The abc conjecture and related topics

David A. Craven

20th May 2009

We begin with polynomials, and then move on to the integers, and finally function fields.

Firstly, if R is a UFD and x is a non-zero element of R, then define $\mathrm{rad}(x) = \prod_{p|x} p$, so if one writes out a factorization of x into primes, then $\mathrm{rad}(x)$ is the product of all the primes dividing x with multiplicities removed.

1 Polynomial Rings

We begin with a theorem.

Theorem 1.1 Let $R = F[X]$, where F is a field of characteristic 0, and let a and b be coprime, non-constant polynomials in R. Write $c = a + b$. Then

$$\deg a, \deg b, \deg c < \deg(\mathrm{rad}(abc)).$$

Proof: Note that $\mathrm{rad}(a) = a/\gcd(a, a')$. Firstly, multiply the equation $a + b = c$ by a' to get $aa' + ba' = ca'$, and multiply $a' + b' = c'$ by a to get $aa' + ab' = ac'$. The difference of the two yields

$$ab' - ba' = ac' - ca'.$$

We have that $ab' - ba' \neq 0$, since else $ab' = ba'$, and since a and b are coprime this yields $b \mid b'$; this expression is divisible by both $\gcd(a, a')$ and $\gcd(b, b')$, and by the equality above, $\gcd(c, c')$ also divides it; i.e.,

$$\gcd(c, c') \mid \frac{ab' - ba'}{\gcd(a, a')\gcd(b, b')},$$

and hence

$$\begin{aligned}
\deg(\gcd(c, c')) &\leqslant \deg(ab' - ba') - \deg(\gcd(a, a')) - \deg(\gcd(b, b')) \\
&< \deg(\mathrm{rad}(a)) + \deg(\mathrm{rad}(b)) \\
&= \deg(\mathrm{rad}(ab)).
\end{aligned}$$

Adding $\deg(\text{rad}(c))$ to both sides gives $\deg(c) < \deg(rad(ab)) + \deg(rad(c)) = \deg(rad(abc))$. Symmetry proves the other two statements. $\square$

Using this, one may prove Fermat's last theorem for polynomial rings.

Corollary 1.2 Let a, b, c be non-constant polynomials in $R = F[x]$, and suppose that $a^n + b^n = c^n$. Then $n \leqslant 2$.

Proof: Firstly, dividing out by the gcd gives a and b coprime, with $a^n + b^n = c^n$, so that the *abc* theorem applies to the triple (a^n, b^n, c^n). Notice that $\text{rad}(a^n b^n c^n) = \text{rad}(abc) \leqslant abc$, so the *abc* theorem yields

$$\deg(a^n), \deg(b^n), \deg(c^n) < \deg(abc).$$

Write d for the element of $\{a, b, c\}$ with the largest degree. Certainly $\deg(d^n) = n\deg(d)$ and $\deg(abc) \leqslant 3\deg(d)$, so that

$$n\deg(d) < 3\deg(d),$$

yielding $n \leqslant 2$, as claimed. $\square$

Another corollary is Davenport's theorem, from 1965.

Corollary 1.3 (Davenport) If u and v are non-constant, coprime polynomials such that $u^3 - v^2 \neq 0$. Then

$$\deg u, \deg v \leqslant 2\deg(u^3 - v^2) - 2.$$

Proof: Again we will apply the *abc* theorem with $a = u^3$, $b = v^2$ and $c = u^3 - v^2$. This yields

$$\deg u, \deg v < \deg(\text{rad}(u^3 v^2 (u^3 - v^2))) \leqslant \deg u + \deg v + \deg(u^3 - v^2).$$

It suffices to show therefore that $\deg u, \deg v \leqslant \deg(u^3 - v^2) - 1$, and this is clearly true for u, and for v it is true unless $\deg v = 1$, and in this case $\deg(u^3 - v^2) \geqslant 3$ since u is also non-constant. $\square$

2 The Integers

A reasonable analogue of the degree function as a measure of size is the logarithm function for integers, and in this case a direct translation would be the statement that if a and b are coprime then, writing $c = a + b$, we have

$$\log c < \log \text{rad}(abc),$$

so taking exponentials yields $c < \mathrm{rad}(abc)$. This is not true however, as the following example shows.

Example 2.1 Let $a = 5^{2^n} - 1$, $b = 1$, and $c = 5^{2^n}$. Clearly, $\mathrm{rad}(abc) = 5\,\mathrm{rad}(a)$, and so if $5^{2^n-1} \geqslant \mathrm{rad}(5^{2^n} - 1)$ for infinitely many n then we are done. However, it is fairly easy to see that $2^n \mid (5^{2^n} - 1)$, and so $5\,\mathrm{rad}(a) \geqslant 5(5^{2^n} - 1)/2^{n-1}$

Firstly, $\log 5 < 3\log 2$, and so if $n \geqslant 4$, we have

$$\begin{aligned}\log(\mathrm{rad}(abc)) &= \log 5 + \log(\mathrm{rad}(a)) \leqslant \log 5 + \log(5^{2^n} - 1) - (n-1)\log 2 \\ &< \log 5 + 2^n \log 5 - (n-1)\log 2 \\ &= \log 5 - (n-1)\log 2 + \log c. \\ &< \log c.\end{aligned}$$

This example shows that there are infinitely many counterexamples to the statment that $c \leqslant \mathrm{rad}(abc)$. However, in number theory often things are only done up to ε. This is justified by taking logs: if we cannot have $\log c \leqslant \log \mathrm{rad}(abc)$, then perhaps we might be able to get $\log c \leqslant (1+\varepsilon)\log \mathrm{rad}(abc)$ for arbitrarily small ε. However, if we are to do this, we need to add a constant in to take account of the increasingly many, hopefully finitely many, counterexamples to the statement $\log c \leqslant (1+\varepsilon)\log \mathrm{rad}(abc)$. Thus we get the *abc* conjecture:

Conjecture 2.2 (The *abc* conjecture) For any $\varepsilon > 0$, there exists $N > 0$ such that, for all coprime natural numbers a and b, we have

$$c \leqslant N\,\mathrm{rad}(abc)^{1+\varepsilon}.$$

This is equivalent to the statement that for a given $\varepsilon > 0$ there are only finitely many pairs (a, b) such that $c > \mathrm{rad}(abc)^{1+\varepsilon}$. Firstly, if there are only finitely many then simply take N to be the largest such c. Conversely, suppose that there are infinitely many triples (a, b, c) satisfying

$$\mathrm{rad}(abc)^{1+\varepsilon} < c < N\,\mathrm{rad}(abc)^{1+\varepsilon}.$$

then taking $\delta = \varepsilon/2$ we find that these infinitude of triples are not universally bounded by any N, and hence disobey the *abc* conjecture for $\varepsilon/2$.

Note that it is not known whether for all triples (a, b, c), we have that $c \leqslant \mathrm{rad}(abc)^2$: this would imply Fermat's last theorem, since then (for $n \geqslant 6$), we have (assuming $a^n + b^n = c^n$)

$$c^n \leqslant \mathrm{rad}(abc)^2 \leqslant (abc)^2 \leqslant c^6,$$

so that $n \leqslant 6$. (At this point one needs the small cases of Fermat's last theorem.) The conjecture that there are only finitely many counterexamples to $c \leqslant \mathrm{rad}(abc)^{1+\varepsilon}$ means that there is some n such that $c \leqslant \operatorname{rad}(abc)^n$, and so the asymptotic version of Fermat's last theorem would hold for all integers at least $3n$. (One hopes at this point that the resulting bound in a proof of the *abc* conjecture is below the threshold of previous calculations of FLT.) Also notice that the asymptotic version of the *abc* conjecture corresponds to the case where $n = 3$ for FLT.

As an example of what the *abc* conjecture says, it claims that numbers like $2^n \pm 1$ should be divisible by large primes to a single power, which is indeed what occurs.

Thinking about FLT, we recall one of the main steps in the proof, which was the Frey polynomial: given $a + b = c$, we associate the *Frey polynomial*

$$y^2 = x(x - 3a)(x + 3b) = x^3 - 3(a - b)x^2 - 9abx.$$

The discriminant of the polynomial is $D = 3^6(abc)^2$. We write $X = x + b - a$ to get rid of the x^2 term, and so

$$Y^2 = X^3 - \alpha X - \beta.$$

Here, $\alpha = 3(a^2+ab+b^2)$ and $\beta = (a-b)(2a^2+2b^2+5ab)$. Doing this, we get $D = 4\alpha^3 - 27\beta^2$. If a, b, c are coprime then either α and β are coprime or their gcd is 9. The discrimant of the Frey polynomial is interesting, and so we want to ask questions about $4\alpha^3 - 27\beta^2$.

Conjecture 2.3 (Generalized Szpiro Conjecture) Let $\varepsilon > 0$, and suppose that u and v are non-zero coprime integers, and let $D = 4u^3 - 27v^2$. Then

$$|u| \leqslant N_1 \operatorname{rad}(D)^{2+\varepsilon} \text{ and } |v| \leqslant N_2 \operatorname{rad}(C)^{3+\varepsilon}.$$

Theorem 2.4 The *abc* conjecture and the generalized Szpiro conjecture are equivalent.

We will not talk about recent progress on the *abc* conjecture, and instead discuss a few theorems and conjectures that it implies.

- The first one is the Erdös–Mollin–Walsh conjecture, which concerns so-called powerful numbers. Recall that an integer n is *powerful* if, whenever p divides n, so does p^2; such numbers can obviously be written as a^2b^3, and the conjecture is that there are never three consecutive powerful integers. The *abc* conjecture, while it does not imply this, it implies that there are only *finitely many* such triples.

- Next, we have Wieferich primes. A prime p is called a *Wieferich prime* if p^2 divides $2^{p-1} - 1$. Such primes are related to FLT again. 1093 and 3511 are the only known Wieferich primes below 4 trillion. The abc conjecture implies the following open problem: Given a positive integer $a > 1$, does there exist infinitely many primes p such that p^2 does not divide $a^{p-1} - 1$?

- The Erdös–Woods conjecture asks the following: is there an integer $k > 1$ such that all integers x are determined by the sequence $\mathrm{rad}(x), \mathrm{rad}(x+1), \ldots, \mathrm{rad}(x+k)$? In other words, if one knows the prime divisors of $x, \ldots, x+k$, does that uniquely determine x? The *abc* conjecture implies that, with only finitely many counterexamples, $k = 3$ will do, and hence there is some $k > 3$ that will do with no counterexamples.

3 Function Fields

Another case, besides polynomial rings, for which the *abc* coonjecture is not a conjecture but a theorem is function fields. If we want to talk about the *abc* conjecture for function fields, we first need to reformulate it over $\mathbb{Q}$. Rewriting $a + b = c$ as $a/c + b/c = 1$. The height of a rational number n/m (in its lowest form) is defined to be $\mathrm{ht}(n/m) = \max(\log(n), \log(m))$. Taking logs in the *abc* conjecture gives the following: given $\varepsilon > 0$, there is some N such that, whenever $u, v \in \mathbb{Q} \setminus \{0\}$ and $u + v = 1$, we have

$$\mathrm{ht}(u), \mathrm{ht}(v) \leqslant N + (1+\varepsilon) \sum_{p \mid ABC} \log p,$$

where A and B are the numerators of u and v and C is their common denominator.

If we want to convert this into a statement about other fields we will need a substitute for height. For function fields there is such a notion, called the *degree*. We will define it now, after we have stated the ABC theorem for function fields.

Theorem 3.1 (ABC theorem for function fields) Let K be a function field with a perfect constant field F. Suppose that u and v are non-zero elements of K with $u + v = 1$. In this case,

$$\deg_s u = \deg_s v \leqslant 2g_K - 2 + \sum_{P \in \mathrm{Supp}(A+B+C)} \deg_K P.$$

In this equation, g_K is the genus of K, A and B are the zero divisors of u and v in K, and C is their common polar divisor.

The rest of the talk will be spent defining the various concepts in the theorem.

Recall that a function field K over a constant field F (of degree 1) contains a transcendental element x such that $K/F(x)$ is a finite field extension. A *prime* in K is a dvr R with maximal ideal P such that $F \subseteq R$ and the field of fractions of R is K. The *degree* of P is defined to be the F-dimension of R/P, which can be shown to be finite.

In order to simplify these concepts, we will assume that $K = F(x)$. In this case, let $A = F[x]$. Every non-zero prime ideal P in A is generated by a monic irreducible, and the localization A_P is a dvr. This maximal ideal P is a prime of $F(x)$, and every prime apart from one appears in this way. The other prime is got by changing the ring A to $A' = F[x^{-1}]$, and the ideal P' generated by x^{-1} is called the prime at infinity, and often denoted ∞. The ord function ord_∞ attaches $-\deg(f)$ to any polynomial $f \in A$ and $\deg(g) - \deg(f)$ to a rational function $f/g \in K$ where $f, g \in A$.

The group of divisors, D_K of a function field is the free abelian group on the primes. A typical divisor will be written $D = \sum_P a(P)P$. Let $a \in K \setminus \{0\}$. The divisor of a, written (a), is the divisor

$$\sum_P \mathrm{ord}_P(a)P.$$

If P is a prime such that $\mathrm{ord}_P(a) = m > 0$, we say that P is a *zero* of a of order m, and similarly if $\mathrm{ord}_P(a) = -m < 0$ we say that P is a *pole* of a of order m. Let

$$(a)_0 = \sum_{\mathrm{ord}_P(a)>0} \mathrm{ord}_P(a)P, \quad (a)_\infty = -\sum_{\mathrm{ord}_P(a)<0} \mathrm{ord}_P(a)P;$$

the divisor $(a)_0$ is called the *divisor of zeroes* of a and the divisor $(a)_\infty$ is called the *divisor of poles* of a. Note that $(a) = (a)_0 - (a)_\infty$.

Proposition 3.2 Let a be a non-zero element of K. Then $\mathrm{ord}_P(a) = 0$ for all but finitely many primes P. Secondly, $(a) = 0$ if and only if $a \in F$. Finally, $\deg(a)_0 = \deg(a)_\infty = |K : F(a)|$. (Therefore every non-zero element has at least one zero and at least one pole.)

The map $a \mapsto (a)$ is a homomorphism from K^* to D_K, and the image of this map is denoted by P_K and is called the group of *principal divisors*. A divisor class is a coset of P_K in D_K. A divisor $D = \sum_P a(P)P$ is called *effective* if none of the $a(P)$ is negative. Define $L(D)$ to be all those $x \in K^*$ such that $(x) + D$ is effective, together with $\{0\}$. This carries the structure of a vector space, and its dimension is written as $l(D)$.

We also need to define the genus of a function field. This will be done via the Riemann–Roch theorem.

Theorem 3.3 (Riemann–Roch theorem) There is some integer $g \geqslant 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $A \in D_K$, we have

$$l(A) = \deg(A) - g + 1 + l(C - A).$$

(This integer g is called the *genus* of K.)

We nearly have enough definitions: the support of a divisor D are the primes that occur with non-zero coefficient, as expected, and $\deg_s(a)$ is the separable degree, in the sense that it is the degree of the largest separable extension $|M : F(a)|$. Since $M \leqslant K$, we have that $\deg_s(a) \leqslant \deg(a)$.