Scratchwork: Geometry of Numbers

As I read attempting to read Manjul Bhargava's papers, a few problems emerge:

- I don't know some of the groups definitions that he refers to
- I don't know what he is calling "geometry of numbers"
- I don't know what the big deal is about class numbers. Or why his contrubtions were so crucial.

Geometry of Numbers has been around since Hermann Minkowski, and there's even the book, written in academic 19th century German *Geometry der Zahlen*. And who knows? Perhaps that bounds have improved since then, ... there is the book of Cassels in the mid 20th century. This area - when I learned it - amounted to a "cute proof" that should be solve using more robust methods - and then Manjul won a Field's medal with it in 2014.[1]

The geometry of numbers proof (e.g. Davenport) that $n = a^2 + b^2 + c^2 + d^2$ uses lattices over $\mathbb{R}^4$. However the proof that $p = 4k+1 = a^2+b^2$ uses a mix of mod p arithmetic – over $(\mathbb{Z}/p\mathbb{Z})^2$ to define (an essentially random) lattice over $\mathbb{R}^2$. So, we are going to combine the two objects.

At this point p is still generic, so it's safe to say we are solving the "family" equations $x^2 + y^2 = n$ **at all primes p**.

$$X = \{x^2 + y^2 - n = 0\} \to \left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{R}\right)^2$$

and we are looking for lattices in this mixed geometirc object. And if we have $X(\mathbb{Z}/p\mathbb{Z})$ and $X(\mathbb{R})$ we could even have:

$$X(\mathbb{Z}_p) \to \cdots \to X(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to X(\mathbb{Z}/p^k\mathbb{Z}) \to \cdots \to X(\mathbb{Z}/p\mathbb{Z})$$

While looking at the scheme $X(\mathbb{Z})$ at one place p is not enough if we look at a generic place p *as well as* $p = \infty$ we can have

$$X(\mathbb{Z})\text{“} \simeq \text{”}X(\mathbb{Z}_p) \cap X(\mathbb{R})$$

and maybe this is sufficient.

Even if you know and prove Fermat's result that $p = 4k + 1$ prime is the sum of two squares what have you gained from that:

$$p = a^2 + b^2 = (a + bi)(a - bi) \text{ then } a + bi \in \sqrt{a^2 + b^2}\, e^{i\theta}$$

so there is an angle, θ that's unpredictiable. In more modern language we could say that primes in $\mathbb{Z}[i]$ are rotationally symmetric in large scale.

There are two good exampls of Fermat's descent:

- $p = a^2 + b^2$
- $\sqrt{2} \notin \mathbb{Q}$

[1] 1) that is my personal opinion, and usually when you ask someone suddenly everyone changes their position ... 2) I have look at him in person, maybe one or two-odd times in my life.

Wikipedia (and other books) indicate that descent can be considered a type of Galois Cohomology. Since a result like this is "clear" from elementary means, why should you build it from this complicated machinary? Here's the basic argumen:

$$x^2 = 2y^2 \to x = 2z \to (2z)^2 = 2y^2 \to 2z^2 = y^2 \to y^2 = 2z^2$$

The rest of the steps amound to identifying a variety (or scheme) basically the equation we are trying to solve, and the appropriate cohomology groups.

$$X = \{x^2 - 2y^2 = 0\}$$

That is the equation we are trying to solve. Now it's our variety or Scheme. We could consider $X(\mathbb{Z})$ or $X(\mathbb{Q})$ or $X(\mathbb{Q}_p)$ or whatever. All these equations we just calculated can be summarized by saying we found a **map**.

$$T : X \to X \text{ with } (x, y) \mapsto (y, x/2)$$

Then we say something interesting... we say our solution has gotten "smaller", e.g.

$$x^2 + y^2 > y^2 + (x/2)^2 \in \mathbb{Z}$$

In what sense have our solutions gotten smaller? We are not longer just using a field, we are using an *ordered* field, either $\mathbb{Q}$ or $\mathbb{R}$:

$$\begin{aligned} X(\mathbb{Z}) = \{x^2 - 2y^2 = 0\} &\subseteq X(\mathbb{Q}) = \{x^2 - 2y^2 = 0\} \\ &\subseteq X(\mathbb{R}) = \{(x - \sqrt{2}y)(x + \sqrt{2}y) = 0\} = \{x - \sqrt{2}y = 0\} \cap \{x + \sqrt{2}y = 0\} \end{aligned}$$

and finally we say that there are no infinitely descending sequences of integers.

In a way, we have done nothing. And we can go even futher . We might do this when the elementary means are unavailable, and when our own sense fail us or lead us astray. Now we consider x as a *function*:

$$x, y : X(\mathbb{Z}) \to \mathbb{Z} \text{ so that } x, y \in H^1(X, \mathbb{Z})$$

I'm not sure if this is the torsor that the Number Theorists use. In fact, they use

$$H^1(k, G) \text{ possibly } H^1(\mathbb{Q}, T)$$

setting $k = \mathbb{Q}$ and $G = \{T^k : k \in \mathbb{Z}\}$ to be iterations of the " $\times 2$ " map we discussed. Then the idea of local-to-global is that we find a solution over k if we solve over all completions k_v:

$$\text{if } [X] = 0 \in H^1(k_v, G) \text{ then } [X] = 0 \in H^1(k, G)$$

or we could state it as some type of product

$$H^1(k, G) \to \prod_v H^1(k_v, G)$$

In our case $k = \mathbb{Q}$, $[X] = \{x^2 - 2y^2 = 0\}$ and G is basically the map $(x, y) \mapsto (y/2, x)$. This amonunts to saying that for two relatively prime numbers $m, n \in \mathbb{Z}$ we could try to solve by unique factorization.

All these homology theories are (sometimes useful) layers that we put over real calculations and real things that are happening. Étale cohomology over $\mathrm{Spec}k$ is Galois cohomology, so we could stop here and I will.

We ought to discuss $p = a^2 + b^2$ a bit (btw I'm using notes of Brian Conrad on desent).

References

[1] Manjul Bhargava . . .