On new interactions between quantum theories and arithmetic geometry

Ivan Fesenko

Abstract One of the aims of this paper is to attract the attention of quantum theorists to certain areas of arithmetic geometry whose ideas and concepts and analogues of objects may find applications in quantum physics. Proposing or drawing these interdisciplinary links is novel and may open up new research directions. We discuss several analogies between some developments in arithmetic geometry, once stemming from Grothendieck and now including the IUT theory of Mochizuki, and some aspects of quantum theory including quantum computing. These analogies were spotted recently and it is hoped that related developments may be fruitful.

In the appendix we also propose a new abc-ABC question about an asymptotic symmetry of the moduli space of Frey–Hellegouarch elliptic curves over rational numbers. This question goes beyond the standard abc inequalities conjectures/questions. We prove that the positive answer to the question and the effective abc-inequalities established in [27] using enhanced IUT theory imply the stronger version of the effective $(1+\varepsilon)$-abc inequality.

Key words: topos theory, non-Boolean logic, étale fundamental group, group theoretic algorithms, algorithmic anabelian geometry, IUT theory, abc inequalities, effective abc inequalities, elliptic curves over rational numbers, improved foundations of quantum mechanics, quantum computing, stabiliser formalism in quantum computing.

Introduction

Quantum theory in its standard formulation uses mathematics mostly known at the time of its creation, i.e. 100–60 years ago. Serious foundational problems and paradoxes of quantum theory affect its further developments and applications, including quantum computing and communication. It is reasonable to expect that the use of modern mathematics to produce mathematically improved versions of quantum theory may lead to the resolution of those foundational problems.

There is huge potential for utilising concepts and visions of modern arithmetic geometry in developments of quantum theory including quantum computing. The following examples will serve as a partial evidence for this opinion. In order to develop implications of these analogies, we need researchers with expertise in quantum theories and in anabelian geometry and IUT.

In sections 1–3 we discuss, using a simple language in order not to frighten potential readers, analogies between some ideas and concepts in arithmetic geometry whose applications in quantum theory may be fruitful. Most of these analogies are not mentioned in the published literature. The author expresses his gratitude to E. Demler, N. Gisin, A. Lvovsky, I. Martin, A. Ustyuzhanin for interesting quantum discussions, to S. Mochizuki for numerous discussions of the IUT theory, and to the referee for valuable suggestions.

In the appendix we propose, using very simple mathematics, new questions about an asymptotic symmetry of the moduli space of Frey–Hellegouarch elliptic curves over rational numbers. These questions are motivated by the study of options to derive stronger effective abc-type inequalities from the already established ones. No knowledge of anabelian geometry or the IUT theory is assumed.

1 Topos-theoretical approach to quantum theory

Non-locality and contextuality (Bell, Kochen–Specker) in quantum mechanics may help obtain quantum advantage over classical computational models in quantum computing. This is closely related to the use of non-Boolean logic in quantum theory.

The notion of topos was introduced in the early sixties by Grothendieck with the original first aim of bringing a topological or geometric intuition in parts of number theory where actual topological spaces do not occur [20], [15]. Grothendieck realised that many important properties of topological spaces X can be naturally formulated as properties of the categories $\mathrm{Sh}(X)$ of sheaves of sets on the spaces. It is important that the map $X \longrightarrow \mathrm{Sh}(X)$ is an embedding of continuous structures into categories which are discrete structures. The crucial unifying notion of topos is to provide the common geometric intuition for many areas of mathematics and to connect continuous with discrete. See the talk of L. Lafforgue [19] for more mathematical and historical details.

A topos has various features similar to the category of sets. Somehow similar to quantisation of a classical physical theory, constructions in topos theory can often be understood by looking at them first in the category of sets or geometrical categories and then lifting to the general case.

However, unlike sets, the law of excluded middle does not need to hold in a topos. Toposes incorporate non-Boolean logic in an organic way. A topos has an internal logical structure that is similar to the way in which Boolean algebra arises in set theory, but instead of two truth values 1 and 0, goes outside Boolean logic with truth values are in a larger set. Topos theory is a math theory that can 'speak' of indeterminism. It may also address the issue of 'real numbers are not real for physicists', mentioned in the papers and talks of Gisin [3], [15].

Isham, Döring and others proposed a partial reformulation of quantum theory in terms of topos theory [17], [18], [4], [5], [6], [7], [8], [9], [12], [13]. The reason for their choice of topos theory is that the latter in the first approximation looks like sets theory and is equipped with an internal logic. Their topos theoretical approach to quantum theory builds locally on the topos of presheaves of commutative (hence classical) sub-algebras of the algebra of all bounded operators on the quantum theory's Hilbert space. This reformulation in several aspects looks like classical physics, propositions can be given truth values without using concepts of measurement or external observer, using the internal non-Boolean logic of appropriate toposes. The non-existence of classical explanations for quantum phenomena can be viewed as corresponding to the non-existence of global points or sections of certain toposes.

2 Etale fundamental group, section conjecture and stabiliser formalism in quantum computing

No quantities show up in category theory and topos theory. What matters is the form of a category and its structure. The notion of a geometric morphism in topos theory has allowed to build general cohomology theories which cannot be otherwise produced. The first example was étale cohomology theory. The Grothendieck definitions of étale sites, étale fundamental group and étale cohomology use toposes.

For any geometrically integral (quasi-compact) scheme X over a perfect field k one has its étale fundamental group $\pi_1(X)$. For example, if C is a complex irreducible smooth projective curve minus a finite set of its points, over an algebraically closed field of characteristic 0, then $\pi_1(C)$ is isomorphic to the profinite completion of the topological fundamental group of the Riemann surface associated to C.

A hyperbolic curve C over a field k of characteristic zero is a smooth projective geometrically connected curve of genus g minus r points such that the Euler characteristic $2-2g-r$ is negative. The étale fundamental group of a hyperbolic curve is highly (in appropriate strict mathematical sense) nonabelian, its centre is trivial. Grothendieck asked a famous questions whether hyperbolic curves over number fields are anabelian, i.e. whether one can restore the curve from its étale fundamental group. A partial positive answer was obtained by Tamagawa [29] and the full positive answer was obtained by S. Mochizuki [21], [22], [23]. This was the foundation of anabelian geometry of hyperbolic curves over number fields and their non-archimedean completions. Most of the further development of this anabelian geometry in the last 30 years has not been digested by mathematicians outside Japan.

A point x in $X(k)$ for a field k, i.e. a morphism $\mathrm{Spec}(k) \longrightarrow X$, determines, in a functorial way, a continuous section from the absolute Galois group G_k of k to $\pi_1(X)$, well-defined up to composition with an inner automorphism, of the surjective map $\pi_1(X) \longrightarrow G_k$. Grothendieck's section conjecture asks whether, for a geometrically connected smooth projective curve X over k, of genus > 1, the map from rational points $X(k)$ to the set of conjugacy classes of sections, $x \mapsto D_x = \mathrm{Stab}(x)$, is surjective. Injectivity was already known. Various other similar conjectures, such as a combinatorial section conjecture, were established by Mochizuki and his collaborators. There are forthcoming discoveries of relations of the section conjecture to some fundamenal open problems in number theory.

One of the key issues for quantum algorithms is whether they can run in polynomial time, instead of exponential time. Controlling loss of information/error correction is crucial. In quantum error correction one uses stabiliser groups in finite dimensional complex spaces.

A map
$$s \mapsto D_s$$
from quantum states s in a $2n$-dimensional vector space over $\mathbb{C}$ to their stabiliser group D_s (unitary matrices acting trivially on s) is injective. However, D_s has too many generators, about 4^n.

Gottesman, Aaronson–Gottesman [1] considered the intersection $D_s \cap P_n$ where P_n is the group of n-qubit Pauli operators: all tensor products of matrices
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$
and their scalar products with roots of order 4. The number of elements of P_n is 4^{n+1}. This intersection $D_s \cap P_n$ has a much smaller number of generators than D_s.

It is easy to show that on the subset of quantum states that are stabilised by exactly 2^n elements of P_n the map
$$s \mapsto D_s \cap P_n$$
is still injective, [1]. This subset is further characterised as obtained from $|0\rangle^{\otimes n}$ by CNOT, Hadamard, and phase gates only.

Recently, Hoshi, Mochizuki and Tsujimura obtained results about the injectivity of the section map
$$x \mapsto D_x \cap G_L$$
from closed points x of hyperbolic curves over number fields to (conjugacy classes of) the intersection of their stabiliser groups (decomposition groups) with the absolute Galois group of various infinite extensions L of the number field k, [16]. Notice the similarity with the injectivity of the map $s \mapsto D_s \cap P_n$ in quantum stabiliser theory.

Note that the variety of decomposition groups and absolute Galois groups in number theory is much larger than the Clifford group (the group of unitary matrices that normalise P_n) and P_n in quantum computing. One perspective is to investigate whether analogues of the decomposition groups and absolute Galois groups in arithmetic geometry may provide new classes of groups useful for quantum computing and lead to new computational models. This may help to go beyond the Clifford ground in quantum computing, an important task indicated by the experts.

At the same time, there is a substantial difference between profinite decomposition groups and discrete stabiliser groups in quantum computing: the centre of the former is trivial while the centre of Clifford group is infinite but the quotient group by its centre is finite. However, when one works with those arithmetic stabiliser groups, one often considers them as the projective limit of their quotients which are extensions of a finite group by an infinite abelian group and such quotients modulo their centre are finite groups.

3 On some similarities between IUT and quantum theory

Algebraic geometry involves locally the correspondence between affine varieties and commutative rings with two algebraic operations. Anabelian geometry for hyperbolic curves over number fields and other fields is a correspondence between these geometric objects and their arithmetic fundamental groups (or slightly more complicated objects). Fundamental groups are non-commutative, but they have one algebraic operation, not two. This opens the perspective to try to perform deformations of these geometric objects not seen by algebraic geometry, using the fact that there are more maps, group homomorphisms and variations of those between topological groups in comparison to ring homomorphisms between commutative rings.

The IUT theory, discovered by Mochizuki, provides, for certain hyperbolic curves (e.g. an elliptic curve minus a point), a new fundamental understanding of how to bound from above the deviation from commutativity of certain crucial diagrams associated to arithmetic deformation aspects of IUT. IUT is a new arithmetic deformation theory that is entirely unavailable in the standard arithmetic geometry dealing with ring structures. IUT is a non-linear algorithmic theory which addresses such fundamental aspects as to which extent the multiplication and addition on integers (or rings of algebraic integers) cannot be separated from one another. Arithmetic deformations in IUT are not compatible with ring structure. Deformations are coded in certain links, ring structures do not pass through the links, groups of symmetries such as Galois and étale fundamental groups do pass. To algorithmically restore certain rings from some groups that pass through a link in IUT, one uses deep results of anabelian geometry about number fields and hyperbolic curves over number fields and their non-archimedean completions. The anabelian algorithms produce from a given input data an object within a set of possible output objects. Several indeterminacies are used to weaken the input data in the algorithm, while mildly increasing the set of possible output objects (container) until that increased set includes the object in the original input data.

There are many analogies and relations between IUT and other areas of number theory, see 2.14 of [10]. We now list several intriguing similarities between IUT and quantum theory, by involving some basic concepts and ideas of IUT, those which can be stated in a relatively simple form and do not require an expertise in IUT. These similarities are even more amazing given the fact that representation theory plays no role in IUT and plays a fundamental role in quantum physics.

• In IUT, multiplication and addition are related to two symmetries, geometric and arithmetic symmetries, see e.g. §3.6 of [24], sect. 2.7 of [10]. These two dimensions are reminiscent of the two parameters, one of which is related to electricity, the other to magnetism. In particular, those two were employed in the experimental study of layers of hexagonal lattices in the growth of graphene and boron nitride layers.

• One of the key issues for quantum algorithms is whether they can run in polynomial time, instead of exponential time. The aspect of reducing exponential to polynomial is crucial for IUT.

• In mono-anabelian geometry and IUT one algorithmically reconstructs objects from étale fundamental groups. IUT produces upper bounds on the change of the relevant data passing through the theta-link, using the action of étale fundamental groups which pass through the link unaffected. As discussed with practitioners, using appropriate group (that goes intact through the algorithmic process) action on a flow of information to control its loss may be useful in quantum computing and quantum computers.

• IUT works with two types of topological monoid structures: étale-like (coming from groups of symmetries) and frobenius-like (coming from 'ordered' objects) and their interactions, see e.g. §2.7 of [24], §3.2 of [25]. A monoid is a set with binary associative operation and an identity element. For example, the multiplicative monoid $\mathbb{Z}_p \setminus \{0\}$ of non-zero elements of p-adic integers $\mathbb{Z}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers is a submonoid of the group of invertible elements of $\mathbb{Q}_p$. It splits into the product of the group of units $\mathbb{Z}_p^\times$ and the monoid of non-negative integer powers of p. The latter monoid is totally ordered. The monoid $\mathbb{Z}_p \setminus \{0\}$ is an example of a frobenius-like object in IUT, p^n can be informally viewed as having 'mass' n. A more interesting example of a frobenius-like object comes at the level of algebraic closures. Denote by O the ring of integers of an algebraic closure K of $\mathbb{Q}_p$. The absolute Galois group G of $\mathbb{Q}_p$ is an example of étale-like object in IUT. Consider the monoid $(O \setminus \{0\}, G)$ of non-zero elements of O with respect to multliplication, under the action by the group G. By class field theory, the maximal abelian quotient of G is isomorphic to $\mathbb{Z}_p^\times$ times the procyclic group $\hat{\mathbb{Z}}$ generated by p. The totally ordered cyclic group $\mathbb{Z}$ is a subgroup of its profinite completion $\hat{\mathbb{Z}}$, the latter is not a totally ordered group, and the image of p^n in it has no longer non-zero 'mass'. The embedding of positive integers in $\hat{\mathbb{Z}}$ plays an important role in explicit class field theory, see e.g. sect. 2 Ch. III of [11].

One can prove that the map that sends $(O \setminus \{0\}, G)$ to G induces an isomorphism from the group of automorphisms of $(O \setminus \{0\}, G)$ to the group of automorphisms of G. If one replaces $O \setminus \{0\}$ with the group of units $O^\times$, the group of automorphisms of $(O^\times, G)$ is isomorphic to the product of $\hat{\mathbb{Z}}^\times$ and automorphisms of G, for more details see Examples 2.12.1 and 2.12.2 of [24].

Étale-like structures are functorial, rigid and invariant with respect to the links in IUT, while frobenius-like structures are used to construct the links. Relations between these two types of structures are of crucial importance in IUT. One of such relations is given by a generalised Kummer map. For example, there is the classical Kummer isomorphism $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n} \simeq H^1(G, \mu_n)$ where μ_n are roots of unity of order n in K. The object on the right hand side of the Kummer isomorphism is solely dependent on the étale-like object G and n, while the object on the left hand side is a frobenius-like object which has the quotient generated by p modulo p^n. Generalised

Kummer maps restore multiplication of sufficiently small fields such as number fields and their non-archimedean completions. The substance of anabelian geometry is to further construct a non-trivial algorithm to restore the addition and the ring structure. The Kummer map embed the frobenius-like object $\mathbb{Z}_p \setminus \{0\}$ into the étale-like object $H^1(G, \mu)$ where μ are all roots of unity in K. This étale-like object can be viewed as a container for the frobenius-like object $\mathbb{Z}_p \setminus \{0\}$. An automorphism of $(O^\times, G)$ produces from a Kummer map $\mathbb{Z}_p^\times \to H^1(G, \mu)$ another one, the corresponding diagram of maps is commutative up to indeterminacy of the action by a suitable element of $\hat{\mathbb{Z}}^\times$, for more details see Example 2.12.2 of [24]. Involving appropriate indeterminacies to make diagrams commutative is important in IUT.

Étale-like objects, unlike frobenius-like objects, pass unmodified through certain non-ring-theoretical links in the IUT theory. For example, the theta-link rescales p to its fixed positive integer power and this is not compatible with the ring structure. In §2.2 of [24] frobenius-like and étale-like structures are compared with nonzero mass objects and zero mass objects. Depending on the context, the same structure can be a frobenius-like object or an étale-like object.

From a certain perspective, the analogues of these two non-archimedean mathematical structures are particles and waves in archimedean mechanics. Interaction of frobenius-like and étale-like structures via Kummer maps in IUT may be sometimes viewed a little analogous to the relation between particles and waves in quantum mechanics.

• In IUT passing to a set-theoretic subquotient by taking the log-volume at the very last stage of the algorithm, see (LVsQ) in §3.9, (Stp7) and (Stp8) in §3.10 of [25], sounds a little similar to a measurement of a quantum system with the wave function collapsing.

Appendix

The IUT theory [26] has applications to the proofs of non-effective abc inequalities for number fields. A recent paper [27] extends the IUT theory and deduces, for the first time, several effective abc inequalities. In the remaining part of the paper we set new questions about an asymptotic symmetry of the moduli space of Frey–Hellegouarch elliptic curves over rational numbers, in relation to how one can deduce from the established effective abc inequalities some stronger abc type inequalities. These questions go beyond the previously asked abc inequalities conjectures. No knowledge of [27] is required.

For a non-zero integer its radical rad is the product of its prime divisors taken each with multiplicity one and its odd radical rad′ is the product of its odd prime divisors taken each with multiplicity one.

One of the established effective abc inequalities in [27] is

for every $\varepsilon > 0$ there is an effectively described constant C'_ε such that for all relatively prime positive integer numbers a, b, the inequality

$$\log(a+b) < 1.5(1+\varepsilon)\cdot\log\mathrm{rad}(ab(a+b)) + C'_\varepsilon$$

holds.

The constant C'_1 is slightly larger than $8.5\cdot 10^{29}$. Note the constant 1.5 instead of the more common constant 1 in most abc inequality conjectures. The appearance of 1.5 is due to lack of some information at archimedean places. A version of the previous inequality is also established in [27] over quadratic imaginary fields.

Another established effective abc inequality in [27] is

for every $\varepsilon > 0$ there is an effectively described constant C_ε such that for all relatively prime positive integer numbers a, b, the inequality

$$\log(ab(a+b)) < 3(1+\varepsilon)\cdot\log\mathrm{rad}(ab(a+b)) + C_\varepsilon$$

holds. The constant C_1 is slightly larger than $1.7\cdot 10^{30}$. The number 10^{30} is approximately the ratio of the average diameter of galaxy to the average diameter of atom.

The second abc inequality implies the first one. The second inequality was stated as a conjecture by Szpiro in [28] in 1990.

One can ask how to deduce an effective $(1+\varepsilon)$-abc inequality from these effective abc inequalities without a further strengthening of IUT and its applications. Towards this aim, let's consider the following situation.

An elliptic curve over $\mathbb{Q}$ with all its 2-torsion points $\mathbb{Q}$-rational is isomorphic over an algebraic closure of $\mathbb{Q}$ to a (Frey–Hellegouarch) curve $E_{a,b}$ with affine equation

$$y^2 = x(x+a)(x-b)$$

for some coprime non-zero integers a, b. It can be written in the Weierstrass form as

$$Y^2 = X^3 - 27c_4X - 54c_6, \quad c_4 = 16(a^2+ab+b^2), \quad c_6 = 32(b-a)(2a+b)(a+2b).$$

Its discriminant $\Delta = (c_4^3 - c_6^2)/1728 = 16(ab(a+b))^2$. The minimal discriminant of $E_{a,b}$ is the same if 16 does not divide abc or if $a \equiv -1 \bmod 4$ and $b \equiv 0 \bmod 16$, and $16^{-2}(ab(a+b))^2$ if $a \equiv 1 \bmod 4$ and $b \equiv 0 \bmod 16$.

In particular,

$$(a^2+ab+b^2)^3 = ((b-a)(2a+b)(a+2b)/2)^2 + 3^3(ab(a+b)/2)^2. \qquad (\dagger)$$

The j-invariant of the Weierstrass equation is

$$j_{a,b} = 2^8\cdot\frac{(a^2+ab+b^2)^3}{(ab(a+b))^2} = 2^6\cdot\frac{((b-a)(2a+b)(a+2b))^2}{(ab(a+b))^2} + 2^6\cdot 3^3.$$

If 16 does not divide $ab(a+b)$ then $\mathrm{cond}(E_{a,b}) < 2^{12}\mathrm{rad}'(ab(a+b))$. If $16|ab(a+b)$ and say $4|(a-1)$, $16|b$ then $\mathrm{cond}(E_{a,b}) = \mathrm{rad}(2^{-4}ab(a+b)) \leqslant \mathrm{rad}(ab(a+b))$. If $16|ab(a+b)$ and say $4|(a+1)$, $16|b$ then $\mathrm{cond}(E_{a,b}) \leqslant 2^{4+2l}\mathrm{rad}'(ab(a+b))$

where l is the maximal power of 2 dividing b. All this is very well known. See e.g. sect. 12.5 of [2]. Note that the statement "Since E has multiplicative reduction at all primes $p|\Delta$" in the top line of its p.434 is incorrect as the example of $E_{1,16}$ shows, but the inequality for the LHS and RHS of the next displayed inequality on that page is correct.

Now let in addition $0 < a < b$, a, b are still coprime. Put $c = a + b$. Define

$$A = (b-a)/d, \quad B = (2a+b)/d, \quad C = A + B = (a+2b)/d,$$

where $d = \gcd(b-a, 2a+b)$ (= 1 or 3). Then $0 < A < B$, and A, B are coprime.

We have

$$a^2 + ab + b^2 = d^2(A^2 + AB + B^2)/3,$$
$$ab(a+b) = d^3(B-A)(A+2B)(2A+B)/3^3,$$
$$(b-a)(2a+b)(a+2b) = d^3 AB(A+B).$$

The map $\phi\colon (a,b) \mapsto (A,B)$ is an involution: $\phi^2 = \mathrm{id}$. The involution ϕ corresponds to $x \mapsto (2+x)/(x-1)$ on $\mathbb{P}^1$ sending b/a to B/A.

Thus we have an involution map on the moduli space of Frey–Hellegouarch elliptic curves: $E_{a,b} \mapsto E_{A,B}$. The map ϕ relates the two terms on the RHS of (†).

From (†) one gets

$$(A^2 + AB + B^2)^3 = 3^3\,(AB(A+B)/2)^2 + ((B-A)(2A+B)(A+2B)/2)^2\,.$$

We also have $j_{A,B} = 12^3 j_{a,b}/(j_{a,b} - 12^3) = (12^{-3} - j_{a,b}^{-1})^{-1}$.

Question (abc-ABC question). *Are the following equivalent statements true?*
1. $\mathrm{rad}(abc)$ *and* $\mathrm{rad}(ABC)$ *are effectively asymptotically equal, i.e. for every* $\varepsilon > 0$ *there are constants* $\mathfrak{c}_\epsilon, \mathfrak{c}'_\epsilon$*, effectively depending on* ϵ*, such that for all relatively prime positive* $a < b$

$$\mathrm{rad}(abc) < \mathfrak{c}_\epsilon \cdot \mathrm{rad}(ABC)^{1+\epsilon}, \quad \mathrm{rad}(ABC) < \mathfrak{c}'_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

2. For every $\epsilon > 0$ *there is a positive constant* κ_ϵ *such that for all positive coprime integers* $a < b$

$$\mathrm{rad}((b-a)(2a+b)(a+2b)) < \kappa_\epsilon \cdot \mathrm{rad}(ab(a+b))^{1+\epsilon}$$

with κ_ϵ *effectively dependent on* ϵ*.*
3. $\mathrm{rad}(\Delta(E_{a,b}))$ *and* $\mathrm{rad}(\Delta(E_{A,B}))$ *are effectively asymptotically equivalent.*
4. $\mathrm{rad}(c_6(E_{a,b}))$ *and* $\mathrm{rad}(\Delta(E_{a,b}))$ *are effectively asymptotically equivalent.*

The proof of the equivalences is immediate. The author does not know the proof of either a positive answer or a negative answer to this abc-ABC question, and several experts in arithmetic of elliptic curves were in a similar situation.

The positive answer to the Question signifies a new asymptotic symmetry of the moduli space of elliptic curves over $\mathbb{Q}$ all of whose 2-torsion points are $\mathbb{Q}$-rational.

Fix a positive integer m. The second abc inequality above implies that *for every positive ε for all non-zero integers a, b, c such that $a + b + c = 0$ and* $\gcd(a, b, c)$ *divides m we have*

$$\log |abc| < 3(1 + \epsilon) \cdot \log \mathrm{rad}(abc) + C_\epsilon + 3 \log m. \qquad (\sharp)$$

In view of (†), consider the equation

$$x^3 = y^2 + 3^3 z^2$$

where x, y, z are positive integers such that $\gcd(x, y, z)|3$. We use the standard notation $f \ll_\epsilon g$ for real functions on positive real numbers depending on parameter $\epsilon > 0$ which means $|f(\epsilon, x)| \leqslant C(\epsilon) g(\epsilon, x)$ for a real $C(\epsilon)$ depending on ϵ.

Applying ($\sharp$), we obtain $x^3 y^2 z^2 \ll_\epsilon \mathrm{rad}(xyz)^{3(1+\epsilon)}$. Since $y^2 \cdot 3^3 z^2 \leqslant x^6/4$, we deduce $yz \ll_\epsilon \mathrm{rad}(xyz)^{1+\epsilon}$. Assume that $y^2 \leqslant 3^3 z^2$, then we deduce $y \ll_\epsilon \mathrm{rad}(xyz)^{(1+\epsilon)/2}$. Since $x^3 \leqslant 2 \cdot 3^3 z^2$, we get $x^6 y^2 \leqslant x^3 \cdot 2 \cdot 3^3 z^2 \cdot y^2 \ll_\epsilon \mathrm{rad}(xyz)^{3(1+\epsilon)}$ and $x^6 y^6 \ll_\epsilon \mathrm{rad}(xyz)^{5(1+\epsilon)}$, so $xy \ll_\epsilon \mathrm{rad}(z)^{5(1+\epsilon)}$. Substituting the latter in the RHS of $y \ll_\epsilon \mathrm{rad}(xyz)^{(1+\epsilon)/2}$, we obtain $y \ll_\epsilon \mathrm{rad}(z)^{3(1+\epsilon)}$. From $x^6 y^2 \ll_\epsilon \mathrm{rad}(xyz)^{3(1+\epsilon)}$ we deduce $x^3 \ll_\epsilon y^{1+\epsilon} \cdot \mathrm{rad}(z)^{3(1+\epsilon)}$ so $x^3 \ll_\epsilon \mathrm{rad}(z)^{6(1+\epsilon)}$, hence $x \ll_\epsilon \mathrm{rad}(z)^{2(1+\epsilon)}$. Thus, ($\sharp$) implies: if $y^2 \leqslant 3^3 z^2$ then $x \ll_\epsilon \mathrm{rad}(z)^{2(1+\epsilon)}$. Similarly, if $y^2 \geqslant 3^3 z^2$ then $x \ll_\epsilon \mathrm{rad}(y)^{2(1+\epsilon)}$. All the implied constants are explicit functions of C_ε.

Now, for positive coprime $a < b$ denote $x = a^2 + ab + b^2$, $y = (b - a)(2a + b)(a + 2b)/2$, $z = ab(a + b)/2$. Then $x^3 = y^2 + 3^3 z^2$. Note that since a and b are coprime, $\gcd(x, y, z)$ divides 3, so we can apply the previous paragraph to x, y, z. We deduce from the previous paragraph: if $((b - a)(2a + b)(a + 2b))^2 \leqslant 3^3 (ab(a + b))^2$ then $3c^2/4 \leqslant a^2 + ab + b^2 \ll_\epsilon \mathrm{rad}(abc)^{2+\epsilon}$ and hence $c \ll_\epsilon \mathrm{rad}(abc)^{1+\epsilon}$; if $((b-a)(2a+b)(a+2b))^2 \geq 3^3 (ab(a+b))^2$, i.e. $((B-A)(2A+B)(A+2B))^2 \leqslant 3^3 (AB(A+B))^2$, then $A^2 + AB + B^2 \ll_\epsilon \mathrm{rad}(ABC)^{2+\epsilon}$ and hence $c \ll_\epsilon \mathrm{rad}(ABC)^{1+\epsilon}$. All the implied constants are explicit functions of C_ε.

Therefore, the inequality ($\sharp$) implies:

Theorem 1. *For every positive ε there is an effectively described constant K_ε such that for all coprime positive integers a, b and their sum $c = a + b$ and A, B, C defined for a, b as above*

$$\log c < (1 + \epsilon) \cdot \log \max\{\mathrm{rad}(abc), \mathrm{rad}(ABC)\} + K_\varepsilon.$$

Using Theorem 1 we obtain

Theorem 2. *Assume that the* abc-ABC Question *has positive answer. Then for every positive ε there is an effectively described constant L_ε such that for all coprime positive integers a, b and their sum $c = a + b$ the inequality*

$$\log c < (1+\varepsilon) \cdot \log \mathrm{rad}(abc) + L_\varepsilon$$

holds.

References

1. S. Aaronson, D. Gottesman, Improved simulation of stabilizer circuits, arXiv:quant-ph/0406196.
2. E. Bombieri, W. Gubler, Heights in Diophantine geometry, CUP 2007.
3. F. Del Santo, N. Gisin, Physics without determinism: alternative interpretations of classical physics, arXiv1909.03697 [quant-ph].
4. A. Döring, C.J. Isham, A topos foundation for theories of physics. I. Formal languages for physics, J. Math. Phys. 49, 053515 (2008), arXiv:quant-ph/0703060 [quant-ph].
5. A. Döring, C.J. Isham, A topos foundation for theories of physics. II. Daseinisation and the liberation of quantum theory, J. Math. Phys. 49, 053516 (2008), arXiv:quant-ph/0703062 [quant-ph].
6. A. Döring, C.J. Isham, A topos foundation for theories of physics. III. The representation of physical quantities with arrows, J. Math. Phys. 49, 053517 (2008), arXiv:quant-ph/0703064 [quant-ph].
7. A. Döring, C.J. Isham, A topos foundation for theories of physics. IV. Categories of systems, J. Math. Phys. 49, 053518 (2008), arXiv:quant-ph/0703066 [quant-ph]
8. A. Döring, C.J. Isham, 'What is a thing?': topos theory in the foundations of physics, arXiv: 0803.0417 [quant-ph].
9. A. Döring, C.J. Isham, Classical and quantum probabilities as truth values, arXiv: 1102.2213v1.
10. I. Fesenko, Arithmetic deformation theory via fundamental groups and nonarchimedean theta-functions, notes on the work of Shinichi Mochizuki, Europ. J. Math. (2015) 1:405–440.
11. I. Fesenko, Core topics in number theory I, lecture notes 2023, available from https://ivanfesenko.org/wp-content/uploads/Q/C1/partI.pdf.
12. C. Flori, A First Course in Topos Quantum Theory, Lect. Notes Physics, 868, Springer 2013.
13. C. Flori, A Second Course in Topos Quantum Theory, Lect. Notes Physics, 944, Springer 2018.
14. N. Gisin, Indeterminism in physics and intuitionistic mathematics, arXiv2011.02348 [quant-ph].
15. R. Goldblatt, Topoi, the Categorial Analysis of Logic, North-Holland, London, 1984.
16. J. Hoshi, S. Mochizuki, S. Tsujimura, Combinatorial construction of the absolute Galois group of the field of rational numbers, preprint 2022, available from https://www.kurims.kyoto-u.ac.jp/~motizuki/Combinatorial%20absolute%20Galois%20groups.pdf.
17. C.J. Isham, Topos theory and consistent histories: the internal logic of the set of all consistent sets, Int. J. Theor. Phys. 36, 785 (1997), arXiv:gr-qc/9607069.
18. C.J. Isham, Topos methods in the foundations of physics, arXiv:1004.3564 [quant-ph].
19. L. Lafforgue, Geometry according to Grothendieck: glimpses from "Récoltes et Semailles", In Unifying Themes in Geometry, Lake Como School of Advanced Studies, 27–30 September 2021, slides are available from https://www.dropbox.com/s/pnq81jcu8yhtlrj/LafforgueSlides.pdf?dl=0, video is available from https://www.youtube.com/watch?v=-CtzBL83bf0.
20. S. MacLane, I. Moerdijk, Sheaves in Geometry and Logic: A First Introduction to Topos Theory, Springer, London, 1968.
21. S. Mochizuki, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, J. Math. Sci. Univ Tokyo 3 (1996) 571–627.

22. S. Mochizuki, The local pro-p Grothendieck conjecture for hyperbolic curves, Invent. Math. 138 (1999) 319–423.
23. S. Mochizuki, Topics surrounding the anabelian geometry of hyperbolic curves, In Galois Groups and Fundamental Groups, MSRI Publications 41, CUP 2003, pp. 119–165.
24. S. Mochizuki, The mathematics of mutually alien copies: from Gaussian integrals to inter-universal Teichmüller theory, In Inter-universal Teichmüller Theory Summit 2016, RIMS Kōkyūroku Bessatsu B84, 2021, pp. 23–192, available from https://www.kurims.kyoto-u.ac.jp/~motizuki/Alien%20Copies,%20Gaussians,%20and%20Inter-universal%20Teichmuller%20Theory.pdf.
25. S. Mochizuki, On the essential logical structure of inter-universal Teichmüller theory in terms of logical and/or relations: report on the occasion of the publication of the four main papers on inter-universal Teichmüller theory, preprint 2023, available from https://www.kurims.kyoto-u.ac.jp/~motizuki/Essential%20Logical%20Structure%20of%20Inter-universal%20Teichmuller%20Theory.pdf.
26. S. Mochizuki, Inter-universal Teichmüller theory I: Constructions of Hodge theaters, *Publ. Res. Inst. Math. Sci.* 57(2021) 3–207; II: Hodge-Arakelov-theoretic evaluation, *Publ. Res. Inst. Math. Sci.* 57(2021) 209–401; III: Canonical splittings of the log-theta-lattice, *Publ. Res. Inst. Math. Sci.* 57(2021) 403–626; IV: Log-volume computations and set-theoretic foundations, *Publ. Res. Inst. Math. Sci.* 57(2021) 627–723.
27. S. Mochizuki, I. Fesenko, Y. Hoshi, A. Minamide and W. Porowski, Explicit estimates in inter-universal Teichmüller theory, Kodai Math. J. 45(2022) 175–236.
28. L. Szpiro, Discriminant et conducteur des courbes elliptiques, *Astérisque* 183(1990) 7–18.
29. A. Tamagawa, The Grothendieck conjecture for affine curves, Compositio Math. 109 (1997) 135–194.