Anabelian geometry — IUT — effective abc — applications

Ivan Fesenko

abc

For an integer $n = \pm \prod p_i^{m_i}$ denote $\mathrm{rad}(n) = \prod p_i$ (the reduced part).

A version of abc conjecture

there is a positive integer m such that
for every $\varepsilon > 0$ *there is a positive* $\kappa(\varepsilon) \in \mathbb{R}$
such that for every three non-zero coprime integers a, b, c *satisfying* $a + b = c$*, the inequality*

$$\boxed{\max(|a|, |b|, |c|) < \kappa(\varepsilon)\, \mathrm{rad}(abc)^{m+\varepsilon}}$$

holds.

In some of the strongest versions of the abc conjectures m is 1.

In some naive version $m = \kappa(1) = 1$, it immediately implies FLT for primes > 5.

abc

For an integer $n = \pm \prod p_i^{m_i}$ denote $\mathrm{rad}(n) = \prod p_i$ (the reduced part).

A version of abc conjecture

there is a positive integer m such that
for every $\varepsilon > 0$ *there is a positive* $\kappa(\varepsilon) \in \mathbb{R}$
such that for every three non-zero coprime integers a, b, c *satisfying* $a + b = c$*, the inequality*

$$\boxed{\max(|a|, |b|, |c|) < \kappa(\varepsilon)\, \mathrm{rad}(abc)^{m+\varepsilon}}$$

holds.

In some of the strongest versions of the abc conjectures m is 1.

In some naive version $m = \kappa(1) = 1$, it immediately implies FLT for primes > 5.

abc inequalities are about a relation between addition and multiplication, and so is the Riemann Hypothesis.

abc conjectures describe a kind of highly nontrivial balance between addition and multiplication, formalising the observation that

when two positive integers a and b are divisible by large powers of small primes then $a+b$ tends to be divisible by small powers of large primes.

For example, 3^n+5^n is divisible by small powers of larger primes when n goes to infinity.

Apparently, the importance of multiplication as opposite to addition was first recognised when developing the theory of music (A. Weil's reference to P. Tannery).

abc

abc inequalities are about a relation between addition and multiplication, and so is the Riemann Hypothesis.

abc conjectures describe a kind of highly nontrivial balance between addition and multiplication, formalising the observation that

when two positive integers a and b are divisible by large powers of small primes then $a + b$ tends to be divisible by small powers of large primes.

For example, $3^n + 5^n$ is divisible by small powers of larger primes when n goes to infinity.

Apparently, the importance of multiplication as opposite to addition was first recognised when developing the theory of music (A. Weil's reference to P. Tannery).

abc

abc inequalities are about a relation between addition and multiplication, and so is the Riemann Hypothesis.

abc conjectures describe a kind of highly nontrivial balance between addition and multiplication, formalising the observation that

when two positive integers a and b are divisible by large powers of small primes then $a+b$ tends to be divisible by small powers of large primes.

For example, $3^n + 5^n$ is divisible by small powers of larger primes when n goes to infinity.

Apparently, the importance of multiplication as opposite to addition was first recognised when developing the theory of music (A. Weil's reference to P. Tannery).

abc inequalities

When $k(\varepsilon)$ is proved to exist but is not explicitly computed, the abc inequality is non-effective.

When the dependence on ε is explicitly described, the abc inequality is effective.

For applications to Diophantine equations one needs effective abc inequalities.

Using elliptic curves

To the a, b, c as above one can associate an elliptic curve with affine equation

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

Every elliptic curve over $\mathbb{Q}$ with all its 2-torsions points $\mathbb{Q}$-rational is isomorphic over an algebraic closure of $\mathbb{Q}$ to such a curve.

The abc inequality mentioned above is closely related with the following Szpiro conjecture (historically stated before abc conjectures were stated):

for every $\varepsilon > 0$ there is a real $C(\varepsilon) > 0$ such that for every elliptic curve E over $\mathbb{Q}$ the inequality

$$\boxed{\mathrm{Disc}_E \le C(\varepsilon)\,\mathrm{Cond}_E^{6+\varepsilon}}$$

holds for the minimal discriminant and conductor of the curve.

Using elliptic curves

To the a, b, c as above one can associate an elliptic curve with affine equation

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

Every elliptic curve over $\mathbb{Q}$ with all its 2-torsions points $\mathbb{Q}$-rational is isomorphic over an algebraic closure of $\mathbb{Q}$ to such a curve.

The abc inequality mentioned above is closely related with the following Szpiro conjecture (historically stated before abc conjectures were stated):

for every $\varepsilon > 0$ there is a real $C(\varepsilon) > 0$ such that for every elliptic curve E over $\mathbb{Q}$ the inequality

$$\boxed{\mathrm{Disc}_E \leq C(\varepsilon)\,\mathrm{Cond}_E^{6+\varepsilon}}$$

holds for the minimal discriminant and conductor of the curve.

The IUT theory

Inter-universal Teichmüller theory (IUT) of Mochizuki was published in 2021.

It uses highly non-trivial results in anabelian geometry.

Anabelian geometry is one of the main generalisations of class field theory, together with higher class field theory and Langlands correspondences.

The IUT theory

Inter-universal Teichmüller theory (IUT) of Mochizuki was published in 2021.

It uses highly non-trivial results in anabelian geometry.

Anabelian geometry is one of the main generalisations of class field theory, together with higher class field theory and Langlands correspondences.

The IUT theory

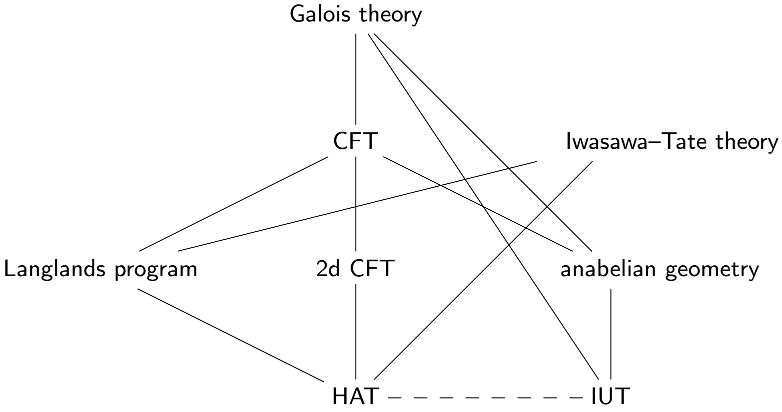
Inter-universal Teichmüller theory (IUT) of Mochizuki was published in 2021.

It uses highly non-trivial results in anabelian geometry.

Anabelian geometry is one of the main generalisations of class field theory, together with higher class field theory and Langlands correspondences.

Part of the tree of number theory

CFT = class field theory
HAT = higher adelic theory
2d = two-dimensional (i.e. for arithmetic surfaces)



Sources of information about IUT

Links to many texts, talks of 4 international IUT workshops, and videos can be found, e.g. at

https://ivanfesenko.org/wp-content/uploads/2021/11/guidesiut.pdf

On 1d anabelian geometry, very briefly

In 1969 Neukirch asked whether if two number fields have isomorphic (as profinite groups) absolute Galois groups then the fields are isomorphic.

This was answered positively by a development involving Neukirch, Ikeda, Uchida and Iwasawa, by 1976.

First, one restores the multiplicative group of a number field k from its absolute Galois group, using Kummer theory

$$k^\times / k^{\times m} \simeq H^1(G_k, \mu_m).$$

Then, after some non-trivial work, one restores addition and the full ring structure of k.

Theorem (Neukirch, Ikeda, Uchida). If k_1, k_2 are both either number fields or function fields of irreducible curves over finite fields of characteristic p, then

$$\text{Ring-Iso}(k_1, k_2) \simeq \text{TopGroup-Iso}(G_{k_1}, G_{k_2})/\text{Inn}(G_{k_2}).$$

On 1d anabelian geometry, very briefly

In 1969 Neukirch asked whether if two number fields have isomorphic (as profinite groups) absolute Galois groups then the fields are isomorphic.

This was answered positively by a development involving Neukirch, Ikeda, Uchida and Iwasawa, by 1976.

First, one restores the multiplicative group of a number field k from its absolute Galois group, using Kummer theory

$$k^\times / k^{\times m} \simeq H^1(G_k, \mu_m).$$

Then, after some non-trivial work, one restores addition and the full ring structure of k.

Theorem (Neukirch, Ikeda, Uchida). If k_1, k_2 are both either number fields or function fields of irreducible curves over finite fields of characteristic p, then

$$\text{Ring-Iso}(k_1, k_2) \simeq \text{TopGroup-Iso}(G_{k_1}, G_{k_2})/\text{Inn}(G_{k_2}).$$

On 1d anabelian geometry, very briefly

In 1969 Neukirch asked whether if two number fields have isomorphic (as profinite groups) absolute Galois groups then the fields are isomorphic.

This was answered positively by a development involving Neukirch, Ikeda, Uchida and Iwasawa, by 1976.

First, one restores the multiplicative group of a number field k from its absolute Galois group, using Kummer theory

$$k^{\times}/k^{\times m} \simeq H^1(G_k, \mu_m).$$

Then, after some non-trivial work, one restores addition and the full ring structure of k.

Theorem (Neukirch, Ikeda, Uchida). If k_1, k_2 are both either number fields or function fields of irreducible curves over finite fields of characteristic p, then

$$\text{Ring-Iso}(k_1, k_2) \simeq \text{TopGroup-Iso}(G_{k_1}, G_{k_2})/\text{Inn}(G_{k_2}).$$

On 1d anabelian geometry, very briefly

Using Kummer theory, there is a purely group-theoretic functorial algorithm to produce from the absolute Galois group G_k a field $\mathscr{F}(G_k)$ endowed with the action of G_k, together with a G_k-equivariant isomorphism

$$\kappa\colon k^{sep} \xrightarrow{\sim} \mathscr{F}(G_k).$$

Consider the diagramme involving the Frobenius map on k^{sep} in positive characteristic:

$$\begin{array}{ccc} k^{sep} & \xrightarrow{\ \kappa\ } & \mathscr{F}(G_k) \\ {\scriptstyle Frob}\downarrow & & \uparrow{\scriptstyle \mathscr{F}(G_k \to G_{\mathrm{Frob}(k)})} \\ k^{sep} & \xrightarrow{\ \kappa\ } & \mathscr{F}(G_k) \end{array}$$

G_k is canonically isomorphic to $G_{Frob(k)}$, so this diagramme is *not commutative*.

On 1d anabelian geometry, very briefly

Using Kummer theory, there is a purely group-theoretic functorial algorithm to produce from the absolute Galois group G_k a field $\mathscr{F}(G_k)$ endowed with the action of G_k, together with a G_k-equivariant isomorphism

$$\kappa\colon k^{sep} \xrightarrow{\sim} \mathscr{F}(G_k).$$

Consider the diagramme involving the Frobenius map on k^{sep} in positive characteristic:

$$\begin{array}{ccc} k^{sep} & \xrightarrow{\kappa} & \mathscr{F}(G_k) \\ {\scriptstyle Frob}\downarrow & & \uparrow{\scriptstyle \mathscr{F}(G_k \to G_{\mathrm{Frob}(k)})} \\ k^{sep} & \xrightarrow{\kappa} & \mathscr{F}(G_k) \end{array}$$

G_k is canonically isomorphic to $G_{Frob(k)}$, so this diagramme is *not commutative*.

Group theoretical constructions in number theory

Which constructions in number theory depend solely on (topological) group theoretical data?

Example: in class field theory one derives purely group theoretically the reciprocity map and its properties from class field theory axioms (class formations axioms).

However, to check these class field theory axioms for a specific class of fields one has to use their ring structure.

Group theoretical constructions in number theory

Which constructions in number theory depend solely on (topological) group theoretical data?

Example: in class field theory one derives purely group theoretically the reciprocity map and its properties from class field theory axioms (class formations axioms).

However, to check these class field theory axioms for a specific class of fields one has to use their ring structure.

On 2d anabelian geometry, very briefly

Algebraic geometry involves locally the correspondence between affine varieties and commutative rings. The most common picture in Grothendieck's volumes is a commutative diagramme of commutative rings and ring homomorphisms and a similar one for local and global geometric objects.

Anabelian geometry in 2d was proposed by Grothendieck in 1983 for hyperbolic curves over number fields and their completions. He was not aware of the work in 1d.

Anabelian geometry conjectures are correspondences between such curves and their arithmetic fundamental groups π_1 (or slightly more complicated objects).

Groups (and not rings) play the key role in anabelian geometry, very different from algebraic geometry.

Anabelian geometry in 2d was developed by Nakamura, Tamagawa and Mochizuki, with many final results published by Mochizuki in 1995–2015.

On 2d anabelian geometry, very briefly

Algebraic geometry involves locally the correspondence between affine varieties and commutative rings. The most common picture in Grothendieck's volumes is a commutative diagramme of commutative rings and ring homomorphisms and a similar one for local and global geometric objects.

Anabelian geometry in 2d was proposed by Grothendieck in 1983 for hyperbolic curves over number fields and their completions. He was not aware of the work in 1d.

Anabelian geometry conjectures are correspondences between such curves and their arithmetic fundamental groups π_1 (or slightly more complicated objects).

Groups (and not rings) play the key role in anabelian geometry, very different from algebraic geometry.

Anabelian geometry in 2d was developed by Nakamura, Tamagawa and Mochizuki, with many final results published by Mochizuki in 1995–2015.

On 2d anabelian geometry, very briefly

Algebraic geometry involves locally the correspondence between affine varieties and commutative rings. The most common picture in Grothendieck's volumes is a commutative diagramme of commutative rings and ring homomorphisms and a similar one for local and global geometric objects.

Anabelian geometry in 2d was proposed by Grothendieck in 1983 for hyperbolic curves over number fields and their completions. He was not aware of the work in 1d.

Anabelian geometry conjectures are correspondences between such curves and their arithmetic fundamental groups π_1 (or slightly more complicated objects).

Groups (and not rings) play the key role in anabelian geometry, very different from algebraic geometry.

Anabelian geometry in 2d was developed by Nakamura, Tamagawa and Mochizuki, with many final results published by Mochizuki in 1995–2015.

On 2d anabelian geometry, very briefly

Anabelian geometry, for number fields and hyperbolic curves over number fields and their completions, restores an arithmetic geometric object from its arithmetic fundamental group.

For a geometrically integral scheme C over a perfect field k there is an epimorphism $\pi_1(C) \to G_k$.

Here is the first reconstruction algorithm that is compatible with localisation and completion:

Theorem (Mochizuki, 2015).

For a hyperbolic curve C over a number field k isogenous to a hyperbolic curve of genus zero (e.g. an elliptic curve with one point removed) there is a universal functorial group theoretical algorithm to reconstruct the field l from the topological group $\pi_1(C_l)$, where $C_l = C \times_k l$, $l = k$ or any of its non-archimedean completions.

Note that in general one cannot restore a mixed characteristic local field with finite residue field from its absolute Galois group.

On 2d anabelian geometry, very briefly

Anabelian geometry, for number fields and hyperbolic curves over number fields and their completions, restores an arithmetic geometric object from its arithmetic fundamental group.

For a geometrically integral scheme C over a perfect field k there is an epimorphism $\pi_1(C) \to G_k$.

Here is the first reconstruction algorithm that is compatible with localisation and completion:

Theorem (Mochizuki, 2015).

For a hyperbolic curve C over a number field k isogenous to a hyperbolic curve of genus zero (e.g. an elliptic curve with one point removed) there is a universal functorial group theoretical algorithm to reconstruct the field l from the topological group $\pi_1(C_l)$, where $C_l = C \times_k l$, $l = k$ or any of its non-archimedean completions.

Note that in general one cannot restore a mixed characteristic local field with finite residue field from its absolute Galois group.

On 2d anabelian geometry, very briefly

Anabelian geometry, for number fields and hyperbolic curves over number fields and their completions, restores an arithmetic geometric object from its arithmetic fundamental group.

For a geometrically integral scheme C over a perfect field k there is an epimorphism $\pi_1(C) \to G_k$.

Here is the first reconstruction algorithm that is compatible with localisation and completion:

Theorem (Mochizuki, 2015).

For a hyperbolic curve C over a number field k isogenous to a hyperbolic curve of genus zero (e.g. an elliptic curve with one point removed) there is a universal functorial group theoretical algorithm to reconstruct the field l from the topological group $\pi_1(C_l)$, where $C_l = C \times_k l$, $l = k$ or any of its non-archimedean completions.

Note that in general one cannot restore a mixed characteristic local field with finite residue field from its absolute Galois group.

On 2d anabelian geometry, very briefly

First one restores multiplication, using generalised Kummer theory.

Then, one restores addition and the full ring/scheme-theoretic structure.

Arithmetic fundamental groups of hyperbolic curves over number fields are highly non-commutative, but they have one algebraic operation, not two.

This opens the perspective of relating these geometric objects in a way not seen by algebraic geometry.

On 2d anabelian geometry, very briefly

First one restores multiplication, using generalised Kummer theory.

Then, one restores addition and the full ring/scheme-theoretic structure.

Arithmetic fundamental groups of hyperbolic curves over number fields are highly non-commutative, but they have one algebraic operation, not two.

This opens the perspective of relating these geometric objects in a way not seen by algebraic geometry.

On IUT, very briefly

Working with hyperbolic curves over number fields adds a geometric dimension to the arithmetic dimension of the field.

Working with the two dimensions, geometric and arithmetic, is needed in IUT in order to work with the additive structure and multiplicative structure and study the extent to which one cannot separate one from another.

When one starts to work with basic diagrammes of groups and hyperbolic curves over number fields in anabelian geometry, one immediately meets non-commutative diagrammes.

On IUT, very briefly

Working with hyperbolic curves over number fields adds a geometric dimension to the arithmetic dimension of the field.

Working with the two dimensions, geometric and arithmetic, is needed in IUT in order to work with the additive structure and multiplicative structure and study the extent to which one cannot separate one from another.

When one starts to work with basic diagrammes of groups and hyperbolic curves over number fields in anabelian geometry, one immediately meets non-commutative diagrammes.

On IUT, very briefly

Already in 1d the example with the Frobenius map provides a non-commutative diagramme.

Mono-anabelian transport uses generalised Kummer theory to go from a scheme-theoretic object to an appropriate topological group, then via some map from the latter to itself, and then from it restoring a scheme-theoretic object using the reverse generalised Kummer map. An associated diagramme is generally non-commutative.

One of key contribution =in the IUT theory for certain hyperbolic curves (e.g. an elliptic curve minus 1 point) is a new fundamental understanding of how to deal with the deviation from commutativity of certain crucial diagrammes (e.g. to get two Kummer maps compatible) by introducing relevant indeterminacies.

These indeterminacies are eventually translated into the bound in abc type inequalities.

On IUT, very briefly

Already in 1d the example with the Frobenius map provides a non-commutative diagramme.

Mono-anabelian transport uses generalised Kummer theory to go from a scheme-theoretic object to an appropriate topological group, then via some map from the latter to itself, and then from it restoring a scheme-theoretic object using the reverse generalised Kummer map. An associated diagramme is generally non-commutative.

One of key contribution =in the IUT theory for certain hyperbolic curves (e.g. an elliptic curve minus 1 point) is a new fundamental understanding of how to deal with the deviation from commutativity of certain crucial diagrammes (e.g. to get two Kummer maps compatible) by introducing relevant indeterminacies.

These indeterminacies are eventually translated into the bound in abc type inequalities.

On IUT, very briefly

Already in 1d the example with the Frobenius map provides a non-commutative diagramme.

Mono-anabelian transport uses generalised Kummer theory to go from a scheme-theoretic object to an appropriate topological group, then via some map from the latter to itself, and then from it restoring a scheme-theoretic object using the reverse generalised Kummer map. An associated diagramme is generally non-commutative.

One of key contribution =in the IUT theory for certain hyperbolic curves (e.g. an elliptic curve minus 1 point) is a new fundamental understanding of how to deal with the deviation from commutativity of certain crucial diagrammes (e.g. to get two Kummer maps compatible) by introducing relevant indeterminacies.

These indeterminacies are eventually translated into the bound in abc type inequalities.

On IUT, very briefly

Example. For a finite extension l of $\mathbb{Q}_p$, one easily sees

$$\mathrm{Aut}(G_l \curvearrowright \mathcal{O}^{\times}_{l^{\mathrm{sep}}}) \xrightarrow{\sim} \mathbb{Z}^{\times} \times \mathrm{Aut}(G_l),$$

so there is a $\mathbb{Z}^{\times} = \{\pm 1\}$ indeterminacy here.

At the same time, $\mathrm{Aut}_{G_l}(\mathcal{O}_{l^{\mathrm{sep}}} \setminus \{0\}, \times) = 1$ and

$$\mathrm{Aut}(G_l \curvearrowright (\mathcal{O}_{l^{\mathrm{sep}}} \setminus \{0\}, \times)) \xrightarrow{\sim} \mathrm{Aut}(G_l).$$

On IUT, very briefly

Let π be the fundamental group $\pi_1(C_l)$ in Mochizuki's theorem.

Example. The log map $\mathscr{O}_{l^{\mathrm{sep}}}^{\times} \to l^{\mathrm{sep}}$, connecting multiplication with addition at the local level, is used in the log-link

$$\pi \curvearrowright (\mathscr{O}_{l^{\mathrm{sep}}} \setminus \{0\}, \times) \longrightarrow \pi \curvearrowright (\mathscr{O}_{l^{\mathrm{sep}}} \setminus \{0\}, \times).$$

One can algorithmically reconstruct $\pi \curvearrowright (\mathscr{O}_{l^{\mathrm{sep}}} \setminus \{0\}, \times)$ from π.

However, there is no compatibility with the Kummer maps on the LHS and RHS.

This failure to commute is dealt with in IUT by means of an indeterminacy (Ind3).

On IUT, very briefly

The theta-link in IUT represents the multiplicative rescaling $q \to q^n$.

This link involves the non-archimedean (étale) theta-function and its special values.

This is related to the Jacobi triple product

$$\theta(u) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u) \prod_{n\geqslant 1} \left((1-q^n)(1-q^n u)(1-q^n u^{-1})\right)$$

Ring structures do not pass through the theta-link or log-link. Galois and fundamental groups do pass.

To restore rings from such groups one uses anabelian geometry results about number fields and hyperbolic curves over them and their completions.

In bounding the non-commutativity of relevant diagrammes one uses that fact that the group acting on the flow of information passes intact through the algorithmic process.

Recently, this idea has found applications in quantum computing and quantum computers.

On IUT, very briefly

The theta-link in IUT represents the multiplicative rescaling $q \to q^n$.

This link involves the non-archimedean (étale) theta-function and its special values.

This is related to the Jacobi triple product

$$\theta(u) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u) \prod_{n \geqslant 1} \left((1-q^n)(1-q^n u)(1-q^n u^{-1})\right)$$

Ring structures do not pass through the theta-link or log-link. Galois and fundamental groups do pass.

To restore rings from such groups one uses anabelian geometry results about number fields and hyperbolic curves over them and their completions.

In bounding the non-commutativity of relevant diagrammes one uses that fact that the group acting on the flow of information passes intact through the algorithmic process.

Recently, this idea has found applications in quantum computing and quantum computers.

On IUT, very briefly

The theta-link in IUT represents the multiplicative rescaling $q \to q^n$.

This link involves the non-archimedean (étale) theta-function and its special values.

This is related to the Jacobi triple product

$$\theta(u) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u) \prod_{n \geqslant 1} \left((1-q^n)(1-q^n u)(1-q^n u^{-1})\right)$$

Ring structures do not pass through the theta-link or log-link. Galois and fundamental groups do pass.

To restore rings from such groups one uses anabelian geometry results about number fields and hyperbolic curves over them and their completions.

In bounding the non-commutativity of relevant diagrammes one uses that fact that the group acting on the flow of information passes intact through the algorithmic process.

Recently, this idea has found applications in quantum computing and quantum computers.

On IUT, very briefly

The theta-link in IUT represents the multiplicative rescaling $q \to q^n$.

This link involves the non-archimedean (étale) theta-function and its special values.

This is related to the Jacobi triple product

$$\theta(u) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u) \prod_{n \geqslant 1} \left((1-q^n)(1-q^n u)(1-q^n u^{-1})\right)$$

Ring structures do not pass through the theta-link or log-link. Galois and fundamental groups do pass.

To restore rings from such groups one uses anabelian geometry results about number fields and hyperbolic curves over them and their completions.

In bounding the non-commutativity of relevant diagrammes one uses that fact that the group acting on the flow of information passes intact through the algorithmic process.

Recently, this idea has found applications in quantum computing and quantum computers.

On IUT, very briefly

The theta-link in IUT represents the multiplicative rescaling $q \to q^n$.

This link involves the non-archimedean (étale) theta-function and its special values.

This is related to the Jacobi triple product

$$\theta(u) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u) \prod_{n\geqslant 1} \left((1-q^n)(1-q^n u)(1-q^n u^{-1})\right)$$

Ring structures do not pass through the theta-link or log-link. Galois and fundamental groups do pass.

To restore rings from such groups one uses anabelian geometry results about number fields and hyperbolic curves over them and their completions.

In bounding the non-commutativity of relevant diagrammes one uses that fact that the group acting on the flow of information passes intact through the algorithmic process.

Recently, this idea has found applications in quantum computing and quantum computers.

On IUT, very briefly

Unlike the Langlands correspondences which rather involve the use of linear objects, one has to use the full arithmetic fundamental groups in anabelian geometry and IUT.

In particular, two properties of such groups, not seen and not used in the Langlands correspondences, play fundamental role in anabelian geometry:

– every open subgroup is centre-free,

– every nontrivial normal closed subgroup H of any open subgroup, with the property that H is topologically finitely generated as a group, is open.

On IUT, very briefly

Unlike the Langlands correspondences which rather involve the use of linear objects, one has to use the full arithmetic fundamental groups in anabelian geometry and IUT.

In particular, two properties of such groups, not seen and not used in the Langlands correspondences, play fundamental role in anabelian geometry:

– every open subgroup is centre-free,

– every nontrivial normal closed subgroup H of any open subgroup, with the property that H is topologically finitely generated as a group, is open.

Enhanced IUT and effective abc

The original IUT theory did not prove effective abc inequalities.

One of the reasons for that was that the residue prime $p = 2$ was excluded from a prerequisite theory of étale function theory.

Porowski (at that time a PhD student) found a way to include the even residue characteristic case into étale theta function theory, using roots of order 6 instead of roots of order 2 as in the previous IUT theory.

This was used in developing an enhanced IUT theory that works in any residue characteristic.

Together with other new ingredients, this led to a paper by Mochizuki, Fesenko, Hoshi, Minamide, Porowski published in 2022. It contains first proofs of effective abc and Szpiro inequalities.

Enhanced IUT and effective abc

The original IUT theory did not prove effective abc inequalities.

One of the reasons for that was that the residue prime $p = 2$ was excluded from a prerequisite theory of étale function theory.

Porowski (at that time a PhD student) found a way to include the even residue characteristic case into étale theta function theory, using roots of order 6 instead of roots of order 2 as in the previous IUT theory.

This was used in developing an enhanced IUT theory that works in any residue characteristic.

Together with other new ingredients, this led to a paper by Mochizuki, Fesenko, Hoshi, Minamide, Porowski published in 2022. It contains first proofs of effective abc and Szpiro inequalities.

Enhanced IUT and effective abc

The original IUT theory did not prove effective abc inequalities.

One of the reasons for that was that the residue prime $p = 2$ was excluded from a prerequisite theory of étale function theory.

Porowski (at that time a PhD student) found a way to include the even residue characteristic case into étale theta function theory, using roots of order 6 instead of roots of order 2 as in the previous IUT theory.

This was used in developing an enhanced IUT theory that works in any residue characteristic.

Together with other new ingredients, this led to a paper by Mochizuki, Fesenko, Hoshi, Minamide, Porowski published in 2022. It contains first proofs of effective abc and Szpiro inequalities.

Enhanced IUT and effective abc

The original IUT theory did not prove effective abc inequalities.

One of the reasons for that was that the residue prime $p = 2$ was excluded from a prerequisite theory of étale function theory.

Porowski (at that time a PhD student) found a way to include the even residue characteristic case into étale theta function theory, using roots of order 6 instead of roots of order 2 as in the previous IUT theory.

This was used in developing an enhanced IUT theory that works in any residue characteristic.

Together with other new ingredients, this led to a paper by Mochizuki, Fesenko, Hoshi, Minamide, Porowski published in 2022. It contains first proofs of effective abc and Szpiro inequalities.

THEOREM B (Effective version of a conjecture of Szpiro). *Let* a, b, c *be nonzero coprime integers such that*

$$a + b + c = 0;$$

ε *a positive real number* ≤ 1. *Then we have*

$$\begin{aligned} |abc| &\leq 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30} \cdot \varepsilon^{-166/81}), (\mathrm{rad}(abc))^{3(1+\varepsilon)}\} \\ &\leq 2^4 \cdot \exp(1.7 \cdot 10^{30} \cdot \varepsilon^{-166/81}) \cdot (\mathrm{rad}(abc))^{3(1+\varepsilon)} \end{aligned}$$

Effective abc and FLT

Let's see how this effective abc inequality can be applied to the Fermat equation.

Assume that x, y, z are coprime positive integers that are a solution of the equation $X^n + Y^n = Z^n$ for a positive integer n.

Denote $a = x^n, b = y^n, c = z^n$.

If $x < y$ then $x \geqslant 2$, $y^n > z^n/2$, $n\log(xyz) > 2n\log(z)$. Using $\mathrm{rad}(xyz) \leqslant xyz < z^3$ the effective abc implies

$$2n\log z < n\log(xyz) \leqslant \log 16 + 1.7 \cdot 10^{30} + 18\log z$$

so

$$(n-9)\log z \leqslant \log 4 + 8.5 \cdot 10^{29}.$$

Since $z \geqslant 5$, we deduce $n < 5.3 \cdot 10^{29}$.

Thus the effective abc inequality (2022) implies that the Fermat equation does not have positive integer solutions when $n \geqslant 5.3 \cdot 10^{29}$.

Effective abc and FLT

Let's see how this effective abc inequality can be applied to the Fermat equation.

Assume that x, y, z are coprime positive integers that are a solution of the equation $X^n + Y^n = Z^n$ for a positive integer n.

Denote $a = x^n, b = y^n, c = z^n$.

If $x < y$ then $x \geqslant 2$, $y^n > z^n/2$, $n\log(xyz) > 2n\log(z)$. Using $\mathrm{rad}(xyz) \leqslant xyz < z^3$ the effective abc implies

$$2n\log z < n\log(xyz) \leqslant \log 16 + 1.7 \cdot 10^{30} + 18\log z$$

so

$$(n-9)\log z \leqslant \log 4 + 8.5 \cdot 10^{29}.$$

Since $z \geqslant 5$, we deduce $n < 5.3 \cdot 10^{29}$.

Thus the effective abc inequality (2022) implies that the Fermat equation does not have positive integer solutions when $n \geqslant 5.3 \cdot 10^{29}$.

Effective abc and FLT

However, modern computers cannot check that the Fermat equation does not have positive solutions for all integers n up to $5.3 \cdot 10^{29}$.

So, some *lower bounds* on possible solutions of the Fermat equation, such as

$$xyz > f(n)$$

with some very rapidly growing function $f(n)$ of n are needed to deduce the full FLT or reduce to the range of n to a much smaller range where FLT can be checked using modern computers.

Effective abc and FLT

However, modern computers cannot check that the Fermat equation does not have positive solutions for all integers n up to $5.3 \cdot 10^{29}$.

So, some *lower bounds* on possible solutions of the Fermat equation, such as

$$xyz > f(n)$$

with some very rapidly growing function $f(n)$ of n are needed to deduce the full FLT or reduce to the range of n to a much smaller range where FLT can be checked using modern computers.

Effective abc and diophantine equations

Getting lower bounds for Diophantine equations is a sort of problem which number theorists had not applied substantial efforts to study to before the 2022 paper, since its value becomes clear only after one gets an effective abc inequality with an explicitly given constant in it.

Finding lower bounds for Diophantine equations and applying effective abc inequalities becomes a new key activity after the 2022 paper.

This fundamentally changes the study of Diophantine equations.

Effective abc and diophantine equations

Getting lower bounds for Diophantine equations is a sort of problem which number theorists had not applied substantial efforts to study to before the 2022 paper, since its value becomes clear only after one gets an effective abc inequality with an explicitly given constant in it.

Finding lower bounds for Diophantine equations and applying effective abc inequalities becomes a new key activity after the 2022 paper.

This fundamentally changes the study of Diophantine equations.

Effective abc and FLT

Example (in the case of FLT):

the 2022 paper contain an elementary argument to show that

$$z > (n+1)^n/2$$

if n is an odd prime.

Substituting this lower bound in the effective abc inequality we get

$$n < 1.62 \cdot 10^{14}$$

Thus, for larger prime n the Fermat equation does not have positive integer solutions.

Effective abc and FLT

More than 30 years ago Coppersmith did computer verification in the first case of FLT (i.e. xyz is prime to n) to check that it holds true for all odd prime numbers $n < 6 \cdot 10^{17}$.

Using his work, the effective abc and the lower bound imply the first case of FLT.

Effective abc and FLT

More than 30 years ago Coppersmith did computer verification in the first case of FLT (i.e. xyz is prime to n) to check that it holds true for all odd prime numbers $n < 6 \cdot 10^{17}$.

Using his work, the effective abc and the lower bound imply the first case of FLT.

Effective abc and FLT

Case II of FLT (i.e. xyz is divisible by n) was computationally known for odd prime numbers n up to 10^{12}.

The best lower bound for Case II of FLT was obtained in 1947 and its use in the application of effective abc reduces $1.62 \cdot 10^{14}$ to $9.39 \cdot 10^{13}$.

The best networks of modern computers currently available could not extend that computation to $9.39 \cdot 10^{13}$.

So, new sharper lower bounds for Case II were needed.

They were produced by Mihăilescu in 2021:

if xyz is divisible by prime $n > 256$ then $z > n^{2.5^{n-1}}$.

Substituting in the effective abc inequality, and using Vandiver's result (1930) that FLT holds for all odd primes n up to 269, one obtains the proof of full FLT.

Effective abc and FLT

Case II of FLT (i.e. xyz is divisible by n) was computationally known for odd prime numbers n up to 10^{12}.

The best lower bound for Case II of FLT was obtained in 1947 and its use in the application of effective abc reduces $1.62 \cdot 10^{14}$ to $9.39 \cdot 10^{13}$.

The best networks of modern computers currently available could not extend that computation to $9.39 \cdot 10^{13}$.

So, new sharper lower bounds for Case II were needed.

They were produced by Mihăilescu in 2021:

if xyz is divisible by prime $n > 256$ then $z > n^{2.5^{n-1}}$.

Substituting in the effective abc inequality, and using Vandiver's result (1930) that FLT holds for all odd primes n up to 269, one obtains the proof of full FLT.

Effective abc and FLT

Case II of FLT (i.e. xyz is divisible by n) was computationally known for odd prime numbers n up to 10^{12}.

The best lower bound for Case II of FLT was obtained in 1947 and its use in the application of effective abc reduces $1.62 \cdot 10^{14}$ to $9.39 \cdot 10^{13}$.

The best networks of modern computers currently available could not extend that computation to $9.39 \cdot 10^{13}$.

So, new sharper lower bounds for Case II were needed.

They were produced by Mihăilescu in 2021:

if xyz is divisible by prime $n > 256$ then $z > n^{2.5^{n-1}}$.

Substituting in the effective abc inequality, and using Vandiver's result (1930) that FLT holds for all odd primes n up to 269, one obtains the proof of full FLT.

Effective abc and generalised FLT

Questions. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of

$$X^p + cY^p = Z^p,$$

for, say, $c = 2, 3, \dots, p$;

$$X^p + Y^p = Z^{s(p)}$$

where $s(p)$ is a strictly increasing positive integer valued function of p;

generalised Fermat's equation

$$X^p + Y^q = Z^r,$$

this equation is expected not to have coprime positive integer solutions when $\min\{p, q, r\} > 2$ (Beal set a \$1m Prize administered by the AMS);

$$aX^p + bY^q = cZ^r.$$

Effective abc and generalised FLT

Questions. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of

$$X^p + cY^p = Z^p,$$

for, say, $c = 2, 3, \dots, p$;

$$X^p + Y^p = Z^{s(p)}$$

where $s(p)$ is a strictly increasing positive integer valued function of p;

generalised Fermat's equation

$$X^p + Y^q = Z^r,$$

this equation is expected not to have coprime positive integer solutions when $\min\{p, q, r\} > 2$ (Beal set a \$1m Prize administered by the AMS);

$$aX^p + bY^q = cZ^r.$$

Effective abc and generalised FLT

Questions. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of

$$X^p + cY^p = Z^p,$$

for, say, $c = 2, 3, \ldots, p$;

$$X^p + Y^p = Z^{s(p)}$$

where $s(p)$ is a strictly increasing positive integer valued function of p;

generalised Fermat's equation

$$X^p + Y^q = Z^r,$$

this equation is expected not to have coprime positive integer solutions when $\min\{p, q, r\} > 2$ (Beal set a \$1m Prize administered by the AMS);

$$aX^p + bY^q = cZ^r.$$

Effective abc and generalised FLT

Questions. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of

$$X^p + cY^p = Z^p,$$

for, say, $c = 2, 3, \dots, p$;

$$X^p + Y^p = Z^{s(p)}$$

where $s(p)$ is a strictly increasing positive integer valued function of p;

generalised Fermat's equation

$$X^p + Y^q = Z^r,$$

this equation is expected not to have coprime positive integer solutions when $\min\{p, q, r\} > 2$ (Beal set a \$1m Prize administered by the AMS);

$$aX^p + bY^q = cZ^r.$$

A deeper question

Do lower bounds for Diophantine equations have their origin in a yet unknown property of addition and multiplication that is kind of dual to abc inequalities?