The ABC Conjecture and Elliptic Curves

Lily Khadjavi
Loyola Marymount University
Los Angeles, CA
lkhadjavi@lmu.edu

Research and Evaluation Center, John Jay College
New York, NY

Sage Days for Women, July 2013

Outline

Collaborator: **Victor Scharaschkin**
University of Queensland
Brisbane, Australia

What is the ABC Conjecture?

Equations of the form $a+b=c$ often occur in number theory.

1. Fermat: $x^n + y^n = z^n$
2. Generalized Fermat: $Au^n + Bv^m = Cw^r$
3. Pell: $x^2 - dy^2 = 1$
4. Catalan $x^n - y^m = 1$

An *abc triple* is a triple (a, b, c) of pairwise relatively prime integers satisfying

$$a + b = c. \tag{1}$$

What is the ABC Conjecture?

Intuition: given such a triple with $a + b = c$, if a and b are full of powers, c is not likely to be. An example:

$$2^5 \cdot 7^3 + 3^3 \cdot 11^4 =$$

What is the ABC Conjecture?

Intuition: given such a triple with $a + b = c$, if a and b are full of powers, c is not likely to be. An example:

$$2^5 \cdot 7^3 + 3^3 \cdot 11^4 = 17 \cdot 23899. \tag{2}$$

What is the ABC Conjecture?

Intuition: given such a triple with $a + b = c$, if a and b are full of powers, c is not likely to be. An example:

$$2^5 \cdot 7^3 + 3^3 \cdot 11^4 = 17 \cdot 23899. \tag{2}$$

Definition: For non-zero integer n let the *radical*, $rad(n)$, be the product of distinct primes dividing n, **not** counted with multiplicity.
For example, $rad(24) = rad(2^3 \cdot 3) = 6$.

Usually $rad(abc) > \max\{a, b, c\}$.

In (2), $a = 10,976$, $b = 395,307$, $c = 406,283$, and $rad(abc) = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 23899 = 187,702,746$.

What is the ABC Conjecture?

We compare the size of the maximum versus the size of the radical. Definition: The *quality* q of an abc triple is

$$q = q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}. \tag{3}$$

In the previous example, $q = 0.677929....$

Generally speaking, it's hard to find triples with $q > 1$.

What is the ABC Conjecture?

We compare the size of the maximum versus the size of the radical. Definition: The *quality* q of an abc triple is

$$q = q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}. \tag{3}$$

In the previous example, $q = 0.677929....$

Generally speaking, it's hard to find triples with $q > 1$.

Pick your favorite $a + b = c$ and find q for the triple.

What is the ABC Conjecture?

We compare the size of the maximum versus the size of the radical. Definition: The *quality* q of an abc triple is

$$q = q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}. \tag{3}$$

In the previous example, $q = 0.677929....$

Generally speaking, it's hard to find triples with $q > 1$.

Pick your favorite $a + b = c$ and find q for the triple.

Did anyone obtain $q > 1$?

What is the ABC Conjecture?

The *quality* q of an abc triple is

$$q = q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}. \tag{4}$$

Generally speaking, it's hard to find triples with $q > 1$.

What is the ABC Conjecture?

The *quality* q of an abc triple is

$$q = q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}. \tag{4}$$

Generally speaking, it's hard to find triples with $q > 1$.

The ABC Conjecture

Given pairwise relatively prime integers a, b, c such that $a + b = c$,

$$\limsup q(a, b, c) = 1$$

as $\max\{|a|, |b|, |c|\} \to \infty$.

In other words, there at most finitely many triples with $q > 1 + \epsilon$, for any $\epsilon > 0$.

What is the ABC Conjecture?

There are alternate formulations of ABC.

The ABC Conjecture

For every $\epsilon > 0$, there exists a constant κ_ϵ such that for all triples (a, b, c) of coprime positive integers, with $a + b = c$, the inequality

$$\max\{|a|, |b|, |c|\} < \kappa_\epsilon rad(abc)^{1+\epsilon}$$

holds.

We can generalize the maximum and radical using heights and norms, extending the ABC Conjecture to a statement over number fields:

$$H(a, b, c) < \kappa_\epsilon N(abc)^{1+\epsilon}$$

Why the interest in the ABC Conjecture?

Consider Fermat's Last Theorem.

For $n > 2$, the equation

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

has no non-trivial solutions for integers x, y, z.

- Conjectured by Fermat in the 1600s
- Proved by Wiles in the 1990s

What if we knew the ABC Conjecture was true? What would it tell us about the existence of integer solutions to the equation of Fermat's Last Theorem?

Why the interest in the ABC Conjecture?

Suppose (contradicting Fermat) that for $n > 3$, we could find a triple, x, y, z, of relatively prime, positive integers where $x^n + y^n = z^n$.

$$\begin{aligned} q = \frac{\log z^n}{\log rad(xyz)} &\geq \frac{n \log z}{\log(rad(x)rad(y)rad(z))} \\ &> \frac{n \log z}{\log (z^3)} \\ &> \frac{n}{3} \\ &> 1 + \epsilon \end{aligned}$$

If the ABC Conjecture holds, there are only finitely many triples with $q > 1 + \epsilon$, i.e., there can only be finitely many n with solutions to the equation of Fermat. ("Asymptotic FLT")

Why the interest in the ABC Conjecture?

The ABC Conjecture implies many famous statements. A partial list:

- Fermat's Last Theorem, up to finitely many exceptions.
- Generalized Fermat: Darmon-Granville.
- Mihăilescu's theorem (Catalan's conjecture): $x^m - y^n = 1$ has only finitely many solutions for $m, n \geq 2$. [posed in 1844; proved in 2002]
- Faltings' Theorem (Mordell's Conjecture): curves of genus $g > 1$ have only finitely many rational points.
- Infinitely many non-Wieferich primes: p with $2^{p-1} \not\equiv 1 \pmod{p^2}$.
- Lang's conjecture: among all elliptic curves E defined over $\mathbb{Q}$ there exists a point of smallest non-zero canonical height.

The ABC Olympics

We claimed that it's "hard" to find triples with quality $q > 1$, so we are especially interested when we find such cases.

The ABC Conjecture

$$\limsup q(a, b, c) = 1$$

as $\max\{|a|, |b|, |c|\} \to \infty$.

By the ABC Conjecture, $\forall \epsilon > 0$ there should only be finitely many triples with $q > 1 + \epsilon$.
In fact, fewer than 240 triples with $q > 1.4$ are known, only 13 triples with $q > 1.5$, and only 3 with $q > 1.6$. The best are:

$$2 + 3^{10} \cdot 109 = 23^5, \qquad q = 1.62991.$$

$$11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23, \qquad q = 1.62599.$$

However, is not even known if 1 is a limit point of a sequence of abc triples.

It's good to have goals

Goals

1. Find triples of high quality, e.g., $q > 1$.

2. Show that $q > 1$ for infinitely many abc triples. (There are already special case arguments for this; can we find a more systematic method?)

3. A weak ABC Conjecture: Show that 1 is a limit point of the qualities, q, for some sequence of abc triples.

Ad-hoc approaches to $q > 1$

Consider the equation $a + b = c$ given by

$$2^{2k+2} - 2^{k+1} + 1 = (2^{k+1} - 1)^2$$

Rewriting as

$$2^{k+1}(2^k - 1) + 1 = (2^{k+1} - 1)^2$$

we find

$$\begin{aligned} rad(abc) & \\ & \leq 2(2^k - 1)(2^{k+1} - 1) \\ & = (2^{k+1} - 2)(2^{k+1} - 1) \\ & < (2^{k+1} - 1)^2 \\ & = c \end{aligned}$$

Thus $q > 1$ for infinitely many n.

Elkies: ABC Implies Mordell

Constructing ABC triples of high quality from rational points on curves

To every abc triple, we can associate a rational number r (not equal to 0, 1, or ∞), and vice versa.

$$(a, b, c) \longleftrightarrow r = c/b$$

Elkies: ABC Implies Mordell

Constructing ABC triples of high quality from rational points on curves

To every abc triple, we can associate a rational number r (not equal to 0, 1, or ∞), and vice versa.

$$(a, b, c) \longleftrightarrow r = c/b$$

Given a rational point $P \in C$, a smooth projective curve defined over $\mathbb{Q}$, and a map $f : C \to \mathbb{P}^1$, consider the quality of the abc triple induced by $f(P) = r = c/b$.

Is there a choice of curves, points, and maps which would lead us to abc triples with high quality q?

Elkies: ABC Implies Mordell

Constructing ABC triples of high quality from rational points on curves

To every abc triple, we can associate a rational number r (not equal to 0, 1, or ∞), and vice versa.

$$(a, b, c) \longleftrightarrow r = c/b$$

Given a rational point $P \in C$, a smooth projective curve defined over $\mathbb{Q}$, and a map $f : C \to \mathbb{P}^1$, consider the quality of the abc triple induced by $f(P) = r = c/b$.

Is there a choice of curves, points, and maps which would lead us to abc triples with high quality q? (Yes!)
Elkies relates the height of a point to the quality of the triple.

Elkies: ABC Implies Mordell

Define the *height* of $r = u/v \in \mathbb{Q}$ to be $H(r) = \max\{|u|, |v|\}$. Let $h(r) = \log H(r)$, the logarithmic height.
Elkies proves the following inequality concerning the quality of a triple, q, where d is the degree of a map f (the map which will give us c/b):

$$\frac{1}{q} \leq \frac{\#f^{-1}(\{0, 1, \infty\})}{d} + \frac{O(1)}{\sqrt{h(P)}}.$$

Elkies: ABC Implies Mordell

Define the *height* of $r = u/v \in \mathbb{Q}$ to be $H(r) = \max\{|u|, |v|\}$.
Let $h(r) = \log H(r)$, the logarithmic height.
Elkies proves the following inequality concerning the quality of a triple, q, where d is the degree of a map f (the map which will give us c/b):

$$\frac{1}{q} \leq \frac{\#f^{-1}(\{0,1,\infty\})}{d} + \frac{O(1)}{\sqrt{h(P)}}.$$

Our goal:
q large $\iff$ $\#f^{-1}(\{0,1,\infty\})$ small while $h(P)$ large

Thus, we would like (1) an infinite sequence of points, P_i, of increasing height, which we obtain using elliptic curves, and (2) f "as ramified as possible" over $\{0,1,\infty\}$. There are maps, called *Belyi* maps, β, which satisfy this.

"Mordell is as easy as ABC" – Don Zagier

Elkies' inequality:

$$\frac{1}{q} \leq \frac{\#f^{-1}(\{0,1,\infty\})}{d} + \frac{O(1)}{\sqrt{h(P)}}$$

Corollary

The ABC Conjecture implies Faltings' Theorem: curves of genus $g > 1$ have only finitely many rational points.

Sketch of proof: Fix $\epsilon > 0$. For genus ≥ 2, Riemann-Hurwitz gives $\#(f^{-1}(\{0,1,\infty\}) < d$ so for $h(P)$ large enough, by the previous inequality, $q > 1 + \epsilon$. So if the ABC Conjecture is correct, there are only finitely many such points of large height.

Belyi maps

Definition: If C is a curve, a *Belyi map*, β, is a finite morphism $C \to \mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$ whose branch points are contained in $\{0, 1, \infty\}$.

- Belyi maps arose when Belyi proved that a curve is defined over $\mathbb{Q}$ if and only if it admits a such a map (conjectured by Grothendieck).
- Belyi's proof is constructive (but with impractically high bounds for the maps).

Belyi maps

Grothendieck was truly excited by Belyi's result. From *Esquisse d'un programme*:

> *. . . quelles sont les courbes algébriques sur* $\overline{\mathbf{Q}}$ *obtenues ainsi – les obtiendrait-on toutes, qui sait? . . . Une telle supposition avait l'air à tel point dingue que j'étais presque gêné de la soumettre aux compétences en la matière. Deligne consulté trouvait la supposition dingue en effet, mais sans avoir un contre-exemple dans ses manches. Moins d'un an après, au Congrès International de Helsinki, le mathématicien soviétique Belyi annonce justement ce résultat, avec une démonstration d'une simplicité déconcertante tenant en deux petites pages d'une lettre de Deligne – jamais sans doute un résultat profond et déroutant ne fut démontré en si peu de lignes!*

> *. . . which are the algebraic curves defined over* $\overline{\mathbf{Q}}$ *obtained in this way – does one obtain them all, who knows? . . . Such a supposition seemed so crazy that I was almost embarrassed to submit it to the competent people in the field. Deligne when consulted found it crazy indeed but without having a counterexample at hand. Less than a year later, at the International Congress in Helsinki, the Soviet mathematician Belyi announced this very result, with a proof of disconcerting simplicity contained in two little pages of a letter of Deligne – never was such a profound and disconcerting result proved in so few lines!*

Belyi maps for elliptic curves

For elliptic curves, we can find constructions that are of low degree.

Theorem (K. and Scharaschkin)

Suppose E is an elliptic curve (in Weierstrass form) over $\mathbb{Q}$, $E : y^2 = x^3 + Ax + B$. Then there exists a Belyi map β for E such that

1. *If $B = 0$ $(j = 1728)$ then $3 \leq \deg(\beta) \leq 4$.*
2. *If $A = 0$ $(j = 0)$ then $3 \leq \deg(\beta) \leq 6$.*
3. *Otherwise $\deg(\beta) \leq 12\, H(j/1728)$.*

Examples of low degree Belyi maps

Degree 3: $E : y^2 = x^3 + D^2$,

$$\beta_3(x, y) = \frac{y + D}{2D}.$$

Degree 4: $E : y^2 = x^3 - Dx$,

$$\beta_4(x, y) = \frac{x^2}{D}.$$

Degree 5: $E : y^2 = x^3 - 120x + 740$,

$$\beta(x, y) = \frac{y(x + 5) + 162}{324}.$$

Degree 6: $E : y^2 = x^3 + D$,

$$\beta_6(x, y) = \frac{y^2}{D}.$$

Open problem: given a curve C, what is a Belyi map of minimal degree for C?

Using Belyi maps for the ABC Conjecture

Implementing Elkies' idea to find examples of high quality, q:

[Our ABC goals: find abc triples with quality $q > 1$; find families of triples of high quality; find a sequence of qualities with limit 1.]

- Pick a curve C and a Belyi map $f : C \to \mathbb{P}^1$. For each point $P \in C(\mathbb{Q})$ obtain a triple via $f(P) = r = c/b$.
- In particular, given a torsion-free point P on an elliptic curve $E(\mathbb{Q})$, consider an infinite sequence of points $P, 2P, 3P, \ldots$, and for each, recover a triple via $r = f(kP)$.

Example

Consider $E: y^2 = x^3 - 6x$ and $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with generators $P = (3, 3)$, and $(0, 0)$ of order 2. A Belyi map is $f(x, y) = -x^2/6$. We use Sage to compute $2P, 3P, \ldots$ and then find q for the corresponding abc triples.

n	a	b	c	$q(nP)$
1	1	2	3	0.61315
2	23^2	$2^5 \cdot 3$	5^4	0.98486
3	1871^2	$2 \cdot 13^4$	$3^5 \cdot 11^4$	1.05569
4	39841^2	$2^9 \cdot 3 \cdot 5^4 \cdot 23^4$	$7^4 \cdot 103^4$	1.11019
5	$19^2 \cdot 29^2 \cdot 101^2 \cdot 25339^2$	$2 \cdot 37^4 \cdot 239^4$	$3 \cdot 17^4 \cdot 41^8$	1.09475
6	$23^2 \cdot 1607^2 \cdot 14159^2 \cdot 21863^2$	$2^5 \cdot 3^5 \cdot 11^4 \cdot 13^4 \cdot 1871^4$	$5^4 \cdot 722977^4$	1.01589
7				0.99030
8				1.03153
9				1.01262

We see that it is plausible that q approaches 1.

Example

Consider $E: y^2 = x^3 + 14904$, with $E(\mathbb{Q}) \cong \mathbb{Z}$, generated by $P = (18, 144)$; a Belyi map is $\beta(x, y) = \frac{y^2}{14904}$. We write $a = Au^3$, $b = Bv^6$, $c = Cw^2$, with A, B, C dividing 14904. $(14904 = 2^3 \cdot 3^4 \cdot 23)$.

n	u	v	w	$q(nP)$
1	1	1	2^2	0.70338
2	$5^2 \cdot 7$	2^3	11	**1.62599**
3	829097	$3 \cdot 101$	$2^2 \cdot 5^2 \cdot 7 \cdot 17 \cdot 71 \cdot 1187$	1.03043
4	$5^2 \cdot 7 \cdot 61 \cdot 7116563$	$2^4 \cdot 11$	$15944329 \cdot 3939782807$	1.11389
5	$2099 \cdot 39451 \cdot 756551369$	$89 \cdot 569 \cdot 4951$	$2^2 \cdot P_{26}$	0.98793
6				1.04113
7				0.99382
8				1.02623
9				1.00606

Elliptic curves and abc triples

Although this may seem ad hoc, we can prove

Theorem (K. and Scharaschkin)

Given any abc triple, there exists an elliptic curve E with rational point P and Belyi map β inducing this triple.

In fact, we can restrict to the curves $y^2 = x^3 + D$. Tom Womack has computed the Mordell-Weil group for these with $|D| < 10^6$. Using his table, we have searched over more than 2 million curves. (No previously unknown triples of high quality emerged.)

Elliptic curves and abc triples

Theorem (Elkies)

Let E be an elliptic curve, $f : E \to \mathbb{P}^1$ a Belyi map and let $\epsilon > 0$. Then $q(f(P)) > 1 - \epsilon$ for almost all points $P \in E(\mathbb{Q})$.

Theorem (K. and Schraschkin)

Suppose $E(\mathbb{Q})$ is infinite, where E has j-invariant 0 or 1728. Then $q(f(P)) > 1$ infinitely often provided that there are infinitely many non-Wieferich primes for some P in $E(\mathbb{Q})$.

Previously there have been ad-hoc examples of equations with abc quality > 1, but this gives us many families (and curves) to choose from.

Wieferich primes

An analogy Fix $a > 1$. On $\mathbb{Z}$ we have a filtration

$$\mathbb{Z} \supseteq p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq \cdots$$

where

$$p^n\mathbb{Z} \to p^{n+1}\mathbb{Z}$$

by multiplication by p, $n \geq 1$. $\mathbb{Z} \to p\mathbb{Z}$ by

$$a \mapsto a^{p-1} - 1.$$

We say p is a *Wieferich prime* to base a if

$$a^{p-1} \equiv 1 \pmod{p^2}$$

iff $a \in \mathbb{Z}$ maps to $p^2\mathbb{Z}$, iff a lands in an unexpectedly high filtrant. Analogous *elliptic Wieferich primes* are the obstacle to showing that 1 is a limit point for a sequence of abc triples.

Obstruction to showing 1 is a limit point of q's

To bound the radical, we calculate ord_p of coordinates by working over $\mathbb{Q}_p$. For $n \geq 1$ let

$$E_n = \{(x, y) \in E(\mathbb{Q}_p) \mid \mathrm{ord}_p(x) \leq -2n\} \cup \{0\}.$$

(E_1 is the kernel of reduction mod p). There is an exhaustive filtration:

$$E(\mathbb{Q}_p) \supseteq E_1 \supseteq E_2 \supseteq \cdots$$

with

$$E(\mathbb{Q}_p)/E_1 \cong \widetilde{E}(\mathbb{F}_p) \quad \text{and} \quad E_n/E_{n+1} \cong \mathbb{F}_p, \quad n \geq 1.$$

For $n \geq 1$,

$$Q \in E_n \setminus E_{n+1} \implies pQ \in E_{n+1} \setminus E_{n+2}.$$

so we can *almost* read $\mathrm{ord}_p(nP_0)$ directly off the filtration. Obstruction to proving that $q \to 1$: a larger than expected power of p may appear (e.g., a large power of 41 in an earlier example).

Elliptic Wieferich primes

Definition: Let m be the order of P_0 in $\widetilde{E}(\mathbb{F}_p)$. Say that p is an elliptic *Wieferich prime* if $mP_0 \in E_2$.

1 is a limit point if the Wieferich primes are sufficiently "rare": If nP_0 does not contain any Wieferich primes, then we can bound the radical from filtration information, to show $q \to 1$.

Thus, provided we can find an infinite sequence of n with nP_0 not containing Wieferich primes, then 1 is a limit point of the ABC conjecture.

Wieferich primes: Heuristics

Good news: there should be infinitely many non-Wieferich primes. Example: $y^2 = x^3 - 6x$. The only Wieferich primes $p < 10^9$ are

p	Order m
41	10
3253	543
7573	1263
81239	40620

Mixed news (Scharaschkin): For CM curves, assuming some standard conjectures, there are infinitely many Wieferichs.

Thank you.