# Hilbert on Elementary Number Theory

Vergegenwärtige man sich Wesensart und Methodik der gewöhnlichen finiten Zahlentheorie. Diese läßt sich gewiß allein durch Zahlenkonstruktionen mittels inhaltlicher anschaulicher Überlegungen aufbauen.

# Hilbert on Elementary Number Theory

Consider the nature and methods of ordinary finite number theory. It can certainly be built through number constructions by means of contentual, intuitive considerations.

Experts emphasize the arithmetic character of Wiles's (and successive) proofs of FLT.

"Nobody who understands such proofs does anything but think about very small structures from the start till the end."

Each step can be checked in any given case.

This is far from banal. Cf. the prime number theorem and other classical analytic number theory.

Seems typical for cohomology in number theory.

Every Fermat triple gives an elliptic curve

$$a^p + b^p = c^p \qquad x(x - a^p)(x + b^p)$$

In Hilbert's terms: we use letters (*Buchstaben*) to communicate that no matter what numerals (*Zahlzeichen*) you put in those places, the conclusion will hold.

You see this step in generic numerical terms.

Every Fermat triple gives an elliptic curve

$$a^p + b^p = c^p \qquad x(x - a^p)(x + b^p)$$

And as explicitly:

a modular curve $X_0(N)$ with $N$ the product of primes in $a, b, c$,

and a dominant map from $X_0(N)$ to the curve,

and related forms have lower $N$,

– down to 2 which is impossible.

Hilbert enunciated a “new finite inference rule (*ebenfalls finite neue Schlußregel*):

*When* $\mathfrak{A}(\mathfrak{z})$ *is proven a correct numerical formula for every assigned numeral* $\mathfrak{z}$*, then the formula*

$$(x)\mathfrak{A}(x)$$

*may be taken as conclusion.*

What holds in every numerical case, is general.

The proofs of FLT are seen numerically in every numerical case.

Hilbert's $\omega$-rule.

A compelling thought – deserves reflection.

Is it an inference rule at all?

How is $\mathfrak{A}(\mathfrak{z})$ proven correct for *every* numeral $\mathfrak{z}$?

*This* is the role of proof.

Even if you knew, by intuition or otherwise, for all concrete numerals $0 < a, b, c$ and $n > 2$

$$a^n + b^n \neq c^n$$

this would *not* show FLT is provable in PA (or in ZFC).

PA does not cover all concrete numerical truth (nor does ZFC)
– Gödel.

We know FLT is provable in ZFC because it has been done.

We know FLT is provable in finite order arithmetic (simple type theory with infinity) because it has been done.

I share the widespread confidence that FLT can be proved in PA.

This is not yet known as other results in proof theory are known.

PA is a natural, pivotal theoretical reference.

It provably cannot be the weakest arithmetic adequate to FLT.

Compactness theorem and reflexivity.

More pointedly, I argue, PA cannot explain the expert feeling that the proofs are concretely arithmetic.

PA is not concrete, finite in Hilbert's sense.

Hilbert: to say every number $n$ is less than some prime $p$, is not a concrete, finite claim.

Concrete: every number $n$ is less than some prime $p \leq n! + 1$.

$$\exists y < 2^{(x^2+2)} \, ( \, x < y \ \wedge \ y \text{ is prime} \, )$$

One does not merely feel the steps in proofs of FLT are calculations which must somehow end in each numerical case.

One sees, or feels, each calculation is concretely bounded.

And that they can be uniformly verified.

Cohomology as an organizing device.

What is a *universe*.

*Grothendieck universe* has a plain, explicit meaning.

Universe in the context of type theories/type constructors.

Replacement.

Grothendieck's perspective.

Macintyre 2011: "Putting proofs of MT into PA will involve finding finite approximations of MT and of all the other principles that go into its proof" (p. 15). Macintyre aims to "convince all except professional skeptics that MT is really $\Pi^0_1$. . . . The mathematical content of MT is conveyed by $\Pi^0_1$ sentences" (pp. 15,20).

The still-popular definitions of elementary number theory as number theory that does not use complex numbers.

A contrast to analytic number theory.

$$\pi(N) \approx \int_2^N \frac{1}{\ln(t)}\, dt$$

A real integral, calculated via Riemann's complex $\zeta(s)$.

Other uses of complex numbers are transparently elementary.

$$p = a^2 + b^2 \text{ iff } p = (a + bi)(a - bi).$$

Since Selberg and Erdös in particular, and Kreisel in general:

$$\int_2^N \frac{1}{\ln(t)}\,dt \;\text{ and } \zeta(s) \text{ are also elementary.}$$

Not all analytic methods are – yet.