Sum of 3 Squares Theorem, Hasse Principle, Banach-Tarski Paradox

John D Mangual

Today we read some difficult papers and do scratchwork.

$n = a^2 + b^2 + c^2$ iff $n = 4^m(8k + 7)$

this requires Hasse principle but there is no way to "multiply" solutions from the various primes into a one solution.

Why does solving $10101 = a^2 + b^2 + c^2$ require factoring at all? We are just adding squares[1].

[1] Woldfram Alpha says $10101 = 3 \times 7 \times 13 \times 37$

The strategy for solving $n = a^2 + b^2 + c^2$ over $\mathbb{Z}$ is to

- solve $n = a^2 + b^2 + c^2$ over $\mathbb{Q}$
- "reduce" to solution over $\mathbb{Z}$

Question[2] : why does this reduction always work?

Integers are a rather clumsy set to work with. Over $\mathbb{R}$ we can find all solutions:

$$(x, y, z) = (\cos\theta, \sin\theta\cos\phi, \sin\theta\sin\phi) \in S^2$$

These are related by rotations of the sphere, which any engineering student can write down:

$$\left[\begin{array}{cc|c} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ \hline 0 & 0 & 1 \end{array}\right], \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{array}\right] \in SO(3, \mathbb{R})$$

This brings us to the topic of **Lie Groups** named after Sophus Lie.

[2] It's like 50/50 I say "it work" I say "produces an integer solution". Weak langage for some people, strong language for others.

If I have a solution $n = a^2 + b^2 + c^2$ I can do a few things to generate more solutions:

- $(x, y, z) \mapsto (-x, y, z)$
- $(x, y, z) \mapsto (x, z, y)$

The rotation group over matrices is not very exciting:

$$\left[\begin{array}{cc|c} 0 & -1 & 0 \\ 1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right], \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & 0 \end{array}\right], \left[\begin{array}{c|c|c} \pm 1 & 0 & 0 \\ \hline 0 & \pm 1 & 0 \\ \hline 0 & 0 & \pm 1 \end{array}\right] \in SO(3, \mathbb{Z})$$

θ can't be too many values: $0°, 90°, 180°, 270°$ just right angles.

We need infinitely many primes in arithmetic progressions to solve $n = a^2 + b^2 + c^2$ over $\mathbb{Q}$

The last step in Serre's recipe to solve over $\mathbb{Z}$ is to **rotate** our solution over the integer fractions into solutions over integers.

The mystery is why does it always work?

It is not hard to write down elements of $SO(\mathbb{Q})$. One second thought... OK... Here $\cos\theta = \frac{3}{5}$.

$$\left[\begin{array}{cc|c} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ \hline 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{cc|c} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ \hline 0 & 0 & 1 \end{array}\right], \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{array}\right] \in SO(3,\mathbb{Q})$$

These two fractions along create infinitely many solutions, which wrap around the sphere... all solving $3^2 + 4^2 = 5^2$

What are our friends, the **Pythagorean triples** doing here? Here in a more chaotic guise..

$$(x,y,z) \mapsto (\frac{3}{5}x - \frac{4}{5}y, \frac{4}{5}x + \frac{3}{5}y, z) \text{ or } (x, \frac{3}{5}y - \frac{4}{5}z, \frac{4}{5}y + \frac{3}{5}z)$$

All pythagorean triples can be generated by two transformstions. So this is called **the free group on two elements**.

I think we understand $SO(3,\mathbb{R})$ very well but what about the other completions? $SO(3,\mathbb{Q}_2), SO(3,\mathbb{Q}_3), SO(3,\mathbb{Q}_5)$?

The (free group on two elements) generated by two rotations[3]

$$\overline{\left\langle \left[\begin{array}{cc|c} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ \hline 0 & 0 & 1 \end{array}\right], \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{array}\right] \right\rangle} = SO(3,\mathbb{Q})$$

These rotations have no where to go but rotation the sphere in various ways.

So infinitely many of these should cluster around a point, so these rotations are dense in the rotation group $SO(3,\mathbb{R})$.

$$\left[\begin{array}{cc|c} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \hline 0 & 0 & 1 \end{array}\right]$$

How close can we get? How much work does it take?

[3] http://mathoverflow.net/q/234869/1358 **Can two rational rotations $F_2 = \langle A, B\rangle \to SO(3)$ efficiently approximate the 3×3 identity matrix?**

References

(1) JP Serre **Course on Arithmetic** Springer-Verlag

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