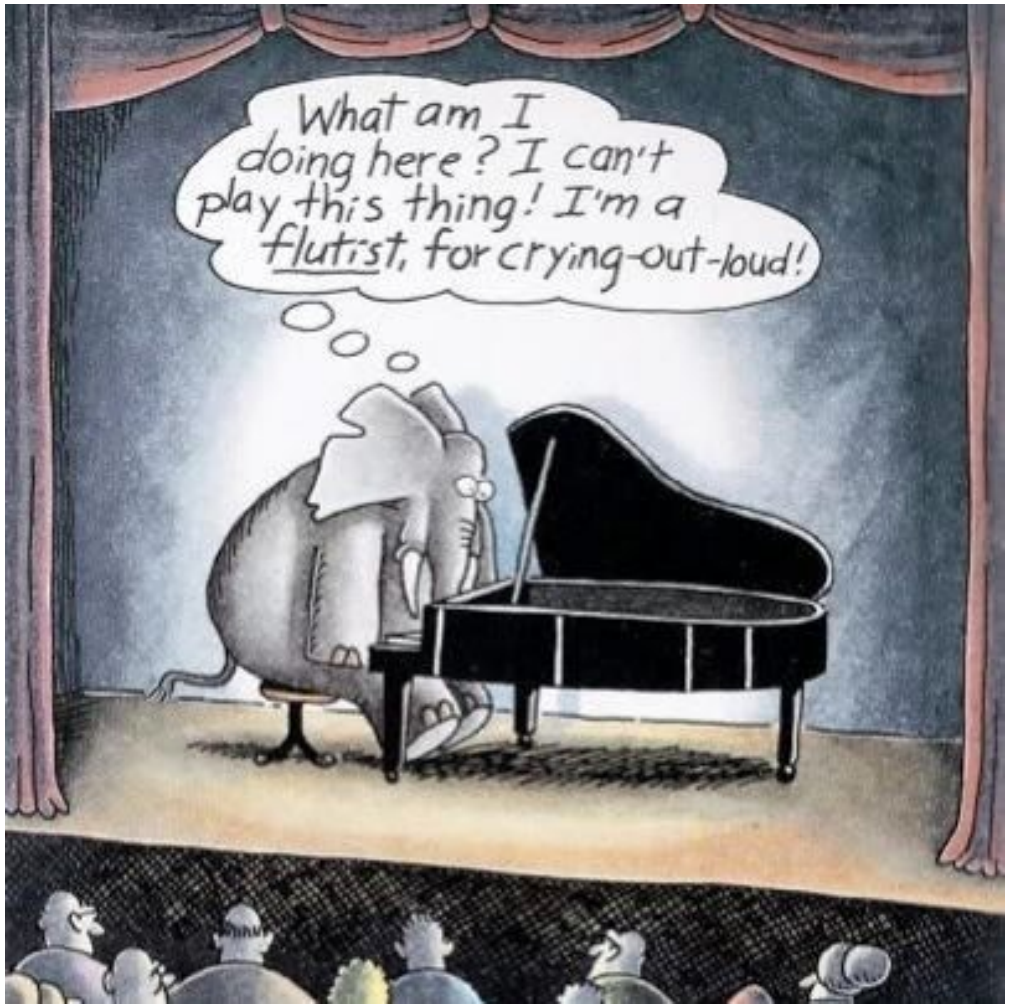
Why the ABC conjecture

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

Kummer classes and anabelian geometry
U. Vermont, September 10–11, 2016



(The Farside, Gary Larson)

What is the ABC conjecture?

Qualitatively it says that if a, b, c are positive integers with $a + b = c$, then the product of the primes in abc cannot be much smaller than c.

To make this more precise, define

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

So, rad(10) = 10, rad(72) = 6, and rad(2401) = 7, for example.

The ABC conjecture is saying that when $a + b = c$, rad(abc) cannot be too small in comparison to c.

But wait, there are counterexamples!

For example, $32 + 32 = 64$, and $\mathrm{rad}(32 \cdot 32 \cdot 64) = 2$. Even more with $2^k + 2^k = 2^{k+1}$.

There are more complicated counterexamples, such as

$$17^4 + 34^4 = 17^5.$$

So, to bar these monsters, we insist that a, b, c be pairwise coprime.

But wait, there are still counterexamples!

Take $1 + 8 = 9$. We have $\text{rad}(1 \cdot 8 \cdot 9) = 6$. And 6 is considerably smaller than 9.

Or take $2 + 3^{10} \cdot 109 = 23^5$, where $2 \cdot 3 \cdot 109 \cdot 23 = 15042$ and $23^5 = 6436343$.

Well, it's in how you measure, and it's in how you treat counterexamples.

Here's the official statement.

The ABC conjecture: *For each $\epsilon > 0$, there are at most finitely many coprime triples a, b, c of positive integers with $a + b = c$ and* $\text{rad}(abc) < c^{1-\epsilon}$.

The conjecture is due to Masser and Oesterlé.

Where did the ABC conjecture come from?

In efforts to prove Fermat's Last Theorem, people wondered if it could be proved in other contexts, such as for polynomials. This was done by Liouville (1851) over $\mathbf{C}$, and then Mason (1983) found the following generalization.

Mason's theorem: *If f, g, h are coprime nonzero polynomials over a field of characteristic* 0 *with $f + g = h$ and* $\deg h > 0$, *then* $\deg \operatorname{rad}(fgh) \geq \max\{\deg f, \deg g, \deg h\} + 1$.

(By $\operatorname{rad}(F)$ we mean the product of the monic irreducible divisors of F.)

Proof: Assume $f + g = h$ with $\deg h$ the maximum of the 3 degrees. Note that for a nonzero polynomial F we have $F/(F, F')$ squarefree, so it divides $\mathrm{rad}(F)$. Hence

$$\deg F - \deg \mathrm{rad}(F) \leq \deg(F, F').$$

From $f + g = h$ we get $f' + g' = h'$, so with some high school algebra:

$$fg' - f'g = g'h - gh'.$$

But $(f, f'), (g, g'), (h, h')$ all divide the two sides of this equation, and they are coprime, so their product divides. Further, the two sides may be assumed nonzero, else g is a constant multiple of h, violating coprimeness. Hence

$$\begin{aligned}\deg f + \deg g + \deg h - \deg \mathrm{rad}(fgh) &\leq \deg(f, f') + \deg(g, g') + \deg(h, h') \\ &\leq \deg(fg' - f'g) \leq \deg f + \deg g - 1\end{aligned}$$

and we're done.

Why is the ABC conjecture "true"?

Let's start with an easier question: Why is Fermat's last theorem true?

Here is an argument due to Erdős and Ulam: Let $k \geq 4$ be an integer and consider a random sequence of positive integers such that the mth term is $\approx m^k$. So, the chance a number n is in the sequence is about $n^{-1+1/k}$. What is the chance that a random number n is the sum of two terms of the sequence? This should be at most about

$$\sum_{a+b=n} a^{-1+1/k} b^{-1+1/k}.$$

Assuming $a \leq b$, we have $b^{-1+1/k} \leq (n/2)^{-1+1/k}$, so the sum is

$$\leq c_0 n^{-1+1/k} \sum_{a \leq n/2} a^{-1+1/k} \leq c_1 n^{-1+1/k} n^{1/k} = c_1 n^{-1+2/k}.$$

Good, and the event that n is a sum of two sequence terms should be independent from n being in the sequence. So, the probability that $a + b = n$ has a solution in sequence terms is $\leq c_2 n^{-2+3/k}$.

But,

$$\sum_{n=1}^{\infty} c_2 n^{-2+3/k} < \infty$$

since $k \geq 4$. Thus, we expect at most finitely many solutions, and if there are no small ones, then no solutions.

Now apply this to the decidedly non-random sequence which is the union of all powers of integers higher than the 3rd power.

The heuristic suggests that

$$a^u + b^v = c^w, \text{ with } u, v, w \geq 4$$

has at most finitely many solutions.

But recall: $2^k + 2^k = 2^{k+1}$, and
$(2^k + 1)^k + (2(2^k + 1))^k = (2^k + 1)^{k+1}$, etc.

So, being a power has some correlations, like the product of two kth powers is again a kth power. Let's assume coprimeness, and maybe we're happy with the heuristic?

One other caution: The heuristic actually suggests that there are infinitely many coprime solutions to $x^3 + y^3 = z^3$.

By the way, Darmon and Granville proved (using Faltings' theorem) that for any triple u, v, w with reciprocal sum ≤ 1, there are at most finitely many coprime solutions to $a^u + b^v = c^w$.

OK, that was a warm-up. **Why is the ABC conjecture "true"?**

We begin with a lemma: *For each fixed $\delta > 0$ and x sufficiently large, the number of integers $n \le x$ with* $\mathrm{rad}(n) \le y$ *is* $\le yx^{\delta}$.

Let i, j, k run over positive integers with $i + j + k \le (1 - \epsilon) \log x$. For each i, j, k consider $a, b \le x$ and $\frac{1}{2}x < c \le x$ with

$$\mathrm{rad}(a) \le e^i, \quad \mathrm{rad}(b) \le e^j, \quad \mathrm{rad}(c) \le e^k.$$

Then $\mathrm{rad}(abc) \le e^{i+j+k} \le x^{1-\epsilon} < 2c^{1-\epsilon}$. By the lemma, the number of choices for a is $\le e^i x^{\delta}$, and similarly for b and c. So, the number of triples a, b, c is $\le e^{i+j+k} x^{3\delta} \le x^{1-\epsilon+3\delta} = x^{1-\frac{1}{2}\epsilon}$, assuming that $\delta = \frac{1}{6}\epsilon$. So the total # of triples: $\le x^{1-\frac{1}{2}\epsilon} \log^3 x$.

Given a, b, the chance that a random $c \in (\frac{1}{2}x, x]$ happens to be $a + b$ is proportional to $1/x$, so letting a, b run, the chance we have an a, b, c triple is at most about $x^{-\frac{1}{2}\epsilon} \log^3 x$. Now let x run over powers of 2, and we get a convergent series.

Why is the ABC conjecture important?

It has tons of interesting consequences. For example:

1. Fermat's last theorem has at most finitely many counterexamples.

2. Pillai's conjecture holds: the gaps between perfect powers tend to infinity.

3. There are at most finitely many coprime powers a^u, b^v, c^w with $1/u + 1/v + 1/w \leq 1$ and $a^u + b^v = c^w$.

4. (Silverman) There are infinitely many non-Wieferich primes.

5. (Granville) For a squarefree polynomial $f \in \mathbf{Z}[x]$, and with B the gcd of the values $f(n)$, then there is a positive density of n's with $f(n)\mathrm{rad}(B)/B$ squarefree.

6. Szpiro's conjecture on the conductors of elliptic curves.

7. The Erdős–Woods conjecture: If x is large and $\mathrm{rad}(x) = \mathrm{rad}(y)$, then $\mathrm{rad}(x+1) \neq \mathrm{rad}(y+1)$.

8. (Granville–Stark) There are no Siegel zeros (following from a uniform ABC conjecture for number fields).

9. Erdős's conjecture that there are at most finitely many triples of consecutive squarefull numbers (n is squarefull if $p^2 \mid n$ whenever $p \mid n$).

10. Dressler's conjecture that if $m < n$ and $\mathrm{rad}(m) = \mathrm{rad}(n)$, then there is a prime in $[m, n]$.

11. Lang's conjecture on the number of integral points on an elliptic curve.

12. Bounds for the order of the Tate–Shafarevich group of an elliptic curve.

13. Vojta's conjecture for curves.

14. The Schinzel–Tijdeman conjecture: If $f(x) \in \mathbf{Z}[x]$ has at least 3 simple roots, then $f(n)$ is squarefull at most finitely many times.

15. (M. R. Murty) There are many quadratic number fields with class number divisible by a fixed integer.

I like to joke that it has been shown that everything can be proved starting from a false statement, so perhaps the ABC conjecture is more and more resembling one!

What has been proved?

One type of result produces triples a, b, c with $a + b = c$ and $\mathrm{rad}(abc)$ is fairly small. For example,

$$a = 1, \quad b = 64^n - 1, \quad c = 64^n.$$

Then $\mathrm{rad}(abc) \leq \frac{2}{3}(64^n - 1) < \frac{2}{3}c$. By this method, there are infinitely many coprime triples $a + b = c$ with

$$\mathrm{rad}(abc) = O(c/\log c).$$

van Frankenhuijsen has shown there are infinitely many coprime triples $a + b = c$ with

$$\mathrm{rad}(abc) \leq c/\exp\Big(6.068(\log c)^{1/2}/\log\log c\Big).$$

(Robert, Stewart, and Tenenbaum have a heuristic that this is close to best possible.)

Another type of result proves a weaker version of the ABC conjecture.

For example, Stewart and Yu have proved that there is some $\kappa > 0$ such that for coprime $a + b = c$,

$$\mathrm{rad}(abc) \geq \kappa(\log c / \log\log c)^3.$$

Baker has a numerically explicit ABC conjecture: If $a + b = c$ are coprime, then

$c \leq \frac{6}{5} R \frac{(\log R)^k}{k!}$, where $R = \mathrm{rad}(abc)$ has k distinct prime divisors.

An ABCD conjecture?

The same heuristics suggest that if $a+b+c+d=0$ where a,b,c,d is a coprime 4-tuple of nonzero integers, then $\mathrm{rad}(abcd) > |d|^{1-\epsilon}$. But consider the polynomial identity

$$(x-1)^5 + 10(x^2+1)^2 - 8 = (x+1)^5,$$

and let x run over numbers of the form $11^k - 1$. This gives

$$(11^k-2)^5 + 10((11^k-1)^2+1)^2 - 8 = 11^{5k},$$

and $\mathrm{rad}(abcd) \le 22(11^k-2)((11^k-1)^2+1) = O(|d|^{0.6})$. Granville has conjectured that infinite-family counterexamples must come from polynomial identities such as this, and that for fixed $\epsilon > 0$, there are only finitely many polynomials.

Thank you!

Further resources:

A. Granville and T. Tucker, *It's as easy as abc*, Notices AMS **49** (2002), 1223–1231; www.ams.org/notices/200210/fea-granville.pdf

A. Nitaj, *The abc home page*, http://www.math.unicaen.fr/∼nitaj/abc.html

C. Pomerance, *Computational number theory*, Princeton Companion to Math., T. Gowers, ed., Princeton U. Press 2008, pp. 348–362.

M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences*, https://webusers.imj-prg.fr/∼michel.waldschmidt/articles/pdf/abcLahore032013.pdf