The *ABC* conjecture

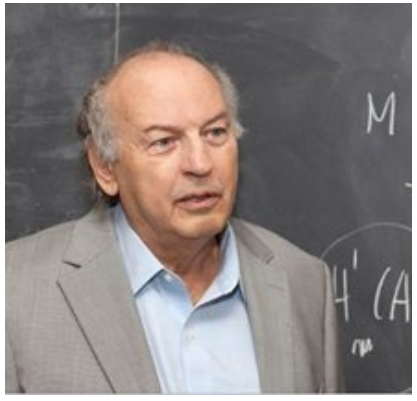
Brian Conrad

September 12, 2013

Introduction

The *ABC* conjecture was made by Masser and Oesterlé in 1985, inspired by work of Szpiro.





A proof was announced in Sept. 2012 by Mochizuki.

Outline

- Diophantine equations.
- The *ABC* conjecture.
- Relation of *ABC* conjecture to other problems in number theory.

The ABC conjecture [...] *always seems to lie on the boundary of what is known and what is unknown.* D. Goldfeld

Diophantine equations

A **Diophantine equation** is a polynomial equation with integral (or rational) coefficients.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Finitely many or infinitely many integral/rational solutions?
- If finitely many, describe all or bound their size.

Example. $x^2 - 7y^2 = 1$ has **infinitely many Z**-solutions: $(1, 0)$, $(8, 3)$, $(127, 48)$, $(2024, 765), \ldots$

Diophantine equations

A **Diophantine equation** is a polynomial equation with integral (or rational) coefficients.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Finitely many or infinitely many integral/rational solutions?
- If finitely many, describe all or bound their size.

Example. $x^2 - 7y^2 = 1$ has **infinitely many Z**-solutions: $(1, 0)$, $(8, 3)$, $(127, 48)$, $(2024, 765), \ldots$ More generally, for non-square $d > 1$, $x^2 - dy^2 = 1$ is called **Pell's equation** and has infinitely many **Z**-solutions.

Diophantine equations

A **Diophantine equation** is a polynomial equation with integral (or rational) coefficients.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Finitely many or infinitely many integral/rational solutions?
- If finitely many, describe all or bound their size.

Example. $x^2 - 7y^2 = 1$ has **infinitely many Z**-solutions: $(1, 0)$, $(8, 3)$, $(127, 48)$, $(2024, 765), \ldots$ More generally, for non-square $d > 1$, $x^2 - dy^2 = 1$ is called **Pell's equation** and has infinitely many **Z**-solutions.

Example. $x^3 - 7y^3 = 1$ has **two Z**-solutions $(1, 0), (2, 1)$ and **infinitely many Q**-solutions: $(1/2, -1/2)$, $(-4/5, -3/5)$, $(-5/4, -3/4)$, $(73/17, 38/17), \ldots$

Mordell's equation

$$y^2 = x^3 + k, \quad k \in \mathbf{Z} - \{0\}$$

Mordell (1888-1972) had an interest in this equation all his life.

Theorem (Mordell, 1920)

For each $k \in \mathbf{Z} - \{0\}$, the equation $y^2 = x^3 + k$ has finitely many integral solutions, i.e., a square and cube differ by k finitely often.

His proof was **ineffective** (that is, no explicit, even impractical, bounds).

Mordell's equation

$$y^2 = x^3 + k, \quad k \in \mathbf{Z} - \{0\}$$

Mordell (1888-1972) had an interest in this equation all his life.

Theorem (Mordell, 1920)

For each $k \in \mathbf{Z} - \{0\}$, the equation $y^2 = x^3 + k$ has finitely many integral solutions, i.e., a square and cube differ by k finitely often.

His proof was **ineffective** (that is, no explicit, even impractical, bounds). Some solutions could be unusually large relative to k.

Example

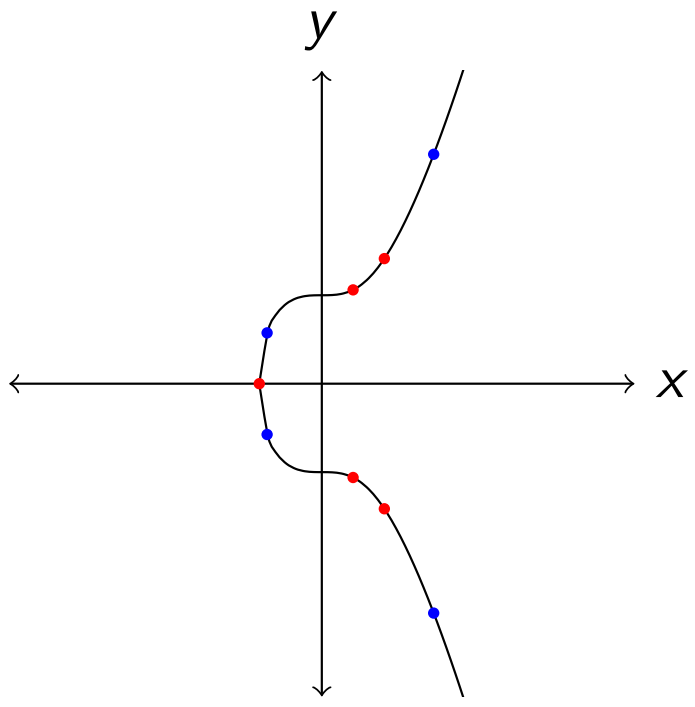
The integral solutions to $y^2 = x^3 + 24$ are

$$(-2, \pm 4), \quad (1, \pm 5), \quad (10, \pm 32), \text{ and } (8158, \pm 736844).$$

A graph of Mordell's equation

The equation $y^2 = x^3 + 8$ has infinitely many rational solutions:

$$(-2, 0), (1, \pm 3), (2, \pm 4), \left(-\frac{7}{4}, \pm\frac{13}{8}\right), \left(\frac{433}{121}, \pm\frac{9765}{1331}\right), \ldots$$

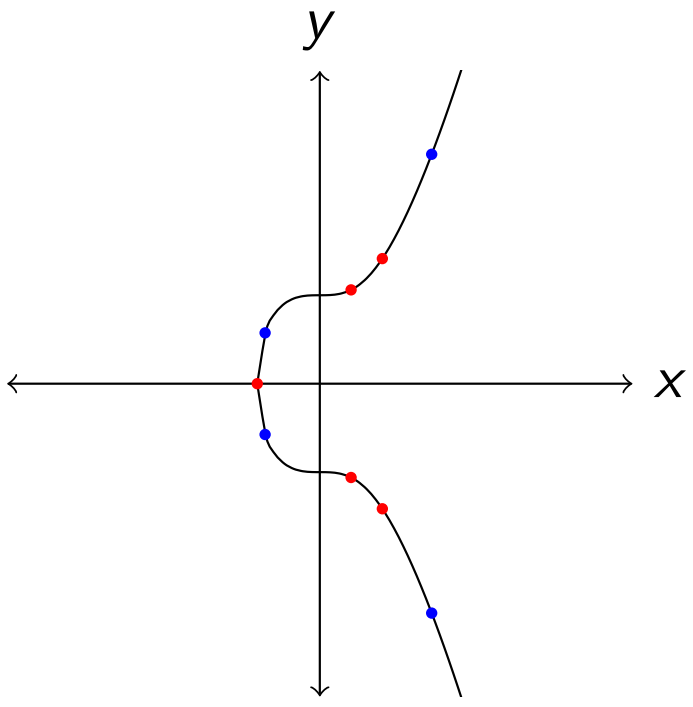


The integral solutions are $(-2, 0)$, $(1, \pm 3)$, $(2, \pm 4)$, $(46, \pm 312)$.

A graph of Mordell's equation

The equation $y^2 = x^3 + 8$ has infinitely many rational solutions:

$$(-2, 0), (1, \pm 3), (2, \pm 4), \left(-\frac{7}{4}, \pm\frac{13}{8}\right), \left(\frac{433}{121}, \pm\frac{9765}{1331}\right), \ldots$$



The integral solutions are $(-2, 0)$, $(1, \pm 3)$, $(2, \pm 4)$, $(46, \pm 312)$.
If $y^2 = x^3 + k$ in $\mathbf{Z}$ and $k \neq 0$, can we bound $|x|$ in terms of $|k|$?

Effective finiteness for Mordell's equation

Theorem (Baker, 1967)

For each $k \in \mathbf{Z} - \{0\}$, *if* $y^2 = x^3 + k$ *in* $\mathbf{Z}$ *then*

$$|x| \leq e^{10^{10}|k|^{10000}} = \left(e^{10^{10}}\right)^{|k|^{10000}}.$$

Effective finiteness for Mordell's equation

Theorem (Baker, 1967)

For each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$|x| \leq e^{10^{10}|k|^{10000}} = \left(e^{10^{10}}\right)^{|k|^{10000}}.$$

The exponent on $|k|$ can be reduced to any value greater than 1:

Theorem (Stark, 1973)

For each $\varepsilon > 0$, there is an effectively computable constant $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$|x| \leq C_\varepsilon^{|k|^{1+\varepsilon}}, \text{ or equivalently, for } x \neq 0, \log|x| \leq (\log C_\varepsilon)|k|^{1+\varepsilon}.$$

Effective does not mean practical!

Effective finiteness for Mordell's equation

Theorem (Baker, 1967)

For each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$|x| \leq e^{10^{10}|k|^{10000}} = \left(e^{10^{10}}\right)^{|k|^{10000}}.$$

The exponent on $|k|$ can be reduced to any value greater than 1:

Theorem (Stark, 1973)

For each $\varepsilon > 0$, there is an effectively computable constant $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$|x| \leq C_\varepsilon^{|k|^{1+\varepsilon}}, \text{ or equivalently, for } x \neq 0, \log|x| \leq (\log C_\varepsilon)|k|^{1+\varepsilon}.$$

The bound on $|x|$ should be **polynomial** in $|k|$, not exponential...

Hall's conjecture

Conjecture (Hall, 1971)

There is a constant $C > 0$ such that if $y^2 = x^3 + k$ in $\mathbf{Z}$ with $k \neq 0$ then $|x| \leq C|k|^2$.

This would be false using $|k|^{2(1-\varepsilon)}$ (Danilov, 1982).
Putting known examples into $|x| \leq C|k|^2$ gives lower bounds on C, and data available to Hall suggested $C = 25$ might suffice.

$$736844^2 = 8158^3 + 24 \Longrightarrow C \geq 14.1$$
$$223063347^2 = 367806^3 - 207 \Longrightarrow C \geq 8.5$$
$$149651610621^2 = 28187351^3 + 1090 \Longrightarrow C \geq 23.7$$

Hall's conjecture

Conjecture (Hall, 1971)

There is a constant $C > 0$ such that if $y^2 = x^3 + k$ in $\mathbf{Z}$ with $k \neq 0$ then $|x| \leq C|k|^2$.

This would be false using $|k|^{2(1-\varepsilon)}$ (Danilov, 1982).
Putting known examples into $|x| \leq C|k|^2$ gives lower bounds on C, and data available to Hall suggested $C = 25$ might suffice.

$$736844^2 = 8158^3 + 24 \Longrightarrow C \geq 14.1$$
$$223063347^2 = 367806^3 - 207 \Longrightarrow C \geq 8.5$$
$$149651610621^2 = 28187351^3 + 1090 \Longrightarrow C \geq 23.7$$
$$44788492842840204230791 8^2 = 5853886516781223^3 - 1641843 \Longrightarrow C \geq 2171.6$$

Hall knew the first 3 examples, but not the 4th (Elkies, 1998).

Hall's conjecture with an ε

Stark and Trotter proposed around 1980 that Hall's conjecture might be true if k^2 is replaced with $|k|^{2(1+\varepsilon)}$.

Conjecture

For each $\varepsilon > 0$ there is a constant $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

If this is true for an ε_0, then true for $\varepsilon > \varepsilon_0$; care about *small* ε.

Hall's conjecture with an ε

Stark and Trotter proposed around 1980 that Hall's conjecture might be true if k^2 is replaced with $|k|^{2(1+\varepsilon)}$.

Conjecture

For each $\varepsilon > 0$ there is a constant $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

If this is true for an ε_0, then true for $\varepsilon > \varepsilon_0$; care about *small* ε.
Try $\varepsilon = .1 : |x| \leq C_{.1}|k|^{2.2}$.

$$736844^2 = 8158^3 + 24 \Longrightarrow C_{.1} \geq 7.5,$$
$$223063347^2 = 367806^3 - 207 \Longrightarrow C_{.1} \geq 2.95,$$
$$149651610621^2 = 28187351^3 + 1090 \Longrightarrow C_{.1} \geq 5.8,$$
$$44788492842840204230791 8^2 = 5853886516781223^3 - 1641843 \Longrightarrow C_{.1} \geq 124.0.$$

Hall's original conjecture has not been disproved, but "Hall's conjecture" now is understood to have ε as above.

Exponential Diophantine equations

An **exponential Diophantine equation** has unknown exponents.

Example (Fermat's Last Theorem (1630s))

For all $n \geq 3$, the equation $x^n + y^n = z^n$ has no solution in positive integers x, y, z. Settled by Wiles in 1994.

Example (Catalan's Conjecture (1844))

The only consecutive perfect powers in $\mathbf{Z}^+$ are 8 and 9. That is, the only solution of $y^n - x^m = 1$ in $\mathbf{Z}^+$ where $m, n \geq 2$ is $3^2 - 2^3 = 1$. Settled by Mihailescu in 2002.

Before work of Mihailescu, analytic methods showed for $y^n - x^m = 1$ that m, n, x, and y are all explicitly bounded above:

Exponential Diophantine equations

An **exponential Diophantine equation** has unknown exponents.

Example (Fermat's Last Theorem (1630s))

For all $n \geq 3$, the equation $x^n + y^n = z^n$ has no solution in positive integers x, y, z. Settled by Wiles in 1994.

Example (Catalan's Conjecture (1844))

The only consecutive perfect powers in $\mathbf{Z}^+$ are 8 and 9. That is, the only solution of $y^n - x^m = 1$ in $\mathbf{Z}^+$ where $m, n \geq 2$ is $3^2 - 2^3 = 1$. Settled by Mihailescu in 2002.

Before work of Mihailescu, analytic methods showed for $y^n - x^m = 1$ that m, n, x, and y are all explicitly bounded above:

$$x^m < y^n < e^{e^{e^{e^{1000}}}}.$$

Search space is too large to fully check. Mihailescu used algebraic methods that bypassed computers.

The *ABC* Conjecture

The radical of a number

The *ABC* conjecture provides a new viewpoint on exponential Diophantine equations. It involves the following concept.

Definition. For any positive integer $n = p_1^{e_1} \cdots p_r^{e_r}$, its **radical** is $\mathrm{rad}(n) = p_1 p_2 \cdots p_r$.

Examples.

1) $\mathrm{rad}(1) = 1$
2) $\mathrm{rad}(252) = \mathrm{rad}(2^2 \cdot 3^2 \cdot 7) = 42$
3) $\mathrm{rad}(10000) = 10$
4) $\mathrm{rad}(a^m) = \mathrm{rad}(a)$

Remark. There is **no known way** to compute $\mathrm{rad}(n)$ without factoring n. By comparison, Euclid's algorithm computes $\gcd(m, n)$ quickly **without** factoring.

The radicals of a, b, and $a+b$ in $\mathbf{Z}^+$

For a and b in $\mathbf{Z}^+$, obviously $a+b \geq \text{rad}(a+b)$. Consider the inequality $a+b \geq \text{rad}(ab(a+b))$ when $\gcd(a,b)=1$.

Example. Among all 3044 pairs (a,b) such that $1 \leq a \leq b \leq 100$ and $\gcd(a,b)=1$, the inequality $a+b \geq \text{rad}(ab(a+b))$ holds 7 times: $(1,1), (1,8)$, $(1,48)$, $(1,63)$, $(1,80)$, $(5,27)$, and $(32,49)$.

The radicals of a, b, and $a+b$ in $\mathbf{Z}^+$

For a and b in $\mathbf{Z}^+$, obviously $a+b \geq \text{rad}(a+b)$. Consider the inequality $a+b \geq \text{rad}(ab(a+b))$ when $\gcd(a,b)=1$.

Example. Among all 3044 pairs (a,b) such that $1 \leq a \leq b \leq 100$ and $\gcd(a,b)=1$, the inequality $a+b \geq \text{rad}(ab(a+b))$ holds 7 times: $(1,1), (1,8), (1,48), (1,63), (1,80), (5,27)$, and $(32,49)$.

Many examples of $a+b \geq \text{rad}(ab(a+b))$ *do* exist, but they're big.

Example. Let $a=1$ and $b=3^{2^{10}}-1$. Then b is divisible by 2^{12}, so

$$\text{rad}(ab(a+b)) = \text{rad}(b \cdot 3) \leq \frac{b}{2^{11}} \cdot 3 < \frac{3}{2^{11}}(a+b).$$

Thus $a+b > \dfrac{2^{11}}{3}\,\text{rad}(ab(a+b)) \gg \text{rad}(ab(a+b))$.

The radicals of a, b, and $a+b$ in $\mathbf{Z}^+$

For a and b in $\mathbf{Z}^+$, obviously $a+b \geq \text{rad}(a+b)$. Consider the inequality $a+b \geq \text{rad}(ab(a+b))$ when $\gcd(a,b)=1$.

Example. Among all 3044 pairs (a,b) such that $1 \leq a \leq b \leq 100$ and $\gcd(a,b)=1$, the inequality $a+b \geq \text{rad}(ab(a+b))$ holds 7 times: $(1,1), (1,8), (1,48), (1,63), (1,80), (5,27)$, and $(32,49)$.

Many examples of $a+b \geq \text{rad}(ab(a+b))$ *do* exist, but they're big.

Example. Let $a=1$ and $b=3^{2^{10}}-1$. Then b is divisible by 2^{12}, so

$$\text{rad}(ab(a+b)) = \text{rad}(b \cdot 3) \leq \frac{b}{2^{11}} \cdot 3 < \frac{3}{2^{11}}(a+b).$$

Thus $a+b > \dfrac{2^{11}}{3}\,\text{rad}(ab(a+b)) \gg \text{rad}(ab(a+b))$.
For $b=3^{2^n}-1$, $(a+b)/\,\text{rad}(ab(a+b))$ becomes arbitrarily large.

The *ABC* conjecture

Definition. An *ABC*-triple is a triple of positive integers (a, b, c) such that $a + b = c$ and $\gcd(a, b, c) = 1$ ($\Longleftrightarrow \gcd(a, b) = 1$).

By previous slide, infinitely often $c > \mathrm{rad}(abc)$. How much bigger?

The *ABC* conjecture

Definition. An *ABC*-triple is a triple of positive integers (a, b, c) such that $a + b = c$ and $\gcd(a, b, c) = 1$ ($\iff \gcd(a, b) = 1$).

By previous slide, infinitely often $c > \mathrm{rad}(abc)$. How much bigger?

Among all known *ABC*-triples such that $c > \mathrm{rad}(abc)$, all fit $c < \mathrm{rad}(abc)^2$, all but 3 fit $c < \mathrm{rad}(abc)^{1.6}$, and all but 13 fit $c < \mathrm{rad}(abc)^{1.5}$.

The *ABC* conjecture

Definition. An *ABC*-triple is a triple of positive integers (a, b, c) such that $a + b = c$ and $\gcd(a, b, c) = 1$ ($\iff \gcd(a, b) = 1$).

By previous slide, infinitely often $c > \text{rad}(abc)$. How much bigger?

Among all known *ABC*-triples such that $c > \text{rad}(abc)$, all fit $c < \text{rad}(abc)^2$, all but 3 fit $c < \text{rad}(abc)^{1.6}$, and all but 13 fit $c < \text{rad}(abc)^{1.5}$.

Conjecture (Masser, Oesterlé, 1985)

For each $\varepsilon > 0$, all but finitely many ABC-triples (a, b, c) satisfy $c < \text{rad}(abc)^{1+\varepsilon}$.

This would be false using $\varepsilon = 0$.

Numerical evidence is indicated above. Unlike Fermat or Catalan, this can't be *disproved* using a single counterexample.

The *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $c < \mathrm{rad}(abc)^{1+\varepsilon}$.

For small ε, right side is "nearly" $\mathrm{rad}(abc)$, the product of primes in a, b, and c **once each**. Conjecture roughly says it is hard to get

$$\underbrace{a}_{\substack{\text{high}\\\text{multip.}}} + \underbrace{b}_{\substack{\text{high}\\\text{multip.}}} = \underbrace{c}_{\substack{\text{high}\\\text{multip.}}}, \quad \gcd(a, b) = 1.$$

Ex: $2^6+3^4 = 5^1 \cdot 19^1$, $2^4 \cdot 3^5+31^1 \cdot 7^6 \cdot 11^3 = 173^1 \cdot 2459^1 \cdot 11411^1$.

The *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, all but finitely many ABC-triples (a, b, c) satisfy $c < \mathrm{rad}(abc)^{1+\varepsilon}$.

For small ε, right side is "nearly" $\mathrm{rad}(abc)$, the product of primes in a, b, and c **once each**. Conjecture roughly says it is hard to get

$$\underbrace{a}_{\substack{\text{high}\\\text{multip.}}} + \underbrace{b}_{\substack{\text{high}\\\text{multip.}}} = \underbrace{c}_{\substack{\text{high}\\\text{multip.}}}, \quad \gcd(a, b) = 1.$$

Ex: $2^6+3^4 = 5^1 \cdot 19^1$, $2^4 \cdot 3^5+31^1 \cdot 7^6 \cdot 11^3 = 173^1 \cdot 2459^1 \cdot 11411^1$. But conjecture has $\varepsilon > 0$, not $\varepsilon = 0$. Infinitely often $x^2 + y^2 = z^2$ with $\gcd(x, y) = 1$, and examples with all multiplicities ≥ 3 occur:

$$2^7 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 2287^3 + 17^3 \cdot 106219^3 = 37^3 \cdot 197^3 \cdot 307^3.$$

In this example, $c \approx \mathrm{rad}(abc)^{1.04163}$.

The *ABC* conjecture reformulated

In defn. of *ABC*-triple, where $a + b = c$ and $\gcd(a, b, c) = 1$, relax "$a, b > 0$" to "$a, b, c \neq 0$". For $n < 0$, set $\mathrm{rad}(n) = \mathrm{rad}(|n|)$.

Conjecture (Allowing nonzero a, b, c)

For each $\varepsilon > 0$, all but finitely many ABC-triples (a, b, c) satisfy $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Conjecture (No finite exceptions)

For each $\varepsilon > 0$, there is a constant $\kappa_\varepsilon > 0$ such that for all ABC-triples (a, b, c), $\max(|a|, |b|, |c|) < \kappa_\varepsilon \, \mathrm{rad}(abc)^{1+\varepsilon}$.

The *ABC* conjecture reformulated

In defn. of *ABC*-triple, where $a + b = c$ and $\gcd(a, b, c) = 1$, relax "$a, b > 0$" to "$a, b, c \neq 0$". For $n < 0$, set $\mathrm{rad}(n) = \mathrm{rad}(|n|)$.

Conjecture (Allowing nonzero a, b, c)

For each $\varepsilon > 0$, all but finitely many ABC-triples (a, b, c) satisfy $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Conjecture (No finite exceptions)

For each $\varepsilon > 0$, there is a constant $\kappa_\varepsilon > 0$ such that for all ABC-triples (a, b, c), $\max(|a|, |b|, |c|) < \kappa_\varepsilon \, \mathrm{rad}(abc)^{1+\varepsilon}$.

PROBLEM OF D.W. MASSER (After Oesterlé)

Disprove (or prove) that for every $\varepsilon > 0$ there exists $C(\varepsilon)$ such that

$$\max(|a|,|b|,|c|) \leq C(\varepsilon)\left(\prod_{p \mid abc} p\right)^{1+\varepsilon}$$

for all coprime integers a,b,c with $a + b + c = 0$.

Motivation for *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

What led Masser and Oesterlé to the *ABC* conjecture?

Motivation for *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

What led Masser and Oesterlé to the *ABC* conjecture?

- Oesterlé was interested in a new conjecture of Szpiro about elliptic curves (smooth cubic curves, such as $y^2 = x^3 + 8$) which has applications to number-theoretic properties of elliptic curves.
- Masser heard Oesterlé lecture on Szpiro's conjecture and wanted to formulate it **without using** elliptic curves.

Motivation for *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

What led Masser and Oesterlé to the *ABC* conjecture?

- Oesterlé was interested in a new conjecture of Szpiro about elliptic curves (smooth cubic curves, such as $y^2 = x^3 + 8$) which has applications to number-theoretic properties of elliptic curves.
- Masser heard Oesterlé lecture on Szpiro's conjecture and wanted to formulate it **without using** elliptic curves.
- Eventually it turned out that the ABC Conjecture and Szpiro's Conjecture are equivalent (and ABC implies Fermat's Last Theorem, as we'll see, but that was not part of the original motivation).

Consequences of the *ABC* Conjecture

Using the *ABC* conjecture

Conjecture

For each $\varepsilon > 0$*, all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Applications use the "for each ε" aspect in different ways:

- one choice of ε (without constraints),
- one choice of ε below some bound (*e.g.*, $\varepsilon < 1/5$),
- all small ε.

Using the *ABC* conjecture

Conjecture

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Applications use the "for each ε" aspect in different ways:

- one choice of ε (without constraints),
- one choice of ε below some bound (*e.g.*, $\varepsilon < 1/5$),
- all small ε.

Before Mochizuki's work, nobody had announced a proof for even a single value of ε.

ABC conjecture implies Fermat's last theorem for large exponents

Suppose *ABC* proved for one ε: $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ for all but finitely many *ABC*-triples. If $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes (x^n, y^n, z^n) an *ABC*-triple.

ABC conjecture implies Fermat's last theorem for large exponents

Suppose *ABC* proved for one ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ for all but finitely many *ABC*-triples. If $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes (x^n, y^n, z^n) an *ABC*-triple.

For all but finitely many *ABC*-triples (x^n, y^n, z^n) in $\mathbf{Z}^+$,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \end{aligned}$$

ABC conjecture implies Fermat's last theorem for large exponents

Suppose *ABC* proved for one ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ for all but finitely many *ABC*-triples. If $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes (x^n, y^n, z^n) an *ABC*-triple.

For all but finitely many *ABC*-triples (x^n, y^n, z^n) in $\mathbf{Z}^+$,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \\ &< z^{3(1+\varepsilon)} \\ \Rightarrow n &< 3(1+\varepsilon). \end{aligned}$$

ABC conjecture implies Fermat's last theorem for large exponents

Suppose *ABC* proved for one ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ for all but finitely many *ABC*-triples. If $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes (x^n, y^n, z^n) an *ABC*-triple.

For all but finitely many *ABC*-triples (x^n, y^n, z^n) in $\mathbf{Z}^+$,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \\ &< z^{3(1+\varepsilon)} \\ \Rightarrow n &< 3(1+\varepsilon). \end{aligned}$$

For exceptions (x^n, y^n, z^n), z^n on finite list & $z > 1 \Rightarrow n$ bounded. Thus FLT true for large exponents, and in an effective way if exceptions to $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ are known for one ε.

ABC conjecture and $x^n + y^n = 5z^n$

Suppose *ABC* proved for one $\varepsilon < 1/3$. If $x^n + y^n = 5z^n$ with $x, y, z \in \mathbf{Z} - \{0\}$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes $(x^n, y^n, 5z^n)$ an *ABC*-triple.

ABC conjecture and $x^n + y^n = 5z^n$

Suppose *ABC* proved for one $\varepsilon < 1/3$. If $x^n + y^n = 5z^n$ with $x, y, z \in \mathbf{Z} - \{0\}$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes $(x^n, y^n, 5z^n)$ an *ABC*-triple.

For all but finitely many *ABC*-triples $(x^n, y^n, 5z^n)$,

$$\begin{aligned} |x|^n, |y|^n, 5|z|^n &< \operatorname{rad}(x^n y^n 5z^n)^{1+\varepsilon} \\ &= \operatorname{rad}(5xyz)^{1+\varepsilon} \\ &\leq (5|xyz|)^{1+\varepsilon}. \end{aligned}$$

ABC conjecture and $x^n + y^n = 5z^n$

Suppose *ABC* proved for one $\varepsilon < 1/3$. If $x^n + y^n = 5z^n$ with $x, y, z \in \mathbf{Z} - \{0\}$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes $(x^n, y^n, 5z^n)$ an *ABC*-triple.

For all but finitely many *ABC*-triples $(x^n, y^n, 5z^n)$,

$$\begin{aligned} |x|^n, |y|^n, 5|z|^n &< \operatorname{rad}(x^n y^n 5z^n)^{1+\varepsilon} \\ &= \operatorname{rad}(5xyz)^{1+\varepsilon} \\ &\leq (5|xyz|)^{1+\varepsilon}. \end{aligned}$$

Let $M = \max(|x|, |y|, |z|) \geq 2$, so

$$M^n < (5M^3)^{1+\varepsilon} \Longrightarrow M^{n-3(1+\varepsilon)} < 5^{1+\varepsilon}.$$

ABC conjecture and $x^n + y^n = 5z^n$

Suppose *ABC* proved for one $\varepsilon < 1/3$. If $x^n + y^n = 5z^n$ with $x, y, z \in \mathbf{Z} - \{0\}$, we want to show n is bounded. Without loss of generality $\gcd(x, y) = 1$, which makes $(x^n, y^n, 5z^n)$ an *ABC*-triple.

For all but finitely many *ABC*-triples $(x^n, y^n, 5z^n)$,

$$\begin{aligned} |x|^n, |y|^n, 5|z|^n &< \operatorname{rad}(x^n y^n 5z^n)^{1+\varepsilon} \\ &= \operatorname{rad}(5xyz)^{1+\varepsilon} \\ &\leq (5|xyz|)^{1+\varepsilon}. \end{aligned}$$

Let $M = \max(|x|, |y|, |z|) \geq 2$, so

$$M^n < (5M^3)^{1+\varepsilon} \Longrightarrow M^{n-3(1+\varepsilon)} < 5^{1+\varepsilon}.$$

If $n \geq 4$ and $\varepsilon < 1/3$ then $n - 3(1 + \varepsilon) > 0$, so $2^n < 2^{3(1+\varepsilon)} 5^{1+\varepsilon}$. Thus n bounded for all but finitely many *ABC*-triples $(x^n, y^n, 5z^n)$. Each exception can occur for finitely many n, so n is bounded.

ABC and integral solutions of $x^3 - 7y^3 = 1$

Earlier: $x^2 - 7y^2 = 1$ has inf. many **Z**-solns, $x^3 - 7y^3 = 1$ has two.

ABC conjecture for one $\varepsilon < 1/2$ implies $x^3 - 7y^3 = 1$ has finitely many **Z**-solutions:

ABC and integral solutions of $x^3 - 7y^3 = 1$

Earlier: $x^2 - 7y^2 = 1$ has inf. many **Z**-solns, $x^3 - 7y^3 = 1$ has two.

ABC conjecture for one $\varepsilon < 1/2$ implies $x^3 - 7y^3 = 1$ has finitely many **Z**-solutions: for all but finitely many (nonzero) x and y,

$$|x|^3, 7|y|^3 < \mathrm{rad}(x^3(7y^3))^{1+\varepsilon} = \mathrm{rad}(7xy)^{1+\varepsilon} \leq 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}.$$

ABC and integral solutions of $x^3 - 7y^3 = 1$

Earlier: $x^2 - 7y^2 = 1$ has inf. many **Z**-solns, $x^3 - 7y^3 = 1$ has two.

ABC conjecture for one $\varepsilon < 1/2$ implies $x^3 - 7y^3 = 1$ has finitely many **Z**-solutions: for all but finitely many (nonzero) x and y,

$$|x|^3, 7|y|^3 < \mathrm{rad}(x^3(7y^3))^{1+\varepsilon} = \mathrm{rad}(7xy)^{1+\varepsilon} \leq 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}.$$

Let $M = \max(|x|^3, 7|y|^3) < 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}$, so

ABC and integral solutions of $x^3 - 7y^3 = 1$

Earlier: $x^2 - 7y^2 = 1$ has inf. many **Z**-solns, $x^3 - 7y^3 = 1$ has two.

ABC conjecture for one $\varepsilon < 1/2$ implies $x^3 - 7y^3 = 1$ has finitely many **Z**-solutions: for all but finitely many (nonzero) x and y,

$$|x|^3, 7|y|^3 < \mathrm{rad}(x^3(7y^3))^{1+\varepsilon} = \mathrm{rad}(7xy)^{1+\varepsilon} \leq 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}.$$

Let $M = \max(|x|^3, 7|y|^3) < 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}$, so

$$M < 7^{2(1+\varepsilon)/3}(|x|^3)^{(1+\varepsilon)/3}(7|y|^3)^{(1+\varepsilon)/3} \leq 7^{2(1+\varepsilon)/3}M^{2(1+\varepsilon)/3}.$$

ABC and integral solutions of $x^3 - 7y^3 = 1$

Earlier: $x^2 - 7y^2 = 1$ has inf. many $\mathbf{Z}$-solns, $x^3 - 7y^3 = 1$ has two.

ABC conjecture for one $\varepsilon < 1/2$ implies $x^3 - 7y^3 = 1$ has finitely many $\mathbf{Z}$-solutions: for all but finitely many (nonzero) x and y,

$$|x|^3, 7|y|^3 < \mathrm{rad}(x^3(7y^3))^{1+\varepsilon} = \mathrm{rad}(7xy)^{1+\varepsilon} \leq 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}.$$

Let $M = \max(|x|^3, 7|y|^3) < 7^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon}$, so

$$M < 7^{2(1+\varepsilon)/3}(|x|^3)^{(1+\varepsilon)/3}(7|y|^3)^{(1+\varepsilon)/3} \leq 7^{2(1+\varepsilon)/3}M^{2(1+\varepsilon)/3}.$$

Therefore M, and thus $|x|$ and $|y|$, can be bounded in terms of ε:

$$M^{(1-2\varepsilon)/3} < 7^{2(1+\varepsilon)/3} \overset{\varepsilon<1/2}{\Longrightarrow} M < 7^{2(1+\varepsilon)/(1-2\varepsilon)}.$$

Similarly, for any $n \geq 3$ and $d \geq 2$, $x^n - dy^n = 1$ has finitely many integral solutions from *ABC* conjecture for one $\varepsilon < \frac{n}{2} - 1$.

ABC conjecture and Catalan's conjecture

Theorem. *If* $c < \mathrm{rad}(abc)^2$ *for all ABC-triples* (a, b, c) *in* $\mathbf{Z}^+$ *then Catalan's conjecture is true:* $y^n = x^m + 1$ *with* $x, y, m, n \geq 2$ *only for* $3^2 = 2^3 + 1$.

ABC conjecture and Catalan's conjecture

Theorem. *If* $c < \mathrm{rad}(abc)^2$ *for all ABC-triples* (a, b, c) *in* $\mathbf{Z}^+$ *then Catalan's conjecture is true:* $y^n = x^m + 1$ *with* $x, y, m, n \geq 2$ *only for* $3^2 = 2^3 + 1$.

Pf: Using $(a, b, c) = (x^m, 1, y^n)$ we have $\gcd(a, b, c) = 1$, so

$$y^n < \mathrm{rad}(x^m y^n)^2 = \mathrm{rad}(xy)^2 \leq x^2 y^2.$$

ABC conjecture and Catalan's conjecture

Theorem. *If* $c < \mathrm{rad}(abc)^2$ *for all ABC-triples* (a, b, c) *in* $\mathbf{Z}^+$ *then Catalan's conjecture is true:* $y^n = x^m + 1$ *with* $x, y, m, n \geq 2$ *only for* $3^2 = 2^3 + 1$.

Pf: Using $(a, b, c) = (x^m, 1, y^n)$ we have $\gcd(a, b, c) = 1$, so

$$y^n < \mathrm{rad}(x^m y^n)^2 = \mathrm{rad}(xy)^2 \leq x^2 y^2.$$

Also $x^m = y^n - 1 < y^n \Rightarrow x < y^{n/m}$, so

$$y^n < (y^{n/m})^2 y^2 = y^{2(1+n/m)}.$$

ABC conjecture and Catalan's conjecture

Theorem. *If* $c < \mathrm{rad}(abc)^2$ *for all ABC-triples* (a, b, c) *in* $\mathbf{Z}^+$ *then Catalan's conjecture is true:* $y^n = x^m + 1$ *with* $x, y, m, n \geq 2$ *only for* $3^2 = 2^3 + 1$.

Pf: Using $(a, b, c) = (x^m, 1, y^n)$ we have $\gcd(a, b, c) = 1$, so

$$y^n < \mathrm{rad}(x^m y^n)^2 = \mathrm{rad}(xy)^2 \leq x^2 y^2.$$

Also $x^m = y^n - 1 < y^n \Rightarrow x < y^{n/m}$, so

$$y^n < (y^{n/m})^2 y^2 = y^{2(1+n/m)}.$$

From $y > 1$ we get $n < 2(1 + m/n)$, so $1/2 < 1/m + 1/n$. The only such exponents are

$$\{m, n\} = \{2, r\}, \quad \{3, 3\}, \quad \{3, 4\}, \quad \{3, 5\},$$

where $r \geq 2$, and all of these were shown by the 1960s to have no solution for x and y in $\mathbf{Z}^+$ other than $m = 3$, $n = 2$, $x = 2$, $y = 3$.

Comparing Hall's conjecture and the *ABC* conjecture

Theorem (*ABC* implies Hall's conjecture)

If ABC conj. **true** *then for each* $\varepsilon > 0$ *there is* $C_\varepsilon > 0$ *such that if* $y^2 = x^3 + k$ *in* $\mathbf{Z}$ *and* $k \neq 0$, *then* $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Theorem (*ABC* implies "radical Hall's conjecture")

If ABC conj. **true** *then for each* $\varepsilon > 0$ *there is* $C'_\varepsilon > 0$ *such that if* $y^2 = x^3 + k$ *in* $\mathbf{Z}$, $k \neq 0$, $\gcd(x, y) = 1$ *then* $|x| \leq C'_\varepsilon \mathrm{rad}(k)^{2(1+\varepsilon)}$.

This bound on $|x|$ is typically **stronger** than Hall, since $\mathrm{rad}(k)$ can be smaller than $|k|$, but the bound is just for $\gcd(x, y) = 1$.

Comparing Hall's conjecture and the *ABC* conjecture

Theorem (*ABC* implies Hall's conjecture)

If ABC conj. **true** *then for each* $\varepsilon > 0$ *there is* $C_\varepsilon > 0$ *such that if* $y^2 = x^3 + k$ *in* $\mathbf{Z}$ *and* $k \neq 0$, *then* $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Theorem (*ABC* implies "radical Hall's conjecture")

If ABC conj. **true** *then for each* $\varepsilon > 0$ *there is* $C'_\varepsilon > 0$ *such that if* $y^2 = x^3 + k$ *in* $\mathbf{Z}$, $k \neq 0$, $\gcd(x, y) = 1$ *then* $|x| \leq C'_\varepsilon \mathrm{rad}(k)^{2(1+\varepsilon)}$.

This bound on $|x|$ is typically **stronger** than Hall, since $\mathrm{rad}(k)$ can be smaller than $|k|$, but the bound is just for $\gcd(x, y) = 1$.

Theorem

Radical Hall conjecture implies ABC, so they are equivalent.

Thus bounding integral solutions to Mordell's equation is far more central (and difficult) than it at first appears to be!

ABC conjecture and gaps between perfect powers

Going beyond Catalan's conjecture about $y^n - x^m = 1$ and Hall's conjecture about $y^2 = x^3 + k$, we can consider the exponential Diophantine equation

$$y^n - x^m = k,$$

where k is a nonzero integer. The sequence of perfect powers in $\mathbf{Z}^+$ starts out as

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125, \ldots.$$

How far apart can two different perfect powers be?

ABC conjecture and gaps between perfect powers

Going beyond Catalan's conjecture about $y^n - x^m = 1$ and Hall's conjecture about $y^2 = x^3 + k$, we can consider the exponential Diophantine equation

$$y^n - x^m = k,$$

where k is a nonzero integer. The sequence of perfect powers in $\mathbf{Z}^+$ starts out as

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125, \ldots.$$

How far apart can two different perfect powers be?

If we fix k as well as m and n (both at least 2), the equation $y^n - x^m = k$ has finitely many integral solutions x, y. This is easy if $\gcd(m, n) \geq 2$ and hard if $\gcd(m, n) = 1$. Studying gaps between perfect powers demands that we fix only k; let x, y, m, n vary.

ABC conjecture and gaps between perfect powers

Going beyond Catalan's conjecture about $y^n - x^m = 1$ and Hall's conjecture about $y^2 = x^3 + k$, we can consider the exponential Diophantine equation

$$y^n - x^m = k,$$

where k is a nonzero integer. The sequence of perfect powers in $\mathbf{Z}^+$ starts out as

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125, \ldots.$$

How far apart can two different perfect powers be?

If we fix k as well as m and n (both at least 2), the equation $y^n - x^m = k$ has finitely many integral solutions x, y. This is easy if $\gcd(m, n) \geq 2$ and hard if $\gcd(m, n) = 1$. Studying gaps between perfect powers demands that we fix only k; let x, y, m, n vary.

The *ABC* conjecture for one $\varepsilon < 1/5$ implies for each $k \neq 0$ that only finitely many perfect powers differ by k (Pillai's conjecture).

Good Rational Approximations and the *ABC* Conjecture

For irrational $\alpha \in \mathbf{R}$, **inf. many** (reduced form) rational a/b satisfy

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Example. Let $\alpha = \sqrt[5]{2} \approx 1.1486$. Compare

$$\left|\sqrt[5]{2} - \frac{1148}{1000}\right| \gg \frac{1}{1000^2} \qquad (.0006 \gg .000001),$$

$$\left|\sqrt[5]{2} - \frac{309}{269}\right| < \frac{1}{269^2} \qquad (.0000005 < .0000138).$$

Good Rational Approximations and the *ABC* Conjecture

For irrational $\alpha \in \mathbf{R}$, **inf. many** (reduced form) rational a/b satisfy

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Example. Let $\alpha = \sqrt[5]{2} \approx 1.1486$. Compare

$$\left|\sqrt[5]{2} - \frac{1148}{1000}\right| \gg \frac{1}{1000^2} \qquad (.0006 \gg .000001),$$

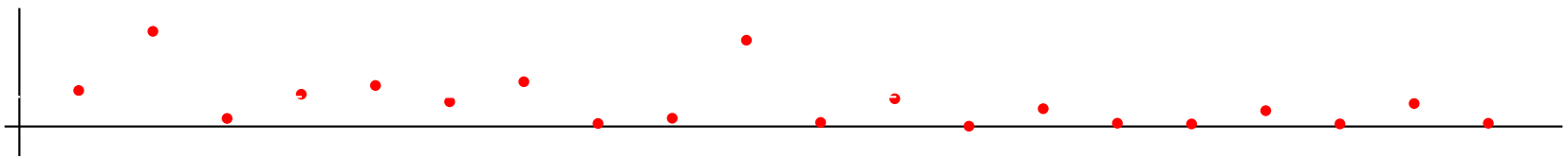
$$\left|\sqrt[5]{2} - \frac{309}{269}\right| < \frac{1}{269^2} \qquad (.0000005 < .0000138).$$

The (reduced form) fractions satisfying $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^2}$, in order of increasing denominator $b > 1$ (found via "continued fractions"):

$$\frac{7}{6}, \frac{8}{7}, \frac{15}{13}, \frac{23}{20}, \frac{31}{27}, \frac{54}{47}, \frac{85}{74}, \frac{139}{121}, \frac{224}{195}, \frac{309}{269}, \ldots.$$

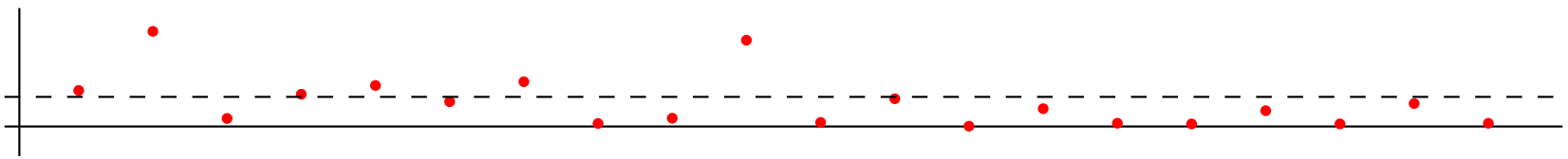
Good Rational Approximations and the *ABC* Conjecture

Let $\frac{a_i}{b_i}$ be the (reduced) fractions with $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ and $b_1 < b_2 < b_3 < \cdots$. Set $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, with $\varepsilon_i > 0$. Below is a plot of ε_i for the first 20 such fractions ($i = 1, 2, \ldots$).



Good Rational Approximations and the *ABC* Conjecture

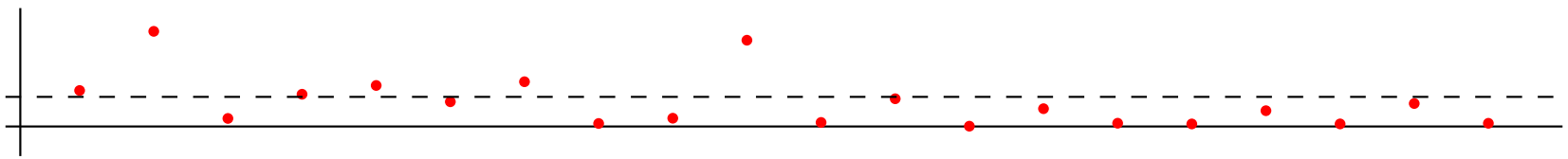
Let $\frac{a_i}{b_i}$ be the (reduced) fractions with $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ and $b_1 < b_2 < b_3 < \cdots$. Set $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, with $\varepsilon_i > 0$. Below is a plot of ε_i for the first 20 such fractions ($i = 1, 2, \ldots$).



The ε_i's fluctuate, but tend to 0.

Good Rational Approximations and the *ABC* Conjecture

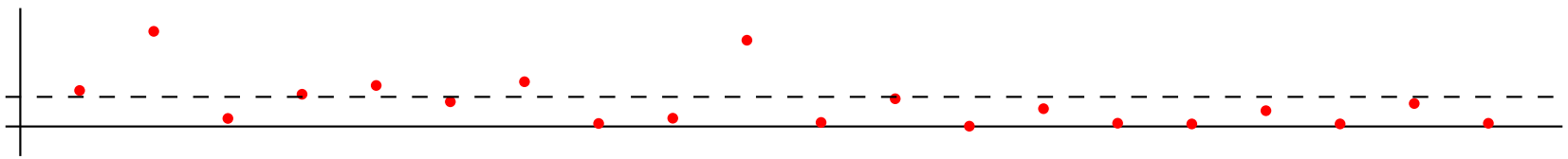
Let $\frac{a_i}{b_i}$ be the (reduced) fractions with $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ and $b_1 < b_2 < b_3 < \cdots$. Set $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, with $\varepsilon_i > 0$. Below is a plot of ε_i for the first 20 such fractions ($i = 1, 2, \ldots$).



The ε_i's fluctuate, but tend to 0. Thus, for each $\varepsilon > 0$, only finitely often is $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}} < \frac{1}{b^2}$.

Good Rational Approximations and the *ABC* Conjecture

Let $\frac{a_i}{b_i}$ be the (reduced) fractions with $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ and $b_1 < b_2 < b_3 < \cdots$. Set $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, with $\varepsilon_i > 0$. Below is a plot of ε_i for the first 20 such fractions ($i = 1, 2, \ldots$).



The ε_i's fluctuate, but tend to 0. Thus, for each $\varepsilon > 0$, only finitely often is $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}} < \frac{1}{b^2}$. This is a special instance of Roth's theorem (1958 Fields Medal) on approximating *algebraic* irrational numbers like $\sqrt[5]{2}$ by rationals. All known proofs are **ineffective** in listing the finitely many $\frac{a}{b}$ for each ε (esp. small ε).

Good Rational Approximations and the *ABC* Conjecture

Conjecture (First version of *ABC*)

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Conjecture (Equivalent form as lower bound on $\mathrm{rad}(abc)$**)**

For each $\varepsilon \in (0, 1)$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\mathrm{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. *Obvious for* $\varepsilon \geq 1$.

Good Rational Approximations and the *ABC* Conjecture

Conjecture (First version of *ABC*)

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Conjecture (Equivalent form as lower bound on $\mathrm{rad}(abc)$**)**

For each $\varepsilon \in (0, 1)$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\mathrm{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. *Obvious for* $\varepsilon \geq 1$.

Elkies and Langevin showed (indep.) this form of *ABC* implies for each $\varepsilon > 0$ that $\mathrm{rad}(a^5 - 2b^5) > \max(|a|, |b|)^{3-\varepsilon}$ for all but finitely many rel. prime a and b. That in turn implies Roth's theorem for $\alpha = \sqrt[5]{2}$, *i.e.*, $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$ finitely often for each ε.

Good Rational Approximations and the *ABC* Conjecture

Conjecture (First version of *ABC*)

For each $\varepsilon > 0$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Conjecture (Equivalent form as lower bound on $\mathrm{rad}(abc)$**)**

For each $\varepsilon \in (0, 1)$, *all but finitely many ABC-triples* (a, b, c) *satisfy* $\mathrm{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. *Obvious for* $\varepsilon \geq 1$.

Elkies and Langevin showed (indep.) this form of *ABC* implies for each $\varepsilon > 0$ that $\mathrm{rad}(a^5 - 2b^5) > \max(|a|, |b|)^{3-\varepsilon}$ for all but finitely many rel. prime a and b. That in turn implies Roth's theorem for $\alpha = \sqrt[5]{2}$, *i.e.*, $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$ finitely often for each ε.

More generally Elkies and Langevin showed *ABC* implies the **full** Roth theorem, and an effective bound on exceptions in Roth's theorem would follow from an effective version of *ABC*.

FAQ about Mochizuki's work on the *ABC* conjecture

1. How does he **use** a solution to the simple equation $a + b = c$?
2. Does his approach to the *ABC* conjecture lead to an explicit bound on exceptions to $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$?

FAQ about Mochizuki's work on the *ABC* conjecture

1. How does he **use** a solution to the simple equation $a + b = c$?
2. Does his approach to the *ABC* conjecture lead to an explicit bound on exceptions to $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$?

1) Associate to $a + b = c$ the **Frey curve** $y^2 = x(x - a)(x + b)$.
He aims to **prove** Szpiro's conjecture on elliptic curves, which implies *ABC* conjecture when applied to Frey curves.

FAQ about Mochizuki's work on the *ABC* conjecture

1. How does he **use** a solution to the simple equation $a + b = c$?
2. Does his approach to the *ABC* conjecture lead to an explicit bound on exceptions to $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$?

1) Associate to $a + b = c$ the **Frey curve** $y^2 = x(x - a)(x + b)$. He aims to **prove** Szpiro's conjecture on elliptic curves, which implies *ABC* conjecture when applied to Frey curves.

2) He does not think so. He has one explicit estimate directly relevant to the *ABC* conjecture, for "generic" elliptic curves, and the "non-generic" case requires reduction steps with **Belyi maps**. He feels this is incompatible with making *ABC* explicit.

Questions?

References

E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*.

V. Dimitrov, http://mathoverflow.net/questions/106560/philosophy-behind-mochizukis-work-on-the-abc-conjecture

A. Granville and T. Tucker, "It's as easy as *abc*", Notices AMS, 2002.

S. Lang, *Math Talks for Undergraduates*.

S. Lang, "Old and New Conjectured Diophantine Inequalities", *Bull. AMS*, 1990.

A. Nitaj, "La conjecture abc", *Enseign. Math.*, 1996.

A. Nitaj, http://www.math.unicaen.fr/~nitaj/abc.html (*abc* conjecture homepage).

M. Waldschmidt, "Perfect Powers: Pillai's works and their developments", http://www.math.jussieu.fr/~miw/articles/pdf/PerfectPowers.pdf.