Group Theory of Lagrange's 3-Squares Theorem

John D Mangual

1 Group Theory

"Number theory problems often relate to orbits of subgroups (periods) and so can be attacked by dynamical methods"

As $\mathbb{Z}$ is a group, I would like to believe that all number theory problems come from group theory. Let's try a specific one: Lagrange's sum of 3 squares theorem.

Let $n = 4^j(8k+7)$ then $n = a^2 + b^2 + c^2$. Like time's arrow one direction is easy and the other is hard. This problem is obviously related to the sphere:

$$S^2 = SO_3(\mathbb{Z})\backslash SO_3(\mathbb{R}) = SO_3(\mathbb{A})\backslash SO_3(\mathbb{A})/SO_3(\hat{\mathbb{Z}})$$

but the sphere is not a group. And this seems like a really complicated way of drawing the sphere. Ellenberg-Venkatesh also quotient out "obvious" $SO_3(\mathbb{Z})$ symmetries:

$$\left(\begin{array}{ccc} \pm 1 & & \\ & \pm & \\ & & \pm 1 \end{array}\right) \qquad \left(\begin{array}{ccc} 0 & 1 & \\ -1 & 0 & \\ & & 1 \end{array}\right)$$

The rotation group on the integers can't have that many symmetries. It has to be smaller than the symmetries of the unit cube $\{0,1\}^3$.

So what could be the group-theoretic content of the sum of three squares?

$$\overline{\mathcal{H}_d} = SO_3(\mathbb{Z})\backslash \mathcal{H}_d = \{(\pm a, \pm b, \pm c) : a^2 + b^2 + c^2 = d\}$$

This space has an adelic formulation. Here ar ethe bijections:

$$SO_3(\mathbb{Z})\backslash \mathcal{H}_d \to SO_3(\mathbb{Q})\backslash \mathcal{P} \leftarrow SO_{x_0}(\mathbb{Q})\backslash SO_{x_0}(\mathbb{Q})/SO_{x_0}(\hat{\mathbb{Z}})$$

There is some notation pecular to that paper, so let's try a few:

- $G = SO_{x_0}(\cdot)$ is the stabilizer of x_0 in $SO_3(\cdot)$. The dot $\cdot$ could be $\mathbb{A}$ or $\mathbb{Z}$ or $\mathbb{Q}_p$ or $\mathbb{R}$.

- Therefore $SO_3(\cdot)$ is a kind of functor from rings (since in matrix multiplication we multiply and add things) to groups (the various groups of rotations on different spaces)

- $\{(L,x) : L \in \mathrm{genus}_{SO_3}, x \in L, x.x = d\}$

This last line looks like a Grassmanian or something we might see when studying Integral Geometry and the **crofton formula**. This term **genus** might be the same genus, that appears in the theory of quadratic forms (e.g. in books of John Conway).

$$\mathrm{genus}_{SO_3}(L_0) \simeq SO_3(\mathbb{A}_f)/SO_3(\hat{\mathbb{Z}}) = SO_3(\mathbb{Q})$$

All of these equations look very comlicated, but one important issue... if we are going to try to solve $n = a^2 + b^2 + c^2$ then we might try to start by finding rational rotations. Here are two:

$$A = \left(\begin{array}{cc|c} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \qquad B = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{array}\right)$$

Showing these two matrices "almost" generate $SO(3)$ we can say the **closure** of the matrices is all rotations:

$$\overline{\langle A, B\rangle} = SO_3(\mathbb{R})$$

This notion of closure is not exotic, I think people on the street just say "almost" but our term closure is more correct.

...

...

We do not discuss matrix integrals at this time.

References

(1) arXiv:1503.05884 Effective equidistribution and property tau. Manfred Einsiedler, Grigory Margulis, Amir Mohammadi, Akshay Venkatesh.

(2) S. Lang and H. Trotter, **Continued fractions for some algebraic numbers**, J. Reine Angew. Math. 255 (1972), 112-134. https://eudml.org/doc/151239

(3) Philipp Fleig, Henrik P. A. Gustafsson, Axel Kleinschmidt, Daniel Persson Eisenstein series and automorphic representations arXiv:1511.04265

(4) arXiv:1001.0897 Linnik's ergodic method and the distribution of integer points on spheres. Jordan S. Ellenberg, Philippe Michel, Akshay Venkatesh.