The effective abc inequality and how it was applied to a new proof of FLT

Ivan Fesenko

abc inequalities

For a non-zero integer $n = \pm \prod p_i^{m_i}$ its radical $\mathrm{rad}(n) = \prod p_i$.

A general abc conjecture (Szpiro, Oesterle, Masser)

there is a real number $m \geqslant 1$ such that
for every positive real ε there is a positive real $\kappa(\varepsilon)$
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.

abc inequalities

For a non-zero integer $n = \pm \prod p_i^{m_i}$ its radical $\mathrm{rad}(n) = \prod p_i$.

A general abc conjecture (Szpiro, Oesterle, Masser)

there is a real number $m \geqslant 1$ *such that*
for every positive real ε *there is a positive real* $\kappa(\varepsilon)$
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.

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, in the West 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, in the West 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, in the West 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 known as a function of ε, 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.

In applications, $\varepsilon = 1$ is often as useful as the case of arbitrary positive ε.

abc inequalities

A naive version with $m = \kappa(1) = 1$ immediately implies FLT for $n > 5$:

Let x, y, z be coprime positive integers that are a solution of $X^n + Y^n = Z^n$.

Put $a = x^n, b = y^n, c = z^n$. Then $z > 1$.

The naive abc inequality for $\varepsilon = 1$ implies

$z^n = c < \mathrm{rad}(x^n y^n z^n)^2 = \mathrm{rad}(xyz)^2 \leqslant (xyz)^2 < z^6$,

so $n \leqslant 5$.

Example. Let $a = 1$, $b = 64^n - 1$, $c = 64^n$.

Then b is divisible by 63 and hence by 9.

We have

$$\mathrm{rad}(abc) = 2\,\mathrm{rad}(b) \leqslant 6\,\mathrm{rad}(b/9) \leqslant 6b/9 = 2b/3 = 2(c-1)/3 < c.$$

So there are infinitely many relatively prime positive integer $a, b, c = a + b$ such that

$$c > \mathrm{rad}(abc),$$

hence ε is needed in the statement of the inequality.

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 after 9 years of referees work, several workshops, and over 1000 questions asked and answered about IUT.

IUT 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 after 9 years of referees work, several workshops, and over 1000 questions asked and answered about IUT.

IUT 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

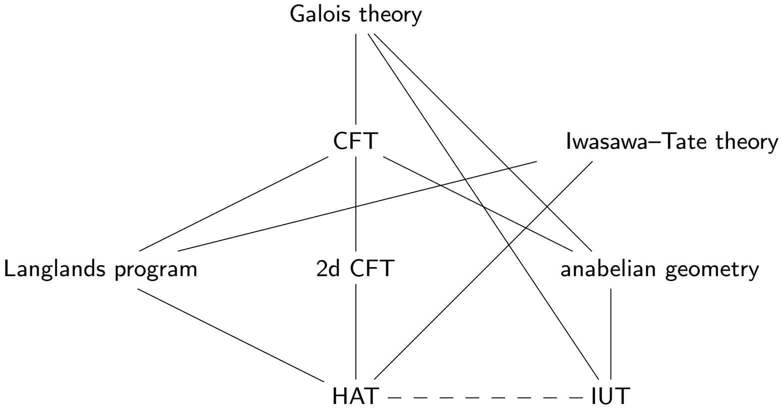
Inter-universal Teichmüller theory (IUT) of Mochizuki was published in 2021 after 9 years of referees work, several workshops, and over 1000 questions asked and answered about IUT.

IUT 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



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 which is the essence of anabelian geometry in this case, one *restores* addition and the full ring structure of k.

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 which is the essence of anabelian geometry in this case, one *restores* addition and the full ring structure of k.

Group theoretical constructions in number theory

Which key constructions/algorithms 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.

So, one of the meanings of class formations axioms in class field theory is that they separate the ring-theoretic part of class field theory from its group-theoretic part.

Group theoretical constructions in number theory

Which key constructions/algorithms 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.

So, one of the meanings of class formations axioms in class field theory is that they separate the ring-theoretic part of class field theory from its group-theoretic part.

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

His 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.

This is fundamentally 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 for hyperbolic curves over number fields and their completions was proposed by Grothendieck in 1983 He was not aware of the work for number fields.

His 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.

This is fundamentally 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 for hyperbolic curves over number fields and their completions was proposed by Grothendieck in 1983 He was not aware of the work for number fields.

His 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.

This is fundamentally 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 for hyperbolic curves over number fields and their completions was proposed by Grothendieck in 1983 He was not aware of the work for number fields.

His 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.

This is fundamentally 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 for hyperbolic curves over number fields and their completions was proposed by Grothendieck in 1983 He was not aware of the work for number fields.

His 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.

This is fundamentally 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)
a universal functorial group theoretical algorithm is explicitly described
to reconstruct the field F from the topological group $\pi_1(C_F)$, where $C_F = C \times_K F$, $F = K$ or any of its non-archimedean completions.

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)
a universal functorial group theoretical algorithm is explicitly described
to reconstruct the field F from the topological group $\pi_1(C_F)$, where $C_F = C \times_K F$,
$F = K$ or any of its non-archimedean completions.

On 2d anabelian geometry, very briefly

Note that in general one cannot restore a mixed characteristic local field with finite residue field from its absolute Galois group, so working with hyperbolic curves (2d world) allows one to see more about the 1d world.

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

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 and even counter-intuitive to working arithmetic geometers.

On 2d anabelian geometry, very briefly

Note that in general one cannot restore a mixed characteristic local field with finite residue field from its absolute Galois group, so working with hyperbolic curves (2d world) allows one to see more about the 1d world.

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

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 and even counter-intuitive to working arithmetic geometers.

On IUT, very briefly

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 contributions 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 by introducing relevant indeterminacies.

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

On IUT, very briefly

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 contributions 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 by introducing relevant indeterminacies.

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

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.

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 problem stated 400 years after Qin Jiushao gave a complete proof of Chinese remainder theorem.

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 $x \geqslant 2$, $y^n > z^n/2$, $n \log(xyz) > 2n \log(z)$.

Since $\operatorname{rad}(xyz) \leqslant xyz < z^3$, 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 $n < 5.3 \cdot 10^{29}$.

Effective abc and FLT

Let's see how this effective abc inequality can be applied to the Fermat problem stated 400 years after Qin Jiushao gave a complete proof of Chinese remainder theorem.

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 $x \geqslant 2$, $y^n > z^n/2$, $n\log(xyz) > 2n\log(z)$.
Since $\mathrm{rad}(xyz) \leqslant xyz < z^3$, 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 $n < 5.3 \cdot 10^{29}$.

Effective abc and FLT

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

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

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

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 in Diophantine Geometry, after our 2022 paper.

This fundamentally changes the study of Diophantine equations, the 2000 years old area of mathematics.

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 in Diophantine Geometry, after our 2022 paper.

This fundamentally changes the study of Diophantine equations, the 2000 years old area of mathematics.

Effective abc and FLT

Examples of lower bounds for FLT.

The 2022 paper contains a math olympiad problem kind of 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 previous lower bound imply the full 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 previous lower bound imply the full 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 only 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.*

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 only 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.*

Effective abc and FLT

They were produced by Mihăilescu in 2021, after my talk at Gottingen.

if xyz *is divisible by prime* $n > 256$ *then* $z > n^{2.5^{n-1}}$ (double exponential lower bound)

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, entirely different from the Wiles proof.

Effective abc and FLT

They were produced by Mihăilescu in 2021, after my talk at Gottingen.

if xyz is divisible by prime $n > 256$ *then* $z > n^{2.5^{n-1}}$ (double exponential lower bound)

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, entirely different from the Wiles proof.

Effective abc and generalised FLT

Questions, to do similar things for other types of Diophantine equations.

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

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

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

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

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

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

3. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of 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 for this equation.

Effective abc and generalised FLT

Questions, to do similar things for other types of Diophantine equations.

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

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

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

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

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

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

3. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of 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 for this equation.

Effective abc and generalised FLT

Questions, to do similar things for other types of Diophantine equations.

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

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

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

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

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

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

3. Find lower bounds to apply effective abc inequalities to find all positive integer solutions of 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 for this equation.

IUT Prizes

There are two recent IUT prizes, funded by Kawakami, and associated to the new Inter-universal Geometry Centre in Tokyo, https://zen-univ.jp/en/iugc

The IUT Innovator Prize will be awarded annually, within a scope from $20,000 to $100,000, to the best paper containing new and important developments in IUT theory and related fields.

The IUT Challenger Prize of $1,000,000 will be awarded to the first mathematician to publish a paper on the IUT theory that shows an inherent serious flaw in the theory.