Introduction to the abc conjecture

Xinyi Yuan

University of California, Berkeley

January 25, 2019

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture.*

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture*.
- *Application to Fermat's last theorem*.

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture.*
- *Application to Fermat's last theorem.*
- *Numerical evidence.*

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture.*
- *Application to Fermat's last theorem.*
- *Numerical evidence.*
- *Polynomial analogue.*

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture*.
- *Application to Fermat's last theorem*.
- *Numerical evidence.*
- *Polynomial analogue.*
- *Effective Mordell conjecture*.

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture.*
- *Application to Fermat's last theorem.*
- *Numerical evidence.*
- *Polynomial analogue.*
- *Effective Mordell conjecture.*
- *More equivalent conjectures.*

Abstract

The goal of this presentation is to introduce the abc conjecture. The following topics will be covered:

- *Statements of the abc conjecture.*
- *Application to Fermat's last theorem.*
- *Numerical evidence.*
- *Polynomial analogue.*
- *Effective Mordell conjecture.*
- *More equivalent conjectures.*
- *Mochizuki's work.*

Overview

Statements of the abc conjecture

Oesterlé and Masser

The abc conjecture was proposed in the 1980s by

- Joseph Oesterlé (French mathematician),

Oesterlé and Masser

The abc conjecture was proposed in the 1980s by

- Joseph Oesterlé (French mathematician),
- David Masser (British mathematician).

Oesterlé and Masser

The abc conjecture was proposed in the 1980s by

- Joseph Oesterlé (French mathematician),
- David Masser (British mathematician).

Oesterlé and Masser

The abc conjecture was proposed in the 1980s by

- Joseph Oesterlé (French mathematician),
- David Masser (British mathematician).

It is also called the Oesterlé–Masser conjecture.

The radical of a positive integer

Let N be a positive integer. The *radical* of N is just

$$\mathrm{rad}(N) = \prod_{p|N \text{ prime}} p.$$

The radical of a positive integer

Let N be a positive integer. The *radical* of N is just

$$\mathrm{rad}(N) = \prod_{p|N \text{ prime}} p.$$

By the unique factorization theorem, we can write

$$N = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

where $p_1, p_2, \cdots, p_r$ are distinct primes numbers and $m_1, m_2, \cdots, m_r$ are positive integers. Then

$$\mathrm{rad}(N) = p_1 p_2 \cdots p_r.$$

abc triple

An *abc triple* is a triple (a, b, c) of positive integers a, b, c such that

$$a + b = c$$

and

$$\gcd(a, b) = 1.$$

abc triple

An *abc triple* is a triple (a, b, c) of positive integers a, b, c such that

$$a + b = c$$

and

$$\gcd(a, b) = 1.$$

The abc conjecture compares the radical $\mathrm{rad}(abc)$ of the product abc with c. A trivial bound is

$$\mathrm{rad}(abc) \leq abc < c^3.$$

However, the conjecture asserts that we can also bound c by a power of $\mathrm{rad}(abc)$.

The conjecture

Conjecture (abc conjecture, Oesterlé–Masser conjecture)

For any real number $\epsilon > 0$, there exists a real number $K_\epsilon > 0$ such that

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

for any abc triple (a, b, c).

The conjecture

Conjecture (abc conjecture, Oesterlé–Masser conjecture)

For any real number $\epsilon > 0$, there exists a real number $K_\epsilon > 0$ such that

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

for any abc triple (a, b, c).

The conjecture says that *abc* cannot have "too many" repeated prime factors of "high multiplicity" if

$$a + b = c, \quad \gcd(a, b) = 1.$$

Other forms

There are many other forms of the conjecture. For example, one can just ask for a single ϵ satisfying the property.

Other forms

There are many other forms of the conjecture. For example, one can just ask for a single ϵ satisfying the property.

Conjecture (abc conjecture: weak form)

There exist $\epsilon > 0$ and $K > 0$ such that

$$c < K \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

for any abc triple (a, b, c).

Other forms

There are many other forms of the conjecture. For example, one can just ask for a single ϵ satisfying the property.

Conjecture (abc conjecture: weak form)

There exist $\epsilon > 0$ and $K > 0$ such that

$$c < K \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

for any abc triple (a, b, c).

Other forms

There are many other forms of the conjecture. For example, one can just ask for a single ϵ satisfying the property.

Conjecture (abc conjecture: weak form)

There exist $\epsilon > 0$ and $K > 0$ such that

$$c < K \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

for any abc triple (a, b, c).

The following may be the most convenient form.

Conjecture (abc conjecture: Baker's form)

One has

$$c < \mathrm{rad}(abc)^{1.75}$$

for any abc triple (a, b, c).

Application to Fermat's last theorem

Fermat's last theorem

Theorem (Fermat's last theorem)

For any integer $n \geq 3$, any integer solution of the equation

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

has $x = 0$, $y = 0$ or $z = 0$.

Theorem (Fermat's last theorem)

For any integer $n \geq 3$, any integer solution of the equation

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

has $x = 0$, $y = 0$ or $z = 0$.

Fermat's last theorem

Theorem (Fermat's last theorem)

For any integer $n \geq 3$, any integer solution of the equation

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

has $x = 0$, $y = 0$ or $z = 0$.

This was stated by Pierre de Fermat in 1637, and finally proved by Andrew Wiles and Richard Taylor in 1994.

Fermat's last theorem

Theorem (Fermat's last theorem)

For any integer $n \geq 3$, any integer solution of the equation

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

has $x = 0$, $y = 0$ or $z = 0$.

This was stated by Pierre de Fermat in 1637, and finally proved by Andrew Wiles and Richard Taylor in 1994.

For stories of Fermat's last theorem, google or wiki...

Fermat's last theorem

Wiles and Taylor actually proved the modularity conjecture, which asserts that any (semistable) elliptic curve over $\mathbb{Q}$ is *modular*, i.e., corresponds to a modular form in a natural way.

Fermat's last theorem

Wiles and Taylor actually proved the modularity conjecture, which asserts that any (semistable) elliptic curve over $\mathbb{Q}$ is *modular*, i.e., corresponds to a modular form in a natural way.

To prove Fermat's last theorem by the modularity conjecture, one also needs Frey's construction and Ken Ribet's theorem of level lowering.

abc implies Fermat

abc implies Fermat

Assume that Fermat's last theorem fails; i.e.,

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

for positive integers $n \geq 3$, x, y, and z. Assume that $\gcd(x, y) = 1$. Then (x^n, y^n, z^n) is an abc triple.

abc implies Fermat

Assume that Fermat's last theorem fails; i.e.,

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

for positive integers $n \geq 3$, x, y, and z. Assume that $\gcd(x, y) = 1$. Then (x^n, y^n, z^n) is an abc triple.

Assume Baker's form of the abc conjecture:

$$c < \mathrm{rad}(abc)^{1.75}.$$

abc implies Fermat

Assume that Fermat's last theorem fails; i.e.,

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

for positive integers $n \geq 3$, x, y, and z. Assume that $\gcd(x, y) = 1$. Then (x^n, y^n, z^n) is an abc triple.

Assume Baker's form of the abc conjecture:

$$c < \mathrm{rad}(abc)^{1.75}.$$

Then we have

$$z^n < \mathrm{rad}(x^n y^n z^n)^{1.75} \leq (xyz)^{1.75} < z^{1.75\times 3} = z^{5.25}.$$

This implies $n = 3, 4, 5$.

abc implies Fermat

If we know the weaker form of the abc conjecture, then we will get a (probably weaker) upper bound of n. Then the problem is still reduced to small n.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.
- $n = 5$: Legendre, Dirichlet, 1825.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.
- $n = 5$: Legendre, Dirichlet, 1825.
- $n = 7$: Lamé, 1839.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.
- $n = 5$: Legendre, Dirichlet, 1825.
- $n = 7$: Lamé, 1839.
- n is a regular prime: Kummer, 1858. Conjecturally, approximately 61% of the primes are regular. The only irregular primes less than 100 are 37, 59 and 67.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.
- $n = 5$: Legendre, Dirichlet, 1825.
- $n = 7$: Lamé, 1839.
- n is a regular prime: Kummer, 1858. Conjecturally, approximately 61% of the primes are regular. The only irregular primes less than 100 are 37, 59 and 67.
- $n < 2521$: Vandiver, 1954.

Fermat's last theorem for small n

Fermat's last theorem was proved for small n before Wiles:

- $n = 4$: Fermat. After this, the problem is reduced to the case that n is a prime.
- $n = 3$: Leonhard Euler, 1770.
- $n = 5$: Legendre, Dirichlet, 1825.
- $n = 7$: Lamé, 1839.
- n is a regular prime: Kummer, 1858. Conjecturally, approximately 61% of the primes are regular. The only irregular primes less than 100 are 37, 59 and 67.
- $n < 2521$: Vandiver, 1954.
- $n < 4 \times 10^6$: 1993.

Numerical evidence

Exponential bounds

We want to bound c by a polynomial of $\mathrm{rad}(abc)$. Unfortunately, we only know exponential bounds. For example, Stewart and Yu proved in 2001 that

$$c < \exp(L_\epsilon \cdot \mathrm{rad}(abc)^{\frac{1}{3}+\epsilon}).$$

The logarithms

For an abc triple (a, b, c), denote

$$q(a, b, c) = \frac{\log c}{\log \mathrm{rad}(abc)}.$$

Recall that Baker's version of the abc conjecture:

$$c < \mathrm{rad}(abc)^{1.75} \Longleftrightarrow q(a, b, c) < 1.75.$$

The logarithms

For an abc triple (a, b, c), denote

$$q(a, b, c) = \frac{\log c}{\log \mathrm{rad}(abc)}.$$

Recall that Baker's version of the abc conjecture:

$$c < \mathrm{rad}(abc)^{1.75} \iff q(a, b, c) < 1.75.$$

The original form of the abc conjecture is equivalent to the following statement:

- For any $\epsilon > 0$, all but finitely many abc triples (a, b, c) satisfies the inequality $q(a, b, c) < 1 + \epsilon$.

numerical evidence

- If $c < 10^{18}$, there are only 160 abc triples with $q(a, b, c) > 1.4$.

numerical evidence

- If $c < 10^{18}$, there are only 160 abc triples with $q(a, b, c) > 1.4$.
- Largest $q(a, b, c)$ we know is given by:

$$2 + 3^{10} \cdot 109 = 23^5, \qquad q(a, b, c) \approx 1.6299.$$

numerical evidence

- If $c < 10^{18}$, there are only 160 abc triples with $q(a, b, c) > 1.4$.
- Largest $q(a, b, c)$ we know is given by:

$$2 + 3^{10} \cdot 109 = 23^5, \qquad q(a, b, c) \approx 1.6299.$$

- Another triple with big $q(a, b, c)$ but relatively small c is given by:

$$1 + 2 \cdot 3^7 = 5^4 \cdot 7, \qquad q(a, b, c) \approx 1.5679.$$

Polynomial analogue

Polynomial analogue

Theorem (Mason–Stothers 1981)

Let $a = a(t)$, $b = b(t)$, and $c = c(t)$ be coprime polynomials with real coefficients such that $a + b = c$ and such that not all of them are constant polynomials. Then

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(\mathrm{rad}(abc)) - 1.$$

Here $\mathrm{rad}(abc)$ is the product of the distinct irreducible factors of abc.

Polynomial analogue

Theorem (Mason–Stothers 1981)

Let $a = a(t)$, $b = b(t)$, and $c = c(t)$ be coprime polynomials with real coefficients such that $a + b = c$ and such that not all of them are constant polynomials. Then

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(\mathrm{rad}(abc)) - 1.$$

Here $\mathrm{rad}(abc)$ is the product of the distinct irreducible factors of abc.

Polynomial analogue

Theorem (Mason–Stothers 1981)

Let $a = a(t)$, $b = b(t)$, and $c = c(t)$ be coprime polynomials with real coefficients such that $a + b = c$ and such that not all of them are constant polynomials. Then

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(\mathrm{rad}(abc)) - 1.$$

Here $\mathrm{rad}(abc)$ is the product of the distinct irreducible factors of abc.

The theorem holds for polynomials over any field k (instead of just $\mathbb{R}$). However, if the characteristic of k is positive, we need to assume that not all of the derivatives of a, b, c are zero. This is to exclude triples like

$$(a^{p^n}, b^{p^n}, (a+b)^{p^n}).$$

Polynomial analogue

Why is it an analogue?

Polynomial analogue

Why is it an analogue?

- $\mathbb{Z}$ and $\mathbb{R}[t]$ are analogous. Both are unique factorization domains (and even principal ideal domains), as a consequence of the division algorithm (the long division).

Polynomial analogue

Why is it an analogue?

- $\mathbb{Z}$ and $\mathbb{R}[t]$ are analogous. Both are unique factorization domains (and even principal ideal domains), as a consequence of the division algorithm (the long division).
- Write $|f| = e^{\deg(f)}$ for any $f \in \mathbb{R}[t]$. This gives a metric over $\mathbb{R}[t]$. It is also multiplicative in the sense that $|fg| = |f| \cdot |g|$. Then it is an analogue of the usual absolute value $|n|$ for $n \in \mathbb{Z}$.

Polynomial analogue

Why is it an analogue?

- $\mathbb{Z}$ and $\mathbb{R}[t]$ are analogous. Both are unique factorization domains (and even principal ideal domains), as a consequence of the division algorithm (the long division).
- Write $|f| = e^{\deg(f)}$ for any $f \in \mathbb{R}[t]$. This gives a metric over $\mathbb{R}[t]$. It is also multiplicative in the sense that $|fg| = |f| \cdot |g|$. Then it is an analogue of the usual absolute value $|n|$ for $n \in \mathbb{Z}$.
- Finally,

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(\mathrm{rad}(abc)) - 1$$

becomes

$$\max\{|a|, |b|, |c|)\} \leq e^{-1}|\mathrm{rad}(abc)|.$$

It corresponds to the integer version with $\epsilon = 0$.

Polynomial analogue: the proof

The polynomial analogue is surprisingly easy to prove, compared to the original integer version. The following proof is due to Snyder in 2000.

Polynomial analogue: the proof

The polynomial analogue is surprisingly easy to prove, compared to the original integer version. The following proof is due to Snyder in 2000.

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

Polynomial analogue: the proof

The polynomial analogue is surprisingly easy to prove, compared to the original integer version. The following proof is due to Snyder in 2000.

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

(1) We have an equality of Wronskians:

$$ab' - a'b = bc' - b'c = ca' - c'a.$$

Polynomial analogue: the proof

The polynomial analogue is surprisingly easy to prove, compared to the original integer version. The following proof is due to Snyder in 2000.

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

(1) We have an equality of Wronskians:

$$ab' - a'b = bc' - b'c = ca' - c'a.$$

Polynomial analogue: the proof

The polynomial analogue is surprisingly easy to prove, compared to the original integer version. The following proof is due to Snyder in 2000.

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

(1) We have an equality of Wronskians:

$$ab' - a'b = bc' - b'c = ca' - c'a.$$

In fact, for the matrix

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix},$$

the sum of the three columns is 0. Therefore,

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = \begin{vmatrix} b & c \\ b' & c' \end{vmatrix} = \begin{vmatrix} c & a \\ c' & a' \end{vmatrix}.$$

Polynomial analogue: the proof

(2) Denote

$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$

Then $W \neq 0$ by $\gcd(a, b) = 1$.

Polynomial analogue: the proof

(2) Denote

$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$

Then $W \neq 0$ by $\gcd(a, b) = 1$.

(3) We have

$$\deg(W) \geq \deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')).$$

Polynomial analogue: the proof

(2) Denote
$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$
Then $W \neq 0$ by $\gcd(a, b) = 1$.

(3) We have
$$\deg(W) \geq \deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')).$$

Polynomial analogue: the proof

(2) Denote

$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$

Then $W \neq 0$ by $\gcd(a, b) = 1$.

(3) We have

$$\deg(W) \geq \deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')).$$

In fact, W is divisible by the coprime polynomials $\gcd(a, a')$, $\gcd(b, b')$ and $\gcd(c, c')$.

(4) We have

$$\gcd(a, a') = a/\mathrm{rad}(a),$$
$$\gcd(b, b') = b/\mathrm{rad}(b),$$
$$\gcd(c, c') = c/\mathrm{rad}(c).$$

Polynomial analogue: the proof

(2) Denote
$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$
Then $W \neq 0$ by $\gcd(a, b) = 1$.

(3) We have
$$\deg(W) \geq \deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')).$$
In fact, W is divisible by the coprime polynomials $\gcd(a, a')$, $\gcd(b, b')$ and $\gcd(c, c')$.

(4) We have
$$\gcd(a, a') = a/\mathrm{rad}(a),$$
$$\gcd(b, b') = b/\mathrm{rad}(b),$$
$$\gcd(c, c') = c/\mathrm{rad}(c).$$

Polynomial analogue: the proof

(2) Denote

$$W = ab' - a'b = bc' - b'c = ca' - c'a.$$

Then $W \neq 0$ by $\gcd(a, b) = 1$.

(3) We have

$$\deg(W) \geq \deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')).$$

In fact, W is divisible by the coprime polynomials $\gcd(a, a')$, $\gcd(b, b')$ and $\gcd(c, c')$.

(4) We have

$$\gcd(a, a') = a/\mathrm{rad}(a),$$
$$\gcd(b, b') = b/\mathrm{rad}(b),$$
$$\gcd(c, c') = c/\mathrm{rad}(c).$$

In fact, if $p = p(t)$ is an irreducible factor of $a = a(t)$ of multiplicity $m > 0$, then the multiplicity of p in $a' = a'(t)$ is $m - 1$.

Polynomial analogue: the proof

(5) Combine (3) and (4). We have

$$\deg(W) \geq \deg(abc) - \deg(\mathrm{rad}(abc)).$$

Polynomial analogue: the proof

(5) Combine (3) and (4). We have

$$\deg(W) \geq \deg(abc) - \deg(\mathrm{rad}(abc)).$$

(6) By (5) and

$$\deg(W) = \deg(ab' - a'b) \leq \deg(ab) - 1,$$

we have

$$\deg(c) \leq \deg(\mathrm{rad}(abc)) - 1.$$

Polynomial analogue: the proof

(5) Combine (3) and (4). We have

$$\deg(W) \geq \deg(abc) - \deg(\mathrm{rad}(abc)).$$

(6) By (5) and

$$\deg(W) = \deg(ab' - a'b) \leq \deg(ab) - 1,$$

we have

$$\deg(c) \leq \deg(\mathrm{rad}(abc)) - 1.$$

(7) By symmetry,

$$\deg(a) \leq \deg(\mathrm{rad}(abc)) - 1,$$

$$\deg(b) \leq \deg(\mathrm{rad}(abc)) - 1.$$

Polynomial analogue: the proof

What is the most important step in the proof?

What is the most important step in the proof?

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

Polynomial analogue: the proof

What is the most important step in the proof?

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

Polynomial analogue: the proof

What is the most important step in the proof?

(0) Start with $a + b + c = 0$, we get the *derivative* $a' + b' + c' = 0$.

Cheating!!!

Effective Mordell Conjecture

The abc conjecture is easily applied to some variants of the Fermat equation, such as bounding integer solutions (x, y, z) of equations of the form

$$ax^m + by^n = cz^k.$$

This is not surprising.

Fermat–Catlan conjecture

The abc conjecture is easily applied to some variants of the Fermat equation, such as bounding integer solutions (x, y, z) of equations of the form

$$ax^m + by^n = cz^k.$$

This is not surprising.

However, the abc conjecture can actually be applied to much more complicated Diophantine equations. For example, it implies the Mordell conjecture.

Mordell Conjecture

Theorem (Mordell Conjecture, Faltings Theorem)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

Mordell Conjecture

Theorem (Mordell Conjecture, Faltings Theorem)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

This was conjectured by Louis Joel Mordell (1922), and proved by Gerd Faltings (1983).

Mordell Conjecture

Theorem (Mordell Conjecture, Faltings Theorem)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

This was conjectured by Louis Joel Mordell (1922), and proved by Gerd Faltings (1983).

Surprisingly, the abc conjecture implies the Mordell conjecture, by the work of Noam Elikies (1991).

Some algebraic geometry

A projective variety X over $\mathbb{Q}$ is a set of homogeneous polynomial equations with rational coefficients:

$$f_i(x_0, \cdots, x_n) = 0, \quad i = 1, 2, \cdots, m.$$

Denote by $X(\mathbb{Q})$ be the set of common rational solutions $(x_0, \cdots, x_n)$, and by $X(\mathbb{C})$ be the set of common complex solutions $(x_0, \cdots, x_n)$.

Some algebraic geometry

A projective variety X over $\mathbb{Q}$ is a set of homogeneous polynomial equations with rational coefficients:

$$f_i(x_0, \cdots, x_n) = 0, \quad i = 1, 2, \cdots, m.$$

Denote by $X(\mathbb{Q})$ be the set of common rational solutions $(x_0, \cdots, x_n)$, and by $X(\mathbb{C})$ be the set of common complex solutions $(x_0, \cdots, x_n)$.

These solutions are understood in homogeneous coordinates. So $(0, \cdots, 0)$ is excluded, and $(ax_0, \cdots, ax_n) = (x_0, \cdots, x_n)$ for any $a \neq 0$.

Some algebraic geometry

A projective variety X over $\mathbb{Q}$ is a set of homogeneous polynomial equations with rational coefficients:

$$f_i(x_0, \cdots, x_n) = 0, \quad i = 1, 2, \cdots, m.$$

Denote by $X(\mathbb{Q})$ be the set of common rational solutions $(x_0, \cdots, x_n)$, and by $X(\mathbb{C})$ be the set of common complex solutions $(x_0, \cdots, x_n)$.

These solutions are understood in homogeneous coordinates. So $(0, \cdots, 0)$ is excluded, and $(ax_0, \cdots, ax_n) = (x_0, \cdots, x_n)$ for any $a \neq 0$.

The dimension of X is the dimension of $X(\mathbb{C})$ as a complex space. We say that X is a curve if the dimension is 1. If X is a smooth curve, then $X(\mathbb{C})$ is a compact orientable surface in the sense of topology, and the genus g of X is just the number of handles on $X(\mathbb{C})$.

Some algebraic geometry

If X is given by a single irreducible homogeneous equation

$$f(x,y,z)=0$$

of degree d, then X is a curve and its (geometric) genus

$$g=\frac{(d-1)(d-2)}{2}-\delta.$$

Here $\delta\geq 0$ is the contribution from singularities.

Some algebraic geometry

If X is given by a single irreducible homogeneous equation

$$f(x, y, z) = 0$$

of degree d, then X is a curve and its (geometric) genus

$$g = \frac{(d-1)(d-2)}{2} - \delta.$$

Here $\delta \geq 0$ is the contribution from singularities.

If X is smooth, $\delta = 0$. This happens most of the time.

Example

For $abc \neq 0$, the twisted Fermat curve

$$X : ax^n + by^n = cz^n$$

has genus

$$g = \frac{(n-1)(n-2)}{2}.$$

Then $g > 1$ if and only if $n > 3$.

Effective Mordell

Theorem (Mordell Conjecture)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

Effective Mordell

Theorem (Mordell Conjecture)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

Problem

For a given curve X of genus $g > 1$ over $\mathbb{Q}$, find an effective algorithm to find all elements of the finite set $X(\mathbb{Q})$.

Effective Mordell

Theorem (Mordell Conjecture)

For any curve X of genus $g > 1$ over $\mathbb{Q}$, the set $X(\mathbb{Q})$ is finite.

Problem

For a given curve X of genus $g > 1$ over $\mathbb{Q}$, find an effective algorithm to find all elements of the finite set $X(\mathbb{Q})$.

We may try to enumerate $(x_0, \cdots, x_n)$ in the set $\mathbb{Z}^{n+1}$ to check if it satisfies the equations. Try from "small tuples" to "big tuples".

When do we know that we have got all the solutions? Is there an upper bound on the size of the solutions?

The proofs of Faltings and Vojta give upper bounds on the number of solutions, but this is not sufficient for our purpose.

Height

Height

Definition (Height)

For a rational solution $P = (x_0, \cdots, x_n)$ of $X(\mathbb{Q})$, after clearing the denominators and the common factors, we can assume that $x_0, \cdots, x_n$ are coprime integers. Then we define the height of P to be

$$h(P) = \log \max\{|x_0|, \cdots, |x_n|\}.$$

This defines a height function $h : X(\mathbb{Q}) \to \mathbb{R}$.

Height

Definition (Height)

For a rational solution $P = (x_0, \cdots, x_n)$ of $X(\mathbb{Q})$, after clearing the denominators and the common factors, we can assume that $x_0, \cdots, x_n$ are coprime integers. Then we define the height of P to be

$$h(P) = \log \max\{|x_0|, \cdots, |x_n|\}.$$

This defines a height function $h : X(\mathbb{Q}) \to \mathbb{R}$.

To have a satisfactory answer to our question, we need a computable constant $C(X)$ depending on X such that

$$h(P) < C(X), \quad \forall\ P \in X(\mathbb{Q}).$$

This is a part of the effective Mordell conjecture.

Effective Mordell

Conjecture (effective Mordell)

Let X be a projective and smooth curve over $\mathbb{Q}$ of genus $g > 1$. Then for any $d \geq 1$, there exist constants $A(X, d)$ and $B(X, d)$ depending only on X and d such that for any finite extension K of $\mathbb{Q}$ of degree d,

$$h(P) < A(X, d) \log |D_K| + B(X, d), \quad \forall\ P \in X(K).$$

Effective Mordell

Conjecture (effective Mordell)

Let X be a projective and smooth curve over $\mathbb{Q}$ of genus $g > 1$. Then for any $d \geq 1$, there exist constants $A(X, d)$ and $B(X, d)$ depending only on X and d such that for any finite extension K of $\mathbb{Q}$ of degree d,

$$h(P) < A(X, d) \log |D_K| + B(X, d), \quad \forall\ P \in X(K).$$

Effective Mordell

Conjecture (effective Mordell)

Let X be a projective and smooth curve over $\mathbb{Q}$ of genus $g > 1$. Then for any $d \geq 1$, there exist constants $A(X, d)$ and $B(X, d)$ depending only on X and d such that for any finite extension K of $\mathbb{Q}$ of degree d,

$$h(P) < A(X, d) \log |D_K| + B(X, d), \quad \forall\ P \in X(K).$$

Finally, (some version of) the effective Mordell conjecture is equivalent to (some version of) the abc conjecture.

More equivalent conjectures

More equivalent conjectures

The following conjectures (in suitable forms) are equivalent:

- The abc conjecture:

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

More equivalent conjectures

The following conjectures (in suitable forms) are equivalent:

- The abc conjecture:

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

- The effective Mordell conjecture:

$$h(P) < A(X,d) \log |D_K| + B(X,d), \quad P \in X(K),\ [K:\mathbb{Q}] = d.$$

More equivalent conjectures

The following conjectures (in suitable forms) are equivalent:

- The abc conjecture:

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

- The effective Mordell conjecture:

$$h(P) < A(X,d)\log|D_K| + B(X,d), \quad P \in X(K),\ [K:\mathbb{Q}] = d.$$

- Szpiro's conjecture: for elliptic curves E over a number field K,

$$\log|\Delta_E| \leq (6+\epsilon)\log|N_E| + C(K,\epsilon).$$

More equivalent conjectures

The following conjectures (in suitable forms) are equivalent:

- The abc conjecture:

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

- The effective Mordell conjecture:

$$h(P) < A(X,d)\log|D_K| + B(X,d), \quad P \in X(K),\ [K:\mathbb{Q}] = d.$$

- Szpiro's conjecture: for elliptic curves E over a number field K,

$$\log|\Delta_E| \leq (6+\epsilon)\log|N_E| + C(K,\epsilon).$$

- Arithmetic Bogomolov-Miyaoka-Yau inequality. The classical Bogomolov-Miyaoka-Yau inequality asserts that $c_1^2 \leq 3c_2$ for compact complex surfaces of general type. There is a conjectural arithmetic version in the setting of Arakelov geometry.

More equivalent conjectures

The following conjectures (in suitable forms) are equivalent:

- The abc conjecture:

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}.$$

- The effective Mordell conjecture:

$$h(P) < A(X,d)\log|D_K| + B(X,d), \quad P \in X(K),\ [K:\mathbb{Q}] = d.$$

- Szpiro's conjecture: for elliptic curves E over a number field K,

$$\log|\Delta_E| \leq (6+\epsilon)\log|N_E| + C(K,\epsilon).$$

- Arithmetic Bogomolov-Miyaoka-Yau inequality. The classical Bogomolov-Miyaoka-Yau inequality asserts that $c_1^2 \leq 3c_2$ for compact complex surfaces of general type. There is a conjectural arithmetic version in the setting of Arakelov geometry.
- Vojta's conjecture for the hyperbolic curve $\mathbb{P}^1 - \{0, 1, \infty\}$.

Mochizuki's work

Mochizuki's work

- Shinichi Mochizuki: Japanese mathematician and professor at Kyoto University. He received a PHD from Princeton University in 1992 (at age 23) under the supervision of Gerd Faltings.

Mochizuki's work

- Shinichi Mochizuki: Japanese mathematician and professor at Kyoto University. He received a PHD from Princeton University in 1992 (at age 23) under the supervision of Gerd Faltings.
- In August 2012, Mochizuki posted 4 papers on his webpage, which contains a proof of the abc conjecture, as a consequence of his theory called the *Inter-universal Teichmüller theory (IUT)*. These 4 papers have about 600 pages in total, and are based on his other works in the past many years.

Mochizuki's work

- Shinichi Mochizuki: Japanese mathematician and professor at Kyoto University. He received a PHD from Princeton University in 1992 (at age 23) under the supervision of Gerd Faltings.
- In August 2012, Mochizuki posted 4 papers on his webpage, which contains a proof of the abc conjecture, as a consequence of his theory called the *Inter-universal Teichmüller theory (IUT)*. These 4 papers have about 600 pages in total, and are based on his other works in the past many years.
- There are few mathematicians in the world who have read part of the proof.

Mochizuki's work

- Shinichi Mochizuki: Japanese mathematician and professor at Kyoto University. He received a PHD from Princeton University in 1992 (at age 23) under the supervision of Gerd Faltings.
- In August 2012, Mochizuki posted 4 papers on his webpage, which contains a proof of the abc conjecture, as a consequence of his theory called the *Inter-universal Teichmüller theory (IUT)*. These 4 papers have about 600 pages in total, and are based on his other works in the past many years.
- There are few mathematicians in the world who have read part of the proof.
- In May 2018, Peter Scholze and Jakob Stix wrote a 10-page report, detailing a serious gap in Mochizuki's proof. In July 2018, Mochizuki wrote a 8-page reaction, claiming that they misunderstood his proof.

Mochizuki's work

- Shinichi Mochizuki: Japanese mathematician and professor at Kyoto University. He received a PHD from Princeton University in 1992 (at age 23) under the supervision of Gerd Faltings.
- In August 2012, Mochizuki posted 4 papers on his webpage, which contains a proof of the abc conjecture, as a consequence of his theory called the *Inter-universal Teichmüller theory (IUT)*. These 4 papers have about 600 pages in total, and are based on his other works in the past many years.
- There are few mathematicians in the world who have read part of the proof.
- In May 2018, Peter Scholze and Jakob Stix wrote a 10-page report, detailing a serious gap in Mochizuki's proof. In July 2018, Mochizuki wrote a 8-page reaction, claiming that they misunderstood his proof.
- Peter Scholze: German mathematician, born in 1987, famous for his theory of perfectoid spaces, receive Fields Medal in 2018.

Mochizuki's work

- Mochizuki's work would actually imply

$$c < \mathrm{rad}(abc)^2$$

for any abc triple (a, b, c). Recall that Baker's version of the abc conjecture asserts

$$c < \mathrm{rad}(abc)^{1.75}.$$

Thank you very much.