Functiones et Approximatio
XXXIX.1 (2008), 103–111

A WEAK EFFECTIVE *abc*-CONJECTURE

Jerzy Browkin

To Władysław Narkiewicz
on his 70th birthday

Abstract: We state an effective version of the *abc*-conjecture, and assuming it we describe all solutions of some diophantine equations. Based on this conjecture we give an effective algorithm for computing an infinite set of primes which are not Wieferich primes.
Keywords: *abc*-conjecture, equations of Ljunggren-Nagell, Catalan, Fermat, and Brocard-Ramanujan, Wieferich primes

1. Introduction

It is well known that assuming the *abc*-conjecture one can prove that some diophantine equations have only a finite number of solutions. In general no bound for the number of solutions or of their size can be obtained in this way. See, e.g. [12], and [13].

On the other hand, assuming a weak effective version of the *abc*-conjecture we can find all solutions of some diophantine equations. Such an approach has been discussed e.g. in [5].

In the present paper we propose a weak effective *abc*-conjecture with some real parameter $r > 1$, denoted by $abc(r)$. We prove that assuming $abc(r)$ with an appropriate r depending on the diophantine equation, all its solutions can be determined. It is interesting to observe that the minimal value of such r depends essentially on the equation in question.

2. Weak effective *abc*-conjecture

For a triple (a, b, c) of relatively prime positive integers satisfying $a + b = c$ define

$$L = L(a, b, c) := \frac{\log c}{\log \operatorname{rad}(abc)} ,$$

where for $m \in \mathbb{N}$ the radical $\operatorname{rad}(m)$ is the product of distinct prime factors of m.

Mathematics Subject Classification: 11D41.

The *abc*-conjecture says that $\limsup_{(a,b,c)} L(a,b,c) = 1$, where (a,b,c) runs over all triples as above.

It is known that $L(a,b,c) > 1$ for infinitely many triples (a,b,c). The maximal known value of L corresponds to the triple $(2,\ 3^{10}\cdot 109,\ 23^5)$ found by E. Reyssat. It equals

$$r_0 := \frac{\log(23^5)}{\log(2\cdot 3\cdot 109\cdot 23)} \approx 1.629912.$$

Lists of all triples (a,b,c) with $L > 1.4$ known at different times can be found in [6], [4], [9].

J. Kanapka [10] computed all triples satisfying $L(a,b,c) > 1.2$ and $c < 2^{30}$, next he extended his computations to $c < 2^{36}$.

Recently T. Dokchitser has found many new triples with $L > 1.4$ and $c > 2^{36}$, see [9]. One of his examples satisfies $L > 1.5$.

We give below the table of all triples (a,b,c) satisfying $L(a,b,c) > 1.5$ known to the author on April 2007.

No.	a	b	c	$\log_{10} c$	$L(a,b,c)$
1.	2	$3^{10}\cdot 109$	23^5	6.8	1.629912
2.	11^2	$3^2\cdot 5^6\cdot 7^3$	$2^{21}\cdot 23$	7.7	1.625991
3.	$19\cdot 1307$	$7\cdot 29^2\cdot 31^8$	$2^8\cdot 3^{22}\cdot 5^4$	15.7	1.623490
4.	283	$5^{11}\cdot 13^2$	$2^8\cdot 3^8\cdot 17^3$	9.9	1.580756
5.	1	$2\cdot 3^7$	$5^4\cdot 7$	3.6	1.567887
6.	7^3	3^{10}	$2^{11}\cdot 29$	4.8	1.547075
7.	$7^2\cdot 41^2\cdot 311^3$	$11^{16}\cdot 13^2\cdot 79$	$2\cdot 3^3\cdot 5^{23}\cdot 953$	20.8	1.544434
8.	5^3	$2^9\cdot 3^{17}\cdot 13^2$	$11^5\cdot 17\cdot 31^3\cdot 137$	13.0	1.536714
9.	$13\cdot 19^6$	$2^{30}\cdot 5$	$3^{13}\cdot 11^2\cdot 31$	9.8	1.526999
10.	$3^{18}\cdot 23\cdot 2269$	$17^3\cdot 29\cdot 31^8$	$2^{10}\cdot 5^2\cdot 7^{15}$	17.1	1.522160
11.	$13^{10}\cdot 37^2$	$3^7\cdot 19^5\cdot 71^4\cdot 233$	$2^{26}\cdot 5^{12}\cdot 1873$	19.5	1.509433
12.	239	$5^8\cdot 17^3$	$2^{10}\cdot 37^4$	9.3	1.502839

Weak effective *abc*-conjecture $abc(r)$: Let $r \geq 1.5$ be a fixed real number. Then all triples (a,b,c) satisfying $L(a,b,c) > r$ are in the table.

In particular, if $r \geq r_0$, where r_0 is the constant of Reyssat, then the conjecture $abc(r)$ says that no triple satisfies $L(a,b,c) > r$.

Of course, the conjecture $abc(1.5)$ can be disproved by giving a new triple (a,b,c) with $L > 1.5$ not appearing in the table. To disprove the conjecture $abc(r_0)$ it is necessary to find a triple (a,b,c) with $L > r_0$, which seems to be much more difficult.

Thus Conjecture 2 in [5] has been disproved when Dokchitser found a new example with $L > 1.5$ (Example no. 11 in the table).

3. The Nagell-Ljunggren equation

The equation is

$$\frac{x^n - 1}{x - 1} = y^q, \qquad \text{where} \quad x > 1,\ y > 1,\ n > 2,\ q \geq 2\,. \tag{3.1}$$

There are known three solutions of the equation:

$$\frac{3^5 - 1}{3 - 1} = 11^2, \quad \frac{7^4 - 1}{7 - 1} = 20^2, \quad \frac{18^3 - 1}{18 - 1} = 7^3\,. \tag{3.2}$$

The survey paper [7] contains the information on results concerning further solutions of (3.1). From theorems 1 and 14 of this paper we get

Proposition 3.1. *Let* (x, y, n, q) *be a solution of* (3.1) *distinct from* (3.2)*, and let* p *be an odd prime divisor of* n*. Then:*

(i) $q \neq 2,\ 4 \nmid n$,
(ii) $p = q \in \{17, 19, 23\}$ *or* $p \geq 29$,
(iii) If $q = 3$, *then* $p \geq 101$.

Theorem 3.1. *From the conjecture* $abc(r)$ *with* $r = \frac{145}{63} \approx 2.3$ *it follows that* (3.2) *are all solutions of* (3.1).

Proof. Assume that (x, y, n, q) is a solution of (3.1) distinct from (3.2). The equation (3.1) can be written in the form

$$1 + (x-1)y^q = x^n\,. \tag{3.3}$$

We consider the triple $(a, b, c) = (1, (x-1)y^q, x^n)$, which evidently satisfies the assumptions of the *abc*-conjecture.

From (3.1) it follows easily that $y^q > x^{n-1}$, then $y > x^{(n-1)/q}$. Next (3.3) implies that $(x-1)y^q < x^n$, hence

$$x(x-1)y < x^{n+1}/y^{q-1} < x^{(n+1)-(q-1)(n-1)/q} = x^{(2q+n-1)/q} < x^{(2q+n)/q}.$$

Therefore

$$\mathrm{rad}(abc) = \mathrm{rad}((x-1)yx) \leq x(x-1)y < x^{(2q+n)/q}\,.$$

Consequently

$$L = L(a,b,c) = \frac{\log c}{\log \mathrm{rad}(abc)} > \frac{n \log x}{((2q+n)/q) \cdot \log x} = \frac{qn}{2q+n} = \left(\frac{2}{n} + \frac{1}{q}\right)^{-1}.$$

Now, from Proposition 3.1 we get: If $q = 3$, then $n \geq p \geq 101$; hence

$$L > \left(\frac{2}{101} + \frac{1}{3}\right)^{-1} = \frac{303}{107} \approx 2.83.$$

If $q > 3$, then $q \geq 5$; hence $p = q \in \{17, 19, 23\}$ or $p \geq 29$. Therefore

$$L > \left(\frac{2}{17} + \frac{1}{17}\right)^{-1} = \frac{17}{3} \approx 5.67,$$

respectively,

$$L > \left(\frac{2}{5} + \frac{1}{29}\right)^{-1} = \frac{145}{63} \approx 2.3.$$

In all cases we obtain a contradiction with the $abc(r)$-conjecture with $r = \frac{145}{63} \approx 2.3$. ∎

4. Catalan's equation

The equation is

$$x^n - y^m = 1, \qquad \text{where} \quad \min(x, y, m, n) \geq 2\ . \tag{4.1}$$

There is known only one solution of (4.1):

$$3^2 - 2^3 = 1. \tag{4.2}$$

By old results of Chao Ko and Nagell (see [16, A6.2 and A7.3]) for every solution of (4.1) distinct from (4.2) we have $\min(m, n) \geq 5$.

Theorem 4.1. *From the $abc(r)$-conjecture with $r = \frac{35}{12} \approx 2.91$ it follows that* (4.2) *is the only solution of* (4.1).

Proof. Suppose that (x, y, m, n) is a solution of (4.1) distinct from (4.2). We can assume that m, n are distinct primes. By the above remark we have $\min(m, n) \geq 5$. The triple $(a, b, c) = (1, y^m, x^n)$ satisfies the assumptions of the abc-conjecture.

Since $y^m < 1 + y^m = x^n$, then $y < x^{n/m}$. Consequently

$$\operatorname{rad}(abc) = \operatorname{rad}(xy) \leq xy < x^{1+n/m}.$$

Hence

$$L(a, b, c) > \frac{n \log x}{(1 + n/m) \log x} = \frac{mn}{m + n} = \left(\frac{1}{m} + \frac{1}{n}\right)^{-1} \geq \left(\frac{1}{5} + \frac{1}{7}\right)^{-1} = \frac{35}{12} \approx 2.91.$$

We obtained a contradiction with the $abc(r)$-conjecture with $r = \frac{35}{12}$. ∎

Remark. Recently P. Mihăilescu proved [11] that the equation (4.1) has only one solution (4.2).

5. Fermat's equation

The equation is

$$x^n + y^n = z^n, \qquad \text{where} \quad x, y, z \in \mathbb{N},\ n \geq 3\ . \tag{5.1}$$

Theorem 5.1. *From the abc$(n/3)$-conjecture, where $n \geq 5$, it follows that the equation* (5.1) *has no solutions.*

Proof. It is well known that (5.1) does not have a solution for $n = 3$ and $n = 4$, see [17]. Assume that there is a solution (x, y, z) of (5.1) in relatively prime positive integers. The triple $(a, b, c) = (x^n, y^n, z^n)$ satisfies the assumptions of the *abc*-conjecture.

We have

$$\operatorname{rad}(abc) = \operatorname{rad}(xyz) \leq xyz < z^3.$$

Then

$$L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)} > \frac{n \log z}{3 \log z} = \frac{n}{3}.$$

We obtained a contradiction with the *abc*$(n/3)$-conjecture, since $\frac{n}{3} > r_0$ for $n \geq 5$. ■

Remark. A. Wiles proved unconditionally that (5.1) does not have a solution, see [21].

6. The Brocard-Ramanujan equation

The following equation has been considered by H. Brocard and later independently by S. Ramanujan (see [2], [3], [15]):

$$1 + n! = m^2\ . \tag{6.1}$$

Evidently, $(m, n) = (5, 4), (11, 5), (71, 7)$ satisfy (6.1). Ramanujan asked if there is a solution of (6.1) with $n > 7$. B. C. Berndt and W. F. Galway [1] proved that there is no other solution with $n \leq 10^9$.

Theorem 6.1. *From the abc(r)-conjecture with $r = 1.8$ it follows that there is no solution of* (6.1) *with $n > 7$.*

Proof. Assume that (m, n) is a solution of (6.1) and $n > 7$. The triple $(a, b, c) = (1, n!, m^2)$ satisfies the assumptions of the *abc*-conjecture. We have

$$\operatorname{rad}(abc) = \operatorname{rad}(m \cdot n!) \leq m \prod_{p \leq n} p < \sqrt{2n!}\ \prod_{p \leq n} p = \sqrt{2n!}\ \exp(\vartheta(n)),$$

where $\vartheta(n) = \sum_{p \leq n} \log p$.

Consequently

$$L(a,b,c) > \frac{\log(n!)}{\frac{1}{2}\log(2n!) + \vartheta(n)} = \frac{2}{\frac{\log 2}{\log n!} + 1 + \frac{2\vartheta(n)}{\log(n!)}}.$$

It is well known that $\vartheta(n) < 1.01624\,n$ (see [18]), and by the Stirling formula

$$\log(n!) > \log(\sqrt{2\pi n}\,(n/\mathrm{e})^n) > n(\log n - 1).$$

Therefore for $n > 10^9$ we get

$$\frac{\log 2}{\log(n!)} < \frac{\log 2}{n(\log n - 1)} < \frac{\log 2}{10^9(\log(10^9) - 1)} < 0.36 \cdot 10^{-10},$$

and

$$\frac{2\vartheta(n)}{\log(n!)} < \frac{2 \cdot 1.01624n}{n(\log n - 1)} < \frac{2 \cdot 1.01624}{\log(10^9) - 1} < 0.10305.$$

Consequently

$$L(a,b,c) > \frac{2}{0.36 \cdot 10^{-10} + 1 + 0.10305} > \frac{2}{1.10306} > 1.8.$$

We get a contradiction with the $abc(r)$-conjecture with $r = 1.8$. ■

Remark. The methods of proof of Theorem 6.1 can be applied to prove an analogous result for a more general equation $n! + A = m^2$ considered in [8] and [1].

7. Wieferich primes

A. Wieferich [20] proved that if an odd prime number p satisfies

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

then there are no solutions of the Fermat equation $x^p + y^p = z^p$ such that $p \nmid xyz$.

Let $g > 1$ be a rational number. We say that a prime number p is a Wieferich prime to the base g, if

$$g^{p-1} \equiv 1 \pmod{p^2}.$$

There are known only two Wieferich primes to the base $g = 2$, namely $p = 1093$ and $p = 3511$, see [17, p. 361].

J. H. Silverman [19] proved, assuming the *abc*-conjecture, that for every base g there are infinitely many prime numbers which are not Wieferich primes to the base g. More precisely, he proved that the number of these primes less than X is at least $c_g \log X$, where c_g is a positive constant depending on g.

Basing on the ideas of Silverman we prove

Theorem 7.1. *From the $abc(r)$-conjecture with $r = 1.75$ it follows that for every $g \in \mathbb{Q}$, $g > 1$, there are infinitely many prime numbers which are not Wieferich primes to the base g.*

Remark. We have chosen the constant $r = 1.75$ for simplicity. From the proof it will follow that 1.75 can be replaced by any number less than 2.

Let $g = \frac{r}{s}$, where $r > s > 0$, $\gcd(r, s) = 1$, and let q be a prime number. Put

$$\frac{r^q - s^q}{r - s} = U_q \cdot V_q \tag{7.1}$$

where $\gcd(U_q, V_q) = 1$, U_q is squarefree and V_q is powerfull, i.e. if a prime number t divides V_q, then $t^2 \mid V_q$.

First we prove a lemma.

Lemma 7.1 (cf. [19, Lemma 3]). *If a prime number p satisfies $p \nmid rs(r-s)$ and $p \mid U_q$, then*

$$g^{p-1} \not\equiv 1 \pmod{p^2},$$

i.e. p is not a Wieferich prime to the base $g = r/s$.

Proof. By the assumption $p \mid U_q$ and U_q is squarefree. Hence $p^2 \nmid U_q$. From (7.1) we get

$$g^q - 1 = \frac{r-s}{s^q} \cdot U_q V_q, \quad \text{consequently} \quad p \mid g^q - 1 \quad \text{and} \quad p^2 \nmid g^q - 1.$$

Therefore $g^q = 1 + up$, where $p \nmid u$. Hence

$$(g^q)^{p-1} = (1 + up)^{p-1} \equiv 1 + (p-1)up \equiv 1 - up \not\equiv 1 \pmod{p^2}.$$

It follows that $g^{p-1} \not\equiv 1 \pmod{p^2}$, i.e. p is not a Wieferich prime to the base g. ∎

Proof of theorem 7.1. The triple $(a, b, c) := ((r-s)U_q V_q, s^q, r^q)$ satisfies the assumptions of the *abc*-conjecture. Since V_q is powerfull we get

$$\operatorname{rad}(abc) = \operatorname{rad}(rs(r-s)U_q V_q) \le rs(r-s)U_q\sqrt{V_q} = \frac{rs(r^q - s^q)}{\sqrt{V_q}} < \frac{r^{q+2}}{\sqrt{V_q}}.$$

Consequently

$$L = L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)} > \frac{q \log r}{(q+2)\log r - \frac{1}{2}\log V_q}.$$

If $V_q > r^{8q/9}$, then $\log V_q > \frac{8q}{9}\log r$, hence

$$L > \frac{q}{(q+2) - 4q/9} = \frac{9q}{5q + 18} > 1.75 \quad \text{for } q > 126,$$

and we get a contradiction with the *abc*(1.75)-conjecture, provided $q > 126$. This last inequality we can assume from the beginning.

If $V_q \le r^{8q/9}$, then by (7.1) we get

$$U_q = \frac{r^q - s^q}{r - s} \cdot \frac{1}{V_q} \ge \frac{r^{q-1}}{r^{8q/9}} = r^{q/9-1}.$$

Therefore U_q is not bounded from above as $q \to \infty$.

It follows that for any fixed set of prime numbers $q_1, \dots, q_k$ there is a prime number q satisfying

$$r^{q/9-1} > rs(r-s) \cdot q_1 \cdots q_k.$$

Then $U_q > q_1 \cdots q_k$, and since U_q is squarefree it has such a prime factor p that $p \nmid rs(r-s)q_1 \cdots q_k$. It follows that $p \ne q_j$ for $j = 1, \dots, k$, and by Lemma 7.1 p is not a Wieferich prime to the base $g = r/s$.

Therefore there are infinitely many prime numbers which are not Wieferich primes to the base g. ■

Remark. The proof of Theorem 7.1 gives an effective algorithm for determining infinitely many prime numbers which are not Wieferich primes to the base g, under the assumption of the abc(1.75)-conjecture.

References

[1] B. C. Berndt, W. F. Galway, *On the Brocard-Ramanujan diophantine equation* $n! + 1 = m^2$, The Ramanujan Journ. **4** (2000), 41–42.
[2] H. Brocard, *Question 166*, Nouv. Corresp. Math. **2** (1876), 287.
[3] ———, *Question 1532*, Nouv. Ann. Math. **4** (1885), 391.
[4] J. Browkin, *The abc-conjecture*, in: Number Theory (R.P. Bambah et al. ed.) Trends in Mathematics, Birkhäuser, Basel (2000), 75–105.
[5] ———, *A consequence of an effective form of the abc-conjecture*, Colloq. Math. **82** (1999), no. 1, 79–84.
[6] J. Browkin, J. Brzeziński, *Some remarks on the abc-conjecture*, Math. Comp. **62** (1994), no. 206, 931–939.
[7] Y. Bugeaud, M. Mignotte, *L'équation de Nagell-Ljunggren* $\frac{x^n-1}{x-1} = y^q$, Enseign. Math. **48**, (2002), 147–168.
[8] A. Dąbrowski, *On the diophantine equation* $x! + A = y^2$, Nieuw Arch. Wisk. **14**, (1996), no. 3, 321–324.
[9] T. Dokchitser, *LLL & ABC*, J. Number Theory **107** (2004), 161–167.
[10] J. Kanapka, private communication.
[11] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
[12] A. Nitaj, *La conjecture abc*, Enseign. Math. **42** (1996), 3–24.
[13] ———, http://www.math.unicaen.fr/~nitaj/abc.html
[14] M. Overholt, *The diophantine equation* $n! + 1 = m^2$, Bull. London Math. Soc. **25** (1993), 104.
[15] S. Ramanujan, *Question 469*, J. Indian Math. Soc. **5** (1913), 59.
[16] P. Ribenboim, *Catalan's Conjecture*, Academic Press, 1994.

[17] ______, *Fermat's Last Theorem for Amateurs*, Springer Verlag, New York, 1999.

[18] J. Barkley Rosser, Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–89.

[19] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.

[20] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136**, (1909), 293–302.

[21] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995) no. 2, 443–551.

Address: Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, P.O. Box 21, PL-00-956 Warszawa, Poland

E-mail: browkin@euron.impan.gov.pl

Received: 27 April 2007; **revised:** 7 January 2008