to consider \(0 \leq x \leq 1\), and in the region \(0 \leq x \leq 1\) and \(y \geq 2\),
\[|y| \ll |z| \ll |y|\]
so
\[f(g(x + iy)) \ll y^{2k} \cdot |f(gz)| \ll_f y^{2k} e^{-2\pi(y-1)} \text{ (in } 0 \leq x \leq 1 \text{ and } y \geq 2)\]

The relevant qualitative point is that this is of rapid decay as \(y \to \infty\). That is, \(f(z)\) is of rapid decay as \(z\) approaches either cusp within a fixed fundamental domain.

Since \(f\) is continuous, \(y^{\frac{2k}{2}}|f(z)|\) is bounded in the fundamental domain. It is also \(\Gamma_0\)-invariant, so is bounded on the whole \(\frak{H}\).

Thus, as with \(SL_2(\mathbb{Z})\), we boot-strap ourselves:
\[|c_n \cdot e^{-\pi ny} \cdot y^{\frac{2k}{2}}| = \frac{1}{2} y \cdot \left| \int_0^y e^{-\pi yx} f(x + iy) \, dx \right| \leq \frac{1}{2} \int_0^y y^k |f(x + iy)| \, dx \ll_f 1\]

From \(|c_n| \ll_f y^{-\frac{2k}{2}} e^{\pi ny}\) for all \(y > 0\), optimize choice of \(y\) to minimize the upper bound: solve
\[0 = \frac{\partial}{\partial y} y^{-k} e^{\pi ny} = -ky^{-k-1} e^{\pi ny} + \pi ny^{-k} e^{\pi ny} = (-k + \pi ny) \cdot y^{-k-1} e^{\pi ny}\]

Thus, \(y = k/\pi n\), giving
\[|c_n| \ll_f \left(\frac{k}{\pi n}\right)^{-\frac{2k}{2}} e^{\pi n \cdot k/\pi n} \ll_f, k n^{\frac{4k}{2}}\]
which is Hecke’s estimate. 

[1.9] **Ramanujan’s Delta** In the discussion of \(SL_2(\mathbb{Z})\), we saw that Ramanujan’s cuspform \(\Delta(z)\) of weight 12 does not vanish on \(\frak{H}\), but only at \(i\infty\). It is certainly also a cuspform for \(\Gamma_0\). Since the width of the cusp 1 is just 1, \(\Delta(z)\) vanishes to order 1 at the cusp 1. However, the width of the cusp \(i\infty\) for \(\Gamma_0\) is 2, so in the appropriate coordinates for \(\Gamma_0\), \(\Delta(z)\) vanishes to order 2 at \(i\infty\).

Apart from this possible surprise, there is the consequence that it is no longer possible to divide general cuspforms for \(\Gamma_0\) by \(\Delta(z)\) and obtain holomorphic modular forms, unless the given cuspform happens to vanish to order 2 at \(i\infty\).

In discussion of the divisor formula below, we will discover that there is an essentially unique cuspform of weight 8, vanishing to first order at both cusps, and not vanishing at any point of \(\frak{H}\).

---

2. **Holomorphic Eisenstein series for \(\Gamma_0\)**

One use of holomorphic Eisenstein series is to subtract them from a given holomorphic modular form to produce a cuspform. That is, referring to the two (equivalence classes of) cusps by their representatives \(i\infty\) and 1, for each weight \(4 \leq 2k \in 2\mathbb{Z}\), we want two Eisenstein series \(E_{2k}^{(i\infty)}\) and \(E_{2k}^1\) so that, with \(g \in SL_2(\mathbb{Z})\) such that \(g(i\infty) = 1\),

\[
\begin{align*}
  E_{2k}^{(i\infty)}(i\infty) &= 1 \\
  E_{2k}^{(i\infty)}|_{2k}g(1) &= 0
\end{align*}
\]

\[
\begin{align*}
  E_{2k}^{(1)}(i\infty) &= 0 \\
  E_{2k}^{(1)}|_{2k}g(1) &= 1
\end{align*}
\]

[2.1] **Remark:** That is, roughly, the Eisenstein series attached to a cusp \(\sigma\) should essentially have value 1 there and should essentially have value 0 at the other cusp. This does not quite literally happen, except at \(i\infty\). Rather, the weight \(2k\) action intervenes, reducing evaluation at other cusps to evaluation at \(i\infty\).
[2.2] Moving Eisenstein series around  For this subsection, we look at Eisenstein series defined by congruence conditions modulo \( N \), because the patterns are clearer than if we’d just treat \( N = 2 \).

Fix \( N \geq 1 \), fix weight \( 4 \leq 2k \in 2\mathbb{Z} \), and for \( c_o, d_o \mod N \) define a slightly different type of Eisenstein series

\[
\tilde{E}_{(c_o, d_o)}(z) = \sum_{(0,0) \neq (c,d), (c,d) = (c_o, d_o) \mod N} \frac{1}{(cz + d)^{2k}} \quad \text{ (with } (c, d) \in \mathbb{Z}^2) \]

Generally, such an Eisenstein series will be a modular form only for the principal congruence subgroup

\[
\Gamma(N) = \Gamma = \{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \mod N \} \]

One virtue of this description is the simplicity of behavior under the weight \( 2k \) action of \( g = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \) in the full group \( SL_2(\mathbb{Z}) \):

\[
\tilde{E}_{(c_o, d_o)}|_{2k} g(z) = (cz + d)^{-2k} \sum_{(0,0) \neq (m,n), (m,n) = (c_o, d_o) \mod N} \frac{1}{(m^2z + b + n(cz + d))^{2k}} = \sum_{(m,n) = (c_o, d_o) \mod N} \frac{1}{(ma + nc)z + (mb + nd))^{2k}}
\]

Mod \( N \) we have

\[
\begin{pmatrix} ma + nc & mb + nd \end{pmatrix} = (m, n) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c_o & d_o \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod N
\]

This gives the useful relation

\[
\tilde{E}_{(c_o, d_o)}|_{2k} g = \tilde{E}_{(c_o, d_o)g}
\]

In particular, the Fourier expansions of these Eisenstein series at various cusps are systematically accessible, as below. A more systematic version of the above description, for fixed level \( N \) and weight \( 2k \), is to let \( \varphi \) be a \( \mathbb{C} \)-valued function on \( (\mathbb{Z}/N)^2 \), and put

\[
\tilde{E}_{\varphi}(z) = \sum_{(0,0) \neq (c,d) \in \mathbb{Z}^2} \varphi(c,d) \frac{1}{(cz + d)^{2k}}
\]

The same computation shows that, for \( g \in SL_2(\mathbb{Z}) \),

\[
\tilde{E}_{\varphi}|_{2k} g = \tilde{E}_{\varphi \circ g^{-1}}
\]

In effect, the previous version \( \tilde{E}_{c_o, d_o} \) used the function

\[
\varphi(c,d) = \begin{cases} 1 & \text{ (when } (c,d) = (c_o, d_o) \mod N) \\ 0 & \text{ (otherwise)} \end{cases}
\]

The form \( \tilde{E}_{\varphi} \) is readily expressed in terms of the \( \tilde{E}_{c_o, d_o} \)'s, by

\[
\tilde{E}_{\varphi}(z) = \sum_{(0,0) \neq (c,d) \in \mathbb{Z}^2} \varphi(c,d) \frac{1}{(cz + d)^{2k}} = \sum_{(c_o, d_o) \mod N} \varphi(c_o, d_o) \sum_{0 \neq (c,d) = (c_o, d_o) \mod N} \frac{1}{(cz + d)^{2k}} = \sum_{(c_o, d_o) \mod N} \varphi(c_o, d_o) \cdot \tilde{E}_{c_o, d_o}(z)
\]
[2.3] Fourier expansions of Eisenstein series  Description of Eisenstein series $\tilde{E}$ as sums with congruence conditions but without the coprimality condition, as just above, facilitates determination of Fourier expansions.

Break the sum expressing the weight $2k$ level $N$ Eisenstein series $\tilde{E}_c$ into subsums invariant under the translation $z \to z + N$ in $\Gamma(N)$:

$$\tilde{E}_c(z) = \sum_{0 \neq (c,d)} \frac{\varphi(c,d)}{(cz + d)^{2k}} = \sum_{0 \neq d} \frac{\varphi(0,d)}{d^{2k}} + \sum_{0 \neq c} \sum_{d \in \mathbb{Z}} \frac{\varphi(c,d)}{(cz + d)^{2k}} = \sum_{0 \neq d} \frac{\varphi(0,d)}{d^{2k}} + \sum_{0 \neq c} \frac{1}{c^{2k}} \sum_{d \in \mathbb{Z}} \frac{\varphi(c,d)}{(z + d)^{2k}}$$

The first of the latter two sums, being a constant, makes a contribution to the $0^{th}$ Fourier coefficient of $\tilde{E}_{c_0,d_0}$. As with the level one holomorphic Eisenstein series, we will see that the rest of the sum does not contribute to the $0^{th}$ Fourier coefficient, that is, we anticipate that

$$\tilde{E}_c(i\infty) = \sum_{0 \neq d} \frac{\varphi(0,d)}{d^{2k}}$$

For each $c \neq 0$, the inner sum over $d$ can be rewritten by letting $d = d_1 + Nc\ell$ with $d_1 \in \mathbb{Z}/Nc$. Since $\varphi(c,N\ell + d_1)$ does not depend on $\ell$,

$$\sum_{d \in \mathbb{Z}} \frac{\varphi(c,d)}{(z + d/c)^{2k}} = \sum_{d_1 \in \mathbb{Z}/Nc} \frac{\varphi(c,N\ell + d_1)}{(z + N\ell + d_1/c)^{2k}} = \sum_{d_1 \in \mathbb{Z}/Nc} \frac{1}{(z + N\ell + d_1/c)^{2k}}$$

The Fourier coefficients of the inner sum unwind:

$$\int_{0}^{1} e^{-2\pi inx/N} \sum_{\ell \in \mathbb{Z}} \frac{1}{(z + N\ell + d_1/c)^{2k}} dx = \int_{\mathbb{R}} e^{-2\pi inx/N} \frac{1}{(x + iy + d_1/c)^{2k}} dx$$

As for Eisenstein series for $SL_2(\mathbb{Z})$, this can be evaluated by residues, treating $x$ as a complex variable, replacing the integral along the real line by the limit of integrals $[-R,R]$ and then over a large arc in either upper or lower half-plane, as $n \leq 0$ or $n > 0$, respectively. The pole at $x = -(iy + d_1/c)$ is in the lower half-plane, so for $n \leq 0$ this is 0. For $n > 0$, because the curve is traced clockwise, it is

$$-2\pi i \text{Res}_{x=-(iy+d_1/c)} e^{-2\pi inx/N} \frac{1}{(x + iy + d_1/c)^{2k}} = \frac{1}{(2k-1)!} \left( \frac{\partial}{\partial x} \right)^{2k-1} e^{-2\pi inx/N} \bigg|_{x=-(iy+d_1/c)}$$

$$= \frac{1}{(2k-1)!} (-2\pi in/N)^{2k-1} \cdot e^{-2\pi i \frac{n}{N}} (-iy + d_1/c) \left( \frac{2\pi i}{2k-1} (n/N)^{2k-1} \cdot e^{-2\pi i \frac{n}{N}} y \cdot e^{2\pi i \frac{n}{N}} \right)$$

The exponential in $y$ is as expected. In the sum

$$\sum_{d_1 \in \mathbb{Z}/Nc} \varphi(c,d_1) e^{2\pi i \frac{n}{N} \frac{d_1}{c}}$$

the coefficient $\varphi(c,d_1)$ is unchanged under $d_1 \to d_1 + N$, and the whole sum is stable under this change of variables, so $[1]$

$$\sum_{d_1 \in \mathbb{Z}/Nc} \varphi(c,d_1) e^{2\pi i \frac{n}{N} \frac{d_1}{c}} = \sum_{d_1 \in \mathbb{Z}/Nc} \varphi(c,d_1) e^{2\pi i \frac{n}{N} \frac{d_1 + N}{c}} = e^{2\pi i \frac{n}{N}} \sum_{d_1 \in \mathbb{Z}/Nc} \varphi(c,d_1) e^{2\pi i \frac{n}{N} \frac{d_1}{c}}$$

[1] This part of the computation is a reproof of an instance of the cancellation lemma.
Thus, the sum over $d_1$ is 0 unless $c|n$, and in the latter case
\[
\sum_{d_1 \in \mathbb{Z}/cN} \varphi(c, d_1) e^{2\pi i \frac{n}{N} d_1} = |c| \sum_{d_1 \in \mathbb{Z}/N} \varphi(c, d_1) e^{2\pi i \frac{n}{N} d_1}
\] (when $c|n$)

Thus, for $n > 0$, using the bijection $c \rightarrow n/c$ on divisors of $n$,
\[
\int_0^1 e^{-2\pi inx/N} \tilde{E}_\varphi(x + iy) \, dx = \frac{(2\pi i)^{2k}}{(2k-1)! N^{2k-1}} e^{-2\pi ny/N} \sum_{0 \neq c|n} |c| \sum_{d_1 \in \mathbb{Z}/N} \varphi \left( \frac{n}{c}, d_1 \right) e^{2\pi i \frac{n}{N} \frac{d_1}{c}}
\]

Since the total measure of $[0, N]$ is $N$, not 1, divide by one further power of $N$ in the $n > 0$ terms to correctly express the Fourier expansion in $x$, obtaining
\[
\tilde{E}_\varphi(x + iy) = \sum_{0 \neq d} \varphi(0, d) \frac{d}{d^{2k}} + \frac{(2\pi i)^{2k}}{(2k-1)! N^{2k}} \sum_{n > 0} \left( \sum_{0 \neq c|n} |c|^{2k-1} \sum_{d_1 \in \mathbb{Z}/N} \varphi \left( \frac{n}{c}, d_1 \right) e^{2\pi i \frac{n}{N} \frac{d_1}{c}} \right) e^{2\pi inz/N}
\]

[2.4] Back to Eisenstein series for $\Gamma_\theta$ Recall the observation
\[
\tilde{E}_{\varphi} g = \tilde{E}_{\varphi \circ g}
\]
and the element
\[
g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : i \infty \rightarrow 1
\]

From the previous computation, to make a $\Gamma_\theta$ Eisenstein series non-zero at $i \infty$ we want $\varphi(c, d)$ defined mod 2 such that $\varphi \circ w = \varphi$ (so that $\tilde{E}_{\varphi} \mid_{2k} w = \tilde{E}_{\varphi}$ with $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma_\theta$)

and
\[
\tilde{E}_{\varphi}(i \infty) = \sum_d \varphi(0, d) \frac{d}{d^{2k}} \neq 0
\]

and
\[
\tilde{E}_{\varphi \circ g}(i \infty) = \sum_{0 \neq d} \varphi((0, d) g^{-1}) \frac{d^{2k}}{d^{2k}} = 0
\]

The space of functions on $(\mathbb{Z}/2)^2$ meeting the symmetry condition $\varphi \circ w = \varphi$ is three-dimensional space, spanned by

$\varphi_1(c, d) = \begin{cases} 1 & \text{(for } (c, d) = (1, 1) \text{ mod 2)} \\ 0 & \text{(otherwise)} \end{cases}$

$\varphi_0(c, d) = \begin{cases} 1 & \text{(for } (c, d) = (0, 0) \text{ mod 2)} \\ 0 & \text{(otherwise)} \end{cases}$

and

$\varphi_2(c, d) = \begin{cases} 1 & \text{(for } (c, d) = (0, 1) \text{ or } (1, 0) \text{ mod 2)} \\ 0 & \text{(otherwise)} \end{cases}$
The data $\phi_0$ gives an Eisenstein series $\tilde{E}$ with non-zero value at $i\infty$, and is not changed by composition with $g^{-1}$ since $(0,0)$ is stable, so gives a non-zero value at 1, as well.

The data $\phi_1$ has the feature that $\phi_1(0,d) = 0$, so gives an Eisenstein series $\tilde{E}$ with value 0 at $i\infty$. Composition with $g^{-1}$ is understood by mapping $(1,1)$ under $g$, mod 2:

$$(1 \ 1) \cdot g = (1 \ 1) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} egin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (1 \ 0) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (0 \ 1) \pmod{2}$$

Thus, the Eisenstein series $\tilde{E}_{\phi_1}$ has value at 1, in an appropriate sense, given by

$$(\text{suitable sense of value of } \tilde{E}_{\phi_1} \text{ at 1}) = \tilde{E}_{\phi_1}(i\infty) = \tilde{E}_{0,1}(i\infty) = \sum_{d=1 \pmod{2}} \frac{1}{d^{2k}} \neq 0$$

The value at $i\infty$ of $\tilde{E}_{\phi_2}$ is

$$\tilde{E}_{\phi_2}(i\infty) = \sum_{d=1 \pmod{2}} \frac{1}{d^{2k}} \neq 0$$

To determine the suitable sense of the value of $\tilde{E}_{\phi_2}$ at 1, first observe

$$(0 \ 1) \cdot g = (0 \ 1) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} egin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (0 \ 1) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (1 \ 0) \pmod{2}$$

and

$$(1 \ 0) \cdot g = (1 \ 0) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} egin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (1 \ 1) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (1 \ 1) \pmod{2}$$

Thus,

$$(\text{suitable sense of value of } \tilde{E}_{\phi_2} \text{ at 1}) = \tilde{E}_{\phi_2}(i\infty) = \tilde{E}_{1,0}(i\infty) + \tilde{E}_{1,1}(i\infty) = 0$$

In summary, up to normalizing constants, $\tilde{E}_{\phi_1}$ is the Eisenstein series attached to 1, and $\tilde{E}_{\phi_2}$ is the Eisenstein series attached to $i\infty$. In both the Fourier expansion of $E_{2k}^{(i\infty)}$ at $i\infty$ and in the Fourier expansion of $E_{2k}^{(1)}$ at 1, the leading non-zero constant is

$$\sum_{d=1 \pmod{2}} \frac{1}{d^{2k}} = 2 \sum_{d \geq 1, \ d=1 \pmod{2}} \frac{1}{d^{2k}} = 2 \cdot \zeta(2k) \cdot (1 - 2^{-2k})$$

Dividing through by this constant to create values 1 at the corresponding cusps,

$$E_{2k}^{(i\infty)}(z) = 1 + \frac{(2\pi i)^{2k}}{(2k)! \zeta(2k)(1 - 2^{-2k})} \sum_{n > 0} \left( \sum_{0 \neq c | n} |c|^{2k-1} \sum_{d_1 \in \mathbb{Z}/2} \varphi_2 \left( \frac{n}{c}, d_1 \right) e^{2\pi i \frac{d_1}{c}} \right) e^{2\pi i nz/2}$$

$$E_{2k}^{(1)}(z) = \frac{(2\pi i)^{2k}}{(2k)! \zeta(2k)(2k - 1)} \sum_{n > 0} \left( \sum_{0 \neq c | n} |c|^{2k-1} \sum_{d_1 \in \mathbb{Z}/2} \varphi_1 \left( \frac{n}{c}, d_1 \right) e^{2\pi i \frac{d_1}{c}} \right) e^{2\pi i nz/2}$$

These admit minor simplification. In both cases, changing the sign of $c$ does not affect the inner sum, so the 2 in the denominators outside can be dropped while summing over $0 < c | n$. In the case of $\varphi_1$, since $\varphi_1(\frac{n}{c}, d) \neq 0$ only when both $\frac{n}{c}, d$ are odd, the inner sum over $d_1$ gives $(-1)^c$, so

$$E_{2k}^{(1)}(z) = \frac{(2\pi i)^{2k}}{(2k - 1)! \zeta(2k)(2k - 1)} \sum_{n > 0} \left( \sum_{0 < c | n, \ c \neq \frac{1}{2} \ \text{odd}} e^{2k-1 \cdot (-1)^c} \right) e^{2\pi i n z} \quad (\text{for } \Gamma_0)$$
For non-vanishing of $\varphi_2(\frac{c}{d}, d_1)$, either $\frac{c}{d}$ is odd and $d$ is even, or vice-versa. For $\frac{c}{d}$ odd and $d_1$ even, the exponential is 1 for all $c$. For $\frac{c}{d}$ even and $d_1$ odd, the exponential is $e^{\pi ic} = (-1)^c$. A formulaic interpolation of the situation is

$$\sum_{d_1 \in \mathbb{Z}/2} \varphi_2\left(\frac{n}{c}, d_1\right) e^{2\pi i \frac{c}{d_1}} = (-1)^{(1+\frac{c}{d})c} = (-1)^{c+n} = (-1)^n \cdot (-1)^c$$

giving

$$E_{2k}^{(i\infty)}(z) = 1 + \frac{(2\pi)^{2k}}{(2k-1)! \zeta(2k)(2^{2k}-1)} \sum_{n>0} (-1)^n \left( \sum_{0 < c | n} c^{2k-1} \cdot (-1)^c \right) e^{\pi iz} \quad \text{(for $\Gamma_0$)}$$

[2.5] Remark: The details of the outcomes of the previous computations are less important than the techniques for doing the computations.

[2.6] Corollary: For a holomorphic modular form $f$ of weight $2k \geq 4$ for $\Gamma_0$, with $g \in SL_2(\mathbb{Z})$ such that $g(i\infty) = 1$,

$$f - f(i\infty) \cdot E_{2k}^{(i\infty)} - f|_{2k} g(i\infty) \cdot E_{2k}^{(1)}$$

is a cuspform of weight $2k$.

Proof: The restriction $2k \geq 4$ is for convergence of the Eisenstein series. The Eisenstein series are normalized to have (in a suitable sense) values 1 at their associated cusp and 0 (in a suitable sense) at the other cusp. In that sense, the evaluations of $f$ and $f|_{2k} g$ at $i\infty$ are correct, as above. \///

3. Divisor formula for $\Gamma_0$

The divisor formula for weight $2k$ holomorphic modular forms $f$ for $SL_2(\mathbb{Z})$ was

$$\frac{\nu_f(i)}{2} + \frac{\nu_f(\rho)}{3} + \nu_f(i\infty) + \sum_{\text{other } z} \nu_f(z) = \frac{2k}{12} \quad \text{(for $SL_2(\mathbb{Z})$)}$$

with $\nu_f(z)$ the order of vanishing of $f$ at $z$. This gave very strong constraints on spaces of level-one holomorphic modular forms of weight $2k$, in particular proving finite-dimensionality of each such space, an analogous result for $\Gamma_0$ is useful, although somewhat less decisively.

For a not-identically-zero holomorphic modular form $f$ of weight $2k$ for $\Gamma_0$, the order of vanishing $\nu_f(c \infty)$ is the smallest $n_o$ such that $c_{n_o} \neq 0$ in the Fourier expansion

$$f(x + iy) = \sum_{n \geq 0} c_n e^{\pi inz}$$

and the order of vanishing $\nu_f(1)$ is the smallest $n_o$ such that $b_{n_o} \neq 0$ in the Fourier expansion

$$f|_{2k}(x + iy) = \sum_{n \geq 0} b_n e^{2\pi inz}$$

The divisor formula is

\[2\] For that matter, these techniques can be further improved by re-expressing Eisenstein series as functions on *adele groups* $GL_2(\mathbb{A})$, completely decoupling the archimedean and the various finite-prime parts of the computation.
[3.1] **Theorem:** For a not-identically-zero holomorphic modular form $f$ of weight $2k$ for $\Gamma_0$,

$$\frac{\nu_f(i)}{2} + \nu_f(i\infty) + \nu_f(1) + \sum_{\text{other } z} \nu_f(z) = \frac{2k}{4}$$

where the sum over other $z$ is over mutually $\Gamma_0$-inequivalent points in $\mathcal{H}$ not $\Gamma_0$ equivalent to $i$.

**Proof:** As with $SL_2(\mathbb{Z})$, this follows from the argument principle, integrating the logarithmic derivative $f'/f$ around the boundary $\sigma$ of a truncated version of the fundamental domain $F = \{ |z| \geq 1, |x| \leq 1 \}$ for $\Gamma_0$, and evaluating that integral in another way using the automorphy relations $f(z + 2) = f(z)$ and $f(-1/z) = z^{2k} f(z)$. The argument principle gives essentially

$$\frac{1}{2\pi i} \int_{\sigma} \frac{f'(z)}{f(z)} \, dz = \text{(number of zeros inside } \sigma)$$

As for $SL_2(\mathbb{Z})$, there are some technicalities. First, points on the verticals $x = \pm 1$ can be accommodated by slightly indenting the path on $x = -1$ and correspondingly out-denting the path on $x = +1$, so that the modified path does not run right through any such 0. Similarly, any zeros on the arcs cutting off the cusps $i\infty$ and 1 can be dodged by moving the cut-off arc slightly. The point $i$ requires more delicacy, since it is the fixed-point of $z \to -1/z$, so cannot be dodged so simply, and half the residue is picked up.

On the other hand, the automorphy conditions give much cancellation in the integral, as for $SL_2(\mathbb{Z})$. By $f(z + 2) = f(z)$, certainly $f'(z + 2) = f'(z)$, and since the $x = -1$ and $x = +1$ paths are traced in opposite directions, those parts of the whole integral cancel each other completely. The circular arcs from $-1$ to $i$ and then $i$ to $+1$ are mapped to each other by $z \to -1/z$, and directions are reversed, so we expect considerable cancellation. However, $f$ and $f'$ are not quite invariant: $f(-1/z) = z^{2k} \cdot f(z)$ gives

$$f'(-1/z) \frac{1}{z^2} = 2kz^{2k-1}f(z) + z^{2k} f'(z)$$

so

$$\frac{f'(-1/z)}{f(-1/z)} \, d(-1/z) = z^2 \cdot \frac{2kz^{2k-1}f(z) + z^{2k} f'(z)}{z^{2k} f(z)} \, dz \frac{dz}{z^2} = \left(2kz^{-1} + \frac{f'(z)}{f(z)}\right) \, dz$$

Thus, the sum of these two are integrals almost cancels, leaving

$$-\frac{1}{2\pi i} \int_0^{\pi/2} 2k(e^{\pi i - it})^{-1} \, d(e^{\pi i - it}) = -\frac{1}{2\pi i} 2k \int_0^{\pi/2} (e^{\pi i - it})^{-1} (-i) e^{\pi i - it} \, dt$$

$$= 2k \cdot \frac{\pi/2}{2\pi} = \frac{2k}{4}$$

The cusps are treated as for $SL_2(\mathbb{Z})$. At $i\infty$ for $\Gamma_0$, the arc cutting off $i\infty$ at some height $T$ captures the negatives of the orders of the zeros above that height, and the negative of $\nu_f(i\infty)$. Similarly at the cusp 1. Thus, referring only to $z$ in the fundamental domain,

$$\nu_f(i) + \sum_{\text{z inside path}} \nu_f(z) = \frac{2k}{4} - \nu_f(i\infty) - \nu_f(1) - \sum_{\text{z outside path}} \nu_f(z)$$

which rearranges to the expected relation.

For $\Gamma_0$ and holomorphic modular forms:

[3.2] **Corollary:** The modular forms of weight 0 are constants. There are no cusps of weights 4 or 6. Up to constant multiples, there is a unique cuspform of weight 8, and this cuspform vanishes to first order at both cusps $i\infty$ and 1, and does not vanish on $\mathcal{H}$. The weight 2 modular forms are multiples of $E_6(i\infty)/E_4(i\infty)$, and also multiples of $E_6(1)/E_4(1)$. For every weight $2k$ the space of holomorphic modular forms is finite-dimensional.
Proof: From the divisor formula, a weight 0 modular form $f$ cannot vanish unless it vanishes identically, so $f - f(z_0)$ is identically 0, for any $z_0 \in \mathcal{H}$.

Since $2k/4 < 2$ for $2k = 4, 6$, and since a cuspform vanishes to order at least 1 at both cusps $i\infty$ and 1, there can be no cuspforms of weights 4 or 6.

Similarly, at weight $2k = 8$, we have $2k/4 = 2$, so the vanishing of a cuspform at the two cusps, would leave no room for any other vanishing. For existence, the product $f$ of the two weight 4 Eisenstein series $E_4^{(i\infty)}$ and $E_4^{(1)}$ vanishes at both cusps, and is not identically 0. Thus, given a cuspform $F$ of weight $2k \geq 8$, the quotient $F/f$ is a modular form of weight $2k - 8$.

The general finite-dimensionality follows essentially by induction. Given a holomorphic modular form $F$ of weight $2k \geq 8$, by subtracting multiples of the two Eisenstein series, without loss of generality $F/k$ of weight 2 modular form for $\Gamma_0$. Divide by the unique weight 8 cuspform so that $F/f$ is of weight 2k – 8. Thus, it suffices to prove finite-dimensionality for weights 0, 2, 4, 6, already accomplished for weights 0, 4, 6. The space of weight 2 modular forms $F$ is mapped linearly to weight 6 modular forms by $F \to F \cdot E_4^{(i\infty)}$. Since $E_4^{(i\infty)}$ vanishes at the cusp 1, and $F$ vanishes at $i$, these are the only zeros of this product. The Eisenstein series $E_6^{(i\infty)}$ has the same vanishing, so

$$\text{weight 2 modular form for } \Gamma_0 = \text{(multiple of)} \frac{E_6^{(i\infty)}}{E_4^{(i\infty)}}$$

A similar argument applies with $E_6^{(1)}/E_4^{(1)}$.

4. Theta series and Poisson summation

The basic harmonic theta series related to sums of $n$ squares is

$$\theta_n(z) = \sum_{v \in \mathbb{Z}} e^{\pi i |v|^2 z} = \left( \sum_{\ell \in \mathbb{Z}} e^{\pi i \ell^2 z} \right)^n$$

For odd $n$ this has more complicated behavior than for $n$ even. The behavior is clearest for $n$ divisible by 8, for reasons visible in the computation below, and we soon specialize to that case.

[4.1] Poisson summation, and inversion $z \to -1/z$ Fourier transform behaves well with respect to dilation: for $y > 0$, letting $(F \circ y)(x) = F(yx)$, a direct computation gives

$$(F \circ y)^\wedge(\xi) = \int_{\mathbb{R}^n} e^{-2\pi i \xi \cdot x} F(yx) \, dx = \int_{\mathbb{R}^n} e^{-2\pi i \xi \cdot \frac{x}{y}} F(x) \, y^{-8n} \, dx$$

$$= y^{-n} \int_{\mathbb{R}^n} e^{-2\pi i \xi \cdot \frac{x}{y}} F(x) \, dx = y^{-n} \left( \hat{F} \circ \frac{1}{y} \right)(\xi)$$

With $y$ replaced by $\sqrt{y}$, invoking Poisson summation

$$\sum_{v \in \mathbb{Z}^n} \varphi(v) = \sum_{v \in \mathbb{Z}^n} \hat{\varphi}(v)$$

compute

$$\theta_n(iy) = \sum_{v \in \mathbb{Z}^n} e^{-\pi |v|^2 y} = \frac{1}{\sqrt{y^n}} \sum_{v \in \mathbb{Z}^n} e^{-\pi |v|/\sqrt{y}^2} = \frac{1}{\sqrt{y^n}} \cdot \sum_{v \in \mathbb{Z}^n} e^{-\pi |v|/\sqrt{y}^2}$$

$$= \frac{1}{(iy)^n} \sum_{v \in \mathbb{Z}^n} e^{-\pi |v|^2 / y} = \frac{1}{(iy)^n} \cdot \theta_n(-1/iy)$$
[4.2] **Remark:** The complication of odd $n$ is visible, namely, choosing a branch of square root. This is an *essential* complication, as it turns out that half-integral weight modular forms have very different behavior from integral-weight.

Thus, to avoid the half-integral weight complication, and to avoid a few further comparatively minor complications, replace $n$ by $8n$. By the identity principle, from the corresponding identity for $y > 0$, $$\theta_n(z) = \frac{1}{z^{4n}} \cdot \theta_n(-1/z)$$

This is the main issue in proving that $\theta_n(z)$ is a weight $4n$ modular form for $\Gamma_0$. The lengths-squared $|v|^2$ are all integers, so the exponentials $e^{\pi i |v|^2 z}$ are all invariant under the translation $z \to z + 2$. We showed that inversion and this translation generate $\Gamma_0$.

[4.3] **Behavior at cusp $i\infty$** Above, we showed that $\theta_f(z)$ is bounded as $y \to +\infty$. The defining expression for $\theta$ shows that its Fourier expansion at the cusp $i\infty$ has no negative-index coefficients.

[4.4] **The other cusp** 1 Checking the behavior of $\theta_n$ at the cusp 1 requires verifying that $(\theta_n|_{4n} g)(z)$ is bounded as $z \to +i\infty$, for $g \in SL_2(\mathbb{Z})$ such that $g(i\infty) = 1$.

That is, the question is not simply about the values of $\theta_f(z)$ as $z$ goes to 1 inside the fundamental domain, but about $\theta_f(z)$ altered by the weight $4n$ action.

With $$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and noting the associativity

$$(\theta_n|_{4n} g) = \left( \theta_n|_{4n} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)|_{4n} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

first compute

$$(\theta_n|_{4n} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})(z) = \sum_v e^{\pi i |v|^2 (z+1)} = \sum_v e^{\pi i |v|^2} e^{\pi i |v|^2 z} = \sum_v (-1)^{|v|^2} e^{\pi i |v|^2 z}$$

That is, the summands are twisted by powers of $-1$, complicating application of Poisson summation to achieve the further effect of inversion $z \to -1/z$. Rewrite the sum as a sum over translates of lattices on each of which $e^{\pi i |v|^2} = (-1)^{|v|^2}$ is constant: replace $v$ by $w + 2v$ with $v \in \mathbb{Z}^n$ and $w \in \mathbb{Z}^n \text{mod} \ 2$:

$$|w + 2v|^2 = |w|^2 + 2(w, 2v) + 4|v|^2 \in |w|^2 + 2\mathbb{Z}$$

so

$$\theta_n(z + 1) = \sum_v e^{\pi i |v|^2} e^{\pi i |v|^2 z} = \sum_{w \in \mathbb{Z}^n/2} \sum_{v \in \mathbb{Z}^n} e^{\pi i |2v + w|^2 z}$$

For each $w$, we will apply Poisson summation to the corresponding inner sum. Recall the behavior of Fourier transform on $\mathbb{R}^m$ under affine transformations $x \to ax + b$: by direct computation,

$$F(ax + b) \hat{e}^\xi(x) = \int_{\mathbb{R}^m} e^{-2\pi i \xi(x)} F(ax + b) \, dx = \frac{1}{|a|^m} \int_{\mathbb{R}^m} e^{-2\pi i \xi(x)} F(x) \, dx$$

$$= \frac{1}{|a|^m} \int_{\mathbb{R}^m} e^{-2\pi i \xi_0(x)} F(x) \, dx = \frac{1}{|a|^m} \int_{\mathbb{R}^m} e^{-2\pi i \xi_0(x-b)} F(x) \, dx$$

$$= \frac{1}{|a|^m} e^{2\pi i \xi_0(x)} \int_{\mathbb{R}^m} e^{-2\pi i \xi_0(x)} F(x) \, dx = \frac{1}{|a|^m} e^{2\pi i \xi_0} \cdot \hat{F}(\frac{\xi}{a})$$

12
Remark: It is certainly not obvious from the original expression for $\theta_n$ that the theta series vanishes (in a suitable sense) at cusp 1.

5. Sums of squares

With $v_{8n}(N)$ the number of ways to express $N$ as a sum of $8n$ squares of integers,

$$\theta_{8n}(z) = \sum_{v \in \mathbb{Z}^{8n}} e^{\pi i |v|^2 z} = \sum_{0 \leq N} v_{8n}(N) e^{\pi i N z}$$

This is a weight 4n holomorphic modular form for $\Gamma_0$, and the previous section shows that it vanishes at the cusp 1. The value of $\theta_{8n}(z)$ at the cusp $i\infty$ is the 0th Fourier coefficient, namely, 1.
[5.1] Eight squares  The divisor formula showed that there are no cuspforms of weight 4 for \( \Gamma_0 \). Thus, \( \theta_{\infty}(z) \) is the Eisenstein series \( E_4^{(\infty)}(z) \) normalized so as to take value 1 at cusp \( i\infty \) and 0 at cusp 1. Thus,

\[
\nu_8(N) = \text{N}^{\text{th}} \text{ Fourier coefficient of } E_4^{(\infty)} = \frac{(2\pi i)^4}{3! \xi(4)(2^4 - 1)} (-1)^N \sum_{0 < c \mid N} c^3 \cdot (-1)^c
\]

\[
= \frac{16\pi^4}{6 \cdot 90 \cdot 15} (-1)^N \sum_{0 < c \mid N} c^3 \cdot (-1)^c = 16 \cdot (-1)^N \sum_{0 < c \mid N} c^3 \cdot (-1)^c
\]

In fact, the value of the constant \( \frac{(2\pi i)^4}{3! \xi(4)(2^4 - 1)} \) could be determined by evaluating \( \nu_8(1) \).

[5.2] 8n squares  For \( 8n > 8 \), the weight 4\( n \) is above the range where there are no cuspforms for \( \Gamma_0 \), so in general we invoke Hecke’s estimate on Fourier coefficients of cuspforms, and can only say

\[
\nu_{8n}(N) = \text{N}^{\text{th}} \text{ Fourier coefficient of } (E_{4n}^{(\infty)} + \text{cuspform of weight } 4n)
\]

\[
= \frac{(2\pi i)^{4n}}{(4n - 1)! \xi(4n)(2^{4n} - 1)} (-1)^N \left( \sum_{0 < c \mid N} c^{4n-1} \cdot (-1)^c \right) + O(N^{2\pi})
\]

[5.3] Corollary:  For every 8\( n \geq 8 \), there is a constant \( C_n > 0 \), such that every sufficiently large \( N \geq 1 \) can be represented in at least \( C_n \cdot N^{4n-1} \) ways as a sum of 8\( n \) squares.

Proof:  The signed sum of powers of divisors function is weakly multiplicative, so it suffices to give a lower bound for prime powers \( p^n \): first, for odd prime \( p \),

\[
(-1)^p \sum_{0 < c \mid p^n} c^{4n-1} \cdot (-1)^c = (p^c)^{4n-1} - (p^{c-1})^{4n-1} + ... + (-1)^p \geq (p^c)^{4n-1} \cdot \left( \frac{1}{1 + p^{-4n-1}} \right)
\]

For \( p = 2 \),

\[
(-1)^{2^r} \sum_{0 < c \mid 2^p} c^{4n-1} \cdot (-1)^c = (2^c)^{4n-1} + (2^{c-1})^{4n-1} + ... + 1 \geq (2^c)^{4n-1} \cdot \left( \frac{1}{1 + 2^{-4n-1}} \right) \geq (2^c)^{4n-1} \cdot \left( \frac{1}{1 + p^{-4n-1}} \right)
\]

The product of \( 1/(1 + p^{-4n-1}) \) over all primes is convergent to a finite non-zero constant \( B_n \). Thus,

\[
(-1)^N \left( \sum_{0 < c \mid N} c^{4n-1} \cdot (-1)^c \right) \geq B_n \cdot N^{4n-1}
\]

Further adjustment by the leading constant does not alter the qualitative conclusion.  //

[5.4] Corollary:  A prime \( p > 2 \) can be written as a sum of 8 squares in \( 16(p^3 + 1) \) ways.  //

6. Appendix: fundamental domain and generators for \( \Gamma_0 \)

[6.1] Fundamental domain for \( \Gamma_0 \) and \( \Gamma(2) \)

The determination of the standard fundamental domain \( F \) for \( \Gamma(1) = SL_2(\mathbb{Z}) \) allows explicit determination of fundamental domains for finite-index subgroups such as the principal congruence subgroups

\[
\Gamma(N) = \{(a \ b \ c \ d) \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}
\]
by choosing coset representatives $\gamma_i$ for $\Gamma(N)$ in $\Gamma(1)$, and then\[3\]

\[
\text{fundamental domain for } \Gamma(N) = \bigcup_i \gamma_i F
\]

It is useful that $\Gamma(N)$ is exactly the kernel of the group homomorphism

\[
\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N) \quad \text{by} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a \mod N & b \mod N \\ c \mod N & d \mod N \end{pmatrix}
\]

so is \textit{normal} in $\Gamma(1)$.

Analytical methods in sums-of-squares problems use the important special choice

\[
\Gamma_\theta = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ mod } 2 \text{ or } \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ mod } 2 \} = \Gamma(2) \cup \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \Gamma(2)
\]

the coset-representative-oriented choice of fundamental domain can be adjusted to prove the corollary that $\Gamma_\theta$ is generated by $z \to -1/z$ and $z \to z + 2$, as below.

[6.2] \textbf{Remark:} The following assertion holds without assuming $p$ is prime, but all we need at the moment is $p = 2$, in any case. Further, the surjectivity of $\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/2)$ is easy to observe directly, since, for example, the elements

\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}
\]

surject to $\text{SL}_2(\mathbb{Z}/2)$.

[6.3] \textbf{Claim:} For $p$ prime, the natural map

\[
\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/p)
\]

\textit{is surjective}

\textbf{Proof:} Let $q$ be the quotient map $\mathbb{Z} \to \mathbb{Z}/p$. First, given $u, v$ not both 0 in $\mathbb{Z}/p$, we will find relatively prime $c, d$ in $\text{SL}_2(\mathbb{Z})$ such that $qc = u$ and $qd = v$.

For $v \notin p\mathbb{Z}$, there is $0 \neq d \in R$ such that $qd = v$. Consider the conditions on $c \in R$

\[
c = u \mod p \quad \text{and} \quad c = 1 \mod d
\]

As $d \notin p\mathbb{Z}$, by the maximality of the ideal $p\mathbb{Z}$ there are $x \in \mathbb{Z}$ and $pm \in p\mathbb{Z}$ such that $xd + pm = 1$. Let $c = xdu + pm$. From $xd + pm = 1$, $xd = 1 \mod pm$ and $pm = 1 \mod d$, so this expression for $c$ satisfies the two congruences conditions. In particular, $qc = u$, and since $c = 1 \mod d$ it must be that $\gcd(c, d) = 1$.

For $v = 0$ in $\mathbb{Z}/p$, necessarily $u \neq 0$, and we reverse the roles of $c, d$ in the previous paragraph.

---

[3] Since $\mathcal{F} = \bigcup_{\gamma \in \Gamma(1)} \gamma F$, for representatives $\gamma_i$ with $\Gamma(1) = \bigcup_i \Gamma(N) \gamma_i$,

\[
\mathcal{F} = \bigcup_{\gamma \in \Gamma(1)} \gamma F = \bigcup_{\gamma \in \bigcup_i \Gamma(N) \gamma_i} \gamma F = \bigcup_{\gamma \in \Gamma(N)} \bigcup_i \gamma_i F = \bigcup_{\gamma \in \Gamma(N)} \gamma \left( \bigcup_i \gamma_i F \right)
\]
Thus, there are coprime \(c, d\) in \(\mathbb{Z}\) whose images mod \(p\) are \(u, v\). For integers \(s, t\) there exist \(a, b\) such that \(\gcd(s, t) = as - bt\). The coprimality of \(c, d\) implies that there are \(a, b\) in \(R\) such that \(ad - bc = 1\). That is, \(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\), and
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ u & v \end{pmatrix} \pmod{p}
\]

Further adjustment to accommodate the upper row is more straightforward: Given \(\begin{pmatrix} r & s \\ u & v \end{pmatrix}\) in \(SL_2(\mathbb{Z}/p)\), and letting \(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\) also denote its image in \(SL_2(\mathbb{Z}/p)\),
\[
\begin{pmatrix} r & s \\ u & v \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \begin{pmatrix} v & -b \\ -u & a \end{pmatrix} = \begin{pmatrix} rv - su & * \\ uv - vu & * \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}
\]

The right-hand side is in \(SL_2(\mathbb{Z}/p)\), so, in fact, it must be of the form \(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\), and
\[
\begin{pmatrix} r & s \\ u & v \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p}
\]

So
\[
\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \pmod{p}
\]
giving the surjectivity. 

\[6.4\] **Claim:** \(\#SL_2(\mathbb{Z}/p) = (p^2 - 1)p\) for prime \(p\).

**Proof:** First, count \(GL_2(\mathbb{Z}/p)\). This is the number of ordered bases for the vector space \((\mathbb{Z}/p)^2\) over \(\mathbb{Z}/p\), since an element of \(GL_2(\mathbb{Z}/p)\) sends one basis to another, is transitive on ordered bases, and \(g \in GL_2(\mathbb{Z}/p)\) fixes a basis \(v_1, v_2\) only for \(g = 1_2\).

The first basis element \(v_1\) can be any non-zero vector in \((\mathbb{Z}/p)^2\), giving \(p^2 - 1\) choices. For each such choice, the second basis element can be anything not on the \(\mathbb{Z}/p\)-line spanned by \(v_1\), giving \(p^2 - p\) choices. Thus, \(\#GL_2(\mathbb{Z}/p) = (p^2 - 1)(p^2 - p)\).

The determinant map surjects \(GL_2(\mathbb{Z}/p) \to (\mathbb{Z}/p)\times\), and has kernel \(SL_2(\mathbb{Z})\), so the index of \(SL_2(\mathbb{Z}/p)\) is \(\#(\mathbb{Z}/p)\times = p - 1\), and the cardinality is as claimed.

\[6.5\] **Corollary:** \(\Gamma(2)\) has six coset representatives in \(\Gamma(1)\):
\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}
\]

**Proof:** The index is \((2^2 - 1)2 = 6\). The six listed matrices are in \(SL_2(\mathbb{Z})\) and are distinct mod 2.

\[6.6\] **Corollary:** \(\Gamma_0\) has three coset representatives in \(\Gamma(1)\):
\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}
\]

**Proof:** The index is 3, since \(\Gamma_0\) is index 2 above \(\Gamma(2)\). The three listed matrices are in \(SL_2(\mathbb{Z})\) and are not only distinct mod 2 but also do not differ mod \(\Gamma(2)\) merely by multiplication by \(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\).
[6.7] Corollary: A fundamental domain for $\Gamma_\theta$ is
\[ F_\theta = \{ z \in \mathbb{H} : |z| \geq 1 \text{ and } |\text{Re}(z)| \leq 1 \} \]

Proof: With standard fundamental domain
\[ F = \{ z \in \mathbb{H} : |z| \geq 1 \text{ and } |\text{Re}(z)| \leq \frac{1}{2} \} \]
for $\Gamma(1)$, the coset representatives for $\Gamma_\theta$ in $\Gamma(1)$ give a fundamental domain
\[ F' = F \cup \left( \frac{1}{0} \frac{1}{1} \right) F \cup \left( \frac{1}{1} \frac{0}{1} \right) F \]
for $\Gamma_\theta$. [... iou ...] pictures! We will symmetrize this into a more easily-describable form. With hindsight, we replace
\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}
\]
by
\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\]
The point is that \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} F \) is understandable as a translate of the inverted $F$.

Move the right half of \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} F \cup \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} F \) left by $z \to z - 2$, so that the two halves are symmetric about the imaginary axis. This produces the region claimed in the theorem. ///

[6.8] Generators for $\Gamma_\theta$

[6.9] Corollary: Inversion $z \to -1/z$ and translation $z \to z + 2$ generate $\Gamma_\theta$.

Proof: Given $z \in \mathbb{H}$, translate $z$ by $2\mathbb{Z}$ to $|\text{Re}(z)| \leq 1$. If $|z| \geq 1$, stop. If not, invert, and then translate back to $|\text{Re}(z)| \leq 1$. This produces a sequence of points $z_1, z_2, \ldots$ with
\[ \text{Im}(z_1) < \text{Im}(z_2) < \ldots \]
As earlier, $\text{Im}(z_n)$ is of the form $\text{Im}(z) / |cz + d|^2$, and any such sequence must be finite. That is, inversion and translation by $1\mathbb{Z}$ eventually put $z$ into the fundamental domain for $\Gamma_\theta$.

Given $\gamma \in \Gamma_\theta$, choose $z$ in the interior of the fundamental region, and let $\delta$ be a composition of inversions and translations by $2\mathbb{Z}$ so that $\delta^{-1} \gamma z$ is back in the fundamental domain. Then $\delta^{-1} \gamma = \pm 1_2$, so $\gamma = \pm \delta$. Since the inversion squares to $-1_2$, $\gamma \in \Gamma_\theta$. ///