

Tutorial : Sum of Four Squares

Zagier's proof that every integer is the sum of 4 perfect squares, is scattered in various parts of his first notes.

$$n = a^2 + b^2 + c^2 + d^2 \text{ for } n \geq 0$$

Here we try to present a different narrative. Number Theory and Modular forms are separate fields of Mathematics, advancing in their own way, but they have many things in common. It's hard to create Number Theory results, that use modular forms and still look elementary.

Step # 1 Observe the coefficients of $\theta(z)^4$ are the number of ways to express n as the sum of four squares:

$$\theta(z)^4 = \left[\sum_{n \in \mathbb{Z}} q^{n^2} \right]^4 = \sum_{n \geq 0} \# \left\{ (a, b, c, d) : a^2 + b^2 + c^2 + d^2 = n \right\} q^n \equiv \sum_{n \geq 0} r_4(n) q^n$$

This is a modular form of weight 2 on $\Gamma_0(4)$ which is generated by $z \mapsto z + 1$ and $z \mapsto -\frac{1}{4z}$. The full group $\text{SL}(2, \mathbb{Z})$ acts on several theta functions at once turning them into each other.

This action is closely related to Poisson summation. For $f \in \mathcal{S}(\mathbb{R})$ the Schwartz class:

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n)$$

In our case, $f(z) = q^{z^2}$, for $z \in i\mathbb{R}$ (and by analytic continuation¹ to all of \mathbb{C}).

Step # 2 The space of modular forms of weight 2 on $\mathbb{H}/\Gamma_0(4)$ is at most two-dimensional.

This is another whopper.

¹What properties of θ were used to define such a continuation?

Step #3 We find a basis of $M_2(\Gamma_0(4))$. The two startfunctions do span:

$$\begin{aligned}\mathbb{G}_2(z) &= -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n = -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \dots \\ G_2(z) &= -4\pi^2 \mathbb{G}_2(z) = \frac{1}{2} \sum_{n \neq 0} \frac{1}{n^2} + \frac{1}{2} \sum_{m \neq 0} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}\end{aligned}$$

This is related to Eisenstein series by a factor of ζ . If $k > 2$ we'd have:

$$\begin{aligned}G_k(z) &= \zeta(k) E_k(z) \\ G_k(z) &= \frac{1}{2} \sum_{(m,n) \neq (0,0)} \frac{1}{(mz + n)^2} \\ E_k(z) &= \sum_{\gamma \in \Gamma_{\infty} \backslash \Gamma_1} 1|_k \gamma = \frac{1}{2} \sum_{(c,d)=1} \frac{1}{(cz + d)^k}\end{aligned}$$

As $k \rightarrow 2$ did the extra terms just magically appear? Zagier just says for $k > 2$ define it this way, for $k = 2$ define this special way.

$$\mathbb{G}_2^*(z) = G_2(z) - \frac{\pi}{2y}$$

There's lot of exciting regularization issues going on here... letting $k = 2 + \epsilon$.

Here are three modular forms of weight 2 on $\Gamma_0(4)$, that are **not** holomorphic:

$$\mathbb{G}_2^*(z), \mathbb{G}_2^*(2z), \mathbb{G}_2^*(4z)$$

Here are two holomorphic forms that's don't have the y -term.

$$\mathbb{G}_2^*(z) - 2 \mathbb{G}_2^*(2z), \mathbb{G}_2^*(2z) - 2 \mathbb{G}_2^*(4z)$$

and now our modular form of interest $\theta(z)^4$ fits into this space $M_2(\Gamma_0(4))$ as well. By search:

$$\theta(z)^4 = 8(\mathbb{G}_2^*(z) - 2 \mathbb{G}_2^*(2z)) + 16(\mathbb{G}_2^*(2z) - 2 \mathbb{G}_2^*(4z))$$

This is essentially the **pigeonhole principle**. This turns a formula for the divisor function:

$$d_4(n) = 8 \sigma_1(n) - 32 \sigma_1(n/4)$$

It's likely there are many more elementary identities of this kind waiting to be discovered.

What's so great, we have incorporated all the basic theorems into a single proof except for:

Theorem Let $f(z)$ be a cusp form of weight k on $\Gamma_1 = \text{SL}(2, \mathbb{Z})$. E.g. let $f(z) = \sum a_n q^n$. Then:

$$a_n \leq C \sqrt{n^k}$$

for $n \geq 0$. The constant C can change with the f (does not depend on n).

The problem is our function $\theta(z)^4 = 1 + 8q + \dots$ is not cusp. However, maybe we can find other related theta functions which have series expansion $\sum a_n q^n$ with $a_0 = 0$. Let's proof this coefficients theorem

Proof We have the Fourier transform formula, integrating across a horocycle:

$$a_n = e^{2\pi n y} \int_0^1 f(x + iy) e^{-2\pi i n x} dx$$

The geometry of the region dictates that we should have a bound for f :

$$|f(z)| < c y^{-k/2}$$

Therefore $|a_n| < c y^{-k/2} e^{2\pi n y}$ A small leap here, if we set $y \asymp \frac{1}{n}$ we should have:

$$|a_n| < (c e^{2\pi}) n^{k/2}$$

This is the bound that Hecke proved.

Exercise

f is cusp $\leftrightarrow f(z) = O(q)$ with $|q| = e^{-2\pi y}$ and $y \rightarrow \infty$.

This just says that $q \rightarrow 0$ is a cusp.

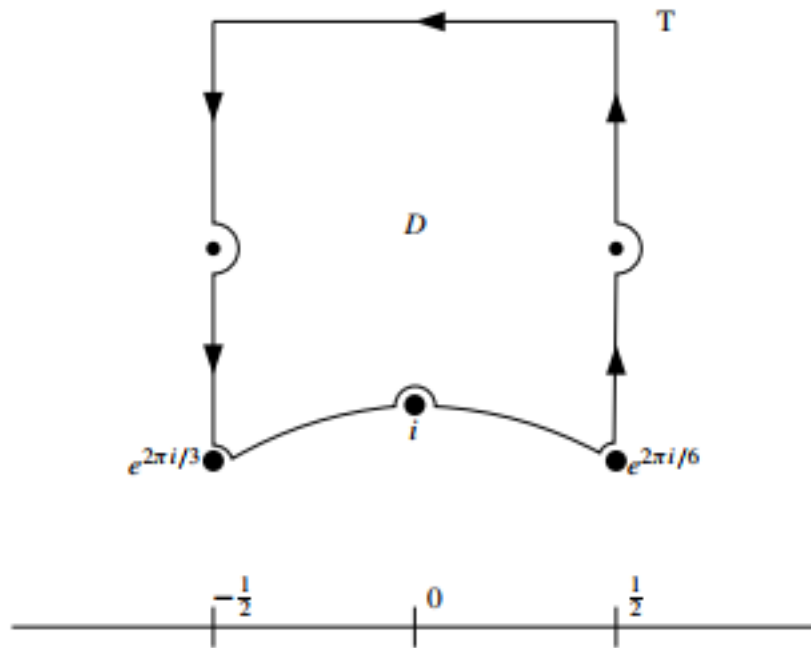
Return to Step #2: Let $f(z)$ be a modular form of weight k . Then

$$\text{ord}_\infty(f) + \sum_{z \in \Gamma_0(4)} \frac{1}{e} \text{ord}(f) = \frac{k}{12}$$

...

This would be the contour for $\Gamma_0(1) = \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H}$

How do we compute the volume of congruence groups?

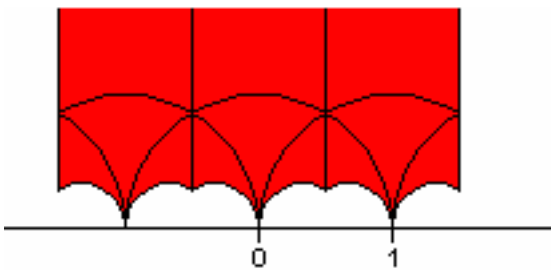


In the case of $\Gamma_0(4)$ the region is exactly 6 times as large (as found by the proposition):

$$\mathrm{Vol}(\Gamma_0(4) \backslash \mathbb{H}) = 6 \times \mathrm{Vol}(\mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H})$$

It would be reasonable to try to draw the region bounded by the two maps $z \mapsto z + 1$ and $z \mapsto -\frac{1}{4z}$. We know the result should be contained in an infinite cylinder, but the second map cuts the region even more. It's not hard, but a discussion is not readily available

Gamma(3)



Proposition² The coset representatives of $\Gamma_0(N)$ are in 1-1 bijection with $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

²For $N = 4$ this would give an answer of 6. The above picture is the region for $\Gamma(4)$ not $\Gamma_0(4)$.

Consulting a textbook:

Proposition The modular group at level N is defined by:

$$\Gamma_0(N) \equiv \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \pmod{N} \right\}$$

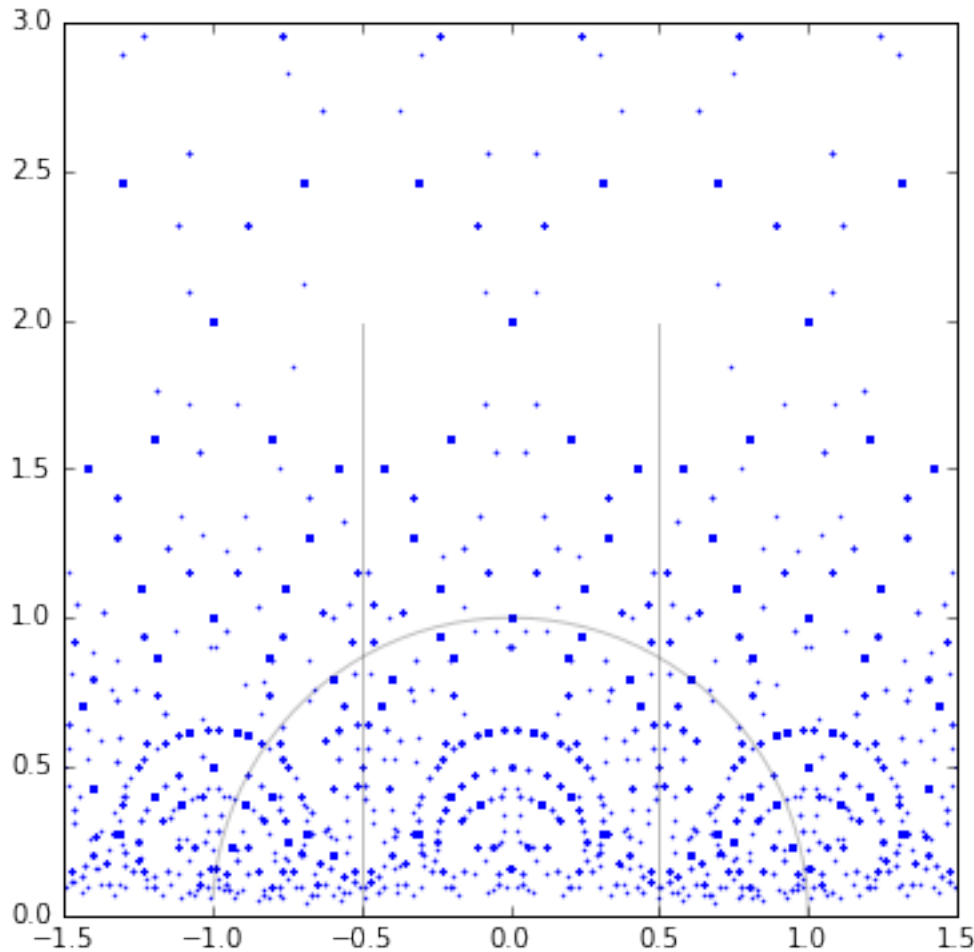
In our case $N = 4$. We are trying to draw: $\mathcal{F} = \mathbb{H}/\Gamma_0(4)$. If I pick two generators:

$$z \mapsto z + 1, \quad z \mapsto -\frac{1}{4z} \in \Gamma_0(4) \subseteq \mathrm{PSL}_2(\mathbb{Z})$$

There are two ways to reason about the fundamental domain, \mathcal{F} .

- As a subgroup, we can compute the index $[\Gamma_0(4) : \mathrm{PSL}_2(\mathbb{Z})] \in \mathbb{N}$ in fact, there is a neat formula for that. The fundamental region for $\Gamma_0(4)$ will be the union of copies of the region for $\mathrm{SL}_2(\mathbb{Z})$.
- I could try, from scratch, to draw the images of $z = i$ for every possible combination of $S : z \mapsto -\frac{1}{4z}$ and $T : z \mapsto z + 1$. Then, maybe I can find the Voronoi polygon of one of the points in the hyperbolic plane \mathbb{H} . This is a good skill to have.

These two methods will give different fundamental domains.

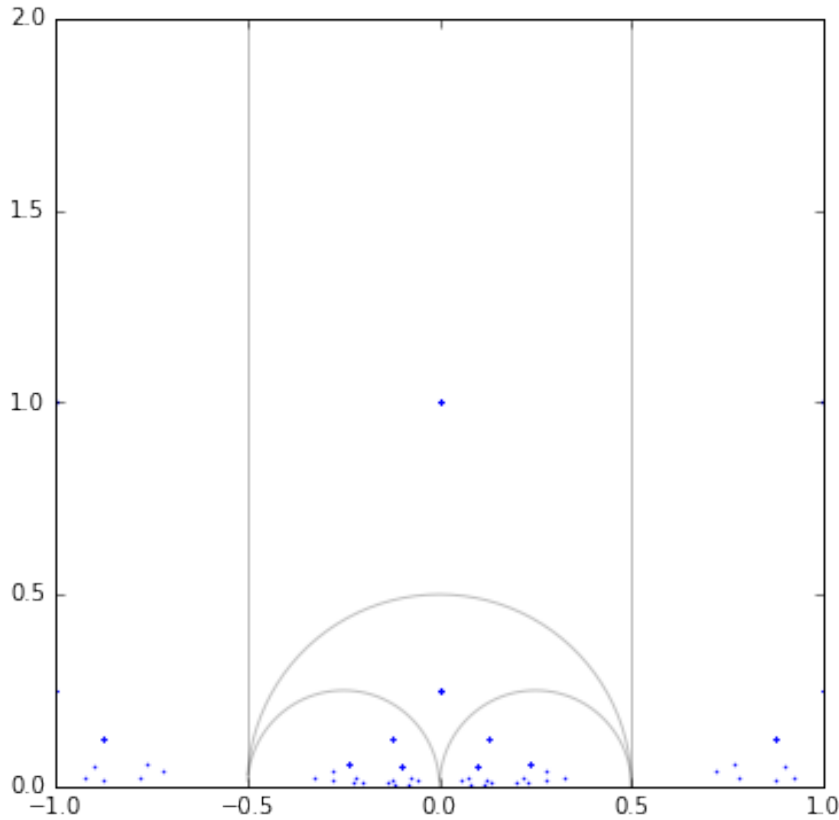


This is not the fundamental domain but it is kind of awesome. It is the set of images:

$$\left\langle S : z \mapsto \frac{4}{z}, \quad T : z \mapsto z + 1 \right\rangle i \in \mathbb{H}$$

The plot after using the correct map is a bit calmer, but it raised a question that the fundamental domain was an infinite-sided polygon. And that's something I'd rather not check.

Or it could be a triangle. It's a different triangle from the one you find in $\mathbb{H}/SL(2, \mathbb{Z})$



It is an infinite triangle, but it has finite hyperbolic area. By Gauss-Bonnet theorem, or whatever:

$$\text{Vol}(\mathbb{H}/\Gamma_0(4)) = \int_{-1/2}^{1/2} \left[\int_{\sqrt{1/4-x^2}}^{\infty} \frac{dy}{y^2} \right] dx = \int_{-1/2}^{1/2} \frac{dx}{\sqrt{1/4-x^2}} = 2 \times \tan^{-1}(x) \Big|_{-\pi/2}^{\pi/2} = 2\pi = 6 \times \frac{\pi}{3}$$

This really is six times the area of the $SL(2, \mathbb{Z})$ fundamental domain suggesting we are correct.

Next Time: using this proof (or another) we hint at equidistribution of the 4-squares points, connections to Hopf fibration, Davenport's geometry of number's proof, and how these things should behave over the Adeles, \mathbb{A} . That the proof uses the Weil conjectures suggests we should reap the many intermediate results first.

References

- (1) Don Zagier **Elliptic Modular Forms and their Applications**
https://doi.org/10.1007/978-3-540-74119-0_1
- (2) Jan Bruinier, Gerard Geer, Günter Harder, Don Zagier.
The 1-2-3 of Modular Forms (Universitext) Springer, 2008.
- (3) Anton Deitmar **Automorphic Forms** (Universitext) Springer, 2013.
- (4) A000118: **Number of ways of writing n as a sum of 4 squares; also theta series of lattice \mathbb{Z}^4** Online Encyclopedia of Integer Sequences <https://oeis.org/A000118>
- (5) Oliver Sargent, Uri Shapira **Dynamics on the space of 2-lattices in 3-space**
arXiv:1708.04464

8/17 We need to get a move-on, I'm afraid. Here's a sentence from a paper of an old colleague of mine, that I'm considering reading.

Let π traverse a sequence of cuspidal automorphic representations of GL_2 with large prime level and bounded infinity type.

Number Theory at the professional level has become so modern I can no longer discern it's elementary counterparts. Think about it, we had enough trouble writing down the boundary of the region $\mathbb{H}/\Gamma_0(4)$ we may also have trouble understanding a group like:

$$\mathrm{SL}_2(\mathbb{Q}) \backslash \mathrm{SL}_2(\mathbb{A}) / \mathrm{SL}_2(\hat{\mathbb{Z}})$$

so while a textbook like Dietmar or Bump may put down all the foundations, all the "elementary" parts (i.e. the good parts) are left as exercises to the reader.

We need more modular forms. Our resources are:

- Eisenstein series \subseteq Poincaré series
- Theta functions
- Hecke Eigenfunctions
- Maaß waveforms

Here is the definition I found for theta function by my friend.

Let $\rho_\psi : \mathcal{S}(\mathbb{A}) \rightarrow \mathcal{S}(\mathbb{A})$ be the Weil representation attached to $\psi \in \mathrm{Mp}_2(\mathbb{A})$ (acting on Adelic Schwartz space). For $\phi \in \rho_\psi$, the "elementary" theta function:

$$\theta(\phi) : \mathrm{SL}_2(F) \backslash \mathrm{Mp}_2(\mathbb{A}) \rightarrow \mathbb{C}$$

is an automorphic form, we can even write down a nice concrete formula for it:

$$\theta(\phi)(g) := \sum_{\alpha \in F} \left(\rho_\psi(g) \right) (\alpha)$$

This is a far cry from $\theta(z) = \sum_{n \in \mathbb{Z}} q^{n^2}$ but at least this style of writing makes the symmetry very very clear. Perhaps.

Obviously, Paul Nelson and his teachers are correct. I just wouldn't be able to tell you.³

³We will go back a few decades and examine space of modular forms constructed by Goro Shimura and some newer constructions by Don Zagier. Orthogonal to all mathematics, these papers were written in the 1970's and type-written in the 1970's. These papers are written in a rather streamlined, mechanical style that makes it difficult to pick out the more salient features. They are very difficult to read: both the symbols are difficult to read and the mathematics is challenging.

Let $n \in \mathbb{Z}$ be a positive integer, and A is a positive definite $n \times n$ matrix⁴ with entries in \mathbb{R} .

Let $x \in \mathbb{R}^n$ and P be a **spherical function** $P : \mathbb{R}^n \rightarrow \mathbb{C}$ with

$$P(x) = \begin{cases} \text{constant} & \text{if } \nu = 0 \\ \sum_q \beta_q (q^T A x)^\nu & \text{if } \nu > 0 \end{cases}$$

These vector q should have $q^T A q = 0$ if $\nu > 1$. I could type this $\langle q | A | q \rangle = 0$. Define $\theta(z; P)$ with

$$\theta(z; P) = \sum_{m \in h + N\mathbb{Z}^n} P(m) \cdot e\left(\frac{1}{2N^2} \cdot z \cdot (m^T A m)\right)$$

Duke calls this u instead of P . It looks good that spherical harmonics $u \in L^2[S^n]$ should count as “spherical functions” in this definition.

Despite being written in 1973, the idea of summing over close-to-random vectors $q \in S^n$ has a very modern flair to it. The care in which Shimura is writing suggests his modular form construction does not always “work”.⁵

⁴The term “matrix” can be thought of a short-hand for the algebra spanned by $e_i \otimes e_i^*$ with $e_i \in V$ and $e_i^* \in V^*$. There should be other algebras defined with other multiplications and they are written in this algebraic way without any matrix shorthand. We should invent our own!

⁵It works! It doesn’t work! This phrase changes every time we use it. Yet, this is our way of connecting all the things. . .