The *abc* Conjecture[*]

Graeme Taylor

January 6, 2007

It is often the case in number theory that a result is deceptively easy to state yet incredibly difficult to solve. The most famous example, of course, is *Fermat's Last Theorem*, the proof of which eluded mathematicians for 350 years. However, the result is more interesting for its ferocious difficulty than for what it actually says- it ended up being a special case of what is now the *Taniyama-Shimura theorem*, a distinctly non-elementary conjecture which suggested deep connections between number theory and topology.

However, in recent years a problem has arisen which combines all these properties. The *abc conjecture* is very easy to state, yet nonetheless has far-reaching implications throughout number theory; and it is probable that if a proof is found, it too will have deep consequences beyond the conjecture itself.

Terminology

In order to state the conjecture, we need just one idea- the notion of the *radical*, or *squarefree kernel*, of an integer (whole number). This is

$$R(n) = \prod_{p|n} p \text{ (for } p \text{ prime)}$$

and if that meant anything to you, feel free to jump onwards to the next section. If it might as well have been hieroglyphics, fear not, for the idea is actually fairly simple. Most numbers can be expressed as multiples of smaller numbers- for instance, 12 is 3×4 or 2×6 or 1×12. Fortunately, it turns out that, using prime numbers only, there is a simplest such representation, e.g., $12 = 2\times2\times3$. What the radical does is pull out each prime number that appears in such a representation, and multiplies them together. The point is that if there are repeated multiples of a prime (such as the 2×2 in 12), only one counts towards the radical. Thus the radical of 12 is $2 \times 3 = 6$: which also happens to be the radical of 6. Hence in some sense the radical gives an indication of how

[*] First appeared on Everything2, at *http://www.everything2.com/index.pl?node_id=1857473*

complicated a number is in terms of its prime factors. Large numbers may therefore be 'simpler' than smaller ones, if they have a lot of repeated factors: $R(32768)$ is just 2, for instance, whereas $R(210) = 210$.

The abc Conjecture

Oesterlé's version

The first version of the abc conjecture was given by J.Oesterlé around 1985.

> Consider a triple of integers a, b, c such that $a + b = c$ and no two share a factor other than 1 (a, b, c are described as being *coprime*). Then let $P(a, b, c)$ be given by
>
> $$\frac{\log \max\{|a|, |b|, |c|\}}{\log R(abc)}$$
>
> Then (it is conjectured) for any real number $\zeta > 1$, there are only finitely many triples with $P(a, b, c) > \zeta$.

In other words, almost all triples satisfy $P(a, b, c) \leq 1$. You might like to test a few values to convince yourself of this: if you pick a and b coprime, then setting $c = a + b$ will automatically meet the criteria. For instance with $a = 2$, $b = 3$ we get $c = 5$, $abc = 30$, $R(abc)$ also 30, and $max\{|a|, |b|, |c|\} = 5$. So $P(2, 3, 5)$ is $log(5)/log(30)$, about 0.47.

With some ingenuity, values greater than 1 can be found; but despite considerable brute-force computation, the record[1] currently stands at just under 1.63, using the less-than-obvious triple $a = 2, b = 3^10 \times 109, c = 23^5$.

In this formulation, it's not immediately apparent how such a conjecture might arise. However, there is another version which is more common and allows for easy comparison with a known result, at the price of some more mathematical abstraction. This refinement was presented by Masser.

Masser's version

> As before, let a, b, c be coprime integers with $a + b = c$. Then, for any $\epsilon > 0$,
>
> $$\max\{|a|, |b|, |c|\} \leq C(\epsilon)R(abc)^{1+\epsilon}$$
>
> where $C(\epsilon)$ is a constant depending only on ϵ (i.e., independent of a, b, c).

(The more mathematically minded may wish to verify that the two versions of the conjecture are equivalent.)

The ABC Theorem for Polynomials

Thanks to the abstract underpinnings, it is often possible to translate a problem from one section of algebra to another, in the hope that the resulting question is easier to tackle and offers insight for the original. Masser's version of the abc conjecture for integers is easy to see as a reformulation of the *ABC theorem for polynomials*, which runs as follows.

A polynomial is simply an expression involving sums of powers of a variable, such as $x^3 - 1$ or $x^2 - 4x + 4$. We observed that an integer can be decomposed into prime numbers. We can perform a similar trick with polynomials, factorising them into simpler ones. Unlike the integers, we can say a bit more about the number and nature of factors, given the luxury of working with complex numbers. If d is the largest power of x which appears in our polynomial (known as the *degree*), then we can (possibly with some effort) write it as the product of d linear polynomials- that is, polynomials of the form $(x - a)$. Further, plugging such an a into the polynomial gives the value of 0, so they are naturally enough called the *zeroes* of the polynomial. However, just as numbers can have repeated factors, so polynomials can have repeated factors and hence repeated zeroes. As an example, $x^2 - 4x + 4$ is $(x - 2) \times (x - 2)$, so we have only one distinct zero despite a degree of 2.

So in place of the radical, we can consider the quantity $n(P)$, the number of distinct zeroes of a given polynomial P. The notion of coprimality carries over exactly: two polynomials are coprime if they don't share any factors (or hence any zeroes). The *ABC theorem* is then:

> Let A, B, C be coprime polynomials over the complex numbers, not all constant and with $A + B = C$. Then
>
> $$\max\{\deg A, \deg B, \deg C\} < n(ABC)$$

From ABC to abc

Whilst there are clear similarities between the two assertions - the ABC theorem, and Masser's form of the abc conjecture - they're not quite identical in structure, due to the ϵ dependence. Why doesn't the conjecture simply assert something like

$$\max\{|a|, |b|, |c|\} \leq C(\epsilon)R(abc)$$

or better still

$$max\{|a|, |b|, |c|\} = K \times R(abc)$$

for some fixed K?

Simply enough, the conjecture doesn't take this form because there are counterexamples! For instance, Jastrzebowski & Spielman give the case of $a = 3^{2^n} - 1, b = 1, c = 3^{2^n}$; for which, if such a K were to exist, we'd arrive at a contradiction as n tended to infinity (for details on this see J.Wheeler's thesis[2]). Thus the extra wriggle room granted by the ϵ is genuinely necessary to the conjecture.

It can be hoped, however, that the expression $C(\epsilon)$ could be given explicitly, rather than simply demonstrated to exist (which would still be a perfectly valid proof); this would then make the bound effective- that is, allow for direct computation.

As easy as abc

An article[3] by Granville and Tucker outlines some connections between the abc conjecture and the number theory "hall of fame"; in particular, an explicit form of the abc conjecture as discussed above would allow for improvements on results themselves impressive enough to merit the Fields medal- such as *Faltings' theorem* (an explicit form of which would be equivalent to explicit abc); *Roth's theorem* (a generalisation of which is equivalent to abc) and *Baker's theorem* (which contains a far from best possible bound which would be considerably sharpened if abc holds). Around thirty significant problems that would be resolved by a positive answer to the abc conjecture are outlined on Abderrahmane Nitaj's abc conjecture homepage[1].

My own interest[4] in the abc conjecture arose from a related conjecture in the theory of elliptic curves. A vital notion is of that of the height of a rational point on such a curve; in some sense the height captures the complexity of the point, and it is therefore natural to ask how low the height can be. A remarkable (and effective!) bound was conjectured by Lang and proven in certain cases, but would apply in all cases were the *Szpiro conjecture* to hold. The Szpiro conjecture itself would be implied by abc but is in fact easier than abc- although there is a modified version of equal strength (that is, modified Szpiro implies abc and vice versa).

But perhaps most fittingly, abc brings us full circle to Fermat's Last Theorem, since the abc conjecture even implies FLT for sufficiently large exponents[5]. Let us hope, however, that it does not take as long to prove!

References

[1] *http://www.math.unicaen.fr/ nitaj/abc.html* .

[2] Jeffrey Paul Wheeler, Master Thesis, University of Tennessee, Knoxville. (Available from [1])

[3] *It's as easy as the abc conjecture*, A. Granville, Notices of the AMS, Volume 49, Number 10. (Available from [1])

[4] See *http://maths.straylight.co.uk/archives/58* for slighlty more details on the Szpiro conjectures and heights.

[5] *Diophantine Analysis*, Jörn Steuding, Chapman & Hall/CRC.