Counting Representations of a Number as Sums of 4 Squares

Lagrange proved in 1770 that every natural number can be expressed as a sum of four squares, which naturally begs the enumerative question. Define the following function for counting ways to express $n \geq 0$ as a sum of $k \geq 0$ squares:

$$r(n,k) := \#\{(m_1, \ldots, m_k) \in \mathbb{Z}^k : n = m_1^2 + \cdots + m_k^2\}.$$

This note presents a scenic development of some of the basic theory of modular forms on subgroups of $\mathrm{SL}_2(\mathbb{Z})$, with the aim of proving the following formula.

For every $n \geq 1$ we have

$$r(n,4) = 8 \sum_{\substack{0<d|n \\ 4\nmid d}} d.$$

Applications in both geometry and number theory require the relaxation of the modularity condition to certain finite-index subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 0.1. The *principal congruence subgroup of level* N, $\Gamma(N) \trianglelefteq \mathrm{SL}_2(\mathbb{Z})$, is the kernel of the entrywise reduction homomorphism

$$\pi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

We call a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ a *congruence subgroup of level* N if it contains $\Gamma(N)$.

There are two other classes of congruence subgroups we will need.

Definition 0.2. Let π be the same mod N reduction map as above. We define the *Hecke congruence subgroup* $\Gamma_0(N)$ as the preimage of the upper triangular matrices:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Similarly, define $\Gamma_1(N)$ as the preimage of the unipotent matrices:

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0,\ a, d \equiv 1 \pmod{N} \right\}.$$

We have a natural filtration

$$\Gamma(N) \trianglelefteq \Gamma_1(N) \trianglelefteq \Gamma_0(N).$$

We can naturally extend our definition of weak modularity to congruence subgroups.

Definition 0.3. For notational convenience, define the *weight k operator*

$$(f[\gamma]_k)(z) := (cz+d)^{-k} f(\gamma(z)).$$

A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is *weakly modular of weight k with respect to* Γ if

$$f[\gamma]_k = f$$

for all $\gamma \in \Gamma$.

Definition 0.4. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. A function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if

1. f is holomorphic,
2. f is weakly modular of weight k with respect to Γ, and
3. for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the function $f[\gamma]_k$ is holomorphic at infinity.

The third condition is the natural way to ask the function to be holomorphic at every point of $\mathbb{P}^1(\mathbb{Q})$, i.e. at all of the cusps. The weight k operator $[\gamma]_k$ should be thought of as performing a change of coordinates to move a specific boundary point to ∞, which we can then test for a holomorphic extension in the punctured disk.

Example 0.5 (Cusps of $\Gamma_0(2)$)**.** Recall that

$$\Gamma_0(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ c \equiv 0 \pmod 2 \right\}.$$

The group acts on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ by $\gamma \cdot z = \frac{az+b}{cz+d}$.

Since $\gamma(\infty) = a/c$ and c is even for $\gamma \in \Gamma_0(2)$, all rationals with even denominator (in lowest terms) lie in the same orbit as ∞.

If c is odd, no element of $\Gamma_0(2)$ can send ∞ to a/c, since $c \equiv 0 \pmod 2$ is required (SHOW DETERMINANT violates $2a/2c$ possibility). Thus rationals with odd denominator form a second orbit, represented for instance by 1.

Hence $\Gamma_0(2)$ has exactly two cusps, represented by

$$\infty \quad \text{and} \quad 1.$$

We consider now modifications of the conditionally convergent Eisenstein series G_2 which give weight 2 modular forms on the subgroup $\Gamma_0(N)$.

Proposition 0.6. For each positive integer N, define the modified Eisenstein series

$$G_{2,N}(z) := G_2(z) - NG_2(Nz).$$

Then $G_{2,N} \in M_2(\Gamma_0(N))$.

Proof Sketch. Remark on similarities from my from last seminar:

One works carefully with the conditionally convergent series for G_2 to check that the steps performed in our Fourier series derivation are valid. Then one checks that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

$$(G_2[\gamma]_2)(z) = G_2(z) - \frac{2\pi i c}{cz+d}.$$

□

With this in hand, we can prove weak modularity of $G_{2,N}$.

Then for any $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$, notice that

$$N\gamma(z) = \gamma'(Nz), \qquad \gamma' = \begin{pmatrix} a & Nb \\ c & d \end{pmatrix}.$$

(SKIP? to result) Applying this we can compute:

$$\begin{aligned}
(G_{2,N}[\gamma]_2)(z) &= (Ncz+d)^{-2}\big(G_2(\gamma(z)) - NG_2(N\gamma(z))\big) \\
&= G_2(z) - \frac{2\pi i c N}{cNz+d} - N\left((c(Nz)+d)^{-2}G_2(\gamma'(Nz))\right) \\
&= G_2(z) - \frac{2\pi i c N}{cNz+d} - N\left(G_2(Nz) - \frac{2\pi i c}{cNz+d}\right) \\
&= G_2(z) - NG_2(Nz).
\end{aligned}$$

So $G_{2,N}$ is weakly modular of weight k with respect to $\Gamma_0(N)$. They are holomorphic on $\mathbb{H}$ since G_2 is. That they are holomorphic at infinity will be a corollary of the previous proposition and the Fourier series we compute below, whose terms are bounded by

$$a_n \leq 8\pi^2\sigma(n) \leq 8\pi^2 n^2.$$

Proposition 0.7. The Fourier series for the modified Eisenstein polynomials $G_{2,2}$ and $G_{2,4}$ are given by

$$G_{2,2}(z) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n \\ 2\nmid d}} d\right)q^n\right), \qquad G_{2,4}(z) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n \\ 4\nmid d}} d\right)q^n\right).$$

Proof. Applying the Fourier series for G_2 gives (for $\sigma(n) = \sigma_1(n) = \sum_{d|n} d$) the expression

$$\begin{aligned}
G_{2,2}(z) &= 2\zeta(2) - 8\pi^2\sum_{n=1}^{\infty}\sigma(n)q^n - 2\left(2\zeta(2) - 8\pi^2\sum_{n=1}^{\infty}\sigma(n)q^{2n}\right) \\
&= -2\zeta(2) - 8\pi^2\sum_{\substack{n\geq 1 \\ n \text{ odd}}}\sigma(n)q^n - 8\pi^2\sum_{\substack{n\geq 1 \\ n \text{ even}}}\big(\sigma(n) - 2\sigma(n/2)\big)q^n.
\end{aligned}$$

But for even n, division by 2 induces a bijection between even divisors of n and all divisors of $n/2$, ' Hence

$$\sum_{\substack{d|n \\ 2\nmid d}} d = \sigma(n) - 2\sigma\left(\frac{n}{2}\right).$$

If n is odd, all divisors of n are odd, so

$$\sum_{\substack{d|n \\ 2\nmid d}} d = \sigma(n).$$

In summary,

$$\sum_{\substack{d|n \\ 2\nmid d}} d = \begin{cases} \sigma(n), & n \text{ odd}, \\ \sigma(n) - 2\sigma\left(\frac{n}{2}\right), & n \text{ even}. \end{cases}$$

so pulling out $-2\zeta(2) = -\frac{\pi^2}{3}$ gives the result. The case of $G_{2,4}$ is similar. □