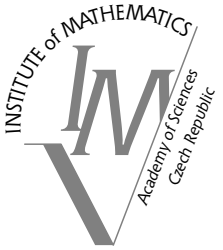

INSTITUTE of MATHEMATICS

ACADEMY of SCIENCES of the CZECH REPUBLIC

Fermat's last theorem and Catalan's conjecture in weak exponential arithmetics

Petr Glivický
Vítězslav Kala

Preprint No. 39-2015

PRAHA 2015

FERMAT'S LAST THEOREM AND CATALAN'S CONJECTURE IN WEAK EXPONENTIAL ARITHMETICS

PETR GLIVICKÝ AND VÍTĚZSLAV KALA

ABSTRACT. We deal with expansions $\langle \mathcal{B}, e\rangle$ of models of arithmetical theories (in the language $L = \langle 0, 1, +, \cdot, \leq\rangle$) by a binary (partial or total) function e intended as an exponential. We provide a general construction of such expansions and prove that it is universal for the class of all exponentials e which satisfy a certain natural set of axioms Exp.

We construct a model $\langle \mathcal{B}, e\rangle \models Th(\mathbb{N}) + Exp$ and its substructure $\langle \mathcal{A}, e\rangle$ with e total and $\mathcal{A} \models \mathrm{Pr}$ (Presburger arithmetic) such that in both $\langle \mathcal{B}, e\rangle$ and $\langle \mathcal{A}, e\rangle$ the Fermat's Last Theorem for e is violated by cofinally many exponents n and (in all coordinates) cofinally many pairwise linearly independent triples a, b, c.

On the other hand, under the assumption of ABC conjecture (in the standard model), we show that the Catalan conjecture for e is provable in $Th(\mathbb{N}) + Exp$ (even in a weaker theory) and thus holds in $\langle \mathcal{B}, e\rangle$ and $\langle \mathcal{A}, e\rangle$.

Finally, we also show that Fermat's Last Theorem for e is provable (again, under the assumption of ABC in $\mathbb{N}$) in $Th(\mathbb{N}) + Exp +$"coprimality for e".

1. INTRODUCTION

Wiles's proof of Fermat's Last Theorem (FLT) [Wil95] has stimulated a lively discussion on how much is actually needed for the proof. Despite the fact that the original proof uses set-theoretical assumptions unprovable in Zermelo-Fraenkel set theory with axiom of choice (ZFC) (namely, the existence of Grothendieck universes; see [McL10] for more on this topic), it is widely believed that

> *"certainly much less than ZFC is used in principle, probably nothing beyond PA, and perhaps much less than that."* [McL10, p. 359]

McLarty showed that Grothendieck's apparatus can be formalized in finite order arithmetic (hence in ZFC) [McL11] and partially even in second order arithmetic [McL12]. Macintyre [Mac11, Appendix] proposed and sketched a project of formalizing Wiles's proof in Peano arithmetic.

2010 *Mathematics Subject Classification.* 03F30, 11U10, 03H15, 03C62.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 339691. First author also supported by the grant GAUK 4372/2011.

Harvey Friedman even conjectured that Fermat's Last Theorem[1] is provable in the so called elementary function arithmetic (EFA) [Fri99]. Here, EFA is a theory in the language $\langle 0, 1, +, \cdot, \exp, \leq \rangle$ which extends usual quantifier free axioms for $0, 1, +, \cdot, \exp, \leq$ by the scheme of bounded induction (see [Avi03, section 2, theory EA] for a possible axiomatic)[2].

Some nice results in the direction of these conjectures are due to Smith, who in [Smi92] proved that the theory IE_1 of bounded existential arithmetic (a $\langle 0, 1, +, \cdot, \leq \rangle$-theory containing induction only for bounded existential quantifications of open formulas, hence even weaker then Friedman's EFA) proves Fermat's Last Theorem for some small even exponents n (e.g., for $n = 4,\ 6,\ 10$). In the same paper, Smith also proves some special cases of FLT in the even weaker theory IOpen + "every two elements have a greatest common divisor". Here, IOpen is the extension of Robinson arithmetic by induction for all quantifier-free formulas.

These results, however, can not be strengthened down to IOpen. In a rather well-known paper [She64], Shepherdson constructed a (recursive) model of IOpen where the equation $x^3 + y^3 = z^3$ has a non-zero solution. Recently, Kołodziejczyk in [Koł11] extended Shepherdson's method to the Buss's arithmetic T_2^0 (containing induction for sharply bounded formulas in the Buss's language; see for example [HP93, V.4.4]). In particular, he showed that T_2^0 does not prove Fermat's Last Theorem for $n = 3$.

In this paper, we consider structures and theories in the language $L^e = \langle 0, 1, +, \cdot, e, \leq \rangle$, where the symbol e is intended for a (partial or total) binary exponential. We show that Fermat's Last Theorem for e (i.e., the statement "$e(a, n) + e(b, n) = e(c, n)$ has no non-zero solution for $n > 2$") is not provable in the L^e-theory $Th(\mathbb{N}) + Exp$, where $Th(\mathbb{N})$ stands for the complete theory of the structure $\mathbb{N} = \langle \mathbb{N}, 0, 1, +, \cdot, \leq \rangle$ and Exp is a natural set of axioms for e (consisting mostly of elementary identities; see Section 4).

In more detail – we construct a model $\langle \mathcal{B}, e \rangle \models Th(\mathbb{N}) + Exp$ and its substructure $\langle \mathcal{A}, e \rangle$ with e total and $\mathcal{A} \models \mathrm{Pr}$ (Presburger arithmetic) such that in both $\langle \mathcal{B}, e \rangle$ and $\langle \mathcal{A}, e \rangle$ the Fermat's Last Theorem for e is violated by cofinally many exponents n and cofinally (in all coordinates) many pairwise linearly independent triples a, b, c. Moreover, we show that for any fixed y the function $e(x, y)$ is a definable (in $\mathcal{B}$) function of x, and that 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". The results are summarized in Theorem 4.8.

On the other hand, under the assumption of ABC conjecture[3] (in the standard model), we show that the Catalan conjecture for e ("the only solution of $e(a, n) - e(b, m) = 1$ with $a, b, m, n > 1$ is $a = m = 3$, $b = n = 2$") is provable in $Th(\mathbb{N}) + Exp$ (even in a weaker theory – see Section 5 and Theorem 5.2) and thus holds in $\langle \mathcal{B}, e \rangle$ and $\langle \mathcal{A}, e \rangle$. (Of

[1] Friedman actually made much stronger conjecture concerning *"every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement)"* in place of FLT.

[2] Let us note that (up to a change of language) EFA is equivalent to $\mathrm{I}\Sigma_0(exp)$ or $\mathrm{I}\Sigma_0$ + "2^x is total" (see [HP93, I.1.28] and the discussion after Proposition V.1.3 ibid.)

[3] Mochizuki recently announced a proof of ABC conjecture [Moc12]. However, its correctness has not yet been completely verified.

course, we also have to use the Catalan conjecture in the standard model, as proved by Mihăilescu [Mih04].)

This gives an interesting separation of the strengths of the two famous Diophantine problems.

As we note in Section 6, a crucial property for the validity of Fermat's Last Theorem is the "coprimality" of e, i.e., the statement that if x and y are coprime, then so are $e(x,a)$ and $e(y,b)$. Assuming this, we can again use the ABC conjecture and show in Theorem 6.1 that Fermat's Last Theorem holds for exponentials e which satisfy this coprimality condition.

Nevertheless, we do not know whether there is a model $\langle \mathcal{B}, e\rangle \models Th(\mathbb{N}) + Exp$ (or at least $\langle \mathcal{B}, e\rangle \models \mathrm{IOpen} + Exp$) with e total, where the Fermat's Last Theorem for e does not hold (see Open Problem 4.9). Note that our model $\mathcal{A}$ (which carries a total e violating FLT) satisfies $\mathrm{Pr} + \mathrm{OpenTh}(\mathbb{N})$, where $\mathrm{OpenTh}(\mathbb{N})$ stands for the set of all open formulas true in the the standard model $\mathbb{N}$.

To relate the presented results with Shepherdson's, let us note that Shepherdson's model is a structure in the language $L = \langle 0, 1, +, \cdot, \leq\rangle$, which is too weak even to define any good notion of exponential.

On the other hand, in our model, its L-part $\mathcal{B}$ is a model of $Th(\mathbb{N})$ and thus "well-behaved". The "weakness" of the model comes from the properties of the exponential e (which differs dramatically from the exponential x^y definable in $\mathcal{B}$). In particular, since both exponentials – x^y and e – coincide for all standard exponents n, in our model FLT for e holds for all exponents $n \in \mathbb{N}$.

The results above are obtained using a general construction of an exponential e over a background model $\mathcal{B}$ of a sufficiently strong (at least $\mathrm{I}\Sigma_1$) arithmetical theory (in the language $L = \langle 0, 1, +, \cdot, \leq\rangle$). We describe this construction in Section 3. We also prove that the construction is universal for the class of all exponentials e which satisfy the set of axioms (e1)-(e7) from Exp (see Proposition 3.1).

Let us also mention that Mlček [Mlč76] has studied the existence of unboundedly many twin primes (i.e., pairs of primes p and $p+2$) in models of weak arithmetics. He constructed three models of the theory Pr+OpenTh($\mathbb{N}$) (the same theory which is satisfied by our model $\mathcal{A}$) with only boundedly many primes, with unboundedly many primes but boundedly many twin primes, and with unboundedly many twin primes, respectively. Let us note that if $\mathcal{B}$ is a model of Peano arithmetic, then our model $\mathcal{A}$ contains unboundedly many primes – see the remark immediately following the proof of Lemma 4.3. It would be interesting to consider the question of twin primes together with Fermat's Last Theorem in more detail.

One can of course consider extending the above methods to the study of other exponential Diophantine equations. They can certainly be used to construct solutions to various homogeneous equations (such as was $a^n + b^n = c^n$) – the crucial thing is having an analogue of Lemma 4.1. One can also proceed similarly if the given equation can be made homogeneous by a suitable substitution for the variables. However, note for example that

if Fermat's Last Theorem for $n = 3$ holds in $\mathcal{B}$, the equation $a^{3n} + b^{3n} = c^{3n}$ can have no solutions even with the new exponential.

In the case of non-homogeneous equations one can sometimes expect to be able to use the ABC Conjecture, as we illustrated by the case of Catalan Conjecture $a^n - b^m = 1$. See the remarks in Section 6 concerning the importance of coprimality for the exponential. In any case, obtaining a truly general theorem seems to be a hard and interesting question for further research.

Acknowledgments

The authors want to thank Professors Leonard Lipshitz and Josef Mlček for their advice and suggestions which have helped improve the quality of this paper.

2. Preliminaries

In this paper, $\mathbb{N}$ denotes the set $\mathbb{N} = \{0, 1, \ldots\}$ of natural numbers.

We shall denote models of theories by "caligraphic" letters $\mathcal{M}$ and their underlining sets by normal letters M.

2.1. Arithmetical theories By the language of arithmetic we mean the language $L = \langle 0, 1, +, \cdot, \leq \rangle$. The L-theory $\mathrm{I}\Sigma_1$ is the extension of Robinson arithmetic by the scheme of induction for all Σ_1-formulas, i.e., for formulas of the form $(\exists x_0, \ldots, x_{n-1})\psi(\overline{x}, \overline{y})$, where ψ contains only bounded quantifiers. Let us note that the usual (Gödel's) coding of formally finite sets is available in $\mathrm{I}\Sigma_1$. We are going to use the coding at many places of the following text, mostly without explicitly mentioning it.

Let $\mathcal{B}$ be a model of $\mathrm{I}\Sigma_1$. We say that a set $X \subseteq B^n$ is coded in $\mathcal{B}$ (or, equivalently, finite in the sense of $\mathcal{B}$) if there is an element $s \in B$ with $\mathcal{B} \models$ "s is a set" and for any $u \in B^n$ one has $\mathcal{B} \models u \in s$ if and only if $u \in X$. Let us note that any bounded part of a Σ_1-definable set in $\mathcal{B}$ is coded in $\mathcal{B}$. However, when dealing with sets definable in an extended language (such as L^e), this no longer needs to be true.

Also note that the usual exponential x^y is Δ_1-definable in $\mathrm{I}\Sigma_1$. Further on, we will strictly use the notation x^y for the definable exponential, while keeping different notation for other "exponentials" with which we will work.

Presburger arithmetic Pr is the complete theory $Th(\langle \mathbb{N}, 0, 1, +, \leq \rangle)$ of the additive structure of natural numbers. It is well-known that Pr is equivalent to the theory with the following axioms:

(Pr1) $0 \neq z + 1$,
(Pr2) $x \neq 0 \to (\exists z)(x = z + 1)$,
(Pr3) $x + z = y + z \to x = y$,
(Pr4) $x + 0 = x$,
(Pr5) $x + (y + z) = (x + y) + z$,
(Pr6) $x + y = y + x$,
(Pr7) $x \leq y \leftrightarrow (\exists z)(x + z = y)$,
(Pr8) $(\exists y)(ny \leq x < n(y + 1))$, for all $0 < n \in \mathbb{N}$.

(Note that (Pr8) is equivalent to the induction scheme for all formulas in the language $\langle 0, 1, +, \leq \rangle$.)

For an L-structure $\mathcal{A}$, by writing $\mathcal{A} \models \mathrm{Pr}$ we mean that all the axioms above are true in $\mathcal{A}$ (this is, of course, a harmless abuse of notation).

2.2. Good matrices In the following sections, we will often need to work with infinite (even in the sense of $\mathcal{B}$) matrices of elements from our background model $\mathcal{B} \models \mathrm{I}\Sigma_1$, i.e., with matrices of the form $M = (M_{ij})_{i,j \in B}$, with $M_{ij} \in B$.

Unlike the addition, multiplication of such matrices can not be generally defined. In fact, there are two obstacles in defining the product $P = MN$ of matrices M and N:

- We want to have $P_{ij} = \sum_{k \in B} M_{ik} N_{kj}$. However, this sum may add up to infinity when both the i-th row of M and the j-th column of N are allowed to contain unboundedly many non-zero elements.
- Even a bounded sum $\sum_{k<b} a_k$ may not exist in B if $(a_k)_{k<b}$ is not coded in $\mathcal{B}$.

If in both M, N, each row and each column contain only boundedly many non-zero elements and all these bounded initial segments are coded in $\mathcal{B}$, the product MN is correctly defined but it may contain a column (or row) with unboundedly many non-zero elements. In order to prevent this, we need that, in M, any bounded set of columns has a common upper bound for the number of rows containing non-zero elements in these columns.

That is why we define a matrix $M = (M_{ij})_{i,j \in B}$ to be good in $\mathcal{B}$ if the following hold: 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 $\mathcal{B}$.

Note that the above condition may be equivalently formulated as follows: M is good in $\mathcal{B}$ if and only if for any $J \in B$ the set $\{(i, j, M_{ij}); j < J,\ i \in B,\ M_{ij} \neq 0\}$ is coded in $\mathcal{B}$.

We will further assume that all matrices are of the form $(M_{ij})_{i,j \in B}$ (i.e. $B \times B$-matrices) and identify any $X \times Y$-matrix $(N_{ij})_{i \in X, j \in Y}$, where $X, Y \subseteq B$ (not necessarily infinite), with the matrix $(M_{ij})_{i,j \in B}$, where $M_{ij} = N_{ij}$ for $(i, j) \in X \times Y$ and $M_{ij} = 0$ otherwise.

We denote by $M_B^{good}(\mathcal{B})$ the set of all $B \times B$-matrices over B good in $\mathcal{B}$.

Lemma 2.3. *$M_B^{good}(\mathcal{B})$ is closed under matrix multiplication.*

Proof. Let $M, N \in M_B^{good}(\mathcal{B})$ and let I_M, I_N be some functions witnessing that M, N, respectively, are good in $\mathcal{B}$. Denote $P = MN$. Take $J \in B$ and $j < J$. We have $P_{ij} = \sum_{k<I_N(J)} M_{ik} N_{kj}$. For $i > I = I_M(I_N(J))$, we get $P_{ij} = \sum_{k<I_N(J)} 0 \cdot N_{kj} = 0$. Also clearly $(P_{ij})_{i<I, j<J}$ is coded in $\mathcal{B}$, since $(M_{ik})_{i<I, k<I_N(J)}$ and $(N_{kj})_{k<I_N(J), j<J}$ are. $\square$

2.4. Semirings By a semiring we shall mean a structure $\langle S, 0, 1, +, \cdot \rangle$ equipped with two constants $0, 1$ and two associative binary operations $+$ and $\cdot$ such that $+$ is commutative, $x + 0 = 0 + x = x$, $x \cdot 1 = 1 \cdot x = x$, $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$.

For semirings S and T, a semiring homomorphism $\varphi : S \to T$ is a map such that $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$, $\varphi(0) = 0$ and $\varphi(1) = 1$.

3. General construction

In this Section, let $\mathcal{B} \models \mathrm{I}\Sigma_1$ be a fixed "background model" and $\mathcal{A} \subseteq \mathcal{B}$ its substructure. We show a method of construction of a function $e : B \times A \to B$ such that the following properties hold in $\langle \mathcal{B}, e \rangle$:

(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 $l \in B$.

For the convenience of the reader regarding our definitions, let us note that at the beginning of Section 4 we introduce an additional axiom (e0) and denote by Exp the axioms (e0) – (e7). Exp' denotes only (e0) – (e4). At the beginning of Section 6 we introduce (e8). In Section 6 we shall also use the following weakening of (e5):
(e5′) $e(xy, z) = e(x, z) \cdot e(y, z)$.

Before delving into the technical construction of the exponential, let us outline the idea. Suppose that we have an exponential $e : B \times A \to B$ satisfying the axioms above. How can we characterize e? First of all, by multiplicativity (e5), the values $e(q, y)$ at primes q determine e. If we write $e(q, y) = \prod_{p \in \mathbb{P}} p^{\varepsilon(y)_{pq}}$ (where $\mathbb{P}$ is the set of prime numbers of $\mathcal{B}$), we can form a matrix $\varepsilon(y) = (\varepsilon(y)_{pq})_{p,q \in \mathbb{P}}$. Property (e7) ensures that the matrix $\varepsilon(y)$ is good in $\mathcal{B}$ (see 2.2) and (e4) and (e6) imply $\varepsilon(y + z) = \varepsilon(y) + \varepsilon(z)$ and $\varepsilon(yz) = \varepsilon(y)\varepsilon(z)$ (see the proof of Proposition 3.1 for details). Thus

$$\begin{array}{rcl} \varepsilon = \varepsilon^e : A & \to & M_{\mathbb{P}}^{good}(\mathcal{B}) \\ y & \mapsto & (\varepsilon(y)_{pq})_{p,q \in \mathbb{P}} \end{array}$$

is a semiring homomorphism, where $M_{\mathbb{P}}^{good}(\mathcal{B})$ denotes the semiring of $\mathbb{P} \times \mathbb{P}$-matrices M over $\mathcal{B}$ which are good in $\mathcal{B}$. Notice also that

$$\varepsilon(y)_{pq} = v_p(e(q, y)) \tag{1}$$

where $v_p(x)$ is the usual additive p-adic valuation of x (in $\mathcal{B}$).

Conversely, to construct an exponential $e : B \times A \to B$, we choose a homomorphism of semirings

$$\begin{array}{rcl} \varepsilon : A & \to & M_{\mathbb{P}}^{good}(\mathcal{B}) \\ y & \mapsto & \varepsilon(y) = (\varepsilon(y)_{pq})_{p,q \in \mathbb{P}}. \end{array}$$

We denote $v : x \mapsto v(x) = (v_p(x))_{p \in \mathbb{P}}$. The exponential $e = e^{\varepsilon} : B \times A \to B$ is then defined as follows:

$$\begin{aligned} e(0,0) &= 1, \\ e(0,z) &= 0, \\ e(x,y) &= v^{-1}(\varepsilon(y)v(x)), \end{aligned} \tag{2}$$

for all $0 \neq x \in B$, $y, z \in A$, $z \neq 0$, where $\varepsilon(y)v(x)$ denotes the product of matrices, calculated inside $\mathcal{B}$. The product makes sense since both $\varepsilon(y)$, $v(x)$ are good matrices in $\mathcal{B}$. Also, by Lemma 2.3, the vector $\varepsilon(y)v(x)$ is good, i.e., its non-zero part is coded in $\mathcal{B}$. Therefore $v^{-1}(\varepsilon(y)v(x))$ exists in B (note that $v^{-1}((a_p)) = \prod p^{a_p}$ for a vector $(a_p)_{p\in\mathbb{P}}$).

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

Proposition 3.1. *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 by (1) and (2), respectively, are mutual inverses and the following are equivalent:*

- *The exponential $e = e^\varepsilon : B \times A \to B$ satisfies (e1) – (e7).*
- *The map $\varepsilon = \varepsilon^e : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ is a semiring homomorphism.*

Moreover:

a) The exponential e is definable in $\mathcal{B}$ from ε and vice versa.

b) For a fixed $y \in A$, the map $x \mapsto e(x,y)$ is definable in $\mathcal{B}$ from $\varepsilon(y)$ and vice versa.

Proof. It is easy to verify the following:

- (e1) $\Leftrightarrow \varepsilon(0) = 0$
- (e2) holds by (2), and ensures the correctness of (1)
- (e3) $\Leftrightarrow \varepsilon(1) = I$
- (e4) $\Leftrightarrow \varepsilon(y+z) = \varepsilon(y) + \varepsilon(z)$
- (e5) holds by (2), its correctness follows from (e7)
- (e5) + (e6) $\Rightarrow \varepsilon(y \cdot z) = \varepsilon(y) \cdot \varepsilon(z)$:
  Proof: $\varepsilon(y\cdot z)_{pq} = v_p(e(q,yz)) = v_p(e(e(q,z),y)) = v_p(e(\prod_{r\in\mathbb{P}} r^{v_r(e(q,z))}, y)) =$
  $= v_p(\prod_{r\in\mathbb{P}} e(r,y)^{v_r(e(q,z))}) = \sum_{r\in\mathbb{P}} v_p(e(r,y)) \cdot v_r(e(q,z)) = (\varepsilon(y)\cdot\varepsilon(z))_{pq}$.
- (e6) $\Leftarrow \varepsilon(y\cdot z) = \varepsilon(y)\cdot\varepsilon(z)$
- (e7) $\Leftrightarrow \varepsilon(y)$ is a good matrix for all y:
  Proof: "$\Rightarrow$": Let $y \in A$, $J \in B$ be given, we find $I \in B$ such that conditions i) and ii) from the definition of a good matrix hold for $\varepsilon(y)$. It is enough to take $I = 1 + \max\{p \in \mathbb{P}; v_p(e(q,y)) \neq 0 \text{ for some } J > q \in \mathbb{P}\}$. This is a correct definition in $\mathcal{B}$ since the sequence $(e(q,y))_{q\in\mathbb{P}}$ is coded in $\mathcal{B}$ by (e7).
  "$\Leftarrow$": Let $y \in A$, $b \in B$ is given. Set $J = b$ and take $I \in B$ such that conditions i) and ii) from the definition of a good matrix hold for $\varepsilon(y)$. Then, in $\mathcal{B}$, we may define the sequence $(e(x,y))_{x<b}$ by the definition (2) where we use $v'(x) = (v_p(x))_{p<J}$ instead of $v(x)$ and $\varepsilon'(y) = (\varepsilon(y)_{pq})_{p<I,q<J}$ instead of $\varepsilon(y)$ (both $(v'(x))_{x<b}$ and $\varepsilon'(y)$ are coded in $\mathcal{B}$ by the assumption).
- $e^{\varepsilon^e} = e$:
  Proof: The case $x = 0$ is trivial. Suppose $x \neq 0$.
  Then $e^{\varepsilon^e}(x,y) = v^{-1}((v_p(e(q,y)))_{pq} \cdot v(x)) = v^{-1}((\sum_{q\in\mathbb{P}} v_p(e(q,y))\cdot v_q(x))_p) =$

$= \prod_{p\in\mathbb{P}} p^{\sum_{q\in\mathbb{P}} v_p(e(q,y))\cdot v_q(x)} = \prod_{q\in\mathbb{P}}(\prod_{p\in\mathbb{P}} p^{v_p(e(q,y))})^{v_q(x)} = \prod_{q\in\mathbb{P}} e(q,y)^{v_q(x)} = e(x,y)$, where we use (e5) in the last equality.

- $\varepsilon^{e^\varepsilon} = \varepsilon$:
  Proof: $\varepsilon^{e^\varepsilon}(y)_{pq} = v_p(v^{-1}(\varepsilon(y)\cdot v(q))) = (\varepsilon(y)\cdot v(q))_p = \varepsilon(y)_{pq}$.

Now, the main statement follows immediately. The "moreover" part is easy. □

Example 3.2. *a) 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 $\mathcal{B}$).*
b) Let $\mathcal{A} = \mathcal{B}$, f an automorphism of $\mathcal{B}$ and $\varepsilon(y) = f(y)I$, for $y \in B$. Then $e(x,y) = x^{f(y)}$.

In general, not much can be said about possible homomorphisms $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ and corresponding exponentials. However, in all important examples of exponentials considered in this paper we will have $\mathcal{A} \models \mathrm{Pr}$. Then more can be said:

Remark 3.3. *If A is closed under subtraction (i.e. under $a-b$ with $a \geq b$), then for $y \neq y'$ the matrices $\varepsilon(y)$, $\varepsilon(y')$ have different values everywhere on the diagonal. (Otherwise, let say $y' < y$. Then the matrix $\varepsilon(y - y' - 1)$ would contain a value $-1 \notin B$.) In particular, for such $\mathcal{A}$, the homomorphism ε is always injective.*

We then get some additional nice properties for the exponential e, such as $y > 0 \to x|e(x,y)$.

Note that we do not know of any example of homomorphism $\varepsilon : B \to M_{\mathbb{P}}^{good}(\mathcal{B})$ with non-diagonal matrices in its range. In Section 6 we show that only such homomorphisms can yield an exponential (total on B) violating FLT (see also the related Open Problem 4.9). Nevertheless, the following construction provides us with a possibility to find interesting examples of "non-diagonal" homomorphisms $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$, if $\mathcal{A} \subseteq \mathcal{B}$ is a suitable substructure.

3.4. Construction of ε

For a semiring homomorphism $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$, the values $\varepsilon(y+n)$, for $n \in \mathbb{Z}$, are uniquely determined by the value $\varepsilon(y)$. Therefore we may construct ε in the following way:
For $y, z \in A$, we define $y \sim z$ if $|y - z| \in \mathbb{N}$.
We choose:

- a $\langle 0, +, \dot{-}, \cdot\rangle$-substructure $\mathcal{O}$ of $\mathcal{A}$ (where $a \dot{-} b = a - b$ if $a \geq b$ and 0 otherwise) such that every $\sim$-factor $[y]_\sim$ of A contains a single element $O_y \in O$ (then $O_0 = 0$, $O_y + O_z = O_{y+z}$ and $O_y \cdot O_z = O_{O_y \cdot O_z}$).
- a $\langle 0, +, \dot{-}, \cdot\rangle$-homomorphism

$$\begin{aligned} \varepsilon : \mathcal{O} &\to M_{\mathbb{P}}^{good}(\mathcal{B}) \\ O_y &\mapsto \varepsilon(O_y) = (\varepsilon(O_y)_{pq})_{p,q\in\mathbb{P}}, \end{aligned}$$

  such that all elements $\varepsilon(O_y)_{pp}$ with $O_y \neq 0$ are nonstandard.

We sometimes call the elements Q of $\mathcal{O}$ "zeroes", as around each of them we have the component $\{Q + z; z \in \mathbb{Z}\}$.

Remark 3.5. *It is not always possible to choose a substructure $\mathcal{O}$ as above. In fact, it is easy to see that for $\mathcal{A} \models \mathrm{Pr}$ such a substructure exists if and only if every $\sim$-factor of A contains an element divisible by all $0 < n \in \mathbb{N}$.*

We may then define

$$\varepsilon(y) = \varepsilon(O_y) + \delta_y I, \tag{3}$$

for $y \in A$, where I is the identity matrix and $\delta_y = y - O_y$.

Lemma 3.6. *Let $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ be defined by (3). Then it is a semiring homomorphism.*

Proof. Clearly, $\varepsilon(0) = 0$ and $\varepsilon(1) = I$.

It is $\varepsilon(y+z) = \varepsilon(O_{y+z}) + \delta_{y+z} I = \varepsilon(O_y + O_z) + (\delta_y + \delta_z) I = (\varepsilon(O_y) + \delta_y I) + (\varepsilon(O_z) + \delta_z I) = \varepsilon(y) + \varepsilon(z)$.

Finally, $\varepsilon(yz) = \varepsilon((O_y + \delta_y)(O_z + \delta_z)) = \varepsilon(O_y O_z) + \varepsilon(\delta_y O_z) + \varepsilon(\delta_z O_y) + \varepsilon(\delta_y \delta_z) = \varepsilon(O_y) \cdot \varepsilon(O_z) + \delta_y \varepsilon(O_z) + \delta_z \varepsilon(O_y) + \delta_y \delta_z I = (\varepsilon(O_y) + \delta_y I) \cdot (\varepsilon(O_z) + \delta_z I) = \varepsilon(y) \cdot \varepsilon(z)$. (For the sake of clarity, we harmlessly abused the notation a bit by writing $\varepsilon(\delta_y O_y)$ even for $\delta_y < 0$.) □

Remark 3.7. *The construction may be further generalized by changing the definition of the equivalence $\sim$. We may define $y \sim z$ if $|y - z| \in D$ where $\mathcal{D}$ is an initial segment of $\mathcal{B}$ and a substructure of $\mathcal{A}$. Then the notion of homomorphism has to be modified to "preserve $\mathcal{D}$".*

4. Violation of FLT

We show that Fermat's Last Theorem for e: "$e(a,n) + e(b,n) = e(c,n)$ has no non-zero solution for $n > 2$", is not provable in the L^e-theory $Th(\mathbb{N}) + Exp$, where $L^e = \langle 0, 1, +, \cdot, e, \leq \rangle$ and Exp consists of the following axioms:

(e0) "$e : B \times A \to B$ for some substructure $\mathcal{A}$ of $\mathcal{B}$ with $\mathcal{A} \models \mathrm{Pr}$",
axioms (e1) – (e7) from Section 3.

(Here (e0) is an axiom schema with infinitely many instances expressing validity of the schema (Pr8) in $\mathcal{A}$.)

More precisely: For any nonstandard $\mathcal{B} \models Th(\mathbb{N})$, we construct an exponential $e : B \times A \to B$ with $\langle \mathcal{B}, e \rangle \models Exp$ such that there is an unbounded (in $\mathcal{B}$) set $E \subseteq A$ of exponents and (in every coordinate) unbounded set $T \subseteq A^3$ of pairwise linearly independent triples such that for every $n \in E$ and $(a,b,c) \in T$ it is

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

Moreover, we ensure that A is closed under e. Hence $\langle \mathcal{A}, e \rangle \models \mathrm{Pr}$ + "all open formulas true in $\langle \mathcal{B}, e \rangle$" + "$e$ is total", and Fermat's Last Theorem for e is violated in $\langle \mathcal{A}, e \rangle$ by cofinally many exponents n and pairwise linearly independent triples of a, b, c.

To first outline the idea, take $\mathcal{B} \models \mathrm{I}\Sigma_1$. To specify the substructure $\mathcal{A}$, we just need to choose a set of "zeroes" O as in Section 3.4. Our zeroes will be a suitable subset of $\{Q; n|Q$ for all $0 < n \in \mathbb{N}\}$ (see Section 4.2) and A will then consist of elements of the form $Q + z$ for some $Q \in O$ and $z \in \mathbb{Z}$. Such an $\mathcal{A}$ will then be a model of Presburger arithmetic (Lemma 4.3).

We then define the matrices $\varepsilon(Q)$ for $Q \in O$ in such a way that $e(2, Q) = e(3, Q) = e(5, Q)$ for $Q \in O$. Then we get $e(2, Q+1)+e(3, Q+1) = 2e(2, Q)+3e(3, Q) = 5e(5, Q) = e(5, Q + 1)$, and so $(2, 3, 5)$ is a counterexample to Fermat's Last Theorem.

This works for any model $\mathcal{B}$ of $\mathrm{I}\Sigma_1$ with essentially the same proofs as in the rest of this Section. To obtain the result for an unbounded set of triples (a, b, c), we shall assume that $\mathcal{B}$ is a model of $Th(\mathbb{N})$, so that we can use the following number-theoretic result, due to Balog [Bal92]:

Lemma 4.1. *For each $K \in \mathbb{N}$, the equation $3p+5q = 2r$ has a solution in primes $p, q, r \in \mathbb{N}$ such that $p, q, r \geq K$.*

Proof. The lemma follows by an application of the main theorem of [Bal92, p. 369]. The matrix $(3, 5, -2)$ is admissible in Balog's sense and satisfies the local solvability conditions (for (C1) choose $3 \cdot 1+5 \cdot 1-2 \cdot 4 = 0$, for (C2) we can choose $3 \cdot (-1)+5 \cdot 1-2 \cdot 1 = 0$, which works for any prime power). Thus the theorem applies in this situation and we know that for sufficiently large X, the number of prime solutions with $p, q, r < X$ is at least $\frac{X^2}{(logX)^3}$.

Now fix K. We can assume for contradiction that in each prime solution of $3p+5q-2r = 0$, at least one of the variables is $< K$. Choose X sufficiently large and let's count the solutions with $p, q, r < X$. For solutions with $p < K$ we have at most K possibilities for p and X possibilities for q. r is then uniquely determined, and so there are at most KX of these solutions. Similarly we have at most KX solutions with $q < K$ and with $r < K$. Hence there are at most $3KX < \frac{X^2}{(logX)^3}$ solutions of the equation, which is a contradiction. □

4.2. Construction

Let $\mathcal{B} \models Th(\mathbb{N})$ be nonstandard. Fix a nonstandard number Δ from $\mathcal{B}$ and denote by P the 2^{Δ}-th prime of $\mathcal{B}$.

By Lemma 4.1 there is an unbounded (in every coordinate) set $S \subseteq B^3$ of pairwise disjoint triples of primes p, q, r such that $3p + 5q = 2r$ and $p, q, r > P$.

We may assume that S is definable in $\mathcal{B}$ (e.g. we take the lexicographic order of B^3 and define S recursively by adding, in each step, the least solution p, q, r disjoint with all previously added.)

We define $\mathcal{A}$ to be the substructure of $\mathcal{B}$ with the universe $A = \{Q + z; z \in \mathbb{Z}$ and $n|Q$, $2^{n\Delta}|Q$ for all $0 < n \in \mathbb{N}\}$ (i.e., A is the union of $\sim$-factors of $\mathcal{B}$ which contain an element divisible by all $n > 0$ and $2^{n\Delta}$ with $0 < n \in \mathbb{N}$).

It is fairly straightforward to check that $\mathcal{A}$ is a model of Presburger arithmetic.

Lemma 4.3. $\mathcal{A} \models \mathrm{Pr}$.

Proof. One directly checks the axioms (Pr1) – (Pr8). The only not entirely trivial one is (Pr8):

Take $x \in A$ and $0 < n \in \mathbb{N}$. Then by the construction we have $x = Q + z$ with $n|Q$ and $z \in \mathbb{Z}$. Thus $Q = na$ and it's easy to see that $a \in A$ as well. If we now write $z = nb + c$, $0 \leq c < n$, we get $x = n(a + b) + c$ as needed. (It is exactly for this argument to work that we require each "zero" Q to be divisible by all $0 < n \in \mathbb{N}$.) □

Let us also note that $\mathcal{A}$ contains unboundedly many primes: Fix an element Q such that $n|Q$ and $2^{n\Delta}|Q$ for all $0 < n \in \mathbb{N}$. By Dirichlet's Theorem on primes in arithmetic progressions (which holds not only in $Th(\mathbb{N})$, but even for any model of PA thanks to an elementary proof by Selberg), $\mathcal{B}$ contains unboundedly many primes of the form $aQ + 1$. Each of these primes in fact lies in $\mathcal{A}$ by definition. Note that if we assume Dickson's conjecture (which is of course quite strong and far from being proved), $\mathcal{A}$ contains an unbounded set of twin primes of the form $aQ - 1$, $aQ + 1$.

However, the model $\mathcal{A}$ is very weak in terms of induction – it is not even a model of IOpen. Indeed, let Q be again an element such that $n|Q$ and $2^{n\Delta}|Q$ for all $0 < n \in \mathbb{N}$, and let $b \in B$, $b \notin A$. Then $Q, Qb \in A$, but the induction axiom for the open formula $Qx \leq Qb$ does not hold in $\mathcal{A}$. (See also Open Problem 4.9.)

Further, unless stated otherwise, we work in $\mathcal{B}$.

Let us now construct the homomorphism ε as in Section 3.4. For $y \in A$, we set O_y to be the unique element in $[y]_\sim$ divisible by all n and $2^{n\Delta}$ with $0 < n \in \mathbb{N}$. Clearly, the set $O = \{O_y; y \in A\}$ is a $\langle 0, +, \dot{-}, \cdot \rangle$-substructure of $\mathcal{A}$. (Moreover, O is closed under multiplication by any element $b \in B$.)

For $Q \in O$ we define $\varepsilon(Q) = (\varepsilon(Q)_{pq})$ as

$$\begin{array}{lcll} \varepsilon(Q)_{pq} & = & Q/2^\Delta & \text{for } p, q \leq P, \\ \varepsilon(Q)_{pq} & = & Q/3 & \text{if } p, q \text{ are members of the same triple } s \in S \\ & & & \text{(allowing } p = q \text{ lying in some triple in } S), \\ \varepsilon(Q)_{pq} & = & Q & \text{for } p = q > P \text{ and } p \text{ in no triple } s \in S, \\ \varepsilon(Q)_{pq} & = & 0 & \text{otherwise.} \end{array}$$

Lemma 4.4. *$\varepsilon : Q \mapsto \varepsilon(Q)$ is a $\langle 0, +, \dot{-}, \cdot \rangle$-homomorphism (even an embedding) from $\mathcal{O}$ to $M_{\mathbb{P}}^{good}(\mathcal{B})$.*

Proof. To check that ε is a homomorphism is easy. All the computations are similar, so as an example, let us just check that the matrices $\varepsilon(QR)$ and $\varepsilon(Q)\varepsilon(R)$ have the same entries at (p, q) with $(p, q, r) \in S$ for some r. We have $(\varepsilon(Q)\varepsilon(R))_{pq} = \sum_j \varepsilon(Q)_{pj}\varepsilon(R)_{jq}$. Since $\varepsilon(Q)_{pj} \neq 0$ only for $j = p, q$, or r, we have $(\varepsilon(Q)\varepsilon(R))_{pq} = \varepsilon(Q)_{pp}\varepsilon(R)_{pq} + \varepsilon(Q)_{pq}\varepsilon(R)_{qq} + \varepsilon(Q)_{pr}\varepsilon(R)_{rq} = 3 \cdot (Q/3) \cdot (R/3) = QR/3 = \varepsilon(QR)_{pq}$.

We also need to check that $\varepsilon(Q) \in M_{\mathbb{P}}^{good}(\mathcal{B})$ for every Q. Thanks to the definability of the set S in $\mathcal{B}$, $\varepsilon(Q)$ is even definable in $\mathcal{B}$ (and obviously there is a definable function $f(q)$ such that all non-zero elements of the q-th column are in the rows p with $p \leq f(q)$). This is clearly enough since $\mathcal{B} \models Th(\mathbb{N})$ codes all finite parts of definable sets. □

By Lemma 3.6 we get a semiring homomorphism $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ and by definition (2) and Proposition 3.1 we obtain an exponential $e : B \times A \to B$ which satisfies the axioms Exp.

Let us note that for fixed y the exponential $e(x, y)$ is a definable function of x in $\mathcal{B}$ (this follows from Proposition 3.1 and from the definability of S). Moreover, using the new predicate $\mathcal{N}(x)$ expressing "x is a standard number", both the set A and the function $y \mapsto O_y$ are definable. Hence, by Proposition 3.1 again, e is definable in $\langle \mathcal{B}, \mathcal{N} \rangle$.

Now we can show that e is a total exponential on A, i.e.,

Lemma 4.5. $e \restriction A \times A : A \times A \to A$.

Proof. Let $x, y \in A$, we want to prove $e(x, y) \in A$. Write $y = Q + \delta$ with $Q \in O$ and $\delta \in \mathbb{Z}$. It suffices to show that $e(x, Q) \in A$, for then $e(x, y) = e(x, Q) \cdot x^{\delta}$ lies also in A. Also, we may further suppose that $Q \neq 0$. Let us now distinguish two cases:
a) x is divisible by some $p \leq P$:
Then $e(x, Q) = e(p, Q) \cdot \alpha$ for some $\alpha \in B$ and $e(p, Q) = \prod_{P \geq q \in \mathbb{P}} q^{Q/2^{\Delta}}$ and for $0 < n \in \mathbb{N}$ clearly both n and $2^{n\Delta}$ divide $e(p, Q)$. Therefore $e(x, Q) \in O \subseteq A$.

b) x is not divisible by any $p \leq P$:
By the definition of $\varepsilon(Q)$ and e, in this case also $e(x, Q)$ will not be divisible by any $p \leq P$. Since all the entries of $\varepsilon(Q)$ at positions (p, q) with $p, q > P$ are divisible by $Q/3$, we see that $e(x, Q) = \alpha^{Q/3}$ with $\alpha \in B$ not divisible by any $p \leq P$.

Now note that $\phi(m)$ divides Q/k (here ϕ is Euler's totient function) for every $0 < m \in \mathbb{N}$ or $m = 2^{n\Delta}$. Since α and m are co-prime, we get $\alpha^{Q/3} \equiv 1 \mod m$ and hence $\alpha^{Q/3} - 1 \in O$. Thus $e(x, Q) = \alpha^{Q/3} \in A$. □

From now on denote $e \restriction A \times A$ just by e.

Remark 4.6. *Before discussing Fermat's Last Theorem, observe that various usual elementary number-theoretic statements are not valid with the new exponential e, for example Fermat's Little Theorem: Fix $Q \in O$, choose a prime $p = aQ - 1 > P$ and consider $e(2, p-1)$. By the definition of e we have*

$$4e(2, p-1) = e(2, p+1) = e(2, aQ) = N^{aQ/2^{\Delta}},$$

where $N = \prod_{q \leq P} q$ is the product of all primes q smaller than our fixed non-standard prime P. Hence

$$(4e(2, p-1))^{2^{\Delta}} = N^{aQ} = N^{p+1} \equiv N^2 \pmod{p}$$

by usual Fermat's Little Theorem in $\mathcal{B}$. If Fermat's Little Theorem held for e, we would have $e(2, p-1) \equiv 1 \pmod{p}$, and so

$$4^{2^{\Delta}} \equiv N^2 \pmod{p},$$

i.e., $p | 4^{2^{\Delta}} - N^2$. There are only finitely many (in the sense of $\mathcal{B}$) such primes p, but infinitely many primes in the arithmetic progression $aQ - 1$, a contradiction.

Let us now finish the construction of our counterexamples to Fermat's Last Theorem.

Lemma 4.7. *For every $Q, R \in O$ and every triple $(p, q, r) \in S$ we have*

$$e(R \cdot 3p, Q + 1) + e(R \cdot 5q, Q + 1) = e(R \cdot 2r, Q + 1).$$

Proof. Note that $e(2, Q) = e(3, Q) = e(5, Q)$ and $e(p, Q) = e(q, Q) = e(r, Q) = (pqr)^{Q/3}$. Thus we have $e(R \cdot 3p, Q) = e(R \cdot 5q, Q) = e(R \cdot 2r, Q) = e(R, Q) \cdot e(2, Q) \cdot (pqr)^{Q/3} =: K$. Then $e(R \cdot 3p, Q + 1) = 3pKR$, $e(R \cdot 5q, Q + 1) = 5qKR$, and $e(R \cdot 2r, Q + 1) = 2rKR$ and the Lemma follows from $3p + 5q = 2r$. □

Let us note that while p, q, r may not be in A, $R \cdot 3p$, $R \cdot 5q$, $R \cdot 2r$ certainly are in A.

We summarize our observations as the following:

Theorem 4.8.

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 $\langle \mathcal{B}, e\rangle$.)*

To construct e, we used the method described in Section 3.4. Then, necessarily, by Remark 3.5, $A \neq B$, i.e., e is not total on $\mathcal{B}$. In general, it is possible to construct a total e by producing a homomorphism $\varepsilon : B \to M_{\mathbb{P}}^{good}(\mathcal{B})$ in a way different from the method of Section 3.4 (e.g., see Example 3.2). However, ensuring that Fermat's Last Theorem for e does not hold in the resulting expansion $\langle \mathcal{B}, e\rangle$, seems to be a harder question.

Open Problem 4.9. *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 $S = Th(\mathbb{N})$?*

Let us note that the problem above makes sense only for sufficiently strong theories S, since two of the axioms from Exp ((e5) and (e7)) use coding in their formulations. However, if we remove (e7) and replace (e5) with its finite version (e5'), then part 2) of Theorem 4.8 gives the positive answer for $S =$ Pr + "all open formulas true in the standard model $\mathbb{N}$".

5. Catalan Conjecture

We show that, unlike the Fermat's Last Theorem, the Catalan Conjecture for e ("the only solution of $e(a, n) - e(b, m) = 1$ with $a, b, m, n > 1$ is $a = m = 3$, $b = n = 2$") is

provable in $Th(\mathbb{N}) + Exp$. It follows that $\langle \mathcal{B}, e\rangle$ and $\langle \mathcal{A}, e\rangle$ from Theorem 4.8 are examples of models where FLT for e does not hold but Catalan Conjecture for e does.

In fact, we can show something slightly stronger, as we need only the axioms (e0) – (e4) for the exponential function (we denote this set of axioms Exp') and we can allow weaker theories than $Th(\mathbb{N})$. We mainly need that ABC and Catalan Conjectures (for the "original", definable exponential) hold in our theory.

To briefly review the statement of the ABC Conjecture, let $\mathcal{B}$ be a model of $I\Sigma_1$. Then every element a of $\mathcal{B}$ has a unique prime factorization and we can define its radical $\mathrm{rad}(a)$ as the product of all primes dividing a (discounting multiplicities, i.e., $\mathrm{rad}(24) = 6$). One of the formulations of the ABC Conjecture is:

Conjecture 5.1 (ABC Conjecture)**.** *For every $\varepsilon > 0$ there is K_ε such that for all coprime a, b, c with $a + b = c$ we have $c < K_\varepsilon \mathrm{rad}(abc)^{1+\varepsilon}$.*

Let us note that Mochizuki has recently announced a proof in the standard model [Moc12].

In the rest of this Section, let S be a theory (in the language of arithmetic $\langle 0, 1, +, \cdot, \leq\rangle$) stronger than $I\Sigma_1$ such that, for some $K \in \mathbb{N}$, S proves ("a, b, c coprime" $\& \, a + b = c) \to c < K\mathrm{rad}(abc)^{1+1/3}$, 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 may also conjecture that PA satisfies the property above and take $S =$PA.)

We prove the following:

Theorem 5.2. *Let S be as above. Catalan Conjecture for e is provable in $S + Exp'$.*

Let $\langle \mathcal{B}, e\rangle$ be an arbitrary model of $S + Exp'$ and $\mathcal{A} \models \mathrm{Pr}$ be a substructure of $\mathcal{B}$ such that $e : B \times A \to B$. Since we are working with the weaker set of axioms Exp', the exponential need not be given using the Proposition 3.1 nor the construction from Section 3.4. However, we still have the following Lemma.

Lemma 5.3. *Let $1 < x, y \in A$.*
a) If y is standard, then $\mathrm{rad}(e(x, y))^2 \leq e(x, y)$.
b) If y is non-standard, then $K\mathrm{rad}(e(x, y))^n < e(x, y)$ for all standard K, n.

Proof. a) If y is standard, then $e(x, y) = x^y$ by (e3) and (e4). Hence $\mathrm{rad}(e(x, y))^2 \leq x^2 \leq x^y$.

b) Assume that y is non-standard and fix standard K, n. Since $\mathcal{A} \models \mathrm{Pr}$ and y is non-standard, we can write $y = n + a$ with $a \in A$ non-standard, and then $a = (n + 1)b + m$ with $b \in A$, $0 \leq m \leq n$ (by (Pr8)).

We then have $e(x, y) = e(x, n + m + (n + 1)b) = x^{n+m} e(x, b)^{n+1}$, and so $\mathrm{rad}(e(x, y)) \leq \mathrm{rad}(x)\mathrm{rad}(e(x, b)) \leq xe(x, b)$. Thus $K\mathrm{rad}(e(x, y))^n \leq Kx^n e(x, b)^n \leq x^n e(x, b)^{n+1} \leq x^{n+m} e(x, b)^{n+1} = e(x, y)$ (we have used that $K \leq e(x, b)$ for $x > 1$ and b non-standard, which follows from (e3) and (e4)). □

Proposition 5.4. *Catalan conjecture for e holds in $\langle \mathcal{B}, e\rangle$.*

Proof. Assume that $e(x,a) - e(y,b) = 1$, where $x, y, a, b > 1$. We distinguish several cases according to a, b.

1) If a, b are both standard then this is just the Catalan conjecture in $\mathcal{B}$.

2) Assume a is non-standard. By the ABC for $\varepsilon = 1/3$ (which is provable in S) we have $e(x,a) < K\mathrm{rad}(e(x,a)e(y,b))^{1+\varepsilon}$, and so using Lemma 5.3 we have (note that $3 + 3\varepsilon = 4$)

$$e(x,a)e(y,b)^2 < e(x,a)^3 < K^3\mathrm{rad}(e(x,a)e(y,b))^{3+3\varepsilon} \leq$$
$$\leq (K^3\mathrm{rad}(e(x,a))^4)\mathrm{rad}(e(y,b))^4 < e(x,a)e(y,b)^2,$$

a contradiction.

Let us note that to show $\mathrm{rad}(e(y,b))^4 < e(y,b)^2$ (in the last inequality), we use Lemma 5.3 a) if b is standard, or b) otherwise.

3) The case of b non-standard is analogous – we only need to start from $e(x,a)^2e(y,b)$ instead of $e(x,a)e(y,b)^2$. □

This proves Theorem 5.2.

6. Coprimality

One may naturally wonder what causes the difference between the validity of Fermat's Last Theorem and Catalan Conjecture and how is it possible that Catalan Conjecture holds even with our weak exponential. It appears to us that the main number-theoretic weakness of the exponential is the fact that for coprime x and y, the values $e(x,a)$ and $e(y,b)$ need not be coprime. In fact, we have crucially exploited this in the construction of our counterexamples to Fermat's Last Theorem in Section 4.2. However, this does not play any role when considering Catalan Conjecture, as $e(x,a) - e(y,b) = 1$ immediately forces $e(x,a)$ and $e(y,b)$ to be coprime (and then we can apply ABC Conjecture).

Let us thus consider the following additional axiom for the exponential e:

(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 – but as Example 3.2 shows, the exponential can still be different from the usual one.

In fact, such "diagonal" homomorphisms $\varepsilon : A \to M_{\mathbb{P}}^{good}(\mathcal{B})$ are exactly homomorphisms of the form $\varepsilon(a) = diag(f_p(a); p \in \mathbb{P})$, where $f_p : A \to B$ are homomorphisms and $diag$ denotes the diagonal matrix. Hence there are $|\mathrm{Hom}(\mathcal{A},\mathcal{B})|^\omega$ exponentials satisfying $Exp+$ (e8), namely those given as $e_f(\prod_i p_i^{e_i}, a) = \prod_i p_i^{e_i f_{p_i}(a)}$ with $f = (f_p; p \in \mathbb{P})$ homomorphisms from $\mathcal{A}$ to $\mathcal{B}$. (If A is closed under subtraction, then by Remark 3.3 all homomorphisms f_p are necessarily injective.)

Note that (e8) is still much weaker than induction for e. Indeed, only the usual exponential x^y satisfies induction: if some exponential e satisfied induction (Σ_1-induction would be enough), it would be total, and we could use the induction to prove that $e(x,y) = x^y$ for all y.

Then we have a direct analogue of Theorem 5.2: 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" $\& \, a+b=c) \to c < K\mathrm{rad}(abc)^{1+\varepsilon}$, and the Fermat's Last Theorem (using the exponential x^y definable in T). We may again take $T = Th(\mathbb{N})$.

Theorem 6.1. *Let T be a theory as above. Fermat's Last Theorem for e is provable in $T + Exp' +$ (e5′) + (e8).*

Let us recall that Exp' denotes the axioms (e0) – (e4).

Proof. The proof is analogous to that of Theorem 5.2, in fact it is a little easier:

Assume that $e(x,n) + e(y,n) = e(z,n)$. First we use (e5′) to divide the equation by $e(g,n)$, where g is the greatest common divisor of x, y, z. Thus we can restrict ourselves to the situation with x, y, z coprime. Hence also $e(x,n), e(y,n)$ and $e(z,n)$ are mutually coprime by (e8).

By the usual Fermat's Last Theorem we can also assume that n is non-standard. By the ABC Conjecture and Lemma 5.3 b) we have

$$e(z,n) < K\mathrm{rad}(e(x,n)e(y,n)e(z,n))^{1+\varepsilon} \leq K\left[\mathrm{rad}(e(x,n))\mathrm{rad}(e(y,n))\mathrm{rad}(e(z,n))\right]^{1+\varepsilon} \leq$$

$$\leq (e(x,n)e(y,n)e(z,n))^{1/3} < e(z,n),$$

a contradiction. □

Theorem 6.1 seems to suggest that (at the very least in the class of models we are considering) full mathematical induction for the exponential function is not necessary to prove Fermat's Last Theorem (and Catalan conjecture), but rather that it suffices to have one particular consequence of it, namely the coprimality property (e8).

We find very interesting the question whether there is a model $\langle \mathcal{B}, e \rangle \models Th(\mathbb{N}) + Exp$ with e total where FLT for e does not hold (see Open Problem 4.9). In the light of Theorem 6.1 we now see that such e would have to be given by a "non-diagonal" $\varepsilon : B \to M_{\mathbb{P}}^{good}(\mathcal{B})$. We therefore state the following

Open Problem 6.2. *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?*

References

[Avi03] J. Avigad, *Number theory and elementary arithmetic*, Philosophia Mathematica **11** (2003), 257–284.

[Bal92] A. Balog, *Linear equations in primes*, Mathematika **39** (1992), no. 2, 367–378.

[Fri99] H. Friedman, *Grand conjectures*, http://cs.nyu.edu/pipermail/fom/1999-April/003014.html, 1999, posted on Foundations of mathematics e-mail list, 16. 4. 1999.

[HP93] P. Hájek and P. Pudlák, *Metamathematics of first order arithmetic*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1993.

[Koł11] L. A. Kołodziejczyk, *Independence results for variants of sharply bounded induction*, Ann. Pure Appl. Logic **162** (2011), 981–990.

[Mac11] A. Macintyre, *The impact of Gödel's incompleteness theorems on mathematics*, Kurt Gödel and the Foundations of Mathematics: Horizons of Truth (M. Baaz, Ch. H. Papadimitriou, H. W. Putnam, D. S. Scott, and Ch. L. Harper, Jr., eds.), Cambridge University Press, Cambridge, 2011.

[McL10] C. McLarty, *What does it take to prove Fermat's Last Theorem? Grothendieck and the logic of number theory*, Bull. Symbolic Logic **16** (2010), 359–377.

[McL11] ———, *The large structures of Grothendieck founded on finite order arithmetic*, arXiv:1102.1773v4 (2011).

[McL12] ———, *Zariski cohomology in second order arithmetic*, arXiv:1207.0276v2 (2012).

[Mih04] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[Mlč76] J. Mlček, *Twin prime problem in an arithmetic without induction*, Comment. Math. Univ. Carolinae **17** (1976), 543–555.

[Moc12] S. Mochizuki, *Inter-universal Teichmuller Theory I – IV*, http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html, 2012.

[She64] J. C. Shepherdson, *A nonstandard model for a free variable fragment of number theory*, Bull. 1'Acad. Pol. Sci. **12** (1964), 79–86.

[Smi92] S. T. Smith, *Fermat's last theorem and Bezout's theorem in GCD domains*, J. Pure Appl. Alg. **79** (1992), 63–85.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Petr Glivický: Charles University, Faculty of Mathematics and Physics, Department of Theoretical Computer Science and Mathematical Logic, Malostranské náměstí 12, 118 00 Praha 1, Czech Republic

: Academy of Sciences of the Czech Republic, Institute of Mathematics, Žitná 25, 115 67 Praha 1, Czech Republic

E-mail address: glivicky@math.cas.cz

Vítězslav Kala: Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 00 Praha 8, Czech Republic

: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany

E-mail address: vita.kala@gmail.com