

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: ...

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.