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

John D Mangual

Scaling back, a much more ambitious project, we try to address three problems from number theory to measure theory:

- Lagrange showed $n = a^2 + b^2 + c^2$ iff $n \neq 4^a(8k+7)$

One quicky way to solve this eq is to solve in congruences:

- Solve equation in 2-adic numbers $n = a^2 + b^2 + c^2$, so $n \not\equiv 0 \mod 4$
- Solve $n = a^2 + b^2 + c^2 \mod p$ for all $p > 2$
- Solve $n = a^2 + b^2 + c^2$ in $\mathbb{R}$ (this just says $n > 0$)

Hasse-Minkowski principle tells us this is sufficient, but why does Hasse-Minkowski principle work at all?

How do we know the Hasse-Minkowski principle?

Case $n = a^2 + b^2 + c^2$

Reading's Serre's *Course on Arithmetic* we can solve in $\mathbb{Q}$:

$$a^2 + b^2 + c^2 - n\,d^2 = 0$$

We are able to find an $x \neq 0$ in $\mathbb{Q}$ solving two quadratic eqs:

$$a^2 + b^2 = x = c^2 - n\,d^2$$

This works because $x \in \mathbb{Q}$ not just $x \in \mathbb{Z}$, we'd better write

$$a^2 + b^2 - x\,e^2 = c^2 - n\,d^2 - x\,f^2 = 0$$

Once we have solved for $x \in \mathbb{Q}$ we solve $(a, b, c), (d, e, f) \in \mathbb{Q}^3$

$\circ\ \circ\ \circ$ This is reduction from 4 variables to 3 variables

How do we know the Hasse-Minkowski principle?

The only case $a^2 + b^2 + c^2 - n\,d^2 = 0$

Reading's Serre's *Course on Arithmetic* we can solve in $\mathbb{Q}$

Reduce 4 variables to 3...

Why is solving all congruences $n = a^2 + b^2 + c^2 \bmod p$ enough?

How do we know the Hasse-Minkowski principle?

The only case $a^2 + b^2 + c^2 - n\,d^2 = 0$

Reading's Serre's *Course on Arithmetic* we can solve in $\mathbb{Q}$

Reduce 4 variables to 3...

Why is solving all congruences $n = a^2 + b^2 + c^2 \bmod p$ enough?

How do we know the Hasse-Minkowski principle?

The only case $a^2 + b^2 + c^2 - n\,d^2 = 0$

Serre's *Course on Arithmetic* is written a little bit out of squence:

Let $f = x^2 + y^2 + z^2 - n\,w^2$ and we are solving[1] $f = 0$ in $\mathbb{Q}$.

For any prime[2] $p \in P$ we can solve in $\mathbb{Q}_p$ two equations at once[3]:

$$x_p = x^2 + y^2 \text{ and } x_p = z^2 - n\,w^2$$

This can be writen in **Hilbert symbols** as a shorthand:

$$(x, -ab)_p = (a, b)_v \text{ and } (x, -cd)_v = (c, d)_v$$

Then, the field of fractions $\mathbb{Q}$ of the integers $\mathbb{Z}$ is exceedingly rich, and we can find a single $x \in \mathbb{Q}$ solving all these Hilbert equations at once, for all $p \in P$.

[1] Sorry for the variable change, to make it look more like Serre.
[2] Think of $p = 12721$ or 32323 or 70507 or 94949 etc.
[3] Therefore $n = x^2 + y^2 + z^2$ solves both **sum of two squares** and **Pell's equation** simultaneously.

Merging solutions over $\mathbb{Q}_p$ to solutions over $\mathbb{Q}$

There is a single $x \in \mathbb{Q}$ such that[4] for every prime $p \in P$

$$ax_1^2 + bx_2^2 - xz^2 = 0$$

can be solved $(x_1, x_2, z) \in \mathbb{Q}_p^3$. There is a single $(x_1, x_2, z) \in \mathbb{Q}$

solving $(*)$ over the rational numbers. Similarly for $x_3^2 - nx_4^2 - xw^2$

Therefore we can solve $f = 0$ over $\mathbb{Q}$

[4]Please excuse all the quantifiers here? You deserve an better explanation! It's just that Serre is a genius.

Sweeping Information under the Rug

In the process of doing our Hilbert symbol calculation we are likely to have used[5]:

- Dirichlet's prime number theorem in arithmetic sequences $|P \cap a(\mathbb{Z} + b)| = \infty$.
- Quadratic Reciprocity $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

I don't understand **diophanine approximation** or **unique factorization** well enough to understand all the Hilbert symbols used.

Bonus problem show there exists $x \in \mathbb{Z}$ such that Pell equation and sum of two squares can both be solved[6] (over $\mathbb{Z}$)

$$x_1^2 + x_2^2 = x \text{ and } -x_3^2 + n\, x_4^2 = x$$

[5] After reading the much shorter 3-pages proof by Ankeny using **Geometry of Numbers** I decided to read this for context

[6] There could be enough "room" since we have both $x \in \mathbb{Z}$ and also $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ but can we satisfy constraints on n for **all** primes $p \in P$?

References

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