Relaxations of the ABC conjecture using integer k'th roots

Version: 18th July 2004

Kevin A. Broughan

University of Waikato, Hamilton, New Zealand
E-mail: kab@waikato.ac.nz

Weakened forms of the ABC conjecture are defined in terms of the upper k'th root functions. These weakened forms, with quite small explicit values of their parameters, are shown to imply the asymptotic Fermat, Beale, general Fermat, and Catalan conjectures, that there exist an infinite number of non-Wieferich primes, that there exist only finitely many consecutive powerful numbers, Hall's conjecture and other consequences. The conjecture is true for a set of parameter values.

Key Words: Integer k'th root, ABC conjecture, diophantine equation, general Fermat conjecture, Catalan conjecture, Wieferich primes, square free values.

MSC2000 11A05, 11A99, 11D41, 11D75.

1. INTRODUCTION

For each whole number $k \geq 2$ and non-zero positive integer n let the integer upper k'th root and conductor be defined by

$$\eta_k(n) = \prod_{p^\alpha || n} p^{\lceil \frac{\alpha}{k} \rceil}, N(n) = \prod_{p|n} p.$$

respectively. If $n = 0$ set $\eta_k(n) = N(n) = 0$.

Since, for each integer n, $N(n) = \eta_k(n)$ for $k \geq k_n$, there is a close relationship between k'th roots and the integer conductor. A range of analytic and other aspects of this relationship are examined in [5]. For other applications see [3, 4].

Consider the ABC conjecture (referred to here as ABC) as follows: For every $\epsilon > 0$, if a, b are co-prime integers with $abc \neq 0$ and $a + b = c$ then

$$\max(|a|, |b|, |c|) \ll_\epsilon N(abc)^{1+\epsilon}.$$

Although this conjecture has many interesting consequences (see for example [13]), it is still quite some distance from being proved or disproved. (See the results of Stewart et al. cited in this section below.)

In this paper the conjecture is weakened, by replacing the conductor by the (larger) integer k'th root.

DEFINITION 1.1. Let $k \geq 2$ be a natural number and $\epsilon > 0$ be given. We say that the ABC-(k,ϵ) conjecture is satisfied if for all co-prime integers a and b with $abc \neq 0$ and $a + b = c$:

$$\max(|a|, |b|, |c|) \ll_{k,\epsilon} \eta_k(abc)^{1+\epsilon}.$$

The use of integer k allows for the potential use of Euler products [5] in derivations. However this restriction is not essential, and the use of k'th roots is expected to take its place in a "family" of relaxations of the original ABC, which would include the alternative given Section 2 "Associated Relaxations". In this paper we focus on ABC-(k,ϵ).

Even if all of these conjectures where true, ABC would not, on the face of it, follow. Hence these conjectures might be regarded as being weaker than ABC in an ultimate sense. If ABC-(k,ϵ) were to imply ABC for some finite value of k, that would be quite surprising (and interesting).

It turns out that many of the consequences of ABC are able to be derived assuming ABC-(k,ϵ) with quite small values of k and large values of ϵ. For example to prove the asymptotic Fermat theorem it is sufficient to chose $k = 4$ and and $\epsilon < 1/3$ (denoted (4,1/3)), the asymptotic Catalan (5,1/9), the existence of an infinite number of non-Wieferich primes (4,1/7), and the existence of only finitely many consecutive powerful numbers (4,1/15).

It is easy to show that ABC-(2,ϵ) is true for all $\epsilon > 0$ and that ABC-(3,1/2) and ABC-(4,1) are also true.

Browkin in [7] defines a more general relaxation of ABC with $p^{\lceil \frac{\alpha}{k} \rceil}$ replaced by $p^{f(\alpha)}$ where f is a given slowly increasing function. Under appropriate assumptions on f he deduces the asymptotic Fermat theorem, Overholt's theorem on solutions of $n! + 1 = m^2$ and a weak form of Hall's conjecture.

Many of the proof methods used here reflect those in the literature where the full ABC conjecture has been used, and acknowledgement of this is underlined.

Successive improvements by Stewart, Tijdeman and Yu (see [19, 20, 21]), mostly dependent on inequalities for linearly independent p-adic logarithms, have resulted in better approximations to ABC itself. Typically these approximations are given in the form of an upper bound for the sum

of two co-prime numbers which is an increasing function of the standard rational integer conductor. To date the best result is:

THEOREM 1.1. *(Stewart-Tijdeman-Yu) If* $(a, b) = 1$ *and* $G = N(ab(a + b))$ *then there is an effectively computable constant* $c > 0$ *such that*

$$a + b < e^{cG^{1/3}(\log G)^3}.$$

Replacing G by $\eta_k(ab(a + b))$ results in an inequality automatically satisfied by $\eta_k(ab(a+b))$, which may be of value, especially for large k. Here (bounds for) the actual size of c would be useful: since $a+b \mid \eta_k(ab(a+b)^k)$, these bounds are of interest only when $\exp(cG^{\frac{1}{3}+\epsilon}) \ll \eta_k(ab(a + b))^l$ for some $l < k$.

In Section 3 a set of lemmas is given. These are used to derive the consequences of ABC-(k,ϵ) given here. They might be useful also for proving cases of the conjecture or applying them, and should be read in conjunction with the composite lemma given in [5].

In Section 4 some relationships with ABC and the elementary proved cases ABC-(2,ϵ), ABC-(3,1/2) and ABC-(4,1) are given.

In Section 5 there are fourteen consequences of ABC-(k,ϵ), including those referred to above. They include a corresponding result to a key theorem in the paper of Granville [11, Theorem 5]. As might be expected, the result is dependent on the polynomial degree parameter D which appears as a consequence of the use of a Belyi function [1]. For a restricted class of polynomials in $\mathbb{Z}[x]$ the use of a Belyi function is avoided and explicit parameter values obtained.

Also in Section 5 are included ABC-(k,ϵ) improved forms of the asymptotic generalized Fermat problem, the Browkin, Filaseta, Greaves, Schnitzel theorem on the square free values of cyclotomic polynomials, and Hall's conjecture giving a lower bound for $|u^3 - v^2|$ where u and v are integers.

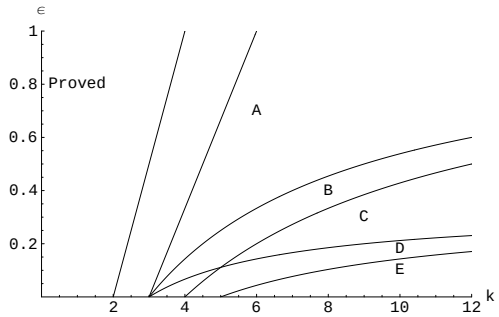

FIG. 1. Some (k, ϵ) regions where theorems are true.

Figure 1 describes the relative regions of the (k, ϵ) plain for which ABC-(k,ϵ) will imply some of the results proved in this paper. Points to the left of the leftmost line have ABC-(k,ϵ) already proved. Points to the right and below the other lines represent (k, ϵ) values where A: the asymptotic Fermat theorem is true, B: the asymptotic Catalan theorem is true, C: there exists an infinite number of non-Wieferich primes, D: there exist only finitely many consecutive triples of powerful numbers, and E: each cyclotomic polynomial has an infinite set of values which are square free. This shows a natural ordering between problems, in terms of their potential ease of solution.

In most of this paper the values of a,b and c, used in relationship to ABC-(k,ϵ), are assumed to be positive. This is without loss in generality.

The effect of these ideas is three fold. Firstly, any theorem of the form "ABC implies D" is improved if a proof "ABC-(k,ϵ) implies D" is obtained. The lower the values of k and larger the value of ϵ, the greater the improvement. Secondly, they offer a path to obtaining unconditional results from ABC based techniques, without having a proof of ABC itself, assuming that ABC-(k,ϵ), for low values of the parameter k and high values of ϵ, should be easier to prove (and more likely to be true). However proofs of the conjectures are expected to get progressively harder as values of k increase and ϵ decrease. Finally, the values of k and ϵ which are required to solve a given problem give, in a sense, a measure of the degree of difficulty of the problem, the smaller the value of k and larger the value of ϵ needed, the easier it should be to solve.

2. ASSOCIATED RELAXATIONS

There is also a related family of "continuous" weaker forms:

DEFINITION 2.1. Let t be a real number with $t \in (0, 1]$ and $\epsilon > 0$ be given. We say that the ABC-$[t, \epsilon]$ conjecture is satisfied if for all co-prime integers a and b with $abc \neq 0$ and $a + b = c$:

$$\max(|a|, |b|, |c|) \ll_{t,\epsilon} \theta_t(abc)^{1+\epsilon}$$

where the multiplicative function θ_t is defined by

$$\theta_t(n) = \prod_{p^\alpha || n} p^{\lfloor t\alpha \rfloor}.$$

The utility of these relaxations of ABC is being investigated.

3. LEMMAS

DEFINITION 3.1. Let $k \geq 2$ and let b be a k-free integer with $b = \prod_{p|b} p^{\alpha_p}$ being the standard prime factorization. Then the integer $\underline{b}$, defined by

$$\underline{b} = \prod_{p|b} p^{k-\alpha_p}$$

is also k-free. If $k = 2$ then $b = \underline{b}$. We call $\underline{b}$ the k-conjugate of b.

The following lemma is given without proof. The results are straightforward consequences of the definitions of ρ_k, η_k and N.

LEMMA 3.1.
For integers $l \geq 1$ and $k \geq 2$:

1. $\max\{N(n), n^{\frac{1}{k}}\} \leq \eta_k(n) \leq n^{\frac{1}{k}} N(n)^{\frac{k-1}{k}}$.
2. $n^{\frac{1}{k}} = \eta_k(n)$ *if and only if* n *is a k'th power.*
3. $\eta_k(n) = n$ *if and only if* n *is square free.*
4. *If* n *is k-free then* $\eta_k(n) = N(n)$.
5. *If* n *is k-full then* $N(n) \leq n^{\frac{1}{k}}$.
6. *If* n *is k-full then* $\eta_k(n) \leq n^{\frac{2}{k+1}}$.
7. *If* n *is f-full and* $2 \leq f$ *then* $\eta_k(n) \leq n^{\frac{1}{k}+\frac{k-1}{fk}}$.
8. $\eta_k(n^l) \leq n^{\frac{l}{k}} N(n)^{\frac{k-1}{k}}$.
9. *If* $1 \leq l \leq k$ *then* $\eta_k(n^l) \leq n$.
10. $\eta_k(ab) \mid \eta_k(a)\eta_k(b)$ *and for all* $l \geq 1$, $\eta_k(a^l) \mid \eta_k(a)^l$.
11. *If* $a \mid b$ *then* $\eta_k(a) \mid \eta_k(b)$.
12. *For all* a *and* b, $\eta_k(ab) \leq \eta_k(a)\eta_k(b)$.
13. $\eta_k(n^l) = n^{\lfloor \frac{l}{k} \rfloor} \eta_k(n^{l \bmod k})$ *where* $l \bmod k$ *denotes the non-negative remainder when* l *is divided by* k.
14. *For all* a *and* b, $\eta_k(a)\eta_k(b) \leq \eta_k(ab)N((a,b))^2$ *where* (a,b) *is the greatest common divisor.*
15. *For all* a, b *and* c, $\eta_k(abc) \geq \frac{\eta_k(a)\eta_k(b)\eta_k(c)N((a,b,c))^2}{(N((a,c)N((a,b))N((b,c)))^2}$.
16. $\eta_k(n) = \rho_k(n)(b\underline{b})^{1/k}$ *where* $n = a^k b$ *with* b *k-free.*

LEMMA 3.2. *If* c *is a k-free unitary divisor of* n *(i.e.* $(c, n/c) = 1$*) then*

$$\eta_k(n) \geq \frac{n^{1/k} N(c)}{c^{1/k}}.$$

Proof. If $n = cd$ with $(c, d) = 1$ then

$$\eta_k(n) = \eta_k(c)\eta_k(d) \geq N(c)d^{1/k} = \left(\frac{n}{c}\right)^{1/k} N(c).$$

∎

LEMMA 3.3. *If $a^k \mid n$ then*

$$\eta_k(n) \leq \frac{n}{a^{k-1}}.$$

Proof. If $n = a^k m$ then

$$\eta_k(n) = \eta_k(a^k m) = a\eta_k(m) \leq am = \frac{n}{a^{k-1}}.$$

∎

4. RELATIONSHIP WITH THE ABC CONJECTURE

Observations: (1) ABC-(k, ϵ_1) implies ABC-(k, ϵ_2) for $\epsilon_1 \leq \epsilon_2$ and ABC-(k', ϵ_1) for $2 \leq k' \leq k$.

(2) If the ABC conjecture is true then ABC-(k, ϵ) is true for all $k \geq 2$ and all $\epsilon > 0$, and the implied constant depends only on ϵ. If ABC-(k,ϵ) is true, with the implied constant depending only on ϵ, then ABC is true.

(3) The same example which shows that in the ABC conjecture, ϵ cannot be taken as 0, provides a limitation on ABC-(k,ϵ), namely the statement there exists a $C > 0$ (independent of k) such that for all $k \geq 2$ and all a, b with $(a, b) = 1$,

$$a + b \leq C\eta_k(ab(a + b)).$$

To see this, for $n = 1, 2, \ldots$ let $k = 2^n$, and define an odd integer u_n by the equation

$$2^{n+2}u_n + 1 = 3^{2^n}.$$

If there was a C so that the above relationship was true, then

$$\begin{aligned} 3^{2^n} &\leq C\eta_{2^n}(2^{n+2}u_n)\eta_{2^n}(3^{2^n}) \\ &\leq C \cdot 3 \cdot 2^{\lceil \frac{n+2}{2^n} \rceil} \eta_{2^n}(u_n) \\ &\leq 3 \cdot C \cdot 2^{\lceil \frac{n+2}{2^n} \rceil} \frac{3^{2^n}}{2^{n+2}} \end{aligned}$$

so therefore $2^{n+2} \leq 6C$, which is false for $n \geq n_o$.

THEOREM 4.1. *If a, b are coprime positive integers and $\frac{k}{2} \leq 1+\epsilon$ then*

$$a+b \leq \sqrt{2}\eta_k(ab(a+b))^{1+\epsilon},$$

that is to say, ABC-(k,ϵ) is true for values of k and ϵ satisfying the inequality.

Proof. Since $a+b \leq 2ab$ we have $a+b \leq 2\eta_k(a)^k\eta_k(b)^k$, by Lemma 3.1(1), so therefore $(a+b)^2 \leq 2\eta_k(ab(a+b))^k$. The result follows by taking square roots. ▌

This shows that ABC-(2,ϵ) is true for all $\epsilon > 0$, and that ABC-(3,1/2) and ABC-(4,1) are also true. If considered in the first quadrant of the x, y plane with $x = k$ and $y = 1/\epsilon$, the equation $\frac{k}{2} = 1+\epsilon$ is a rectangular hyperbola with vertical asymptote through $x = 2$. The points on or under this curve correspond to values of (k, ϵ) for which ABC may be regarded as "the trivial case".

5. CONSEQUENCES OF ABC-(k,ϵ)

5.1. Fermat and extensions

Of course the unconditional full Fermat Last Theorem was proved by Wiles and Taylor [23]. A small value of k large epsilon values are all that is needed using ABC-(k,ϵ):

THEOREM 5.1. *(asymptotic Fermat) Assume ABC-(k,ϵ) for some $k \geq 4$ and $\epsilon > 0$ which satisfy $\epsilon < \frac{k}{3} - 1$. Then there exists a positive integer $n_o \geq 3$ such that the equation $x^n + y^n = z^n$ has no solution in positive integers with $(x, y) = 1$ for any $n \geq n_o$.*

Proof. Then for all a, b with $(a, b) = 1$,

$$(a+b)^{\frac{1}{1+\epsilon}} \ll_{k,\epsilon} \eta_k(a)\eta_k(b)\eta_k(a+b).$$

If $x^n + y^n = z^n$ let $x^n = a$ and $y^n = b$ so

$$z^{\frac{n}{1+\epsilon}} \ll \eta_k((xyz)^n) \leq z^{\frac{3n}{k}}z^3 \text{ by Lemma 3.1 (8).}$$

Hence $z^{\frac{n}{1+\epsilon} - \frac{3n}{k} - 3} \ll_{k,\epsilon} 1$ which is false for $z > 1$ and $n > n_o$, since the exponent of z can be written $n((\frac{k}{3} - 1) - \epsilon)/(3k(1+\epsilon)) - 3$. ▌

Note that the pair (k, ϵ) which satisfies the inequality in the theorem statement with k minimal and for that k is (4,ϵ) with $\epsilon < 1/3$.

THEOREM 5.2. *(Asymptotic Beale) Assume ABC-(k,ϵ) for some $k \geq 2$ and $\epsilon > 0$ and positive integers r, s, t which satisfy*

$$(k-1)(\frac{1}{r}+\frac{1}{s}+\frac{1}{t})+3 < \frac{k}{1+\epsilon}.$$

Then the equation $x^r + y^s = z^t$ has at most a finite number of solutions with $(x, y) = 1$.

Proof. First note that $x \leq z^{\frac{t}{r}}$ and $y \leq z^{\frac{t}{s}}$. From ABC-(k,ϵ)with $a = x^r$ and $b = y^s$ it follows from Lemma 3.1 (8) that

$$\begin{aligned} z^{\frac{t}{1+\epsilon}} &\ll \eta_k(x^r)\eta_k(y^s)\eta_k(z^t) \\ &\ll x^{\frac{r}{k}} y^{\frac{s}{k}} z^{\frac{t}{k}} (xyz)^{\frac{k-1}{k}} \\ &\ll z^{(1-\frac{1}{k}+\frac{r}{k})\frac{t}{r}+(1-\frac{1}{k}+\frac{s}{k})\frac{t}{s}+(1-\frac{1}{k}+\frac{t}{k})}. \end{aligned}$$

It follows from this equation that $z^{t(\frac{1}{1+\epsilon}-\frac{3}{k}-\frac{k-1}{k}(\frac{1}{r}+\frac{1}{s}+\frac{1}{t}))} \ll 1$. ∎

An unconditional proof of Catalan's conjecture has been provided by Mihăilescu [14]. See also [2]. The asymptotic form of the theorem was proved earlier by Tijdeman [22]. The proof of the asymptotic case based on ABC-(k,ϵ) is quite straight forward:

THEOREM 5.3. *(Asymptotic Catalan) Assume ABC-(k,ϵ) with*

$$\frac{2}{k}+\frac{1}{2} < \frac{1}{1+\epsilon}.$$

Then the equation $x^p - y^q = 1$ has at most a finite number of solutions in positive integers p, q, x and y when $p, q > 1$.

Proof. Assume $x, y \geq 2$ and $p, q \geq 4$. Then by Lemma 3.1 (1), there is a constant $K > 0$ such that

$$x^{\frac{p}{1+\epsilon}} \leq K x^{\frac{p}{k}+1} y^{\frac{q}{k}+1}.$$

Since $x^p > y^q$ the inequality

$$y^{\frac{q}{1+\epsilon}} \leq K x^{\frac{p}{k}+1} y^{\frac{q}{k}+1}$$

also holds. Take logarithms of both inequalities and add to obtain

$$\frac{p}{1+\epsilon}\log x + \frac{q}{1+\epsilon}\log y \leq 2\log K + 2(\frac{p}{k}+1)\log x + 2(\frac{q}{k}+1)\log y.$$

It follows that

$$(\frac{p}{1+\epsilon} - 2\frac{p}{k} - 2)\log x + (\frac{q}{1+\epsilon} - 2\frac{q}{k} - 2)\log y \leq 2\log K.$$

But because $p, q \geq 4$, it follows from the given inequality satisfied by k, ϵ that $p(\frac{1}{1+\epsilon} - \frac{2}{k}) > 2$ with a similar inequality holding with p replaced by q. So the coefficients of $\log x$ and $\log y$ are positive and they can be replaced by their lower bound $\log 2$ leading to

$$(p+q)(\frac{1}{1+\epsilon} - \frac{2}{k}) \leq 2\frac{\log K}{\log 2} + 4.$$

Thus, there are only a finite number of exponents (p, q) for which the Catalan equation has a solution. By Mordell's theorem, for fixed (p, q) the equation has at most a finite set of integral solutions. Therefore the equation has only a finite set of integral solutions. ▌

Note that the pair (k, ϵ) with k minimal satisfying the inequality in the theorem statement has $k = 5$ and $\epsilon < 1/9$.

The following should be compared with the theorem of Darmon and Granville [8].

THEOREM 5.4. *(Generalized Fermat) Assume ABC-(k,ϵ). If a, b, c, r, s, t are fixed strictly positive integers with a, b, c co-prime and*

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} + \frac{3}{k} < \frac{1}{1+\epsilon}$$

then the equation

$$ax^r + by^s = cz^t$$

has at most a finite number of solutions x, y, z in strictly positive co-prime integers.

Proof. Use Lemma 2.4 (1,8,12) and apply ABC-(k,ϵ) to $u + v$ where $u = a^r$ and $v = b^y$. The implied constants depend on $a, b, c, r, s, t, k, \epsilon$:

$$\begin{aligned} cz^t &\ll \eta_k(ax^r by^s cz^t)^{1+\epsilon} \\ c^{\frac{1}{1+\epsilon}} z^{\frac{t}{1+\epsilon}} &\ll \eta_k(ax^r)\eta_k(by^s)\eta_k(cz^t) \\ &\ll \eta_k(a)\eta_k(b)\eta_k(c)x^{\frac{r}{k}} xy^{\frac{s}{k}} yz^{\frac{t}{k}} z. \end{aligned}$$

But $x \leq (\frac{c}{a}z^t)^{1/r}$ and $y \leq (\frac{c}{b}z^t)^{1/s}$ so therefore:

$$z^{\frac{t}{1+\epsilon}} \ll z^{[1+\frac{t}{k}+(1+\frac{r}{k})\frac{t}{r}+(1+\frac{s}{k})\frac{t}{s}]}$$

and hence

$$z^{t[\frac{1}{1+\epsilon}-(\frac{1}{r}+\frac{1}{s}+\frac{1}{t})-\frac{3}{k}]} \ll 1.$$

The result follows. ∎

5.2. Wieferich Primes

THEOREM 5.5. *(Wieferich Primes) Assume ABC-(k,ϵ) where $k \geq 2$ and $\epsilon > 0$ are such that*

$$\frac{1}{2} + \frac{3}{2k} < \frac{1}{1+\epsilon}.$$

Then there exists an infinite number of non-Wieferich primes. That is to say, primes p such that $p^2 \nmid 2^{p-1} - 1$.

Proof. First note that, by [15, Lemma 5.1], if p is an odd prime and there exists an $n \in \mathbb{N}$ such that $2^n = 1 \bmod p$ but $2^n \neq 1 \bmod p^2$ then p is non-Wieferich.

Let $n \in \mathbb{N}$ and write $2^n - 1 = u_n v_n$ where v_n is the maximal powerful divisor of $2^n - 1$. Then u_n is square free and $(u_n, v_n) = 1$. If $p \mid u_n$ then $2^n \equiv 1 \bmod p$ but $2^n \not\equiv 1 \bmod p^2$ since u_n is square free. So all the prime divisors of u_n are non-Wieferich.

Assume that there are only a finite number of non-Wieferich primes. Then the set of all possible u_n is finite also (and thus bounded) and the set of v_n must therefore be infinite. This also implies there is a constant $c > 0$ such that for all $n \in \mathbb{N}$

$$c2^n < v_n < 2^n \ (1).$$

Write $a = 2^n - 1$ and $b = 1$ so $a + b = 2^n$. By ABC-(k,ϵ):

$$\begin{aligned} 2^{\frac{n}{1+\epsilon}} &\ll \eta_k(2^n)\eta_k(u_n v_n) \\ &\ll 2^{\frac{n}{k}}\eta_k(2^{n \bmod k})\eta_k(u_n)\eta_k(v_n) \\ &\ll 2^{\frac{n}{k}} u_n {v_n}^{\frac{1}{k}} {v_n}^{\frac{k-1}{2k}} \text{ using Lemma 3.1 (7)} \\ &\ll 2^{\frac{n}{k}} {v_n}^{\frac{1}{2}+\frac{1}{2k}}. \end{aligned}$$

Hence, using equation (1)

$$2^{\frac{n}{1+\epsilon}} \ll 2^{n(\frac{1}{2}+\frac{3}{2k})}$$

and therefore

$$2^{n(\frac{1}{1+\epsilon}-(\frac{1}{2}+\frac{3}{2k}))} \ll 1.$$

Hence the set of n's is finite, which is a contradiction, since the set of v_n is infinite. Therefore the number of non-Wieferich primes is infinite. ∎

Note that the inequality in the theorem statement is satisfied minimally with $k = 4$ provided $\epsilon < 1/7$.

The next theorem comes from that of Silverman, who used the full ABC conjecture to derive a result which is more general than the previous theorem.

THEOREM 5.6. *(Generalized Wieferich Primes) Let $a \in \mathbb{Z} \setminus \{\pm 1\}$. Assume ABC-(k,ϵ) with*

$$\frac{1}{1/\epsilon + 1} + \frac{1}{k} \leq \frac{\log 2}{24 \log a}.$$

Then there exist an infinite number of primes p such that

$$a^{p-1} \not\equiv 1 \bmod p^2.$$

Proof. We need only consider [17, Silverman, Lemma 7] in the special case $b = 1, \alpha = a/1, a \geq 3$ and adopt the same meaning for c, ϵ_1 (Silvermans's ϵ) and δ as used in that proof. Then an inspection of the proof of [18, Silverman, Lemma 5.4] shows that in this case the inequality

$$|\Phi_n(a, 1)| \geq e^{c\phi(n)}$$

can assume the form $|\Phi_n(a)| \geq 2^{\phi(n)/2} = e^{c\phi(n)}$, where $c = \log 2/2$, since $||a| - 1| \geq 2$.

Now apply ABC-(k, ϵ) to $a^n = 1 + u_n v_n$, where v_n is the powerful part of $a^n - 1$:

$$\begin{aligned}
a^{\frac{n}{1+\epsilon}} &\ll_\epsilon \eta_k(a^n u_n v_n) \\
&\leq a^{\frac{n}{k}+1} \eta_k(u_n)\eta_k(v_n) \text{ using Lemma 3.1 (8,12)} \\
a^{n(\frac{1}{1+\epsilon})} &\ll_{\epsilon,a} a^{n/k}\eta_k(u_n)\eta_2(v_n) \\
&\ll_{\epsilon,a} \frac{a^{n+n/k}}{v_n} v_n^{2/3} \text{ using Lemma 3.1 (6).}
\end{aligned}$$

Therefore

$$v_n \ll_{\epsilon,a} a^{3n(\frac{1}{1/\epsilon+1}+\frac{1}{k})}$$

Choose $\delta = \frac{1}{2}$ and $\epsilon_1 = \log 2/(8 \log a)$ and (k, ϵ) so that

$$3(\frac{1}{1/\epsilon+1} + \frac{1}{k}) \leq \frac{\log 2}{8 \log a}.$$

∎

5.3. Powerful Numbers

THEOREM 5.7. *(Erdös conjecture [9]) Assume ABC-(k,ϵ) with k even and with $k \geq 2$ and $\epsilon > 0$ satisfying*

$$\frac{3}{2} + \frac{3}{2k} < \frac{2}{1+\epsilon}.$$

Then there exist only finitely many triples of consecutive powerful numbers.

Proof. Let $n-1, n, n+1$ be powerful. Then

$$\begin{aligned}
\eta_k(n^2) &= \prod_{p|n} p^{\lceil \frac{2\alpha}{k} \rceil} \\
&= \eta_{k/2}(n) \\
&\leq n^{\frac{2}{k}} N(n)^{\frac{k-2}{k}} \text{ by Lemma 3.1 (1)} \\
&\leq n^{\frac{2}{k}} (\sqrt{n})^{\frac{k-2}{k}} \\
&= n^{\frac{1}{2}+\frac{1}{k}}.
\end{aligned}$$

Therefore $\eta_k(n^2) \leq n^{\frac{1}{2}+\frac{1}{k}}$. Call this (1).
Also $l = (n-1)(n+1)$ is powerful so

$$\begin{aligned}
\eta_k(l) &\leq l^{\frac{1}{k}} N(l)^{\frac{k-1}{k}} \text{ by Lemma 3.1 (1)} \\
&\leq l^{\frac{1}{k}} \sqrt{l}^{\frac{k-1}{k}} \\
&= l^{\frac{1}{2}+\frac{1}{2k}}.
\end{aligned}$$

Hence

$$\begin{aligned}
\eta_k((n-1)(n+1)) &\leq ((n-1)(n+1))^{\frac{1}{2}+\frac{1}{2k}} \\
&\leq (n^2)^{\frac{1}{2}+\frac{1}{2k}} \\
&= n^{1+\frac{1}{k}}.
\end{aligned}$$

Therefore $\eta_k(l) \leq n^{1+\frac{1}{k}}$. Call this (2).

Now apply ABC-(k,ϵ) with $a = n^2 - 1, b = 1, a + b = n^2$ and use (1) and (2) to derive

$$n^{\frac{2}{1+\epsilon}} \leq K n^{\frac{3}{2}+\frac{3}{2k}}$$

so $[\frac{2}{1+\epsilon} - (\frac{3}{2} + \frac{3}{2k})] \log n \leq \log K$ and therefore the set of all possible n's is bounded. ▌

Note that the inequality in the theorem statement satisfied by minimal k has $k = 4$ and then $\epsilon < 1/15$ is required.

THEOREM 5.8. *Assume ABC-(k,ϵ) with a positive integer f satisfying*

$$2(1 + \epsilon)(f + k - 1) < fk.$$

Then there exists at most a finite number of pairs of successive f-full numbers.

Proof. Let x and $x + 1$ be successive f-full numbers. Then

$$\begin{aligned} x^{\frac{1}{1+\epsilon}} &\ll \eta_k(x)\eta_k(x+1) \\ &\leq x^{\frac{1}{k}+\frac{k-1}{fk}}(x+1)^{\frac{1}{k}+\frac{k-1}{fk}} \text{ by Lemma 3.1 (7)} \\ &\ll x^{2(\frac{1}{k}+\frac{k-1}{fk})}. \end{aligned}$$

Since $fk > 2(1 + \epsilon)(f + k - 1)$ it follows that

$$\frac{1}{1+\epsilon} > 2(\frac{1}{k} + \frac{k-1}{fk}).$$

Hence the set of values of x must be finite. ▌

The selection $f = 5, k = 3, \epsilon < 1/14$ satisfies the inequality of the theorem. Reciprocally, $f = 3, k = 5, \epsilon < 1/14$ is also sufficient.

Successive powerful numbers are quite rare. In a computer search of numbers up to $12 * 10^6$ the following 10 were found. The first element of each list is n where $(n, n + 1)$ are a powerful pair. The next integer is the power of n, being the minimum α such that $p^\alpha \| n$ for all $p \mid n$. The final integer is the power of $n + 1$. For example $\{12167, 3, 2\}$ means each prime dividing 12167 has order 3 or more and each prime dividing 12168 has order 2 or more:

{8, 3, 2}, {288, 2, 2}, {675, 2, 2}, {9800, 2, 2}, {12167, 3, 2}, {235224, 2, 2}, {332928, 2, 2}, {465124, 2, 2}, {1825200, 2, 2}, {11309768, 2, 2}.

THEOREM 5.9. *Assume ABC-(k,ϵ) with, for some $f \geq 2$*

$$3(1+\epsilon)(f+k-1) < fk.$$

Then the number of pairs of positive integers (a,b) with $(a,b) = 1$, and such that a, b and $a+b$ are all f-full is finite.

Proof. Use Lemma 3.1 (7):

$$\begin{aligned}(a+b)^{\frac{1}{1+\epsilon}} &\ll \eta_k(ab(a+b)) \\ &\ll (ab)^{\frac{1}{k}+\frac{k-1}{fk}}(a+b)^{\frac{1}{k}+\frac{k-1}{fk}} \\ (ab)^{\frac{1}{2}(\frac{1}{1+\epsilon}-\frac{1}{k}-\frac{k-1}{fk})} &\ll (ab)^{\frac{1}{k}+\frac{k-1}{fk}} \\ (ab)^{\frac{1}{1+\epsilon}-\frac{3}{k}-\frac{3(k-1)}{fk}} &\ll 1.\end{aligned}$$

And the result follows. ∎

Note that $f = 6$, $k = 6$, $\epsilon < 1/11$ is a set of choices which will satisfy the inequality in the theorem statement.

5.4. Polynomial Values

A key to Theorem 6.11 below is the use of a Belyi function [1] to prove the following theorem, A proof of which is given in [11].

THEOREM 5.10. *Let $f(x,y) \in \overline{\mathbb{Q}}[x,y]$ be homogeneous with no repeated factors. Then there exist homogeneous polynomials a(x,y), b(x,y) and c(x,y), with a and b having the same degree $D \geq 1$ and c degree less than or equal to D, with no common factors (in $\overline{\mathbb{Q}}$), where the polynomial $a(x,y)b(x,y)c(x,y)$ has exactly $D+2$ non proportional linear factors (in $\overline{\mathbb{Q}}$), including all of the factors of $f(x,y)$, $f(x,y) \mid a(x,y)b(x,y)c(x,y)$ and*

$$a(x,y) + b(x,y) = c(x,y).$$

The following corresponds to [11, Theorem 5].

THEOREM 5.11. *Assume ABC-(k,μ). Let $f(x,y) \in \mathbb{Z}[x,y]$ be homogeneous with no repeated factors. Let D be the degree referred to Theorem 6.10 stated above. Then if m,n are any two co-prime integers:*

$$\max(|m|,|n|)^{\deg(f)-2-\frac{D(2+\frac{k}{1/\mu+1})}{k-1}} \ll_{k,\mu,f} N(f(m,n)).$$

Proof. By clearing denominators if necessary, there is a polynomial $h(x,y)$ in $\mathbb{Z}[x,y]$ such that $a(x,y)b(x,y)c(x,y) = f(x,y)h(x,y)$.

Let m,n be integers with $(m,n) = 1$ and let $d = gcd(a(m,n), b(m,n))$.

Apply ABC-(k,μ) to the equation $a(m,n)/d + b(m,n)/d = c(m,n)/d$:

$$\max(|a(m,n)/d|, |b(m,n)/d|)^{1-1/(1/\mu+1)} \ll_{k,\mu} \eta_k(a(m,n)b(m,n)c(m,n)/d^3).$$

Since $a(x,y)$ and $b(x,y)$ have no common factors, their resultant is a non-zero integer, which is a multiple of the integer d. Therefore d is bounded, with the bound dependent only on f ($d \ll_{a,b} 1$), and using Lemma 3.1 (1) we can write:

$$\max(|a(m,n)|, |b(m,n)|)^{1-1/(1/\mu+1)} \ll_{k,\mu,f} \eta_k(a(m,n)b(m,n)c(m,n))$$

$$\ll_{k,\mu,f} (a(m,n)b(m,n)c(m,n))^{1/k} N(a(m,n)b(m,n)c(m,n))^{\frac{k-1}{k}}.$$

Now let $H = \max(|m|, |n|)$. Then the argument in [11, Theorem 5] shows that $\max(|a(m,n)|, |b(m,n)|) \gg H^D$. Let the product of the linear factors of $a(x,y)b(x,y)c(x,y)$ be $f(x,y)g(x,y)$. Then $|g(m,n)| \ll H^{D+2-\deg f}$ so therefore:

$$(H^D)^{1-1/(1/\mu+1)} \ll_{k,\mu,f} H^{\frac{3D}{k}+(D+2-\deg f)\frac{k-1}{k}} N(f(m,n))^{\frac{k-1}{k}}.$$

This inequality readily simplifies to:

$$H^{\deg f - 2 - \frac{D(2+k/(1/\mu+1))}{k-1}} \ll N(f(m,n)).$$

∎

The same definition $f(x,y) = y^{\deg g+1} g(x/y)$ used by Granville [11, Corollary 1], enables the following to be deduced:

THEOREM 5.12. *Assume ABC-(k,μ). Let $g(x) \in \mathbb{Z}[x]$ have no repeated factors. Let D be the degree referred to in Theorem 6.10 stated above. Then if m is any integer:*

$$|m|^{\deg(g) - 1 - \frac{D(2+k/(1/\mu+1))}{k-1}} \ll_{k,\mu,g} N(g(m)).$$

Application of these theorems awaits an investigation of the relationship between D and other problem parameters such as the $\deg f$ or $\deg g$.

For a class of univariate polynomials it is possible to avoid use of Belyi's theorem. These polynomials include some of those used in deriving number theory results from ABC by Granville [11]. The class is all polynomials $f(x) \in \mathbb{Z}[x]$ such that there exist a set of distinct integers $a_1, \cdots, a_n$ with

$$f(x) = \prod_{j=1}^{n}(x - a_j).$$

THEOREM 5.13. *Let $f(x)$ be a polynomial in the given class. Assume ABC-(k,μ). If the degree of $f(x)$ is even define d by* $\deg f = 2d$. *Then for all integers m*

$$|m|^{\frac{k}{k-1} - d(\frac{2}{k-1} + \frac{k}{(k-1)(1/\mu+1)})} \ll_{k,\mu,f} N(f(m)).$$

If the degree of $f(x)$ is odd let $\deg f = 2d + 1$. *Then for all integers m*

$$|m|^{\left(\frac{dk}{k-1}\right)\left((1+\frac{1}{d})(\frac{1}{1+\mu} - \frac{2}{k})-1\right)} \ll_{k,\mu,f} N(f(m)).$$

Proof. If $\deg f$ is even let

$$\begin{aligned} a(x) &= \prod_{j=1}^{d}(x - a_j) \\ b(x) &= -\prod_{j=d+1}^{2d}(x - a_j) \\ c(x) &= a(x) + b(x). \end{aligned}$$

Then $a(x)b(x)c(x) = f(x)h(x)$ and the degree of $h(x)$ is at most $d - 1$ since the degree of $c(x)$ is at most $d - 1$. The given formula follows in the same manner as the result of Theorem 6.11.

If $\deg f$ is odd let

$$\begin{aligned} a(x) &= \prod_{j=1}^{d+1}(x - a_j) \\ b(x) &= -(\prod_{j=d+2}^{2d}(x - a_j))(x - a_{2d+1})^2 \\ c(x) &= a(x) + b(x). \end{aligned}$$

Then the product of the distinct linear factors of $a(x)b(x)c(x)$ is $f(x)h(x)$ and the degree of $h(x)$ is at most d. Again, the given formula follows in the same manner as the result of Theorem 6.11. ▌

Note that in the even degree case the exponent is positive if and only if

$$\frac{2}{k} + \frac{1}{1/\mu + 1} < \frac{1}{d}.$$

For degree 4 the minimum value of k is 5 and then $1/\mu > 9$ is required.

In the odd degree case it is positive when

$$2 + \frac{k}{1 + 1/\mu} < \frac{1}{d+1}.$$

For degree 3 the minimum value of k is 4 and $1/\mu > 9$.

In attempting to use the above theorem, which does not have the disadvantage of the parameter D, to obtain an improvement of [11, Theorem 5] the best result that could be obtained was the following: If $g(x) \in \mathbb{Z}[x]$ has integer factors and no repeated roots, then if $q^2 \mid g(m)$,

$$q \ll_{g,\epsilon} |m|^{\deg g - 1 - \eta(k,\mu)}$$

where $\eta(k, \mu)$ is an explicit function of k and μ with expected asymptotic behavior.

The following proof is based on that of Browkin, Filaseta, Greaves and Schinzel [6] who use the full ABC conjecture.

THEOREM 5.14. *(Square free values of cyclotomic polynomials) Assume ABC-(k,ϵ). For every positive integer $n \geq 2$ for which the inequality*

$$\frac{n^2}{1/\epsilon + 1} + \frac{n^2 + 1}{k} < 1$$

is satisfied, there exist infinitely many integers l for which the cyclotomic polynomial $\Phi_n(l)$ is square free.

Proof. Fix $n > 1$ and let $F(x) = x(x^{n^2} - 1)$. Then the argument of Browkin et al [6, Theorem 3], shows that there are an infinite number of integers t such that if p is a prime with $p \leq t$ then $p^2 \nmid F(t)$. We claim that if t is sufficiently large with this property then one of the numbers $\Phi_n(t)$ or $\Phi_n(t^n)$ is square free.

Assume that neither is square free and let $a = t^{n^2}-1, b = 1$ so $a+b = t^{n^2}$. There exists a polynomial $g(x)$ with integer coefficients such that

$$F(x) = \Phi_n(x)\Phi_{n^2}(x)g(x).$$

By the assumption there exist primes p and q such that $p^2 \mid \Phi_n(t)$ and $q^2 \mid \Phi_{n^2}(t)$ so $(pq)^2 \mid F(t)$. Since for all $p \leq t$, $p^2 \nmid F(t)$, both $p > t$ and $q > t$. Therefore, $N(F(t)) \leq F(t)/(pq) < F(t)/t^2$. Hence, using Lemma 3.1 (8):

$$\begin{aligned} t^{\frac{n^2}{1+\epsilon}} &\ll \eta_k(ab(a+b)) = \eta_k(t^{n^2-1}F(t)) \\ &\ll ((t^{n^2}(t^{n^2}-1))^{1/k} N(F(t))^{\frac{k-1}{k}} \\ &\leq t^{\frac{2n^2}{k}} \big(\frac{F(t)}{t^2}\big)^{\frac{k-1}{k}}. \end{aligned}$$

But $\frac{F(t)}{t^2} < t^{n^2-1}$ so therefore

$$t^{1-\frac{1+n^2}{k}-\frac{n^2}{1/\epsilon+1}} \ll 1$$

for an infinite number of values of t, which is impossible.

Hence at least one of $\Phi_n(t)$ or $\Phi_{n^2}(t) = \Phi_n(t^n)$ is square free, so there exist an infinite number of square free values for $\Phi_n(x)$. ▌

Note that for $n = 2$ the smallest value of k for which the inequality of the theorem statement is satisfied is $k = 6$ and then $\epsilon = 1/23$ is required.

5.5. Hall's Conjecture

THEOREM 5.15 (Hall's conjecture [12]). *Assume ABC-(k, μ). If*

$$\epsilon = \frac{3}{1/\mu + 1} + \frac{7}{2k}$$

then for every pair of integers u, v with $u^3 \neq v^2$,

$$|u^3 - v^2| \gg_{k,\mu} |u|^{\frac{1}{2}-\epsilon}.$$

Proof. (1) Assume $u^3 = a + v^2$ with $a > 0$ so $v < u^{3/2}$. Let $d = (u, v)$ be the greatest common divisor and apply ABC-(k, μ) to

$$\frac{u^3}{d^2} = \frac{a}{d^2} + \frac{v^2}{d^2}.$$

By Lemma 3.1 (11) $\eta_k(u^3/d^2) \le \eta_k(u^3)$ and we can make the following derivation:

$$\begin{aligned}
(\frac{u^3}{d^2})^{\frac{1}{1+\mu}} &\ll_{k,\mu} \eta_k(\frac{u^3}{d^2})\eta_k(\frac{v^2}{d^2})\eta_k(\frac{a}{d^2}) \\
\frac{u^{\frac{3}{1+\mu}}}{d^{\frac{2}{1+\mu}}} &\ll u^{1+\frac{2}{k}}(\frac{v}{d})^{\frac{2}{k}} N(\frac{v}{d})^{\frac{k-1}{k}} \cdot \frac{a}{d^2} \\
&\ll \frac{u^{1+2/k}v^{2/k}v^{(k-1)/k}}{d^{3+1/k}} \cdot a \\
&\ll \frac{u^{5/2+7/(2k)}}{d^{3+1/k}} \cdot a.
\end{aligned}$$

It follows that

$$u^{1/2-\epsilon} \ll a \cdot d^{2/(1+\mu)-3-1/k} \le a$$

where ϵ is defined in the theorem statement.

(2) Now assume $v^2 = a + u^3$, again with $a > 0$. Then there exists a minimal integer v_1 with $u^3 < v_1^2$. Let a_1 be defined by $v_1^2 = a_1 + u^3$, so $a_1 \le a$. Since $(v_1 - 1)^2 \le u^3$, we have $v_1 \sim u^{3/2}$. Now proceed as in 1. letting $d = (u, v_1)$ and applying ABC-(k,μ) to obtain the same inequality for a_1, and hence for a.

3. From (1) and (2) we obtain the result of the theorem. ▌

For this result to have any effect, we must have $k \ge 8$.

ACKNOWLEDGMENT

The contributions of Dorian Goldfeld who sparked the interest of the author in the ABC conjecture is gratefully acknowledged. Part of this work was done at the University of Waikato and part at Columbia University. The support of both institutions is also gratefully acknowledged.

REFERENCES

1. Belyi, G.V. *On galois extensions of maximal cyclotomic fields*, Math. U.S.S.R. Izvestija **14** (1980), 247-256.
2. Bilu, Y. F. *Catalan's conjecture [after Mihăilescu]*, Seminaire Bourbaki, 55eme annee, November 2002, 2002-2003, no 909, 1-25.
3. Broughan, K. A. *Restricted Divisor Sums.* Acta Arithmetica, **101** (2002), 105-114.
4. Broughan, K. A. *Asymptotic order of the square free part of n!* Integers: Electronic Journal of Combinatorial Number Theory **2**, (2002) A10, p1-6.
5. Broughan, K. A. *Relationships between the conductor in integer k'th roots*, International Journal of Pure and Applied Mathematics **5** (2003), 253-275.

6. Browkin, J., Filaseta, M., Greaves, G. and Schinzel, A. *Squarefree values of polynomials and the abc-conjecture*, in: Sieve Methods, Exponential Sums and their applications in number theory, Greaves, G. R. H et al. (eds.), Cambridge University Press, 1996, 65-85.
7. Browkin, J. *The abc-conjecture*, in: R. P. Bambah et al. (eds.), *Number Theory*, Birkhäuser, Basel, Trends in Mathematics (2000), 75-105.
8. Darmon, H. and Granville, A. *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$., Bull. London Math. Soc. **27** (1995), 513-543.
9. Erdös, P. *Problems and results on consecutive integers* Publ. Math. Debrecen, **23** (1976), 271-282.
10. Gegenbauer, L. *Asymptotische Gesetze der Zahlentheorie.* Denkschriften Akad. Wien **49** (1885), 37-80.
11. Granville, A. *ABC allows us to count squarefrees*, I.M.R.N. (1998) No. 19, 991-1009.
12. Hall, M. *The diophantine equation* $x^3 - y^2 = k$, Computers and Number Theory, ed. by A. O. L. Atkin and B. Birch, Academic Press, 1971, 173-198.
13. Lang, S. *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37-75.
14. Mihăilescu, P. *Primary cyclotomic units and and proof of Catalan's conjecture*, (preprint, 2002).
15. Nathanson, M. B. *Elementary Methods in Number Theory*, Springer-Verlag, 2000.
16. Nitaj, A. *La conjecture abc*, Enseignement Math. **42** (1996), 3-24.
17. Silverman, J. H. *Wierferich's criterion and the abc-conjecture*, J. of Number Theory **30** (1988) 226-237.
18. Silverman, J. H. *Integral points on curves and surfaces*, Journées Arithmétiques-Ulm, 1987, Lecture Notes in Mathematics, **1380** Springer-Verlag, 1990.
19. Stewart, C.L. and Tijdeman, *On the Oesterlé Masser Conjecture*, Mh. Math. **102** (1986). 251-257.
20. Stewart, C.L. and Kunrui, Yu, *On the abc conjecture*, Math. Ann. **291**, 225-230.
21. Stewart, C.L. and Kunrui, Yu, *on the abc conjecture II*, Duke Math. J. **108**, (2001), 169-181.
22. Tijdeman, R. *On the equation of Catalan*, Acta Arith. **29**, (1978), 197-209.
23. Wiles, A. *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), 443-551.