Proposal: Sum of Three Squares

John D Mangual

In order to tie up loose ends I thought I'd study some easy diophantine equations:

$$n = x^2 + y^2 + z^2$$

This one turns out to be too difficult and one is better of starting in four variables:

$$n = x^2 + y^2 + z^2 + w^2$$

I had a good laugh to see professionals get when asking about these, being warned that I was not ready.

#1 Legendre's Sum of Three Squares Theorem

$$n = x^2 + y^2 + z^2 \quad \text{iff} \quad n \neq 4^a(8b + 7)$$

#2 Lagrange's Sum of Four Squares Theorem

$$n = x^2 + y^2 + z^2 + w^2 \quad \text{if} \quad n \geq 0$$

so with four squares we finally get enough numbers.

These problems look easy and by now they are solved.

- **1988** As $n \to \infty$ the solutions to $x^2 + y^2 + z^2 = n$ become evenly distributed over the sphere.

This one is credited to William Duke in 1988, using difficult Kloosterman sums. So let's try an easier one:

- **196?** As $n \to \infty$ the solutions to $x^2+y^2+z^2+w^2 = n$ become evenly distributed over the sphere.

This is credited to Malyshev (with no first name). Both problem use difficult spectral theory techniques.

Both of these problems are considered resolved, I feel like they can be re-opened at will.

I am wrong.

In 2003, Hee Oh and Wee-Tek Gan consider $f(x)$ a homogenous polynomial (such as $x^2 + y^2 + z^2$):

$$V_m = \{x \in \mathbb{R}^n : f(x) = m\}$$

and they prove equidistribution for all of these:

$$\frac{\#\left(\frac{1}{m^k} V_m(\mathbb{Z}) \cap \Omega_1\right)}{\#\left(\frac{1}{m^k} V_m(\mathbb{Z}) \cap \Omega_2\right)} \sim \frac{\mathrm{vol}(\Omega_1)}{\mathrm{vol}(\Omega_2)} \text{ as } m \to \infty$$

These proof are written in a very streamlined way, meant to solve many problems at once. The reasoning is a bit circular.

If we ask about other number fields. What about in $\mathbb{Z}[i]$?

$$x^2 + y^2 + z^2 = n$$

There certainly is a Hasse principle here and I can find the rule so there is a solution for certain values of n.

Have I stated it for you? No, but an expert can.[1] It is the difference between fixing my own car, and having someone fix it for me.

Problem A lot of proofs are written purely in terms of "wave-functions" on hyperbolic manifolds. How to express them in terms of integers again or in terms of shapes living on these hyperbolic spaces?[2]

Example Show that if we can find one solution to:

$$x^2 + y^2 + z^2 = n$$

we can find another such that $x \geq y \geq z \geq 0$.

There are infinitely many n with solutions so that

$$x \geq 2y \geq 3z \geq 0$$

This is contained inside one of the proofs of Duke's Theorem.

[1] The line of reasoning I keep hearing over and over is that such-and-such smart person knows how to solve it, so you should take their word for it. **This is going to stop.** This defeats the purpose of having a mathematical proof, which is about exhibiting the details so that one can verify the solution.

[2] There might even be a name for this process of turning wavefunctions into integers such as "Fourier transform" or "Functor of points". All the things I am complaining about might have a mathematical name.

If I go on the internet, on Google there seems to be an answer to all my question. All of them written in this kind of lame, obfuscated way, but also packed with insight.

Let's try simultaneous quadratic forms:[3]

$$x^2 + y^2 + 3z^2 = m$$
$$x^2 + y^2 + 5z^2 = n$$

The results like Hee Oh's show that my question has an answer. As $m, n \to \infty$ the integer points will become equidistriuted in some way. But not much else.

There is a hodge-podge of techniques. The line between what is known and what is impossible to solve is very thin.

Reminder to self: the starting point for solving the sum of four squres problems is to observe you can solve it with a theta function:

$$\theta(z)^4 = \left(\sum q^{n^2}\right)^4 = \sum r_4(n) q^n$$

[3]There are two papers by Lillian Pierce and others which consider quadratic forms in several variables. Like 20 or 100.

References

(1) S.G. Dani **Diophantine approximation and dynamics of unipotent flows on homogeneous spaces** *(online)*

(2) Elon Lindenstrauss **Effective Estimates on Indefinite Ternary Forms**

(3) Jean Bourgain **A quantitative Oppenheim Theorem for generic diagonal quadratic forms** arXiv:1604.02087

(4) Gergely Harcos **Twisted Hilbert modular L-functions and spectral theory** arXiv:1402.1332

(5) Yves Benoist, Hee Oh. **Effective equidistribution of S-integral points on symmetric varieties arXiv:0706.1621**

There are several proofs that every every integer is the sum of 4 squares. Let's try:

$$5 = 2^2 + 1^2 + 0^2 + 0^2$$

and how about another number see if we get lucky:

$$17 = 4^2 + 1^2 + 0^2 + 0^2$$

Then we can multiply solutions in some kind of way

$$5 \times 17 = (...)^2 + (...)^2 + (...)^2 + (...)^2$$

there should be maybe some kind of multiplication rule:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

is going to be also the sum of four squares:

$$\begin{aligned} &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &+ (x_1y_4 + x_4y_1 + x_2y_3 + x_3y_2)^2 \end{aligned}$$

It's a bit of a typographical nightmare. As a mathematician, I rarely think about the clarity of my writing from the literary or orthographic perspective.

$$85 = (2 \times 4 + 1 \times 1)^2 + (4 \times 1 - 1 \times 2)^2 + 0^2 + 0^2$$

At least we get a formula.

In the case of 3 squares the answers are still multiplicative, but there's no formula.

$$5 = 4^2 + 1^2 + 0^2$$

Therefore, 25 should also be admissible. And in fact:

$$25 = 4^2 + 3^2 + 0^2$$

and the third power of five should also have an answer:

$$125 = 5^2 \times (4^2 + 1^2 + 0^2)$$

We are glad just to have an answer. 3 is even easier:

$$3^2 = 1^2 + 1^2 + 1^2$$

and therefore we should also get 15:

$$\begin{aligned} 15 &= 3^2 + (...)^2 + (...)^2 \\ &= 2^2 + 2^2 + (...)^2 \end{aligned}$$

I am trying the different combinations. There is no solution. $n \neq 4^a(8b + 7)$ and yet

$$7 \times 23 = 161 = 4^2 + 8^2 + 9^2$$

Are we guaranteed a solution? The answer is yes. And we are quickly led to rich objects

- geometry of numbers
- Kloosterman sums
- quantum computation
- the Weil conjectures

Here's a way to get lots of three-squares type results:

$$3^2 + 4^2 = 5^2$$

therefoe we can arrange them into a rotation matrix:

$$\det \begin{bmatrix} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1$$

but we can also get a matrix by rearranging the numbers:

$$\det \begin{bmatrix} \frac{3}{5} & 0 & -\frac{4}{5} \\ 0 & 1 & 0 \\ \frac{4}{5} & 0 & \frac{3}{5} \end{bmatrix} = 1$$

and then if we multiply them, we don't have any chance of getting a simpler matrix:

$$\begin{bmatrix} \frac{9}{25} & -\frac{4}{5} & -\frac{12}{25} \\ -\frac{4}{5} & \frac{3}{5} & 0 \\ \frac{4}{5} & 0 & \frac{3}{5} \end{bmatrix}$$

the more we multiply, and these denominators will never get smaller. However a sphere has volume 4π and the space of rotation matrices has volume

$$\pi \times 4\pi \stackrel{?}{=} 4\pi^2$$

so we have countably infinitely many matrices in a finite (or "compact") space, so we can find matrices unnervingly close to the diagonal $(1, 1, 1)$ matrix.