Proposal: Sum of Two Squares

John D Mangual

The beginning of the Étale cohomology book says we did it whenver we used **height functions** and **descent** to prove Fermat's Theorem:

$$p = 4k + 1 \leftrightarrow p = a^2 + b^2$$

It's not fair. You can't sell me on that and then I never see so much as an equation again.

There are several arguments – all of which I enjoy. Here's one:

#1 The equation $a^2 + b^2 \equiv 0 \bmod p$ has two solutions:

- $(a, b) = (p, 0)$
- $(a, b) = (x, 1)$ with $x \equiv \sqrt{-1} \bmod p$

The two solutions generate a lattice - some element of $SL(2, \mathbb{Z}) \backslash SL(2, \mathbb{R})$ - I can't say much more, just a random element. The area of the rhombus is $A = p$.

Next we intersect with a circle. $\{x^2 + y^2 = 2p\} \subset \mathbb{R}^2$ with area $A = \pi p$.

This argument solved the equation $x^2 + y^2 = p$ in two different venues:

- finite fields $\mathbb{F}_p \times \mathbb{F}_p$ with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- the Euclidean plane $\mathbb{R} \times \mathbb{R}$

What geometric object merges them both?

No matter which proof you choose, these arguments all seem to come from nowhere.[1] I have found 3 types:

- descent
- heights
- geometry of numbers
- factorials
- Viete Jumping

and all of these will fall out of Etale Cohomology.

Somehow, when we write all these equations we are already doing this wonderful thing.

Now we read the book - which has virtually no equations whatsoever - hoping we can recover Fermat.

Remark $x^2 = -1 \bmod p$ has a probabilistic solution:

$$\left[(\frac{p-1}{2})!\right]^2 \equiv -1 \bmod p$$

[1] While this problem is almost totally useless, the argument style. Real problems are difficult, have no symmetry

I do not know a whole lot about Schemes but the equation:

$$x^2 + y^2 - 1 = 0$$

can be solved over anything where the operations of $+$ and $\times$ make sense.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and also $\mathbb{Q}_p$
- $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{A} = \prod' \mathbb{Q}_p = \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3 \times \mathbb{Q}_5 \times \dots$

Or similarly we can find points on the circle of radius -1:

$$x^2 + y^2 = 0 \text{ or } +1 \text{ or } -1$$

since I am not sure about radius let's consider all possible radii,

$$\mathbf{X}(\mathbb{A}) = \left\{ x^2 + y^2 + n = 0 \right\}$$

The Adeles are not a field, they are a ring (not all the fractions work perfectly), but there is information about all fields.

This is very mechanical: now we have every possible number we can think of, and different solutions are related to each other and we can study the various "group actions".

Hopefully this becomes the modern formulation of descent.

References

(1) Christoph Soulé **Lectures on Arakelov Geometry** Cambridge Studies in Advanced Mathematics (Book 33) CUP, 1995.