(Un)provability of Fermat's last theorem and Catalan's conjecture in formal arithmetics

Petr Glivický
(with V. Kala)

petrglivicky@gmail.com

JAF 37
Villa Finaly, Florence
May 28, 2018
Slides available at http://www.glivicky.cz

Content

Section 1

(Un)provability of Fermat's Last Theorem

Fermat's Last theorem

Theorem (FLT, Wiles, 1995)

For $n > 2$ the equation

$$x^n + y^n = z^n$$

has no soultion $x, y, z \neq 0$ in $\mathbb{N}$.

The original Wiles's proof is **not** done in ZFC. It uses existence of Grothendieck's universes which is equivalent to existence of (strongly) inaccessible cardinals.

Nevertheless, it is believed that much less is used in principle.

Provability of FLT

- McLarty, 2011-12: the core parts of the Wiles's proof can be done in ZFC, even in finite order arithmetic *[C. McLarty, The large structures of Grothendieck founded on finite order arithmetic, arXiv:1102.1773v4]* and partially in second order arithmetic *[C. McLarty, Zariski cohomology in second order arithmetic, arXiv:1207.0276v2]* (use of Grothendieck's universes can be eliminated in the Wiles's proof)
- Macintyre, 2011: A (quite detailed) sketch of a project of proving FLT in PA (according the same lines as Wiles's proof but not a routine translation) *[A. Macintyre, The impact of Gödel's incompleteness theorems on mathematics – Appendix, Kurt Gödel and the Foundations of Mathematics: Horizons of Truth, Cambridge University Press, Cambridge, 2011.]*
- Smith, 1992: FLT for some small even values of exponent (e.g. $n = 4, 6, 10$) is provable in IE_1 (= bounded existential induction) *[S. T. Smith, Fermat's last theorem and Bezout's theorem in GCD domains, J. Pure Appl. Alg. 79 (1992), 63–85.]*

Unprovability of FLT

- Shepherdson, 1964: FLT for $n = 3$ is not provable in IOpen (open induction) *[J. C. Shepherdson, A nonstandard model for a free variable fragment of number theory, Bull. 1'Acad. Pol. Sci. 12 (1964), 79–86.]*
- Kołodziejczyk, 2011: FLT for $n = 3$ is not provable in T^0_2 (sharply bounded induction – bounded by length of term) *[L. A. Kołodziejczyk, Independence results for variants of sharply bounded induction, Ann. Pure Appl. Logic 162 (2011), 981–990.]*

Section 2

Exponential arithmetics

We will be working with models $\langle \mathcal{B}, e \rangle$ where $\mathcal{B} \models I\Sigma_1$ is a background model and e an exponential satisfying axioms Exp:

(e0) "$e : B \times A \to B$ for some substructure $\mathcal{A}$ of $\mathcal{B}$ with $\mathcal{A} \models \mathrm{Pr}$"

(e1) $(x = 1 \vee y = 0) \leftrightarrow e(x, y) = 1$,

(e2) $x \neq 0 \to e(x, y) \neq 0$,

(e3) $e(x, 1) = x$,

(e4) $e(x, y + z) = e(x, y) \cdot e(x, z)$,

(e5) $e(\prod_{i<l} x_i, y) = \prod_{i<l} e(x_i, y)$ (right hand side is correct thanks to (e7)),

(e6) $e(e(x, y), z) = e(x, yz)$,

(e7) "for any $b \in B$, the set $\{(x, e(x, y)); x < b\}$ is coded in $\mathcal{B}$",

whenever $y, z \in A$, $x \in B$ and $(x_i)_{i<l}$ is a sequence coded in $\mathcal{B}$ of length $l \in B$.

Note that in $\mathcal{B}$ the usual exponential x^y is definable. In general, e differs from x^y (although it follows from Exp that $e(m,n) = m^n$ for $m, n \in \mathbb{N}$).

Besides FLT, we will be also interested in the Catalan's conjecture:

Theorem (Catalan's conjecture, Mihăilescu, 2004)

The only solution of

$$e(a,n) - e(b,m) = 1$$

in $\mathbb{N}$ *with* $a, b, m, n > 1$ *is* $a = m = 3$, $b = n = 2$.

Let us also recall the statement of the ABC conjecture:

Conjecture (ABC, Mochizuki, 2012???)

For every $\varepsilon > 0$ there is K_ε such that for all coprime a, b, c with $a + b = c$ we have $c < K_\varepsilon \mathrm{rad}(abc)^{1+\varepsilon}$,

where $\mathrm{rad}(x)$ is the product of all different primes dividing x.

Results

We will prove:

- $Th(\mathbb{N}) + Exp \nvdash \mathrm{FLT}$ (moreover, FLT can be violated by unboundedly many exponents n and, independently on n, by unboundedly many pairwise linearly independent triples x, y, z),
- (assuming ABC conjecture in $\mathbb{N}$) $Th(\mathbb{N}) + Exp \vdash$ Catalan's conjecture (moreover, Exp can be replaced here just by axioms (e0)–(e4)),
- (assuming ABC conjecture in $\mathbb{N}$) $Th(\mathbb{N}) + Exp + (e8) \vdash \mathrm{FLT}$, where (e8) is "If x and y are coprime, then so are $e(x, a)$ and $e(y, b)$" (moreover, Exp can be replaced here by (e0)–(e4) and (e5'), which is a finite variant of (e5)).

Section 3

Construction of exponentials

Let $\mathcal{B} \models I\Sigma_1$ be fixed and assume we have an exponential $e : B \times A \to B$ satisfying Exp.

Then by (e5) the values of e are uniquely determined by values $e(q, y)$ for q primes in $\mathcal{B}$. Moreover, by (e7),

$$e(q, y) = \prod_{p \in \mathbb{P}} p^{\varepsilon(y)_{pq}}$$

.

So e is completely determined by the matrices $\varepsilon(y)_{pq}$ where p, q are prime numbers in $\mathcal{B}$ and $y \in A$.

Moreover, by (e4) and (e6), $\varepsilon : y \mapsto \varepsilon(y)_{pq}$ is a semiring homomorphism from $\mathcal{A}$ to the ring $M_{\mathbb{P}}^{good}(\mathcal{B})$ of all good $\mathbb{P} \times \mathbb{P}$-matrices over $\mathcal{B}$.

A matrix M is good if for any $J \in B$ there is $I = I_M(J) \in B$ such that

i) all non-zero values M_{ij} from first J columns are in the first I rows,

ii) the restricted matrix $(M_{ij})_{i<I, j<J}$ is coded in $\mathcal{B}$.

On the other hand if a semiring homomorphism $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ is given, then we can define an exponential e by:

$$
\begin{aligned}
e(0,0) &= 1,\\
e(0,z) &= 0,\\
e(x,y) &= v^{-1}(\varepsilon(y)v(x)),
\end{aligned}
$$

where $v : x \mapsto (v_p(x))_{p\in\mathbb{P}}$ is the usual (additive p-adic) valuation in $\mathcal{B}$.

In fact, there is a bijection between these semiring homomorphisms and exponentials:

Proposition

Let $\mathcal{B} \models \mathrm{I}\Sigma_1$ and $\mathcal{A} \subseteq \mathcal{B}$. Then the maps $e \mapsto \varepsilon^e$ and $\varepsilon \mapsto e^\varepsilon$ defined above, are mutual inverses and the following are equivalent:

- *The exponential $e = e^\varepsilon : B \times A \to B$ satisfies Exp.*
- *The map $\varepsilon = \varepsilon^e : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ is a semiring homomorphism.*

Examples of exponentials

- Let $\mathcal{A} = \mathcal{B}$ and $\varepsilon(y) = yI$, for $y \in B$, where I is the identity matrix. Then $e(x, y) = x^y$ (the original exponential in $\mathcal{B}$).
- Let $\mathcal{A} = \mathcal{B}$, f an automorphism of $\mathcal{B}$ and $\varepsilon(y) = f(y)I$, for $y \in B$. Then $e(x, y) = x^{f(y)}$.
- An exponential e satisfies (e8) $\Leftrightarrow$ all matrices $\varepsilon(y)$ are diagonal $\Leftrightarrow$ e is of the form $e_f(\prod_i p_i^{e_i}, a) = \prod_i p_i^{e_i f_{p_i}(a)}$ with $f = (f_p; p \in \mathbb{P})$ homomorphisms from $\mathcal{A}$ to $\mathcal{B}$.

Non-diagonal example

Suppose that $\mathcal{A} \subseteq \mathcal{B}$ is a model of Pr and that every $\mathbb{Z}$-component of $\mathcal{A}$ contains an element O divisible by all $n \in \mathbb{N}$.
Denote $\mathcal{O}$ the set of all such elements O. Easily, $\mathcal{O}$ is closed under $+, -, \cdot$ and contains 0.

Then any $(0, +, -, \cdot)$-homomorphism $\varepsilon : \mathcal{O} \to M_{\mathbb{P}}^{good}(\mathcal{B})$ can be easily extended to a semiring homomorphism $\varepsilon : \mathcal{A} \to M_{\mathbb{P}}^{good}(\mathcal{B})$ (by setting $\varepsilon(O + n) = \varepsilon(O) + nI$, where $O \in \mathcal{O}$ and $n \in \mathbb{Z}$).

Example:

$$\varepsilon : O \mapsto \begin{pmatrix} O/n & O/n & \cdots & O/n & 0 & \cdots & \\ \vdots & \vdots & \ddots & \vdots & 0 & \cdots & \\ O/n & O/n & \cdots & O/n & 0 & \cdots & \\ 0 & 0 & \cdots & 0 & O & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & 0 & \ddots & \end{pmatrix}$$

Section 4

Results and proofs

Theorem

1) *There is a model* $\langle \mathcal{B}, e\rangle \models Th(\mathbb{N}) + Exp$ *containing an unbounded set* $E \subseteq B$ *of exponents and (in every coordinate) unbounded set* $T \subseteq B^3$ *of pairwise linearly independent triples* (a, b, c) *such that for every* $n \in E$ *and* $(a, b, c) \in T$ *we have*

$$e(a, n) + e(b, n) = e(c, n).$$

Moreover:

- *For any fixed* y, $e(x, y)$ *is a definable function of* x *in* $\mathcal{B}$.
- e *is definable in the expansion* $\langle \mathcal{B}, \mathcal{N}\rangle$ *of* $\mathcal{B}$ *by a predicate* $\mathcal{N}(x)$ *expressing "x is a standard number".*

2) *There is a substructure* $\langle \mathcal{A}, e\rangle \subseteq \langle \mathcal{B}, e\rangle$ *with* e *total and* $\mathcal{A} \models \mathrm{Pr}$ *such that* $E \subseteq A$, $T \subseteq A^3$. *(Thus, in addition to axioms of* Pr, $\langle \mathcal{A}, e\rangle$ *satisfies all quantifier-free statements true in* $\langle \mathcal{B}, e\rangle$*.)*

Proof: See the board.

Let S be a theory (in the language of arithmetic $\langle 0, 1, +, \cdot, \leq \rangle$) stronger than $\mathrm{I}\Sigma_1$ such that, for some $K \in \mathbb{N}$, S proves (“a, b, c coprime” & $a + b = c) \rightarrow c < K\mathrm{rad}(abc)^{1+1/3}$, and the Catalan conjecture (using the exponential x^y definable in S). By Mochizuki's (?) and Mihăilescu's results, we may take $S = Th(\mathbb{N})$.

We denote by Exp' the axioms (e0)–(e4).

Theorem

Let S be as above. Catalan Conjecture for e is provable in $S + Exp'$.

Proof: See the board.

Recall

(e8) "If x and y are coprime, then so are $e(x, a)$ and $e(y, b)$."

This is equivalent to all corresponding matrices $\varepsilon(a)$ being diagonal. Note also that (e8) is still much weaker than induction for e.

We denote the finite version of (e5) by

(e5') $e(xy, z) = e(x, z) \cdot e(y, z)$

Let T be a theory (in the language of arithmetic $\langle 0, 1, +, \cdot, \leq \rangle$) stronger than $\mathrm{I}\Sigma_1$ such that, for some $K \in \mathbb{N}$ and some $\varepsilon > 0$, T proves ("a, b, c coprime" & $a + b = c$) $\rightarrow c < K\mathrm{rad}(abc)^{1+\varepsilon}$, and the Fermat's Last Theorem (using the exponential x^y definable in T). We may again take $T = Th(\mathbb{N})$.

Theorem

Let T be a theory as above. Fermat's Last Theorem for e is provable in $T + Exp' + (e5') + (e8)$.

Proof: Analogous to the proof of Catalan's conjecture.

Open Queustions

Open Problem

For which arithmetical theories S does there exist a model $\langle \mathcal{B}, e \rangle \models S + Exp +$ "e is total" such that Fermat's Last Theorem for e does not hold in $\langle \mathcal{B}, e \rangle$? In particular, is there such a model for $S = Th(\mathbb{N})$?

Open Problem

Is there a model $\mathcal{B} \models Th(\mathbb{N})$ (or at least of $\mathrm{I}\Sigma_1$) that permits a semiring homomorphism $\varepsilon : B \to M_{\mathbb{P}}^{good}(\mathcal{B})$ with some values $\varepsilon(b)$ non-diagonal?

Thank you.

[P. Glivický and V. Kala, Fermat's last theorem and Catalan's conjecture in weak exponential arithmetics, Mathematical Logic Quarterly 63 (2017), no. 3-4, 162-174, arXiv: 1602.03580]