Introduction to the \textit{abc} conjecture

Joseph R. Heavner$^*$

Abstract. These notes are based on a lecture I gave at the University of Maryland as a part of the Advanced Elementary Number Theory Research Interaction Team on October 20, 2016. This talk is meant to be suitable for an undergraduate audience. We state the \textit{abc} conjecture and realize its significance. Then, we provide a probabilistic argument for the conjecture's truth based on that presented by Tao in [6]. A number of equivalent statements are provided, which are significant in the literature. The elementary proof of the polynomial case due to Snyder (c.f. [7]) is briefly outlined before surveying some of the incremental progress achieved over the last three decades. We end by discussing the work of Shinichi Mochizuki in developing arithmetic deformation theory [8] and its prerequisites [14] before looking toward what the future might hold.

\textit{Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.}

– David Hilbert

0 Hilbert’s tenth problem

The quote above is the original statement of Hilbert’s tenth problem, one of some twenty-three problems Hilbert posed to the mathematical community at the turn of the twentieth century. Some of these problems were quickly solved, some were deemed imprecise, some were deemed physics rather than mathematics, and some are still unsolved (e.g., his eighth problem, the Riemann hypothesis). Regardless, few other problem lists have driven progress like Hilbert’s did. For us, the most important problem Hilbert posed was his tenth on Diophantine analysis.

Solving Diophantine equations is very difficult. Problems that ask students to solve just one relatively simple Diophantine equation are common in mathematics competitions at the highest level, and generalizing beyond particular solutions to particular equations is soundly in the category of hard problems. Hilbert and others hoped that there might be a way to avoid this by having an algorithm to solve these equations, which arise fairly frequently and are of some fundamental interest. In 1970, Martin Davis, Hilary Putnam, Julia Robinson, and Yuri Matiyasevich proved that the answer to Hilbert’s question was “no.” This reassured us that Diophantine equations really are hard to solve, and we have been trying even harder to study the solving of them ever since.

$^*$Department of Mathematics, University of Maryland, e-mail Address: jheavner@umd.edu
Theorem 0.1. (DPRM Theorem) Hilbert’s tenth problem is unsolvable.

Proof. □

Actually, the DPRM theorem proved something much stronger, but we will not discuss that here. The problem for \( \mathbb{Q} \) is still open. However, there has been a little bit of progress.

Theorem 0.2. (Robinson) The first order theory of \( \mathbb{Q} \) is undecidable.

Proof. □

It is probably fair to say that we do not understand what we are doing when trying to tackle this for \( \mathbb{Q} \), but there is a nice result due to Vojta, which is an analogy of a formal sort, and which is where we first see the \( abc \) conjecture shine.

Theorem 0.3. (Vojta) There is a formal dictionary between Diophantine approximation dealing with number fields and Nevanlinna theory (value distribution theory) involving meromorphic functions, thus connecting number theory and complex analysis.

Note that if the left hand side (respectively, right hand side) is undecidable, then the right hand side (respectively, left hand side) should be undecidable.

Theorem 0.4. The \( abc \) conjecture is needed to have a complete dictionary in the direction of meromorphic functions to number fields.

It is somewhat surprising that we know more about the number field case than the meromorphic function side. This is a time where using analytic tools may not help us much. Luckily, some people are working on this. Prominent mathematicians such as Bjorn Poonen and Barry Mazur have had some involvement (e.g., Mazur’s conjecture). Héctor Pastén Vásquez, who is not as well known as Poonen or Mazur but who is nonetheless a postdoctoral fellow at IAS, has proved some results on the matter as well, and his lectures at IAS are part of what brought this to my attention to use in this talk.

With that, we begin the lecture proper.

1 The conjecture and its importance

The \( abc \) conjecture, sometimes called the Oesterlé-Masser conjecture after its founders, was posed in 1985 by David Masser and again in 1988 by Joseph Oesterlé. The conjecture was seen immediately as fundamental, and it intrigued many for its vast, powerful consequences. Goldfeld once described the \( abc \) conjecture as “the most important unsolved problem in Diophantine analysis” \( \Pi \). Before we can state our first version of the \( abc \) conjecture, we must define a fundamental number-theoretic quantity.

Definition 1.1. The radical of a positive integer \( n \), which we denote \( \text{rad}(n) \), is the product of the integer’s distinct prime factors. In symbols, the radical is

\[
\text{rad}(n) := \prod_{p | n} p.
\]
Some authors use the notation $N(n)$ to denote the radical of $n$.

**Example 1.2.** We compute the following radicals:

$$
\text{rad}(12) = \text{rad}(2^2 \cdot 3) = 2 \cdot 3 = 6 \; ; \; \text{rad}(16) = \text{rad}(2^4) = 2 \; ; \; \text{rad}(23) = 23.
$$

**Exercise 1.3.** Find the radical of a few other small integers, say $n < 500$.

**Conjecture 1.4.** $(abc)$ For every $\epsilon > 0$, there exist only finitely many $(a, b, c)$ of pairwise coprime positive integers satisfying the equation $a + b = c$ such that

$$c > \text{rad}(abc)^{1+\epsilon}.$$

What this says in plain English is something like this:

For $a, b, c$ coprime with $a + b = c$, rad$(abc)$ is usually not much smaller than $c$. Perhaps more clearly, if $a, b$ can be decomposed into large prime powers, then $c$ is usually not divisible by large prime powers.

It is easy to see why this is fairly fundamental. Of course, prime number theory is a major area of mathematical research, because the prime numbers are the building blocks of all numbers by the fundamental theorem of arithmetic and the fact that most objects we call “numbers” are derived from $\mathbb{Z}$. This is a key role of prime numbers in the simple equation $a + b = c$.

Diophantine analysis is another major area of number theory. In Diophantine analysis we study of solutions of Diophantine equations. A Diophantine equation is simply an integer polynomial equation in any finite number of variables (i.e., an equation drawing from $\mathbb{Z}[x_1, \ldots, x_n]$). Diophantine geometry is the use of algebraic geometry to study these equations. It is widely held that the abc conjecture is among the deepest results in Diophantine geometry and indeed number theory as a whole. Perhaps the easiest way to see why the abc conjecture is as important as it is is to look at its consequences.

**Consequences:**

1. Fermat’s last theorem, which states that $a^n + b^n = c^n$ has no solutions in integers for $n > 2$, follows from abc. Famously, Andrew Wiles and Richard Taylor proved Fermat’s last theorem in 1995 by following a program of Frey and Serre and proving the Taniyama–Shimura–Weil conjecture (now known as the modularity theorem) for semi-stable elliptic curves.

2. The Beal conjecture, which generalizes Fermat’s last theorem by saying that if $a, b, c, x, y, z \in \mathbb{N}$ where $a^x + b^y = c^z$ with $x, y, z > 2$, then $a, b, c$ are with common prime factor, has at most finitely many counterexamples follows from the abc conjecture. The Beal conjecture has not yet been proven, but Beal has offered – perhaps somewhat jokingly – one million dollars for a proof.

---

1More precisely, it follows for $n \geq 6$, but we can ignore this technicality, because classical results reduce Fermat’s last theorem to considering $n$ a prime power greater than 10.

2Diamond, Conrad, Taylor, and Breuil proved the conjecture in full over the six years between Wiles proof of the special case and 2001.
3. The Mordell conjecture, also known as Faltings’ theorem, which states that curves of genus \( g > 1 \) over a number field \( K \) have only finitely many rational points, follows from the abc conjecture. This theorem was proved by Faltings in 1984.

4. An effective version of Roth’s theorem, a celebrated theorem of Diophantine approximation which states that if \( \alpha \) is an irrational algebraic number and \( \epsilon > 0 \) is fixed, then

\[
\left| \frac{\alpha - p}{q} \right| < \frac{1}{q^{2+\epsilon}}
\]

can have only finitely many solutions in coprime integers \( p, q \), is given by the abc conjecture. Equivalently, the Thue-Siegel-Roth theorem can be stated in terms of \( C(\alpha, \epsilon) \), a positive value depending only on the parameters \( \alpha \) and \( \epsilon \), by saying every algebraic irrational \( \alpha \) satisfies

\[
\left| \frac{\alpha - p}{q} \right| > \frac{C(\alpha, \epsilon)}{q^{2+\epsilon}}.
\]

Here, not being “effective” means not being computationally effective. So, there is no known bound on the possible values \( p, q \) for a given \( \alpha \). A non-effective version of Roth’s theorem was proved by Klaus Roth in 1955 after incremental progress by Liouville in 1844, Thue in 1909, Siegel in 1921, and Dyson in 1947.

5. Catalan’s conjecture, which states that the only integral solution to the equation \( x^a - y^b = 1 \) for \( a, b > 1 \), and \( x, y > 0 \) is \( x = 3, a = 2, y = 2, b = 3 \), follows from the abc conjecture. This conjecture was proved in 2002 by Mihăilescu.

6. The Fermat-Catalan conjecture states that \( a^m + b^n = c^k \) has only finitely many solutions \((a, b, c, m, n, k)\) with distinct triplets of values \((a^m, b^n, c^k)\), where \( a, b, c \) are coprime positive integers and \( m, n, k \) are positive integers such that the sum of their reciprocals is less than unity. The abc conjecture would give the Fermat-Catalan conjecture. The Fermat-Catalan conjecture has not yet been proven.

7. The Erdős-Woods conjecture states that there exists an absolute constant \( k > 2 \) such that for all positive integers \( x, y \), if \( \text{rad}(x + i) = \text{rad}(y + i) \) for \( i = 1, 2, \ldots, k \), then \( x = y \). The abc conjecture implies the conjecture holds with at most finitely many counter-examples. The Erdős-Woods conjecture is still an open problem.

8. A Wieferich prime \( p \) is one such that \( p^2 \mid 2^{p-1} - 1 \). In 1988, Silverman showed the abc conjecture implies there are infinitely many non-Wieferich primes. To prove there are infinitely many non-Wieferich primes is still an open problem.

9. The Brocard-Ramanujan problem asks what integers \( n, m \) solve \( n! + 1 = m^2 \). The abc conjecture would imply that \( n! + A = m^2 \) has only finitely many solutions for a given \( A \in \mathbb{Z} \). This problem is still unsolved, but many conjecture the only pairs that work to be \((n, m) = (4, 5), (5, 11), (7, 71)\).
10. The Erdős-Ulam conjecture can be stated as follows. Let $U \subset \mathbb{R}^2$ be a set such that the distance between any two points in $U$ is rational. Can $U$ be dense? Tao showed the Erdős-Ulam conjecture follows from a special case of the Bombieri-Lang conjecture [2], which can be stated as follows. Let $X$ be a smooth projective irreducible algebraic surfaced over $\mathbb{Q}$ of general type. The set $X(\mathbb{Q})$ of rational points of $X$ is not Zariski dense in $X$. The $abc$ implies a case of the Bombieri-Lang conjecture, and in particular it answers the Erdős-Ulam conjecture by saying that the only infinite rational distance sets are contained in a line with four additional points or a circle with three additional points. Both the Erdős-Ulam and the Bombieri-Lang conjecture are open.

11. Granville showed that the $abc$ conjecture can be used to count the number of squarefree positive integers $n$ for which $f(n)$ is squarefree, where $f \in \mathbb{Z}[x]$. For $\deg f > 3$ this is still an open problem.

12. In 2003, Luca showed that the $abc$ conjecture implies $p^w - p^y - q^x - q^y$ has only finitely many positive integer solutions for $p, q$ prime. At the time of writing, this problem is still open.

13. The $abc$ conjecture implies an affirmative answer to the following problem of Julia Robinson. Are the operations $=, +, \times$ definable in the language $(\mathbb{N}, \perp, S)$, where $\perp$ is the binary operation of coprimality and $S$ is the successor function? This is very much an open problem.

14. The Dirichlet $L$-function $L(s, \chi_d)$ formed with the Legendre symbol has no Siegel zeros. This is still open in general.

15. A polynomial $P(x)$ has only finitely many perfect powers for $x \in \mathbb{Z}$ whenever $P$ has at least three simple zeros [5]. This is an open problem.

16. The ideal Waring’s theorem is the conjecture that for any $k \geq 2$, the equality $g(k) = 2^k + (\frac{3}{2})^k - 2$ holds, where $g(k)$ denotes the minimum number of $k$th powers needed to represent all integers. An explicit version of the $abc$ conjecture due to Baker implies the ideal Waring’s theorem. This problem has gone unsolved for over a century.

We might try to break the consequences of $abc$ into categories: ternary equation questions (e.g., Fermat’s last theorem, which was at one time thought to be best tackled with $abc$), rational point questions (e.g., Faltings’ theorem, which Elkies proved to follow from $abc$), polynomial value counting questions (e.g., Granville’s observation), prime questions (e.g., the existence of infinitely many non-Wieferich primes), definability questions (e.g., the problem of Robinson, which was proven to follow from $abc$ by Woods and Langevin), $L$-function questions (e.g., the question of the Siegel zeroes of $L(s, \chi_d)$, etc. The $abc$ Conjecture Homepage [3] cites some thirty-one consequences. At this time, Wikipedia lists some sixteen consequences, many of which are discussed in some detail [4].

---

It is said that Tarski proposed this problem to Robinson in the process of writing her Ph.D. thesis, but both found it intractable.
A more fundamental reason why $abc$ is important is that it connects an additive condition with a multiplicative structure in the sense that $a, b, c$ cannot have too many repetitions in their prime factorization. We have a lower bound for the radical, so in other words it cannot be too small, and so we can erase factors without losing too much.

Going back to the consequences for a moment, I should make a note about the fourteenth element of the list. The Riemann hypothesis, which many consider the most important unsolved problem in mathematics, and which is very much related to $L$ functions, cannot even achieve a proof of the non-existence of Siegel functions in this case. On the other hand, the most general form of the Riemann hypothesis gives that Siegel zeros do not exist in any case.

2 Why we suspect it is true

We will soon present a fairly convincing probabilistic argument for $abc$’s truth, but first we will look at a few concrete examples.

**Example 2.1.** First, we look at an example of what usually happens. Take $a = 1024$ and $b = 81$, so $a + b = c = 1105$. Note that $a = 2^{10}$ and $b = 3^4$ whereas $c = 5 \cdot 13 \cdot 17$. Clearly,

$$c = 1105 < \text{rad}(abc) = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 17 = 13260.$$

Now, let us look at one of the exceptional cases, which $abc$ claims there are only finitely many of.

**Example 2.2.** Take $a = 3$ and $b = 125$, so that $c = 128$. Note that $a = 3$, $b = 5^3$, and $c = 2^7$. We see that

$$c = 128 > \text{rad}(abc) = 3 \cdot 5 \cdot 2 = 30.$$

For $\epsilon = 0$, i.e., not raising the radical to a power, we know there are infinitely many exceptions. Still, we typically expect there to be many more prime powers on the left hand side of $a + b = c$ than the right hand side, and so we might think that simply raising the radical to a power might reduce the counterexamples to a finite number. Still, it is not immediately obvious that for any $\epsilon > 0$ the exponent $1 + \epsilon$ should work.

**Exercise 2.3.** Play with some other examples.

We now make a heuristic argument using probability, which is adapted from a blog post of Tao [6]. To achieve this, we will pretend that number-theoretic statements are probabilistic events rather than deterministic, and if $n$ heuristically probabilistic events have no apparent reason to be strongly correlated, they can be considered independent. Moreover, we can say that if $E_1, \ldots,$ is a sequence of number-theoretic statements with probabilities $P(E_1), \ldots,$ then we can say, if we again expect no correlation, that

$$\sum_{i=1}^{\infty} P(E_i) < \infty \implies \text{we should expect only finitely many } E_i \text{ to be true.}$$
\[ \sum_{i=1}^{\infty} \mathbb{P}(E_i) \ll 1 \implies \text{we should expect none of the } E_j \text{ to be true.} \]

\[ \sum_{i=1}^{\infty} \mathbb{P}(E_i) = \infty \implies \text{we should expect infinitely many } E_j \text{ to be true.} \]

Note that here we use \( \ll \) to mean “much less than.” This meaning is common, but we will define a more precise notion in a moment. Before moving onto the main argument, let us define a few symbols.

**Definition 2.4.** The notation \( \ll \) is the Vinogradov symbol. If \( f(x) \ll g(x) \), then there exists some \( N \) and \( k > 0 \) such that, for all \( x > N \), \( f(x) < kg(x) \).

Informally, we might say that the asymptotic growth of \( f \) is no faster than that of \( g \).

**Definition 2.5.** Let \( f \) and \( g \) be two functions defined on some \( D \subset \mathbb{R} \). The notation \( f(x) = O(g(x)) \) as \( x \to \infty \) means there exists a positive constant \( M \) such that for all sufficiently large \( x \), \( |f(x)| \leq M|g(x)| \). Somewhat more precisely, \( f(x) = O(g(x)) \) if and only if there exists \( M \in \mathbb{R}^+ \) and \( x_0 \in \mathbb{R} \) such that

\[ |f(x)| \leq M|g(x)| \text{ for all } x \geq x_0. \]

It should be clear that the Vinogradov symbol and big-\( O \) notation are different ways of expressing the same thing. We will also need the little-\( o \) notation, which is a stronger notion.

**Definition 2.6.** If \( f(x) = o(g(x)) \), then for every \( M > 0 \) there exists an \( x_0 \in \mathbb{R} \) such that

\[ |f(x)| \leq M|g(x)| \text{ for all } x \geq x_0. \]

The intuition here is that \( g(x) \) grows much faster than \( f(x) \), or that the growth of \( f(x) \) is negligible compared to that of \( g(x) \).

Now, we write the \( abc \) conjecture in a new form using \( \ll \). Note that \( \ll_{\epsilon} \) means that the relation depends only on \( \epsilon \).

**Conjecture 2.7.** (\( abc \)) If \( a + b = c \) are pairwise coprime natural numbers and we have that for every \( \epsilon > 0 \), then

\[ c \ll_{\epsilon} \text{rad}(abc)^{1+\epsilon}. \]

**Theorem 2.1.** For relatively prime \( a, b, c \), the following identity holds:

\[ \text{rad}(abc) = \text{rad}(a) \text{ rad}(b) \text{ rad}(c). \]

**Proof.** Easy. \( \Box \)

Given this, it can be shown that the following is an equivalent characterization of \( abc \).
Conjecture 2.8. (abc) Let $\alpha, \beta, \gamma \in \mathbb{R}_{\geq 0}$ with $\alpha + \beta + \gamma < 1$. Then, for sufficiently large values of $N$, there is no solution to the equation $a + b = c$ with $N \leq c \leq 2N$ and $a, b, c$ coprime, and
\[
\text{rad}(a) \leq N^\alpha, \text{rad}(b) \leq N^\beta, \text{rad}(c) \leq N^\gamma.
\]

To investigate whether or not we think $abc$ should be true, we will try to find counterexamples by the following procedure.

1. Choose some large $N$.
2. Choose coprime squarefree $x \leq N^\alpha, y \leq N^\beta, z \leq N^\gamma$.
3. Choose $a, b, c = O(N)$ with $\text{rad}(a) = x, \text{rad}(b) = y, \text{rad}(c) = z$ where $c$ is comparable to $N$.
4. Check whether or not $a + b = c$.

We take for granted the following divisor bound.

Lemma 2.2. If $x \leq N$ is a squarefree integer, then there are at most $O(N^{o(1)})$ integers $n < N$ with radical $x$. \hfill \Box

Let us now apply probabilistic heuristics to the procedure. Select $N$ as a large power of 2 for (1). There are $O(N^{\alpha+\beta+\gamma})$ choices for $x, y, z$ in (2), but we know that for each $x, y, z$ there are $O(N^{o(1)})$ choices for $a, b, c$ that are on order $O(N)$ by [2.2]. Assuming (when $a, b, c$ coprime) that there is no correlation between $a + b$ and $c$, which we consider as if randomly distributed amongst numbers of that size, there should be a probability on order $1/N$ that $a + b = c$. Whence, the total probability
\[
\mathbb{P} = \sum_{N} O(N^{\alpha+\beta+\gamma-1+o(1)})
\]
converges, because $\alpha + \beta + \gamma < 1$. Because there is no reason to expect $\mathbb{P} \ll 1$, we expect only finitely many counterexamples, which is what the $abc$ conjecture claims.

3 Equivalent characterizations

The $abc$ conjecture has several important equivalent statements. A few are easy to see as equivalent, because they are similar in form to [1.4] but nonetheless worth stating. Two equivalent statements are deep number theoretic conjectures in their own right, the Vojta conjecture in dimension one (hyperbolic) and the modified (general) Szpiro conjecture. The conjectures of Vojta and Szpiro are fairly technical, involving non-trivial ideas from modern algebraic number theory such as the conductor of an elliptic curve. It is for this reason that we will not discuss them in detail; we will merely state them for the sake of the interested reader.

Conjecture 3.1. (abc conjecture) Given $\epsilon > 0$ there exists $K_\epsilon$ such that for all coprime positive integers $a, b, c \neq 0$ with $a + b = c$, we have
\[
H(a, b, c) < K_\epsilon \text{rad}(abc)^{1+\epsilon},
\]
where the height is the obvious $H(a, b, c) = \max\{|a|, |b|, |c|\}$.

If you take $q = a/c$ to be a rational number, a point on the projective line $\mathbb{P}^1_{\mathbb{Q}}$, then

$p|a \iff q \equiv 0 \mod p$

$p|b \iff q \equiv 1 \mod p$

$p|c \iff q \equiv \infty \mod p$

This is saying how $q$ approximates the three targets $0, 1, \infty$ in the non-Archimedean sense. With this fact, we get the following characterization of the $abc$ conjecture.

**Conjecture 3.2.** ($abc$) Fix $\epsilon > 0$ and three distinct targets $b_1, b_2, b_3 \in \mathbb{P}^1_{\mathbb{Q}}$. All but finitely many $q \in \mathbb{P}^1_{\mathbb{Q}}$ satisfy

$$(1 - \epsilon)h(q) < \sum_{j=1}^{3} N^{(1)}(b_j, q),$$

where $h(q)$ is the logarithmic height $h(q) = \log(\max\{|a|, |c|\})$ and $N^{(1)}$ is the counting function

$$N^{(1)}(b_j, q) := \sum_{b \equiv q \mod p} \log p,$$

which measures the coincidences of the points $b_j, q$ modulo a prime $p$ for many different $p$ but forgetting multiplicity and adding a weight.

The main reason I mention this version is because it is now quite explicit how this is a geometric conjecture. Note that Möbius transformations allow us to have the distinct targets as arbitrary rather than $0, 1, \infty$ as before. One can also generalize the $abc$ conjecture to number fields in a natural way from this.

Let us state some elementary equivalences now, before ending with the two deep ones.

**Conjecture 3.3.** ($abc$) For every $\epsilon > 0$, there exists a constant $K(\epsilon)$ such that for all $(a, b, c)$ triples of coprime positive integers, with $a + b = c$, the following holds:

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

**Definition 3.4.** The quality $q(a, b, c)$ of a triple $(a, b, c)$ is defined as

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

**Conjecture 3.5.** ($abc$) For all $\epsilon > 0$, there exist only finitely many $(a, b, c)$ of coprime integers with $a + b = c$ such that $q(a, b, c) > 1 + \epsilon$.

The primary reason I mention this is that it Mochizuki deals with an object known as the log-theta lattice in his third paper, where he seems to prove the $abc$ conjecture. There is not an obvious direct link between the log there and the log here, but we can pretend there is.
Those are all the worthwhile equivalent characterizations I know of aside from the two major conjectures we state now.

**Conjecture 3.6.** (Szpiro) For $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that for any elliptic curve $E/\mathbb{Q}$ with minimal discriminant $\delta$ and conductor $f$, the following holds:

$$|\delta| < C(\epsilon)f^{6+\epsilon}.$$  

**Conjecture 3.7.** (modified Szpiro) Given $\epsilon > 0$, there exists $C(\epsilon)$ such that for any elliptic curve $E$ over $\mathbb{Q}$ with invariants $c_4, c_6$ and conductor $f$, we have

$$\max\{|c_4|^3, |c_6|^2\} \leq C(\epsilon)f^{6+\epsilon}.$$  

**Conjecture 3.8.** (Vojta) Let $F$ be a number field, $X/F$ be a non-singular algebraic variety, $D$ be an effective divisor on $X$ with at worst normal crossings, $H$ be an ample divisor on $X$, $K_X$ be the canonical divisor on $X$. Choose Weil height functions $h_H$ and $h_{K_X}$, and for each absolute value $\nu$ on $F$, a local height function $\lambda_{D,\nu}$. Fix a finite set of absolute values $S$ of $F$, and let $\epsilon > 0$. Then, there is a constant $C$ and a non-empty Zariski open set $U \subset X$, depending on all the above choices, such that

$$\sum_{\nu \in S} \lambda_{D,\nu}(P) + h_{K_X}(P) \leq \epsilon h_H(P) + C \text{ for all } P \in U(F).$$

Vojta’s conjecture can actually generalize the $abc$ conjecture to higher dimensions in some sense.

4 A special case: polynomials

The Mason-Stothers theorem in the analog of $abc$ for polynomials. It was proved in 1981.

**Theorem 4.1.** (polynomial $abc$) Let $K$ be an algebraically closed field with $\text{char}(K) = 0$. Let $a, b, c \in K[x]$ be coprime polynomials with

$$a(X) + b(X) = c(X).$$

It follows that

$$h \leq \deg(\text{rad}(abc)) - 1,$$

where $h = \max\{\deg a, \deg b, \deg c\}$.

We will outline a proof of this fact here. The original proofs are fairly technical, including some amount of classical algebraic geometry, but Snyder found an elementary proof in 2000 [7], which is the one presented here. Snyder was a high school student at the time that he started to see this, and he published it as a sophomore mathematics major at Harvard University, where he graduated magna cum laude with highest honors in Mathematics in 2002 under the advisement of Benedict Gross. Snyder then went on to obtain a Ph.D. in mathematics from Berkeley in 2009, writing his thesis Quantum groups, tensor categories, and know invariants, after which he was at Columbia University as an NSF
postdoctoral fellow until 2012. He is now an assistant professor at Indiana University. It seems fair to say he discovered a proof “from the book.” We provide a variant of that proof.

Before moving on, we need to note two things.

**Definition 4.1.** The Wronskian of the functions \(f, g\) is \(W(f, g) := fg' - f'g\).

**Theorem 4.2.** The Mason-Stothers theorem as stated above is the same as taking \(K\) to be any field with the functions \(a, b, c\) not all having vanishing derivative.

**Proof.**

Proof. Note that \(a + b + c = 0\) implies equality of the Wronskians \(W(a, b) = W(b, c) = W(c, a)\). Write \(W\) for that value. By assumption, at least one of the derivatives is nonzero and the functions are coprime. This can be used to show \(W\) is nonzero. If \(W = 0\), then \(ab' = a'b\) so \(a|a'\) (\(a, b\) coprime) and whence \(a' = 0\) (\(\deg a > \deg a'\) except when \(a\) is constant); repeating this gives the fact. The Wronskian is divisible by each of \((a, a'), (b, b'), (c, c')\). Because these are coprime, \(W\) is divisible by the product of the greatest common divisors, and moreover \(W\) has been shown to be non-zero, so we get

\[
\deg(a, a') + \deg(b, b') + \deg(c, c') \leq \deg W.
\]

Substituting in the inequalities, we get

\[
\begin{align*}
\deg(a, a') &\geq \deg a - (\text{number of distinct roots of } a) \\
\deg(b, b') &\geq \deg b - (\text{number of distinct roots of } b) \\
\deg(c, c') &\geq \deg c - (\text{number of distinct roots of } c),
\end{align*}
\]

where roots are taken in an algebraic closure \(\bar{K}/K\). Moreover,

\[
\deg W \leq \deg a + \deg b - 1,
\]

and we conclude

\[
\deg c \leq (\text{number of distinct roots of } abc) - 1,
\]

which proves the theorem. □

The original proof also shows that equality holds exactly when \(b/c\) is a Belyi map, which is a type of special map from a curve \(X\) to \(\mathbb{P}^1\).

5 Incremental bounds

Before 2012, the best theoretical bound I know of is due to Stewart & Yu and involves a constant \(K\) depending only on \(\epsilon\). It can be stated as

\[
c < \exp \left( K(\epsilon) \text{rad}(abc)^{1 + \epsilon} \right).
\]

If one wishes to have an unconditional constant, then the best bound I know is due to Stewart & Tijdeman, which states that

\[
c < \exp \left( K\text{rad}(abc)^{15} \right).
\]
These bounds are *something*, but they are not particularly good in comparison with what we want. Yitang Zhang’s original bound for the twin-prime conjecture at some seventy million was probably better in some sense; certainly, it was more significant, as it was the first bound! Of course, this incremental progress was still worth all the effort, else we would not mention it.

Leiden University hosts a project called ABC@Home, which is based on grid computing, and tries to find \((a, b, c)\) with \(\text{rad}(abc) < c\). The project has found over thirty million triples. To be clear, this could never resolve the infinite number of cases, but it could, in theory, make some patterns clear.

6 Inter-universal Teichmüller Theory

In August 2012, Japanese mathematician Shinichi Mochizuki of Kyoto University – Professor, Research Institute of Mathematical Sciences (RIMS) – announced he had a proof of \(abc\) by posting a set of four papers spanning nearly 600 pages in which he had developed large area of mathematics, which he called “inter-universal Teichmüller theory.” (Many mathematicians today call the work “arithmetic deformation theory” after the suggestion of Fesenko in a review article; also, the initialization “IUT” is now commonplace.) Mochizuki has long been a respected mathematician, but for the past decade or so he has been working on a number of theories of his own, each depending on the previous, which have not been widely studied even by experts in anabelian geometry. Mochizuki completed his Ph.D. studies under Gerd Faltings at Princeton, where he is said to have read all of the works of Grothendieck in his undergraduate years. It was clear early on that he would become a respectable mathematician, and he gained notoriety for his proof of the Grothendieck conjecture. In some ways, this marked the beginning of anabelian geometry becoming a proper field of mathematics.

In 1984, Grothendieck wrote his Esquisse ‘un Programme ("sketch of a program") in which he proposed (among other things) the grand idea of anabelian geometry, but it took some time to develop algebraic geometry and algebraic number theory far enough to attempt to tackle the idea in earnest. To explain what anabelian geometry is, we should first look to the following “chain of inclusions”:

\[
\text{Algebraic Geometry} \supset \text{Arithmetic Geometry} \supset \text{Anabelian Geometry}.
\]

I have quotes above, because classifying mathematics is difficult. Nonetheless, there will do for our purposes. Let us try to define what these are in a somewhat satisfactory manner.

**Definition 6.1.** Algebraic geometry is the study of the geometry of curves and surfaces via algebra. In particular, algebraic geometry studies the zero set of polynomials (possibly in \(n\) variables). The main object of study is known as a *variety*, which has since been abstracted in many ways through the use of category theory, homological algebra, and more, largely due to Grothendieck and others in the early French school, to schemes, motives, and so forth.
Algebraic geometry has somewhat of a reputation among mathematicians and laypeople alike. It is seen as very difficult, esoteric, and abstract, which is not entirely unfair. The subject has also come to dominate mathematics since it was placed in its modern setting during the 1960s. Many problems in number theory find use for algebra and geometry, so we might expect that algebraic geometry might come up as well. Indeed, this is the case.

**Definition 6.2.** Arithmetic geometry, or arithmetic algebraic geometry, is the field of study that applies algebraic geometry to number theory.

While far from the majority of research is algebraic geometry or arithmetic geometry, the subjects do still seem to be gaining in popularity. Some departments might even be over-saturated with experts in these areas. Certainly, grand programs such as Langlands, great mathematicians such as Deligne, and wonderful problems such as the abc conjecture have contributed to the fame of this area.

Anabelian geometry is substantially more difficult to describe. We will make two prerequisite definitions before we even try. Some of this may be unintelligible to a general audience, but hopefully it is of some value to the majority of readers.

**Definition 6.3.** If \( k \) is an algebraically closed field and \( \mathbb{A}^n_k \) is affine \( n \)-space over \( k \), then we can consider the zero-locus \( Z(S) \) of a set \( S \) of polynomials \( f \in k[x_1, \ldots, x_n] \)

\[
Z(S) := \{ x \in \mathbb{A}^n_k : f(x) = 0 \text{ for all } f \in S \}.
\]

Any subset \( V \subset \mathbb{A}^n_k \) is an affine algebraic set if \( V = Z(S) \) for some \( S \), and if that set is nonempty and irreducible (not expressible as the union of two proper algebraic subsets), then it is called an affine variety.

**Definition 6.4.** The fundamental group is a group (a set with an operation that is associative, with identity, and with inverses) associated to any topological space (a space with a well defined notion of continuity) that gives a way to determine when two paths can be continuous deformed into each other. The \( \acute{E} \)tale fundamental group is an analogue in algebraic geometry, for schemes, of this idea.

**Definition 6.5.** Anabelian geometry attempts to describe the way the algebra (\( \acute{E} \)tale) fundamental group \( G \) of an algebraic variety \( V \), or some other geometry object, determines how \( V \) can be mapped into another geometry object \( W \), where \( G \) is highly non-commutative.

Anabelian geometry is, in some sense, a generalization of an area of mathematics known as class field theory.

**Definition 6.6.** Class field theory deals with abelian quotients of Galois groups and abelian extensions of local and global fields (starting with the Kronecker-Weber theorem).

**Theorem 6.1.** (Kronecker-Weber) Every finite abelian extension of \( \mathbb{Q} \) lies in a cyclotomic field \( \mathbb{Q}(\zeta_m) \) for some \( m \).
Another generalization of class field theory is Langlands program.

**Definition 6.7.** Langlands correspondences and related matters in algebraic number theory deals with Galois group representations.

By comparison, we might remark the following about anabelian geometry.

**Theorem 6.2.** Anabelian geometry treats the entire absolute Galois group, thus generalizing class field theory.

An interesting viewpoint is that class field theory and all its generalizations are just analogies of reciprocity laws in elementary arithmetic! Even such conjectures as those of BSD and Riemann can be found to be related to these laws.

Anyway, let us briefly discuss what has happened with IUT and where we are now. Not long after Mochizuki posted his proof, an error was found, somewhat reminiscent of what happened to Wiles and FLT; however, this was quickly resolved, even if the error discouraged some people from pursuing the work. Most expected Mochizuki to be going around giving lectures and workshops on the papers, as is usually done, but he did not do this, very much unlike Wiles. This slowed progress significantly, as did the fact that Mochizuki’s writing could be clearer in many ways. He often uses fantastical analogies and so forth in surveys, which can be very difficult to grasp for people struggling to grasp the basic technical details, but which are often quite nice to look back on after one has a better idea of what is going on. There was a tremendous amount of chatter on blogs and coverage in the media, but relatively few mathematicians gave Mochizuki’s work a serious go, due in no small part to the fact that the vast majority of mathematicians do not specialize in a near enough field to go anywhere near IUT after, say, only a few weeks.

There was a Polymath project, which collected some good resources and so forth. (One of the citations is actually a blog post of mine, which gained some traction for this reason. Amusingly, a fifteen year old’s rapidly written Quora post was put alongside the serious work of world-class mathematicians.) Ivan Fesenko wrote a survey article, Go Yamashita wrote a Q&A, and Shinichi Mochizuki himself wrote a review piece, all of which helped the few mathematicians interested. As time went on, mention of IUT became more and more sparse. I was fascinated from the very beginning, so it was interesting to see the occasional spikes in activity surrounding the work, e.g., when Minhyong Kim began posting questions on Math Overflow in 2013 and encouraging others to seriously consider the papers. Thankfully, Mochizuki has, even if slowly, gotten better at interacting with the community at large. In particular, Mochizuki gave video lectures at a conference at Oxford in 2015 organized by Brian Conrad et al., which was successful, albeit not massively so. Mochizuki also gave in person lectures at a more recent workshop in Japan earlier this year. This workshop was actually quite successful. A third conference was held at Vermont just over one month ago, which was for non-experts and covered anabelian geometry more broadly, and which was organized in part by Taylor Dupuy, one of the younger...
mathematicians who has taken a serious interest in IUT. This workshop seems to have accomplished what it set out to, as I learned via personal communication with three participants.

There are still many problems facing us. Mochizuki still refuses to leave Japan to lecture. The papers still span a lot of space. Most people still need to catch up on Mochizuki’s earlier works. There is much to do.

7 What is to come

The interesting question is where this will go. I can only conjecture as to the answer to this question, but I think it worthwhile. I suspect that Mochizuki will continue to slowly become more reasonable, giving lectures in the U.S. and other nations, for instance. I also suspect more people will become seriously involved as Mochizuki starts to participate and a decent number of mathematicians feel confident with the key aspects of the theory. Ultimately, I predict the research pool will go from something like twenty-five serious individuals to closer to one hundred fifty, and I expect the proof will be deemed correct, perhaps with modification, in two to four years. What consequences Mochizuki’s work will have on math as a whole or number theory in particular is hard to say. From what I understand, I think there could be some very interesting projects coming from IUT, including one involving a good bit of mathematical logic.

8 Further reading

If you find questions of Diophantine geometry related to the $abc$ conjecture and beyond as fascinating as I do, a good elementary reference is [9], which assumes fairly minimal algebraic geometry and number theory background. Those with more background might find [10], [11], or even [12] or [13] helpful as well. Be sure to check the prerequisites of these texts and others, which might include anything from basic abstract algebra to some fairly modern algebraic geometry and algebraic number theory, depending on how in depth and rigorous the book wants to be.

Frankly, a ridiculous amount of background is needed to study anabelian geometry, especially Mochizuki’s theory. Putting aside the standard graduate courses, one will want an excellent background in standard algebraic geometry (e.g., Vakil’s notes or Hartshorne or EGA & SGA as a foundation) as well as algebraic number theory, one will want to know a fair bit about Hodge theory and Teichmüller theory as well, and one should have studied Hodge-Arakelov theory at some point. Only after that is one is fairly well off to begin studying Mochizuki’s early papers on this framework, but even then, it might be to one’s benefit to know more. Granted, it is possible to learn a great deal about IUT without less background than this, indeed much less. For example, I do not have all the background needed to be an ideal student of the theory, and I at least know some non-trivial amount of it. None of the individuals best versed
in arithmetic deformation theory seem to quite have that background, either, though some come amazingly close.

References


[14] Joseph Heavner, “An overview of Inter-universal Teichmüller Theory and Shinichi Mochizuki’s proof of the ABC Conjecture, along with the current situation and how we can begin to understand this theory” *Joseph Heavner’s Posts*, 2013.