THE ABC Conjecture

Mark Saul, Ph.D.
Center for Mathematical Talent
Courant Institute of Mathematical Sciences
New York University

I

The abc conjecture was formulated independently by Joseph Oesterle and David Masser in 1985. It concerns integer solutions to the very simple equation $a + b = c$ (hence the name). In the summer of 2012 Shinichi Mochizuki, a noted Japanese mathematician, released a series of four papers in which he may have succeeded–by very advanced methods–in proving this conjecture. As of this writing, the proof is being checked by the handful of mathematicians around the world with expertise in this field.

Inspirational note: Mochizuki graduated from Phillips Exeter Academy in New Hampshire after only two years of attendance. He then entered Princeton University as an undergraduate at age 16 and received a Ph.D. at age 23. He is now a professor at the University of Kyoto. You can view his personal website (including a mpg file demonstrating how to pronounce his name!) at:

http://www.kurims.kyoto-u.ac.jp/ motizuki/top-english.html.

What does the abc conjecture say?

Let us look at the numbers with prime factors only of 2 or 3. The first few are:

1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, ...

Notice how these numbers 'thin out' pretty quickly. Yet we can find plenty of triples of numbers (a, b, c) such that a+b = c.

Problem 1. Show that if a, b, and c have prime factors only of 2 or 3, and if $1 < a < b < c$, then these three numbers cannot be pairwise prime. Can they be relatively prime, as a triple of numbers?

Now let us look at those numbers which have prime factors of 2, 3, or 5. The first few are:

1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32, 36, 40, 45, ...

These don't thin out so quickly. But they do thin out. Certainly there are more of them between 1 and 10 than there are, say, between 30 and 40. And if we were to continue listing these numbers, the list would get thinner and thinner. The abc conjecture describes this thinning out in a very precise way.

As a measure of this thinning, we can look at two of these numbers that add up to a third. The more the numbers bunch up, the more reasonable it is to expect that you find three of them, a, b, and c, such that a+b = c.

This is not quite true. We have the following infinite sequence of a, b, c for which a + b = c:

$$9 + 3 = 12$$
$$27 + 9 = 36$$
$$81 + 27 = 108$$
$$243 + 81 = 324$$

Problem 2. Write the general form of all the numbers above.

We want to eliminate these 'easy' infinite sequences of triples. We can do this by requiring that the numbers $\{a,\ b,\ c\}$ be relatively prime.

Problem 3. Suppose that we didn't require $a,\ b$, and c to be relatively prime. Show that if we have even one triple such that $a + b = c$, then we have infinitely many of them.

This is one way to think about the abc conjecture. Another way to think of it is the following assertion: if the three relatively prime numbers $a,\ b,\ c$ are products of small primes, then $a + b$ can not be equal to c very often.

A third way is: If $a + b = c$, then the primes that divide any one of $a,\ b$, and c cannot all be small.

(We are working our way towards an exact statement of the famous conjecture.)

Yet another way to think about it: If $a + b = c$ and these positive numbers are all products of small primes, then c is bounded (and therefore a and b are bounded).

But a formal statement of the conjecture requires a bit more.

Definition: For any number n, rad (n) is the product of one copy of each prime that divides n.

So, for example rad (3) = 3; rad $(3k) = 3k$ if 3 does not divide k; rad (500) = rad $(5^3 \cdot 2^2)$ = rad $(5 \cdot 2) = 10$, etc.

Problem 4. Find

a) rad (72)
b) rad (27)
c) rad (100)
d) rad (p^3), where p is prime
e) rad(p^2q^3), where p and q are prime.

Problem 5. For each number below, tell whether or not it could be a value of rad (n), for some integer n.

(a) 23
(b) 27
(c) 35
(d) 30
(e) 42
(f) 72
(g) 100

(h) 101
(i) 111

Problem 6. Can you characterize the possible values of rad (n)? For a hint, try 'simplyifying,' wherever possible, the following radicals:
(j) $\sqrt{8}$
(k) $\sqrt{10}$
(l) $\sqrt{12}$
(m) $\sqrt{242}$
When can a radical be simplified? When is it already in simplest form?
Problem 7. Show that for any integer a, we have rad $(a) \leq a$.
Problem 8. True or false: If $a < b$ then rad(a) <rad(b)?
Problem 9. Show that for any integers $a,\ n$, we have rad(a^n) = rad (a).
Problem 10. Show that for any integers $a,\ b,\ c,\ m,\ n,\ p$, we have rad $(a^n b^m c^p)$ = rad (abc).
Problem 11. Show that if $a < c,\ b < c$, then rad $(abc) < c^3$.
Problem 12. Show that the function rad (x) is *multiplicative*. That is, show that if a and b are relatively prime, then rad(ab) = rad(a) rad(b). Is the converse of this statement true?

Mathematicians invented rad(abc) because it is, in some sense, a measure of all the primes that divide a or b or c. If all are products of 2 or 3, then rad $(abc) = 2 \cdot 3 = 6$. If all the numbers are products of 2, 3, or 5, then rad$(abc) = 2 \cdot 3 \cdot 5 = 30$.

The abc conjecture, formally is about a bound on c. Given this idea, a first guess might be that c$\leq$ rad (abc). But this guess is wrong.

Problem 13. Show that $a = 243,\ b = 225$ is a counter example to the statement above.

We can even construct infinitely many counter-examples in which rad(abc) is not bounded by c. That is, we can find an infinite sequence of relatively prime triples $(a,\ b,\ c$ such that $a + b = c$ and $c \leq$rad(abc).

To do this, we let $a = 1$. Then we let $c = 3,\ 3^2,\ 3^4,\ 3^8, \ldots 3^{(2^n)}$. We can show that each value of c generates a counter-example. To complete our triple, we must have $b = 3 - 1,\ 3^2 - 1\, 3^(2^2) - 1, \ldots 3^{(2^n)} - 1$ (so that $a + b = c$).

That is, we consider the triple $(a, b, c) = (1,\ 3^{(2^n)} - 1,\ 3^{(2^n)})$, for any positive integer n. What is rad(abc)? Well, a doesn't contribute anything, and c contributes only a factor of 3. (See problem 9). So we must look at the prime factors of b. One of them is certainly 2, and we don't care how many 2's there are. There of course may be other factors in b.

Determining the other factors of b may not be easy. But we don't need their numerical value. All we need to show is that $c \leq$rad(abc) =rad$(3b)$ = 3rad(b) (by problem 12). So let us try to determine a relationship between c and rad(b).

Problem 14. Simplify the product

$$(x + 1)(x^2 + 1)(x^4 + 1)(x^8 + 1) \ldots (x^{64} + 1).$$

Hint: what happens if you multiply by $(x - 1)$?

Problem 15. Show that $3^{128} - 1$ is divisible by $2 \cdot 2^9$.

Problem 16. More generally, show that 2^{n+2} always divides $3^{2n} - 1$.

Problem 16 shows that the number c in our triple $(a,\ b,\ c)$ is always a multiple of 2^{n+2}. We use this to relate $\text{rad}(b)$ to c. In computing $\text{rad}(b)$, we can ignore all but one of the factors of 2. That is,

$$\text{rad}(b) = \text{rad}(3^{2^k} - 1) = 2 \cdot \text{rad}\left(\frac{3^{2^n} - 1}{2^{n+2}}\right),$$

where we've divided out all the factors of 2 from b, then multiplied by a single 2. Further, we have:

$$\frac{3^{2^n} - 1}{2^{n+2}} < \frac{3^{2^n}}{2^{n+2}} < \frac{3^{2^n} - 1}{2^{n+1}} = \frac{c}{2^{n+1}}.$$

(We just keep making the numerator of the fraction larger, and the denominator smaller.) Thus

$$\text{rad}(b) < \frac{c}{2^{n+1}}$$

and

$$\text{rad}(abc) = 3 \cdot \text{rad}(b) < \frac{3c}{2^{n+1}}.$$

Turning this 'backwards', we find that $c >$rad $(abc) \cdot \frac{2^{n+1}}{3}$. So for any $n \geq 1$, the triple $(1,\ 3^{(2^n)} - 1,\ 3^{(2^n)})$ shows that the notion that c is bounded by $\text{rad}(abc)$ is definitely false. It has infinitely many counter-examples.

Problem 17. Show that this argument actually 'comes true', by computing $\text{rad}(abc)$ for $n = 1$ and $n = 2$.

In fact, we've done a bit more damage to the simple notion of bounding c. The number $\frac{2^{n+1}}{3}$ increases without bound as n increases. So even if we thought that we could bound c by some fixed multiple M of $\text{rad}(abc)$, we would be wrong. Just take n large enough so that $\frac{2^{n+1}}{3} > M$ and our hopes are dashed.

We cannot bound c simply by $\text{rad}(abc)$. But maybe we can bound c by $(\text{rad}(abc))^2$. In fact, as of this writing we don't know if this is possible.

But let's pretend that it is not possible. Let us assume, just for now, that if we have three relatively prime integers $a,\ b,\ c$ such that $a+b = c$, then $c < (\text{rad}(abc))^2$.

Given this assumption, we can already show a connection with Fermat's Last Theorem!

Problem 18. Show that if our assumption were true, then Fermat's Last Theorem holds for $n \geq 6$. That is, suppose $x,\ y,\ z$ are relatively prime positive integers such that $x^n + y^n = z^n$ for some positive integer $n \geq 3$. Letting $a = x^n,\ b = y^n, c = z^n$ in our assumption, show that n must be smaller than 6.

Yet another way to think about the abc conjecture is that it 'salvages' this whole situation. It gives us a way to bound c by a combination of a multiple of

rad(abc) and a power of rad(abc).

Formal Statement of the abc conjecture. Take any positive number ϵ. Then there is some number $k = k(\epsilon)$ such that if $a + b = c$, (where $a,\ b,\ c$ are relatively prime), then $c \leq k \cdot \text{rad}(abc)^{1+\epsilon}$.

So the numbers can't be too big, and how big depends on how big the primes are that divide them, as measured by rad(abc).

We can test this formal statement against our earlier formulations: If $a+b=c$, then rad (abc) measures the size of the primes dividing $a,\ b$, and c. And if we fix the value of rad(abc), the number c is bounded.

We can now prove Fermat's Last Theorem(!) assuming the truth of the abc conjecture. Actually, we'll prove a variant of Fermat's Last Theorem (FLT, for short), called the 'asymptotic form' of FLT:

FLT, as original stated, says that there are no positive integers $x,\ y,\ z$, such that for some positive integer $n \geq 3$ we will have $x^n + y^n = z^n$.

Problem 19. If the relationship in FLT holds for some $x,\ y,\ z,\ n$, show that $z > 3$.

The asymptotic form of FLT says: There is a number N_0 such that FLT is true for $n > N_0$.

Problem 20. The asymptotic version of FLT says that if there is a counter-example to the theorem, then it must occur for a value of n smaller than the given bound. Joe Blogg thinks that this means that we can perform a computer check to get the usual statement of Fermat's Last Theorem. That is, he thinks that once we establish an upper bound on n, we can just check, using a computer, that there are no solutions to $x^n + y^n = z^n$, where n is smaller than that upper bound. Is Joe Blogg correct?

Here's how the asymptotic form of FLT follows from the abc conjecture.

Clearly, we should at least try letting $a = x^n,\ b = y^n,\ c = z^n$. And in fact this works.

We also need a number ϵ. Again this is easy: we let $\epsilon = 1$.

The abc conjecture then states that there is some constant $k = k(1)$, such that if $a + b = c$, then $c < k \cdot \text{rad}(abc)^2$.

Problem 21. Where did the exponent '2' come from?

Now let $x,\ y,\ z,\ n$ be positive integers such that $x^n + y^n = z^n$.

Then (problem 10) rad $(x^n y^n z^n)$ = rad (xyz). And (problem 7) rad$(xyz) \leq xyz$. Now certainly $z > x$ and $z > y$, so from problem10, we have rad $(xyz) < z^3$.

Now we (carefully!) harness the abc-conjecture. We have:

$$z^n < k \cdot \text{rad}(x^n y^n z^n)^2 < k(z^3)^2 = kz^6.$$

Now z is bigger than 3 (problem 19), so this inequality bounds n. Some simple algebra will make this specific:

$$\begin{aligned} z^{n-6} &< k; \\ 3^{n-6} < z^{n-6} &\leq k; \\ (n-6) \cdot \log 3 &< \log k; \\ n &< \frac{\log k}{\log 3} + 6. \end{aligned}$$

That is: if the abc conjecture is true, then there can be no counter-examples to FLT (no triples $x,\ y,\ z$ such that $x^n + y^n = z^n$) for n greater than a certain fixed number.

So if we know that the abc conjecture is true, we also know that the asymptotic form of FLT is true. It has been shown that the asymptotic form of FLT implies the original form of the theorem–the one Fermat wrote in the margin of his book.

The Catalan Conjecture

This conjecture was actually proven about 10 years ago, before the recent activity with the abc conjecture. It starts with the observation that $9 - 8 = 3^2 - 2^3 = 1$. The Catalan conjecture says roughly that this won't ever happen again: two powers of natural numbers will never differ by 1.

Definition. The set of powers (of natural numbers) is the set $\{x^n\}$, for natural numbers x and $n \geq 2$.

The Catalan conjecture says that 8 and 9 are the ONLY consecutive integers in the set of powers.

We will prove the 'asymptotic' Catalan conjecture:

There exists some number N_0 such that for $m,\ n > N_0$ the Catalan conjecture holds.

(That is, there can exist only finitely many pairs of consecutive powers. After a certain point, there are none at all.)

To show how the abc conjecture implies the Catalan conjecture, we need two interesting theorems that have been known for a while. While their proofs are elementary (in the sense of not using high-powered mathematical tools), we will not give them here.

Theorem I. The only solution of the diophantine equation $x^2 - y^3 = 1$, with $x,\ y > 1$, is $x = 3,\ y = 2$. In fact, the Diophantine equation $x^2 - y^n = 1$, for $n \geq 3$ has only one solution: x = 3, y=2, n = 3.

So the only square which is one more than a power is 9.

Theorem II. The diophantine equation $x^m - y^2 = 1$ has no solutions in integers.

So there is no square that is 1 less than a power (of an integer). Taken together, these two theorems tell us that if we're looking for solutions of the Catalan equation other than 9 and 8, both m and n have to be greater than 3.

So here's the proof of the asymptotic Catalan conjecture, assuming the truth of the abc conjecture:

Suppose there are natural numbers $x,\ y,\ m,\ n$ such that $x^m - y^n = 1$ and $m,\ n \geq 3$.

Problem 22. Show that if there are natural numbers $x,\ y,\ m,\ n$ such that $x^m - y^n = 1$, then x and y must be relatively prime.

Problem 23. Show that (in the same situation) both x and y must be greater than or equal to 2.

How are we going to 'fit' this situation into the abc conjecture? It's not so obvious as in the case of FLT. But we can write $x^m - y^n = 1$ in the form $1 + y^n = x^m$, then let $a = 1,\ b = y^n,\ c = x^m$, and we have an equation of the form treated by the abc conjecture.

In the statement of the conjecture, we take $\epsilon = \frac{1}{4}$. (We'll discuss this choice of ϵ later on.) Then the abc conjecture says that there is a number k (which depends on ϵ) such that if $1 + y^n = x^m$, then $x^m \leq k \cdot \operatorname{rad}(1 \cdot x \cdot y)^{\frac{5}{4}}$.

Again, it's all algebra from hereon in. We have:

$$x^m \leq k \cdot \operatorname{rad}(xy)^{\frac{5}{4}}.$$

By problem 7, we then have:

$$x^m \leq k \cdot (xy)^{\frac{5}{4}};$$
$$m \log x \leq \log k + \frac{5}{4}(\log x + \log y).$$

Now certainly $y^n < x^m$, so $n \log y < m \log x$ and we also have

$$n \log y < \log k + \frac{5}{4}(\log x + \log y).$$

We add these two inequalities:

$$m \log x + n \log y < 2 \log k + \frac{5}{2}(\log x + \log y).$$

(Note that $\leq$ is replaced by $<$, since y^n is strictly less that x^m.)

Problem 24. Show that this last equation is equivalent to $(m - \frac{5}{2}) \log x + (n - \frac{5}{2}) \log y \leq 2 \log k$.

Now (problem 23) $x,\ y \geq 2$, so $\log x,\ \log y \geq \log 2$, and we have

$$(m - \frac{5}{2}) \log 2 + (n - \frac{5}{2}) \log 2 \leq (m - \frac{5}{2}) \log x + (n - \frac{5}{2}) \log y \leq 2 \log k,$$

or

$$(m + n - 5) \log 2 \leq 2 \log k,$$

and finally:

$$m + n \leq \frac{2 \log k}{\log 2} + 5.$$

This bounds the numbers m and n. That is, neither m nor n can be larger than the number on the right side of this inequality, so if we take N_0 to be an integer slightly greater than $\frac{2 \log k}{\log 2} + 5$, then $x^m y^n$ can never equal 1 for $m,\ n$ larger than N_0.

Problem 25. There is a logical gap in the argument above. Can you find it before continuing on? (We'll give the answer a bit later).

Extensions of the Catalan Conjecture.

We can ask if the equation $x^m - y^n = 3$ has solutions in integers, or replace 3 by some other number. It has been proven that if you line up all the integers which are powers of other integers, the differences of adjacent terms in this sequence approaches infinity. So for any such equation, there are at most finitely many solutions in integers.

But many questions like this are actually answered by the argument above, if you assume the truth of the abc conjecture.

Problem 26. Assuming the truth of the abc conjecture, show that there are only finitely many solutions in integers to the equation $x^m - y^n = 17$.

Hint: In applying the abc conjecture, we have control over ϵ, and therefore over k. A judicious choice of ϵ will get the job done. Why did we choose $\epsilon = \frac{1}{4}$ in the argument above? Well, we need ϵ small enough so that $m - \frac{5}{2}$ would be a positive number. The number $\frac{5}{2}$ is really $2(1+\epsilon)$, and $2(1+\epsilon) < 3$, so $\epsilon < \frac{1}{2}$. So we chose $\frac{1}{4}$ for safety.

That logical gap referred to above? Well, we wanted to show that the equation $x^m - y^n = 1$ has only finitely many solutions. What we showed was that m and n are bounded by a certain number N_0. But it could happen that there is one of these small pairs of m and n such that there are infinitely many pairs of number x and y, and the equation still has infinitely many solutions.

Luckily, this gap is not hard to fill. We have argued that there are only finitely many pairs of values of m and n. So fix one such pair, say $m = m_0,\ n = n_0$. Then $(m_0 - \frac{5}{2}) \log x + (n_0 - \frac{5}{2}) \log y \leq 2 \log k$ (by problem 24). This will bound x and y as well. That is, we have $2 \leq y$, so

$$\left(m_0 - \frac{5}{2}\right) \log x + \left(n_0 - \frac{5}{2}\right) \log 2 \leq \left(m_0 - \frac{5}{2}\right) \log x + \left(n_0 - \frac{5}{2}\right) \log y \leq 2 \log k,$$

or

$$\left(m_0 - \frac{5}{2}\right) \log x \leq 2 \log k - \left(n_0 - \frac{5}{2}\right) \log 2,$$

or

$$\log x \leq \frac{2 \log k - (n_0 - \frac{5}{2}) \log 2}{m_0 - \frac{5}{2}} = \frac{\log\left(\frac{k^2}{2^{n_0 - \frac{5}{2}}}\right)}{m_0 - \frac{5}{2}},$$

which is a bound on $\log x$, and therefore on x. A similar argument shows that y is also bounded.

This fills the logical gap. So given the truth of the abc conjecture, it really is true that there can only be finitely many solutions to the equation in Catalan's conjecture.

Do you like this stuff? Do you want to know more?

Here are a few more consequences of the abc conjecture. The proofs of some of them, if we assume the abc conjecture, are not that difficult.

1. The *Fermat-Catalan Equatiion*: For relatively prime integers $p,\ q,\ r$, there are only finitely many solutions to the diophantine equation $p^a + q^b = r^c$, where $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$. The cases where $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \geq 1$ are also interesting, but easier.

2. The existence of *non-Weiferich Primes*. A Weiferich prime is a prime number p such that $2^{p-1} \equiv 1 \bmod p^2$. The truth of the abc conjecture implies that there are infinitely many primes which do *not* satisfy this condition.

3. (A weak form of the *Erdös-Mollin-Walsh conjecture*.) Define a *powerful* number n to be a number such that if some prime p divides n, then p^2 also divides n. The abc conjecture implies that there are only finitely many triples of consecutive integers, each of which is powerful.

4. There exist only finitely many *Brown pairs*: pairs of integers $m,\ n$ such that $m! + 1 = n^2$.

5. Only finitely many numbers of the form n(n+11)(n+111) are perfect cubes.

6. Only finitely many numbers of the form n! + 1111 are perfect squares.

...and there are many more, whose statements involve more advanced contexts, and are not as easily given.

SOURCES AND RESOURCES

I am indebted to Melvyn Nathanson, of Lehman College, CUNY for the majority of the material appearing above. His book *Elementary Methods in Number Theory* (Graduate Texts in Mathematics, Vol. 195, Springer-Verlag, New York, 2000) gives a comprehensive but advanced discussion of the more advanced theory behind the abc conjecture (but was written before recent developments in its proof.)

The following web resources were all accessed in October, 2012:

www.staff.science.uu.nl/ beuke106/ABCpresentation.pdf An interesting and accessible presentation by mathematician Frits Beukers of the University of Leiden

http://www.math.unicaen.fr/ nitaj/abc.html An excellent index to all kinds of web resources concerning the abc conjecture.

http://abcathome.com A whole website devoted to results about the abc conjecture.