On a Problem Related to the ABC Conjecture

Daniel M. Kane

Department of Mathematics / Department of Computer Science and Engineering
University of California, San Diego
dakane@ucsd.edu

October 18th, 2014
The ABC Conjecture

For integer $n \neq 0$, let the radical of $n$ be

$$\text{Rad}(n) := \prod_{p|n} p.$$ 

For example, $\text{Rad}(12) = 2 \cdot 3 = 6$.

The ABC-Conjecture of Masser and Oesterlé states that

**Conjecture**

For any $\epsilon > 0$, there are only finitely many triples of relatively prime integers $A, B, C$ so that $A + B + C = 0$ and

$$\max(|A|, |B|, |C|) > \text{Rad}(ABC)^{1+\epsilon}.$$
Applications

The ABC Conjecture unifies several important results and conjectures in number theory

- Provides new proof of Roth’s Theorem (with effective bounds if ABC can be made effective)
- Proves Fermat’s Last Theorem for all sufficiently large exponents
- Implies that for every irreducible, integer polynomial $f$, $f(n)$ is square-free for a constant fraction of $n$ unless for some prime $p$, $p^2 | f(n)$ for all $n$
- A uniform version of ABC over number fields implies that the Dirichlet $L$-functions do not have Siegel zeroes.
The function field version of the ABC conjecture follows from elementary algebraic geometry. In particular, if $f, g, h \in \mathbb{F}[t]$ are relatively prime and $f + g + h = 0$ then

$$\max(\deg(f), \deg(g), \deg(h)) \geq \deg(\text{Rad}(fgh)) - 1.$$ 

The version for number fields though seems to be much more difficult. In 2012, Shinichi Mochizuki submitted a purported proof of the conjecture. The proof uses Mochizuki’s “inter-universal Teichmüller theory”, making it difficult to check. The proof has still not been fully verified.
Experimental Results

The ABC@Home project has been searching for ABC triples since 2006. Define the *quality* of a triple to be

\[ q(A, B, C) = \frac{\log(\max |A|, |B|, |C|)}{\log(\text{Rad}(ABC))}. \]

The highest quality triples found to date are:

\[
\begin{align*}
2 + 3^{10} &= 23^5 & q &= 1.63 \\
11^2 + 3^2 \cdot 3^2 \cdot 5^6 \cdot 7^2 &= 2^{21} \cdot 23 & q &= 1.63 \\
19 \cdot 1307 + 2 \cdot 3^7 &= 2^8 \cdot 3^{22} \cdot 5^4 & q &= 1.62 \\
283 + 5^{11} \cdot 13^2 &= 2^8 \cdot 3^8 \cdot 17^3 & q &= 1.59
\end{align*}
\]

As these are all relatively small they seem to provide some support for the conjecture.
Heuristics

Why might we expect ABC to be true?

- Count number of solutions with $|A|, |B|, |C| \approx N$ and $\text{Rad}(A) \leq N^a$, $\text{Rad}(B) \leq N^b$, $\text{Rad}(C) \leq N^c$ for fixed $a, b, c$ with $a + b + c < 1$.
- How many such $A, B, C$ are there?

Lemma

For any $m$, the number of $n$ with $|n| \leq N$ and $\text{Rad}(n) = m$ is $O_{\epsilon}(N^c)$.

Proof.

- Let $m = \prod_{i=1}^{k} p_i$
- $n = \prod_{i=1}^{k} p_i^{a_i}$ with $a_i \geq 1$ and $\sum_{i=1}^{k} a_i \log(p_i) \leq \log(N)$. 
Heuristics

Why might we expect ABC to be true?

- Count number of solutions with $|A|, |B|, |C| \approx N$ and $\text{Rad}(A) \leq N^a, \text{Rad}(B) \leq N^b, \text{Rad}(C) \leq N^c$ for fixed $a, b, c$ with $a + b + c < 1$.
- How many such $A, B, C$ are there?

Lemma

For any $m$, the number of $n$ with $|n| \leq N$ and $\text{Rad}(n) = m$ is $O_\epsilon(N^\epsilon)$.

Proof.

- Let $m = \prod_{i=1}^{k} p_i$
- $n = \prod_{i=1}^{k} p_i^{a_i}$ with $a_i \geq 1$ and $\sum_{i=1}^{k} a_i \log(p_i) \leq \log(N)$.
- At most $\frac{1}{k!} \prod_{i=1}^{k} \frac{\log(N)}{\log(p_i)}$
- Largest when $p_i$ as small as possible. Optimizing over $k$ gives $N^{O(\log \log \log(N) / \log \log(N))} = O_\epsilon(N^\epsilon)$. 
Heuristics

Why might we expect ABC to be true?

- Count number of solutions with $|A|, |B|, |C| \approx N$ and $\text{Rad}(A) \leq N^a, \text{Rad}(B) \leq N^b, \text{Rad}(C) \leq N^c$ for fixed $a, b, c$ with $a + b + c < 1$.
- How many such $A, B, C$ are there?

Lemma

For any $m$, the number of $n$ with $|n| \leq N$ and $\text{Rad}(n) = m$ is $O_\epsilon(N^\epsilon)$.

- $N^{a+b+c+\epsilon}$ many triples with small radicals.
- About $1/N$ of them should have $A + B + C = 0$.
- Expect finitely many solutions if $a + b + c < 1$
Extended Conjecture

However, these heuristics also suggest what happens if \( a + b + c \geq 1 \).

**Conjecture (Mazur)**

For \( a + b + c \geq 1 \), let \( S_{a,b,c}(N) \) be the number of relatively prime triples \( A, B, C \) with \( |A|, |B|, |C| \leq N \), \( \text{Rad}(A) \leq |A|^a \), \( \text{Rad}(B) \leq |B|^b \), \( \text{Rad}(C) \leq |C|^c \) and \( A + B + C = 0 \). Then for any \( \varepsilon > 0 \) and \( d = a + b + c - 1 \),

\[
N^{d+\varepsilon} \gg_\varepsilon S_{a,b,c}(N) \gg_\varepsilon N^{d-\varepsilon}.
\]

Our goal is to prove this conjecture for \( a + b + c \geq 2 \).
Lower Bounds

Theorem

For $0 < a, b, c \leq 1$, with $a + b + c > 1$, $S_{a,b,c}(N) = \Omega(N^d \log(N)^{-2})$.

Basic idea:

- Force $A, B, C$ to have small radicals by making them divisible by $2^x, 3^y, 5^z$.
- Lattice problem
- Difficulties
  - Lattice too skew
  - Need $A, B, C$ relatively prime
The Lattice

- Pick $x, y, z$ as small as possible so that
  \[ 2^{x-1} \geq N^{1-a}, \quad 3^{y-1} \geq N^{1-b}, \quad 5^{z-1} \geq N^{1-c}. \]
- Let $\alpha = 2^x, \beta = 3^y, \gamma = 5^z$
- If $|A| \leq N$ and $\alpha | A$,
  - $|A|/\text{Rad}(A) \geq \alpha/\text{Rad}(\alpha) \geq N^{1-a} \geq |A|^{1-a}$
  - Thus $\text{Rad}(A) \leq |A|^a$
  - Similar argument for $B$ and $C$.
- Consider triples $(A, B, C)$ so that $A + B + C = 0$ and $\alpha | A, \beta | B, \gamma | C$
- This is a 2-dimensional lattice $L$
- Let $P$ be the polygon given by the set of $(x_1, x_2, x_3)$ with
  \[ x_1 + x_2 + x_3 = 0 \text{ and } |x_i| \leq N \text{ for all } i \]
- Points of $P \cap L$ whose coordinates are relatively prime give us solutions
Geometry of Numbers

- Count points in $L \cap P$
- Draw fundamental domain of $L$ around each point in intersection
- Roughly approximates $P$
- Compare areas
**Lemma**

Let $L$ be a lattice in a two dimensional vector space $V$ and $P$ a convex polygon in $V$. Let $m$ be the minimum separation between points of $L$. Then

$$|L \cap P| = \frac{\text{Volume}(P)}{\text{CoVolume}(L)} + O\left(\frac{\text{Perimeter}(P)}{m} + 1\right).$$

**Proof (sketch).**

- Make $L$ a square lattice (this can be done without increasing $\text{Perimeter}(P)$ by too much)
- Put fundamental domain around each point of intersection
- Covers $P$ exactly up to points within $m$ of the perimeter
- Comparing area to area of $P$ yields result
Application

- Recall:
  - $L = \{ (A, B, C) \in \mathbb{Z}^3, A + B + C = 0, \alpha|A, \beta|B, \gamma|C \}$
  - $\alpha = 2^x \approx N^{1-a}, \beta = 3^y \approx N^{1-b}, \gamma = 5^z \approx N^{1-c}$
  - $P = \{ (x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0, |x_i| \leq N \text{ for all } i \}$

- By Lemma
  \[
  |L \cap P| = \Theta \left( \frac{N^2}{N^{3-a-b-c}} \right) + O \left( \frac{\text{Perimeter}(P)}{m} + 1 \right)
  = \Theta \left( N^{a+b+c-1} \right) + O \left( \frac{\text{Perimeter}(P)}{m} + 1 \right)
  \]

- Problem: $m$ might be very small
Modified Lattice

- Suppose $L$ has short vector $(\alpha r, \beta s, \gamma t)$
- Idea: replace $L$ by some similar $L'$ for which we do not have an exceptionally short vector (want shortest vector $\approx \sqrt{\text{CoVol}}$)
- Technique
  - Let $2^h \mid \gcd(\alpha r, \beta s, \gamma t)$
  - Let $2^k \approx N^{(3-a-b-c)/2}/m$
  - Let $q$ be a prime $q > 5$, $q \mid r$ and $q$ small $O(\log(N))$
  - Let $q^{w-1} > 2^{h+k}$
  - Replace $\alpha$ by $\alpha' := 2^{x-h-k}q^w$, define $L' = \{(A, B, C) \in \mathbb{Z}^3, A + B + C = 0, \alpha'|A, \beta|b, \gamma|C\}$
- Analysis
  - $\frac{\alpha'}{\text{Rad}(\alpha')} = \frac{\alpha}{\text{Rad}(\alpha)}2^{-h-k}q^{w-1} > N^{1-a}$, good enough
  - $L'$ has short vector $v = (\alpha'2^kr, \beta2^{-h}q^ws, \gamma2^{-h}q^wt)$
  - $|v| \approx N^{(3-a-b-c)/2}$
  - $v$ not a multiple of other vectors in $L'$
  - For any $w$ in $L'$ either $w$ is a multiple of $v$ or $|w||v| \geq \text{CoVolume}(L') = \Theta(\alpha'\beta\gamma)$
  - Shortest vector in $L'$ has length at least $\Omega(N^{(3-a-b-c)/2}/\log(N))$
Summary

- Have lattice $L'$ and polygon $P$
- Have intersection

\[ |L' \cap P| = \frac{\text{Vol}(P)}{\text{CoVol}(L')} + O\left(\frac{\text{Perim}(P)}{m} + 1\right) \]

\[ = \Omega(N^d / \log(N)) + O(N^{d/2} \log(N) + 1) \]

If $(A, B, C) \in L' \cap P$ then:

- $A + B + C = 0$
- $|A|, |B|, |C| \leq N$
- $A/\text{Rad}(A) \geq N^{1-a} \geq |A|^{1-a}$ so $\text{Rad}(A) \leq |A|^a$
- Similarly, $\text{Rad}(B) \leq |B|^b, \text{Rad}(C) \leq |C|^c$
- Still need: $A, B, C$ relatively prime.
Sieving

- Need to count just the relatively prime triples
- Let \( L'_n = \{(A, B, C) \in L' : n | A, n | B, n | C\} \)
- Want

\[
\sum_{(A, B, C) \in L' \cap P} \begin{cases} 
  1 & \text{if } \gcd(A, B, C) = 1 \\
  0 & \text{otherwise}
\end{cases}
= \sum_{(A, B, C) \in L' \cap P} \sum_{n | \gcd(A, B, C)} \mu(n)
= \sum_n \mu(n) | L'_n \cap P|
\]
Approximation

Deal with sum

\[ \sum_n \mu(n) |L'_n \cap P| \]

- Truncate sum at \( n = N^{d/2} \log^2(N) \)
- Use Lemma to approximate inner sum

\[
\begin{align*}
\tilde{O}(N^{d/2}) &= \sum_{n=1} \frac{\mu(n) \text{Vol}(P)}{\text{CoVol}(L'_n)} + O \left( \frac{\text{Perimeter}(P)}{\text{ShortVec}(L'_n)} + 1 \right) \\
\tilde{O}(N^{d/2}) &= \sum_{n=1} \left( \frac{\text{Vol}(P)}{\text{CoVol}(L')} \right) \frac{\mu(n) \gcd(30q, n)}{n^2} + \tilde{O}(N^{d/2}/n) \\
= \Theta &\left( \frac{\text{Vol}(P)}{\text{CoVol}(L')} \right) + \tilde{O}(N^{d/2}) = \Omega(N^{a+b+c-1} \log^{-2}(N))
\end{align*}
\]

This proves the lower bound.
Lattice Upper Bounds

Idea: $A, B, C$ must have large repeated parts in their factorization with few ways to select them. Consider first fixing the repeated parts and then use lattice techniques to bound the number of solutions. First we need some definitions:

$$u(n) := \prod_{p \mid |n} p$$

$$e(n) := \prod_{p^\alpha \mid |n, \alpha > 1} p^\alpha = |n|/u(n)$$

$$v(n) := \prod_{p^2 \mid n} p = \text{Rad}(e(n)) = \text{Rad}(n)/u(n)$$
Basic Technique

- Fix the values of $A, B, C, v(A), v(B), v(C)$ each to within a factor of 2 (there are only $\log^6(N)$ ways to do this)
- Fix the exact values of $v(A), v(B), v(C)$ (there are $O(v(A)v(B)v(C))$ ways to do this)
- Fix the exact values of $e(A), e(B), e(C)$ (there are $O(N^\epsilon)$ ways to do this since $\text{Rad}(e(X)) = v(X)$ and $e(X) \leq N$)
- Count the number of $A, B, C$
Conditions on $A, B, C$

1. $A + B + C = 0$
2. $e(A)|A, e(B)|B, e(C)|C$
3. $|A|, |B|, |C| \leq N$ and are of at most the prespecified sizes.
4. We also need that the selected values $e(A), e(B), e(C)$ are the appropriate quantities for $A, B, C$, but we will ignore this condition as we only need an upper bound.

Note that conditions 1 and 2 above define a lattice, while condition 3 defines a polygon.
Another Lattice Lemma

Lemma

Let $L$ be a 2 dimensional lattice and $P$ a centrally symmetric convex polygon. Then the number of vectors in $L \cap P$ which are not positive integer multiples of other vectors in $L$ is

$$O \left( \frac{\text{Volume}(P)}{\text{CoVolume}(L)} + 1 \right).$$

Proof (sketch).

- If $P$ only contains, multiples of a single point, we have at most 2 and are done.
- Otherwise, $P$ contains a fundamental domain of $L$
- Thus, $2P$ contains a fundamental domain around each point of $L \cap P$
- Thus, $4\text{Volume}(P) = \text{Volume}(2P) \geq |L \cap P|\text{CoVolume}(L)$
Upper Bound

- Fix $A, B, C, \nu(A), \nu(B), \nu(C)$ to within factors of 2. Assume $|C| \geq |A|, |B|$
- At most $O(\nu(A)\nu(B)\nu(C)N^\epsilon)$ ways to select $e(A), e(B), e(C)$
- Number of triples is at most number of non-multiple points in $L \cap P$, bound with Lemma

$$\#\text{Solutions} \leq \nu(A)\nu(B)\nu(C)N^\epsilon \left( \frac{\text{Volume}(P)}{\text{CoVolume}(L)} + 1 \right)$$

$$\leq O \left( \frac{|A||B|\nu(A)\nu(B)\nu(C)N^\epsilon}{e(A)e(B)e(C)} + \nu(A)\nu(B)\nu(C)N^\epsilon \right)$$

$$\leq O \left( \frac{N^\epsilon \text{Rad}(A)\text{Rad}(B)\text{Rad}(C)}{|C|} + \nu(A)\nu(B)\nu(C)N^\epsilon \right)$$

$$\leq O(N^\epsilon |A|^a|B|^b|C|^{c-1} + \nu(A)\nu(B)\nu(C)N^\epsilon)$$

The above is at most

$$O(N^{a+b+c-1+\epsilon} + \nu(A)\nu(B)\nu(C)N^\epsilon)$$
Upper Bound

Proposition

Fix $0 < a, b, c \leq 1$. The number of solutions to the ABC problem with parameters $(a, b, c, N)$ and with $\nu(A), \nu(B), \nu(C)$ lying in fixed dyadic intervals is

$$O(N^{a+b+c-1+\epsilon} + \nu(A)\nu(B)\nu(C)N^\epsilon).$$

This bound works well when $\nu(A)\nu(B)\nu(C) \ll N^{a+b+c-1}$. In particular, if $a + b + c \geq 5/2$, the second term can be ignored. On the other hand, we could run into trouble otherwise.

We need a new upper bound technique to cover this case.
Basic idea: If $\nu(A)$ is large, then $A$ is divisible by a large square

Let

$$T(n) := n/\nu(n)^2$$

Bound solutions to

$$T(A)\nu(A)^2 + T(B)\nu(B)^2 + T(C)\nu(C)^2 = 0$$
Solutions to the Equation

Thus, we are left with trying to bound the number of integer solutions to the equation

\[ x_1 y_1^2 + x_2 y_2^2 + x_3 y_3^2 = 0 \]

with \(x_i, y_i\) within certain bounds. Fortunately, this problem is well studied

**Lemma (Pierre Le Boudec)**

The number of solutions to the above equation with \(|x_i| \leq U_i \leq N\) and \(|y_i| \leq V_i \leq N\) and \(x_1 y_1, x_2 y_2, x_3 y_3\) pairwise relatively prime is at most

\[ O(N^\epsilon (U_1 U_2 U_3)^{2/3} (V_1 V_2 V_3)^{1/3}). \]

Thus, letting \(V_1 = \nu(A), V_2 = \nu(B), V_3 = \nu(C), U_i = N/V_i^2\), we find that the number of solutions to the ABC problem with \(\nu(A), \nu(B), \nu(C)\) in given ranges is at most

\[ O(N^{2+\epsilon} (\nu(A)\nu(B)\nu(C))^{-1}). \]
Putting it Together

Theorem

For any $a, b, c, N, \epsilon > 0$ we have that

$$S_{a,b,c}(N) = O_{\epsilon}(N^{a+b+c-1+\epsilon} + N^{1+\epsilon}).$$

Proof.

- Fix the values of $\nu(A), \nu(B), \nu(C)$ to within factors of 2 (there are only $\log^3(N)$ ways to do this).
- If $\nu(A)\nu(B)\nu(C) \ll N$, then the lattice upper bound yields $O_{\epsilon}(N^{a+b+c-1+\epsilon} + N^{1+\epsilon})$.
- If $\nu(A)\nu(B)\nu(C) \gg N$, then the cubic solutions upper bound yields $O_{\epsilon}(N^{1+\epsilon})$.
- Summing over all ranges for $\nu(A), \nu(B), \nu(C)$ yields the appropriate bound.
Further Improvements

- We suspect that the lower bounds are essentially optimal
- These techniques cannot easily improve the upper bound
  - Case when $\nu(A)\nu(B)\nu(C) \approx N$
  - Lattice problem cannot exclude one solution per choice of $\nu(A), \nu(B), \nu(C)$
  - We expect that cubic in question actually has $N$ solutions in the appropriate range
  - Need something new
- Perhaps bound solutions to equation

$$x_1y_1^2z_1^3 + x_2y_2^2z_2^3 + x_3y_3^2z_3^3 = 0$$

for $x_i, y_i, z_i$ in some appropriate ranges.
Acknowledgements

This work was done with the support of an NSF graduate fellowship.

Pierre Le Boudec *Density of Rational Points on a Certain Smooth Bihomogeneous Threefold*, preprint  
http://arxiv.org/abs/1308.0033

J. W. S. Cassels, *An Introduction to the Geometry of Numbers*  

Andrew Granville *Notes on Mazur’s “Questions about Powers of Numbers”*, unpublished.