THE ABC CONJECTURE
OPEN PROBLEMS IN NUMBER THEORY
SPRING 2018, TEL AVIV UNIVERSITY

ZEÉV RUDNICK

Contents

0.1. Formulation.

Conjecture 1 (Masser-Oesterlé 1985)**.** *Let $\varepsilon > 0$. Then for all but finitely many triples of coprime integers a, b, c with $a + b = c$, we have*

$$\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}.$$

Any polynomial bound $\ll \mathrm{rad}(a, b, c)^N$ would have far reaching consequences. The known result, due to C.L. Stewart, R. Tijdeman and Yu Kunrui (1991), falls far short of that

$$\max(|a|, |b|, |c|) \ll \exp(\mathrm{rad}(abc)^{1/3+o(1)})$$

0.2. Asymptotic Fermat.

We can use the *abc* conjecture to deduce that for $N \gg 1$, there are no nontrivial solutions of $x^N + y^N = z^N$ in coprime integers, that is with all variables nonzero.

Assume that $x^N + y^N = z^N$, with $x, y, z > 0$ (so $z \geq 2$) and coprime. Apply the *abc* conjecture to obtain

$$z^N = \max(x^N, y^N, z^N) \leq C(\varepsilon)\,\mathrm{rad}(x^N y^N z^N)^{1+\varepsilon} = C(\varepsilon)\,\mathrm{rad}(xyz)^{1+\varepsilon} \leq C(\varepsilon) z^{3(1+\varepsilon)}$$

and so

$$2 \leq z \leq C(\varepsilon)^{1/(N-3(1+\varepsilon))}.$$

But for $N \geq N(\varepsilon)$, we have $C(\varepsilon)^{1/(N-3(1+\varepsilon))} < 2$ which gives a contradiction.

Date: June 12, 2018.

0.3. **Why the exponent $1+\varepsilon$?** Here is a quick example showing why one needs the exponent to be bigger than 1 in the conjecture: For any constant $M > 0$, there are infinitely many coprime triples a, b, c with $a + b = c$ such that

$$\max(|a|, |b|, |c|) \geq M \operatorname{rad}(abc).$$

Exercise 1. *Let $A_k = 3^{2^k} - 1$, $B_k = 1$, $C_k = 3^{2^k}$. Show that for all $k \geq 2$,*

$$C_k \geq \frac{2^{k+1}}{3} \operatorname{rad}(A_k B_k C_k)$$

and hence that

$$C_k \gg R_k \log R_k,$$

where $R_k := \operatorname{rad}(A_k B_k C_k)$.

Hint: Show that 2^{k+2} divides $3^{2^k} - 1$.

0.4. **The conjectures of Catalan and Pillai.** Catalan (1844) conjectured that there are no *consecutive perfect powers*, other than the pair $(8, 9) = (2^3, 3^2)$. That is there are no solutions of $x^m - y^n = 1$ with $x, y > 1$, $m, n \geq 2$ except for $(8, 9)$.

This conjecture attracted a huge amount of attention over the years. We can clearly suppose both $m = p$ and $n = q$ are prime. The case $(p, q) = (2, 3)$ or $(3, 2)$ was already solved by Euler about a 100 years prior to Catalan. The case $q = 2$, i.e. the equation $x^p - y^2 = 1$, was solved in 1850 by Victor-Amédée Lebesgue[1]. The case $x^2 - y^q = 1$ ($q > 2$ prime) remained open until the 1960's (published 1964), when it was solved by Chao Ko (Ke Zhao).[2] Already in 1921, Nagell showed that $\min(p, q) \neq 3$.

Tijdeman (1976) uses Baker's method to show finiteness of the set of solutions, which in principle (but not in practice) settles the case. His bound was effective, but all subsequent refinements gave bounds which were far too large, (e.g. $x^m < \exp\exp\exp\exp 730$).

Catalan's conjecture was finally proven by Preda Mihailescu in 2002.

More generally, S. S. Pillai (1931) conjectured that the gaps in the sequence of perfect powers tend to infinity. This is equivalent to saying that each positive integer occurs only finitely many times as a difference of perfect powers. This conjecture follows from *abc*.

Exercise 2. *Show that the abc conjecture implies Pillai's conjecture: each positive integer occurs at most finitely many times as a difference of perfect powers. For each $k \geq 1$, there are at most finitely many solutions of $x^m - y^n = 1$ with $x, y, m, n \geq 2$.*

0.5. **The polynomial *abc* theorem.** For a polynomial $P(x) \in \mathbb{C}[x]$, if we factor $P(x) = c \prod (x - a_j)^{n_j}$ with $a_j \in \mathbb{C}$ the distinct roots, the radical is

$$\operatorname{rad}(P) := \prod (x - a_j).$$

We note some immediate consequence of the definition of $\operatorname{rad} P$:

Multiplicativity: If P, Q, are pairwise coprime then

$$\operatorname{rad}(PQ) = \operatorname{rad}(P) \operatorname{rad}(Q).$$

[1]Not to be confused by the more famous Henri Lebesgue, 1875-1941.

[2]Ke Zhao 1910-2002 was a student of Mordell in Manchester, obtaining his Ph.D. in 1937.

What is new for $\mathbb{C}[x]$ relative to $\mathbb{Z}$ is that we have a relation with the derivative:

$$\operatorname{rad} P = \frac{P}{\gcd(P, P')}$$

because the multiple roots of P are also roots of P' with multiplicity exactly one less.

Remarkably, the analogue of the *abc* conjecture is an easy result (in sharper form) in this context, as was found independently by R. Mason (1983) and by W. Stothers (1981).

Theorem 0.1. *Let $A, B, C \in \mathbb{C}[x]$ be pairwise coprime, with $A + B = C$. Then*

$$\max(\deg A, \deg B, \deg C) < \deg \operatorname{rad}(ABC).$$

Proof. Note that on differentiation

$$A + B = C \quad \longrightarrow \quad A' + B' = C'.$$

Hence

$$AB' - A'B = AC' - A'C.$$

Since $\gcd(C, C')$ divides $AC' - A'C$, it also divides $AB' - A'B$, which is divisible by the product of the coprime polynomials $\gcd(A, A')$ and $\gcd(B, B')$, which are both coprime to $\gcd(C, C')$ since A, B, C are mutually coprime. Hence

$$\gcd(C, C') \mid \frac{AB' - A'B}{\gcd(A, A') \cdot \gcd(B, B')} = \operatorname{rad}(A)\frac{B'}{\gcd(B, B')} - \operatorname{rad}(B)\frac{A'}{\gcd(A, A')}$$

The RHS visibly has degree at most

$$\begin{aligned}\deg \operatorname{rad}(A) + (\deg \operatorname{rad} B' - \deg \gcd(B, B')) &< \deg \operatorname{rad} A + (\deg \operatorname{rad} B - \deg \gcd(B, B')) \\ &= \deg \operatorname{rad} A + \deg \operatorname{rad} B = \deg \operatorname{rad}(AB)\end{aligned}$$

(same computation for the second factor), and so

$$\deg \gcd(C, C') < \deg \operatorname{rad}(AB).$$

Since $\operatorname{rad} C = C/\gcd(C, C')$, we obtain

$$\deg C = \deg \gcd(C, C') + \deg \operatorname{rad} C < \deg \operatorname{rad}(AB) + \deg \operatorname{rad} C = \deg \operatorname{rad}(ABC)$$

as claimed. □

An immediate corollary is Fermat's theorem for $\mathbb{C}[x]$ (due originally to Liouville, 1851):

Corollary 0.2. *If $f, g, h \in \mathbb{C}[x]$ are coprime, at least one of which has positive degree, with $f^n + g^n = h^n$, then $n \leq 2$.*

Proof. Take $A = f^n$, $B = g^n$, $C = h^n$. Then since they are all coprime, we have

$$\operatorname{rad}(ABC) = \operatorname{rad}(f^n g^n h^n) = \operatorname{rad}(fgh).$$

Hence if $\deg f = \max(\deg f, \deg g, \deg h) > 0$, we find from the Mason-Stothers theorem that

$$n \deg f = \deg(f^n) < \deg \operatorname{rad}(fgh) \leq \deg fgh \leq 3 \deg f$$

which gives $n < 3$ as claimed. □

Exercise 3. *Prove the polynomial Catalan conjecture: There are no consecutive perfect powers of positive degree in $\mathbb{C}[x]$, i.e. no solutions of $f(x)^m - g(x)^n = 1$ with $f, g \in \mathbb{C}[x]$, $m, n \geq 2$ and $\deg f > 0$.*

0.6. **Wieferich primes.** A *Wieferich prime* is p such that $2^{p-1} = 1 \bmod p^2$. These primes are named after Arthur Wieferich who in 1909 proved that if the first case of Fermat's last theorem[3] is false for the exponent p, then p satisfies the criteria $2^{p-1} = 1 \bmod p^2$.

The only known Wieferich primes are 1093 and 3511. Non other exist up to 10^{17} (as of 2015). It is conjectured that there are infinitely many Wieferich primes AND infinitely many non-Wieferich primes, but neither is known. A heuristic suggests that the number of Wieferich primes up to x is about $\log\log x$.

J. H. Silverman (1988) showed that if the *abc* conjecture holds, then there exist infinitely many non-Wieferich primes, moreover that the number of non-Wieferich primes (to base 2) with $p \le x$ is $\gg \log x$ as $x \to \infty$.

Theorem 0.3 (Silverman 1988)**.** *Assuming the abc conjecture, there are infinitely many non-Wieferich primes.*

Proof. Let S be the set of non-Wieferich primes, which we will assume to be finite. Note that if $n \ge 1$ and p is a prime, $\boxed{\text{with } p \nmid n}$ such that $2^n = 1 \bmod p$ then

$$2^n \ne 1 \bmod p^2 \quad \text{if and only if} \quad p \in S. \tag{1}$$

Indeed, let $d = \mathrm{ord}(2, p)$, which divides $p-1$ and also divides n since $2^n = 1 \bmod p$. Moreover, since $2^n \ne 1 \bmod p^2$ and $d \mid n$ and so $2^d \ne 1 \bmod p^2$. Since $d \mid p-1$, write $p - 1 = dm$, and

$$2^{p-1} = 1 + pk, \quad p \nmid k$$

Then

$$2^{p-1} = (2^d)^m = (1+pk)^m = 1 + pkm \bmod p^2$$

which is not $1 \bmod p^2$ because $p \nmid k$, and certainly $p \nmid m$ since $m \mid p-1$. Thus $2^{p-1} \ne 1 \bmod p^2$, so that $p \in S$. (HERE we didn't use $p \nmid n$).

Conversely, if $p \in S$, so that $2^{p-1} \ne 1 \bmod p^2$, then also $2^d \ne 1 \bmod p^2$ and so as before $2^d = 1 + pk$ with $p \nmid k$. Write $n = Md$,

$$2^n = (2^d)^M = (1+pk)^M = 1 + pkM \bmod p^2$$

and recall that $p \nmid n$ so that $p \nmid M$, hence $2^n \ne 1 \bmod p^2$.

Assume that S is finite. Write for n coprime to S

$$2^n - 1 = s_n v_n$$

where s_n is made up of powers of primes in S, and v_n is not divisible by any prime in S.

We claim that s_n is bounded. In fact we claim that s_n is squarefree, hence is a divisor of $\prod_{p \in S} p$. To see this, first note that for any $p \mid s_n$, we have $2^n = 1 \bmod p$ and since $p \in S$ we have $2^{p-1} \ne 1 \bmod p^2$. Since we assume that n is coprime to S, that forces $2^n \ne 1 \bmod p^2$ by (1), that is $p^2 \nmid 2^n - 1$ so that $p^2 \nmid s_n$.

Now if $p \mid v_n$, so that $p \notin S$, since $p \mid 2^n - 1$ this implies that $p^2 \mid 2^n - 1$ by (1). Hence $\mathrm{rad}(v_n) \le v_n^{1/2}$.

Now consider the equation

$$(2^n - 1) + 1 = 2^n$$

[3]he first case of Fermat's last theorem says that for three integers x, y and z and a prime number p, where $p \nmid xyz$, there are no solutions to the equation $x^p + y^p + z^p = 0$.

According to the *abc* conjecture, given $\varepsilon > 0$, we have for $n \gg_\varepsilon 1$

$$(2^n)^{1-\varepsilon} < \operatorname{rad}((2^n-1)2\cdot 2^n) = 2\operatorname{rad}(s_n v_n) \le 2(\prod_{p\in S} p)\operatorname{rad}(v_n) \ll v_n^{1/2}$$

But also $2^n > s_n v_n \ge v_n$ so that we find

$$v_n \ll v_n^{1/2}$$

Thus there are only finitely many possibilities for v_n, and also for s_n, so that n has to be bounded. Thus there are only finitely many possibilities for n, which is a contradiction since we only assumed that n is coprime to the finitely many primes in S. □

0.7. **Langevin Elkies.** There is a seemingly stronger statement which turns out to be a consequence of the *abc* conjecture, and which is very useful in applications: Let

$$F(x,y) = \sum_{i+j=d} a_{i,j} x^i y^j \in \mathbb{Z}[x,y]$$

be a binary homogeneous polynomial of total degree d. We assume that $F(x,y)$ has *distinct* factors over $\mathbb{C}$, that is

$$F(x,y) = c\prod_{j=1}^{d}(x-\alpha_j y) \quad \text{or} \quad F(x,y) = cy\prod_{j=1}^{d-1}(x-\alpha_j y),$$

with $\alpha_j \in \mathbb{C}$ distinct, $c \in \mathbb{C}^*$. For instance we can take $F(x,y) = xy(x+y)$.

Theorem 0.4 (Langevin 1994, Elkies)**.** *Assume the abc conjecture. Let $F(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous binary form, without repeated factors. Then for all $\varepsilon > 0$, $\exists C(F,\varepsilon) > 0$ so that for all pairs $(m,n) \in \mathbb{Z}^2$ with $\gcd(m,n) = 1$ and $F(m,n) \neq 0$,*

$$\operatorname{rad}(F(m,n)) \ge C(F,\varepsilon)\max(|m|,|n|)^{\deg F - 2 - \varepsilon}. \tag{2}$$

For instance, taking $F(x,y) = xy(x+y)$ we substitute $a = x$, $b = y$, $c = a+b = x+y$ to obtain $F(a,b) = abc$ and so

$$\operatorname{rad}(abc) \gg_\varepsilon \max(a,b)^{1-\varepsilon}$$

and since $c \le 2\max(a,b)$ we can derive

$$\max(a,b,c) \ll_\varepsilon \operatorname{rad}(abc)^{1+\varepsilon}$$

which is the original *abc* conjecture. So certainly (2) includes the *abc* conjecture. The remarkable thing is that Theorem 0.4 is actually implied by the *abc* conjecture. The proof uses some fairly simple Riemann surface theory (Belyi maps), but will not be presented here.

0.8. **Roth's theorem.** The main result in Diophantine approximation theory is Roth's theorem (1950):

Theorem 0.5. *Let α be a real algebraic number. Then for all $\varepsilon > 0$ there is some $C(\alpha,\varepsilon) > 0$ so that for any rational $p/q \neq \alpha$, with p, q (coprime) integers,*

$$|\alpha - \frac{p}{q}| \ge C(\alpha,\varepsilon)\frac{1}{q^{2+\varepsilon}}$$

It is worth recalling the basic result that set off much of the work in Diophantine approximation theory:

Theorem 0.6 (Liouville, 1844)**.** *Let α be a real algebraic number of degree d. Then there is an explicit $c(\alpha) > 0$ so that for any coprime p, q with $\alpha \neq p/q$*

$$|\alpha - \frac{p}{q}| \geq c(\alpha)\frac{1}{q^d}$$

To prove both results, we start with a computation: Let $f(x) \in \mathbb{Z}[x]$ be "the" minimal polynomial for α, which is an irreducible polynomial (hence with distinct roots) whose degree is $\deg \alpha$, and set

$$F(x, y) = y^{\deg \alpha} f(x/y) \in \mathbb{Z}[x, y],$$

which is a binary form of degree $d = \deg \alpha$. For instance, of $\alpha = \sqrt[3]{2}$ then we can take $F(x, y) = x^3 - 2y^3$.

We claim

Lemma 0.7. *(the implied constant is effective):*

$$|F(m, n)| \ll |N|^d |\frac{m}{n} - \alpha| \tag{3}$$

Proof. Let $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_d$ be the roots of f (all distinct). We may suppose that m/n is closer to α then to any of the other roots, otherwise

$$|\alpha - m/n| \geq \frac{1}{2}c_0(f) := \frac{1}{2}\min |\alpha_i - \alpha_j|$$

and there is nothing to prove. Hence

$$|\frac{m}{n} - \alpha_j| \leq |\frac{m}{n} - \alpha| + |\alpha - \alpha_j| \leq 2c_0(f).$$

We have $F(x, y) = c\prod_{j=1}^d (x - \alpha_j y)$ and so

$$\begin{aligned} |F(m, n)| &= |n|^d |c| |\frac{m}{n} - \alpha| \prod_{j=2}^d |\frac{m}{n} - \alpha_j| \\ &\leq |n|^d |\frac{m}{n} - \alpha| |c| c_0(f)^{d-1} \ll_\alpha |n|^d |\frac{m}{n} - \alpha|. \end{aligned}$$

which proves (3) . □

We can now quickly prove Liouville's theorem:

Proof. We use the minimal polynomial and associated binary form $F(x, y)$ as before, and the inequality (3)

$$|F(m, n)| \ll_\alpha |n|^d |\frac{m}{n} - \alpha|$$

which is completely effective. Then we note that $F(m, n) \neq 0$ since $F(x, y)$ is irreducible over $\mathbb{Q}$ and in the case of $d = 1$ (so $\alpha \in \mathbb{Q}$) we assume that $\alpha \neq m/n$. Since $F(m, n) \in \mathbb{Z}$, this forces $|F(m, n)| \geq 1$ and so

$$1 \ll_\alpha |n|^d |\frac{m}{n} - \alpha|$$

which is the statement of Liouville's theorem. □

Let's see how Roth's theorem follows from the version of *abc* given by Theorem 0.4.

Proof. Again use (3), and note that $|F(m,n)| \geq \operatorname{rad}(F(m,n))$, and inserting Theorem 0.4 gives

$$|n|^d|\frac{m}{n} - \alpha| \gg_\alpha |F(m,n)| \geq \operatorname{rad} F(m,n) \gg_{F,\varepsilon} |n|^{d-2-\varepsilon}$$

(here $|m|, |n|$ have the same size since m/n is close to the fixed number α). Hence we obtain

$$|\frac{m}{n} - \alpha| \gg_{\alpha,\varepsilon} |n|^{-2-\varepsilon}$$

which is Roth's theorem. □

0.9. **Squarefree values of polynomials.** A further application of the *abc* conjecture is to completely settle the problem of representing square-free integers by integer polynomials.

It is conjectured that a separable polynomial (that is, without repeated roots) $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. A clear necessary condition is that the sequence $f(n)$ has no fixed square divisor; the conjecture is that this is the only obstruction:

Conjecture 2. *Let $f(x) \in \mathbb{Z}[x]$ be a separable polynomial (i.e. with no repeated roots) of positive degree. Assume that* $\gcd\{f(n) : n \in \mathbb{Z}\}$ *is squarefree*[4] *. Then there are infinitely many square-free values taken by $f(n)$, in fact that a positive proportion of the values are square-free:*

$$\#\{1 \leq n \leq X : f(n) \text{ is square-free } \} \sim c_f X, \quad \text{as } X \to \infty ,$$

with

$$c_f = \prod_p (1 - \frac{\rho_f(p^2)}{p^2}) , \tag{4}$$

where

$$\rho_f(D) = \#\{c \bmod D : f(C) = 0 \bmod D\} . \tag{5}$$

The problem is most difficult when f is irreducible. Nagell (1922) showed the infinitude of squarefree values in the quadratic case. Estermann (1931) gave positive density for the case $f(x) = x^2 + k$. The general quadratic case was solved by Ricci in 1933. For cubics, Erdös (1953) showed that there are infinitely many square-free values, and Hooley (1967) gave the result about positive density. Beyond that nothing seems known unconditionally for irreducible f, for instance it is still not known that $a^4 + 2$ is infinitely often square-free.

Granville (1998) showed that the ABC conjecture completely solves the conjecture 2.

[4]In fact one can even allow fixed, square divisors of $f(n)$, provided we divide them out in advance, by replacing $f(n)$ by $f(n)/B'$, where B' is the smallest divisor of $B := \gcd\{f(n) : n \in \mathbb{Z}\}$ so that B/B' is square-free, and if we replace c_f by $\prod_p (1 - \frac{\omega_f(p)}{p^{2+q_p}})$, where for each prime p, we denote by p^{q_p} the largest power of p dividing B', and by $\omega_f(p)$ the number of $a \bmod p^{2+q_p}$ for which $f(a)/B' = 0 \bmod p^2$.