THE ABC CONJECTURE AND PRIME DIVISORS OF THE LUCAS AND LEHMER SEQUENCES

RAM MURTY AND SIMAN WONG

1. Introduction

A straightforward consequence of Thue's pioneering work on Diophantine approximation [24] is: Let m be a non-zero integer and let $f \in \mathbf{Z}[x, y]$ be a binary form. Then the equation $f(x, y) = m$ has finitely many integer solutions, unless f is the multiple of either a power of a linear form, or a power of a binary quadratic form with positive nonsquare discriminant. Thue's techniques were refined by Pólya [15] and Siegel [18] to show that if $f \in \mathbf{Z}[x]$ has at least two distinct roots, then

$$P(f(x)) \to \infty \tag{1}$$

as $|x| \to \infty$, where $P(a)$ denotes the largest prime divisor of a non-zero integer a. Using the Gelfond-Baker method, Shorey, van der Poorten, Tijdeman and Schinzel [17] showed that if $f \in \mathbf{Z}[x, y]$ is a binary form with at least three distinct linear factors (over $\mathbf{C}$), then for any positive integer d and all pairs of integers x, y with $(x, y) = d$ and $\max(|x|, |y|) > e$,

$$P(f(x, y)) \gg_{f,d} \log\log \max(|x|, |y|). \tag{2}$$

with an effective constant. Using the so-called sharpening of Baker [2], in the case of binomials, Stewart [20] improved this to

$$P(ax^n - by^n) \gg_{a,b} \sqrt{n/\log n}.$$

Furthermore, if we let n run through the set S_κ of integers n with at most $\kappa \log\log n$ distinct prime divisors ($0 < \kappa < 1/\log 2$ fixed), Stewart ([21], [22]) showed that there exists an effective constant $C(\kappa, a, b) > 0$ such that

$$\frac{P(a^n - b^n)}{n} > C(\kappa, a, b)\frac{\log^{1-\kappa\log 2} n}{\log\log\log n}. \tag{3}$$

Ram Murty's research was supported in part by a Killam Research Fellowship and Bankers Trust Company Foundation by a grant to the Institute for Advanced Study. The first author also thanks Brown University where this work was initiated and the Institute for Advanced Study where it was completed.

(note that the set S_κ has density 1). There are also similar results when n is restricted to the set of primes. In 1962, Erdös [3, p. 218] conjectured that

$$\lim_{n\to\infty} \frac{P(2^n-1)}{n} = \infty. \tag{4}$$

While heuristic arguments (see section 4 below) suggest the stronger result

$$P(a^n-1) \overset{?}{\gg} a^{n^{1-\epsilon}}, \tag{5}$$

currently we do not even know that $P(a^n-b^n) > C(a,b)n^\theta$ for some $\theta > 1$. For more information on the history of these problems, see [3] and the introduction in Shorey et.al.[17].

Let $Q(n)$ denote the largest prime power divisor of n. Clearly, $Q(n) \geq P(n)$ and so a consequence of the conjecture of Erdös is that $Q(2^n-1)/n \to \infty$ as $n \to \infty$. In this paper, we prove this. In fact, we can prove a more general result:

Theorem 1. *For any $\epsilon > 0$ and any integers $a > b > 0$, we have $Q(a^n-b^n) \gg n^{2-\epsilon}$, where the implied constant depends on a, b and ϵ.*

One can sharpen the theorem so that

$$Q(a^n-b^n) \gg n^{2-c/\log\log n}$$

for a suitable constant $c > 0$. Most likely, $Q(2^n-1) = P(2^n-1)$ but we are unable to prove this. If we write $2^n-1 = u_n v_n$ with u_n squarefree, v_n squarefull and $(u_n, v_n) = 1$, then a result of Silverman [S] states that u_n is "large" under the ABC conjecture. We therefore apply the ABC conjecture (see section 2) to resolve Erdös conjecture (4), in this way. More precisely, we prove assuming ABC that for any $\epsilon > 0$,

$$P(2^n-1) \gg n^{2-\epsilon},$$

for n sufficiently large. Under the same hypothesis, we deduce sharper forms of (1) and (2) above. A key role is played by the Brun-Titchmarsh theorem on primes in arithmetic progressions which is a familiar theorem in sieve theory. More generally, we prove:

Theorem 2. *Assume the ABC conjecture. For any $\epsilon > 0$ and any integers $a > b > 0$, we have*

$$P(a^n-b^n) \gg n^{2-\epsilon},$$

(where the implied constant depends on a, b and ϵ).

Recall that if α, β are algebraic integers such that $\alpha+\beta$ and $\alpha\beta$ are coprime, non-zero rational integers and that α/β is not a root of unity, then the n-th Lucas number with respect to α, β is defined to be

$$t_n = (\alpha^n - \beta^n)/(\alpha - \beta)$$

Now, if α, β are algebraic integers subjected to the weaker conditions that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime, non-zero rational integers and that α/β is not a root of unity, then the n-th Lehmer number with respect to α, β is defined to be

$$u_n = (\alpha^n - \beta^n)/(\alpha^{\delta_n} - \beta^{\delta_n}),$$

where $\delta_n = 1$ if n is odd, and $\delta_n = 2$ if n is even. These sequences arise naturally in the study of primality testing [25]. Using the same techniques as in ([21], [22]), Stewart proved that for almost all integers n and κ as in (3),

$$P(u_n), P(t_n) \gg_{\alpha,\beta,\kappa} C\frac{\log^{1-\kappa\log 2} n}{\log\log\log n} n. \tag{6}$$

Using Frey's refined ABC conjecture for number fields (cf. section 2) and the Brun-Titchmarsh theorem for number fields [9], the same argument for Theorem 2 yields a corresponding improvement of (6) (we will omit the proof).

Theorem 3. *Let α, β be non-zero algebraic integers in a number field K such that α/β is not a root of unity. Fix an integer $\delta > 0$. Under Frey's refined ABC conjecture, for any $\epsilon > 0$, if n is sufficiently large (depending on α, β and δ), then*

$$P\Big(\mathrm{Norm}_{K/\mathbf{Q}}\Big(\frac{\alpha^n - \beta^n}{\alpha^\delta - \beta^\delta}\Big)\Big) > n^{2-\epsilon}.$$

□

Remark 1. As the referee points out, Theorem 1 can be readily generalized to more general sequences such as those given in Theorem 3. Cf. also the recent results of Ribenboim and Walsh [16] along these lines.

For prime divisors of polynomial values we have the following strengthening of (1).

Theorem 4. *Assume the ABC conjecture. Let $f(x) \in \mathbf{Z}[x]$ be a non-constant polynomial with no repeated roots. Then for any $\epsilon > 0$ and $n \gg_{\epsilon,f} 1$, we have the lower bound*

$$P(f(n)) > (\deg(f) - 1 - \epsilon)\log n.$$

Erdös [3, p. 218] also raised the question of studying $P(n!+1)$. The best results to date [4] are that $P(n!+1) > n(1+o(1))\frac{\log n}{\log\log n}$, and that $\limsup_{n\to\infty} P(n!+1)/n > 2+\delta$ for some $\delta > 0$. The ABC conjecture yields the following improvement.

Theorem 5. *Under the ABC conjecture, for every $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$ such that*

$$P(n!+1) > \left(n+\frac{1}{2}\right)\log n - (2+\epsilon)n + c(\epsilon).$$

In the same paper, Erdös asked if numbers of the form $2^n \pm 1$ represent infinitely many k-th power-free integers. In the case of $2^n - 1$ there is a curious relation with Artin's conjecture on primitive roots. More generally, for any integer d, the Artin's conjecture with index d states that for any positive square-free integer $a \neq 1$, there exists infinitely many primes p such that $a \pmod p$ generates a subgroup of index d in $(\mathbf{Z}/p\mathbf{Z})^\times$. The argument in [11] readily shows that this generalized Artin conjecture follows from the generalized Riemann hypothesis. We have the following curious theorem which is suggested by the previous discussion and is of independent interest. It can be viewed as a variation on the work of Murty and Srinivasan [12].

Theorem 6. *Either Artin's conjecture on primitive roots with index 2 holds for $a = 2$, or there exist infinitely many primes p such that $2^p - 1$ is composite.*

Remark 2. Most likely, both possibilities of the Theorem are true. However, at present, neither assertion has been established unconditionally so the Theorem is of some interest.

2. Statements of the ABC conjectures

We begin by stating the usual ABC conjecture [14]. See [13] for a survey of its many conjectural applications.

Conjecture 1 (The ABC conjecture)**.** *For every $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$, such that for any triple of nonzero, pairwise coprime integers A, B, C with $A + B + C = 0$, we have*

$$\max(|A|,|B|,|C|) < c(\epsilon)\prod_{p|ABC} p^{1+\epsilon},$$

where the product is taken over the distinct prime divisors of ABC.

Now, let $K/\mathbf{Q}$ be a number field with discriminant Δ_K. Denote by $\mathcal{O}_K$ the ring of integers of K. For any $x \in K^\times$, denote by $h_K(x)$ the

exponential height of x over K. Frey [5] proposed the following refined version of the ABC conjecture:

Conjecture 2 (Frey)**.** *For any $\epsilon > 0$ and any ideal $\mathfrak{a} \subset \mathcal{O}_K$ there exists a constant $c(\epsilon, \Delta_K, \mathfrak{a})$ which depends linearly on $\log|\Delta_K|$ and $\log \operatorname{Norm}\mathfrak{a}$ but otherwise not depending on K, such that for any pair of elements $A, B \in \mathcal{O}_K$ which generate the ideal $\mathfrak{a}$, we have the upper bound*

$$\max\big(h_K(A), h_K(B), h_K(A-B)\big)$$

$$\leq (1+\epsilon)\Big(\prod_{\mathfrak{p}|AB(A-B)} \operatorname{Norm}(\mathfrak{p})\Big) + c(\epsilon, \Delta_K, \mathfrak{a}).$$

Remark 3. It is a standard fact from commutative algebra that every non-zero ideal in a Dedekind domain can be generated by two elements. (cf. [1, exer. 7]).

3. Proof of Theorem 1

Denote by $\Phi_d(x, y)$ the homogenized d-th cyclotomic polynomial, so

$$a^n - b^n = \prod_{d|n} \Phi_d(a, b).$$

Fix $\epsilon > 0$. Recall the fact from elementary number theory that the number of divisors of n, denoted $d(n)$, satisfies the estimate $d(n) = O(n^\epsilon)$. Thus, for any $z \geq 1$ and $a > b > 0$,

$$\begin{aligned} a^n - b^n &= \prod_{\substack{d|n \\ d \leq z}} \Phi_d(a,b) \cdot \prod_{\substack{d|n \\ d > z}} \Phi_d(a,b) \\ &\leq a^{zn^\epsilon} \cdot \prod_{\substack{d|n \\ d>z}} \Phi_d(a,b). \end{aligned}$$

Let p be a prime not dividing ab. It is an easy exercise to show that $p|\Phi_d(a,b)$ implies $p \equiv 1 \pmod d$ or $p = P(d)$ and this occurs to at most the first power. Let $Q = Q(a^n - b^n)$. As usual, write

$$\psi(x, d, 1) = \sum_{\substack{n \leq x \\ n \equiv 1 \pmod d}} \Lambda(n)$$

where $\Lambda(n)$ is the von Mangoldt function. Then, for $z = n^{1-2\epsilon}$, we obtain

$$\begin{aligned}\log(a^n - b^n) &\ll n^{1-\epsilon} + \sum_{\substack{d|n \\ d>z}} \log \Phi_d(a,b) \\ &\ll n^{1-\epsilon} + O(n^\epsilon) + \sum_{\substack{d|n \\ d>z}} \psi(Q,d,1),\end{aligned}$$

where the implied constants depend only on a, b and ϵ. The last sum is

$$\leq \sum_{\substack{d|n \\ d>z}} \log Q\frac{Q}{d} \ll \frac{Q}{z} d(n) \log Q \ll Q(\log Q) n^{-1+3\epsilon}$$

so that $Q \gg n^{2-3\epsilon}$. □

4. Prime divisors of binomials

For any integer $n > 1$, define the powerful part of n to be the product $\kappa(n) := \prod_{p:p^2|n} p^{ord_p(n)}$. The quotient $n/\kappa(n)$ is called the powerfree part of n.

Denote by $\Phi_d(x,y)$ the homogenized d-th cyclotomic polynomial. For any integers $a > b > 0$, write $\Phi_d(a,b) = U_d(a,b)V_d(a,b)$, where $U_d(a,b)$ (resp. $V_d(a,b)$) is the power-free part of $\Phi_d(a,b)$ (resp. powerful part), so $(U_d(a,b), V_d(a,b)) = 1$.

Lemma 1. *Under the ABC conjecture, for every $\epsilon > 0$ there exists an absolute constant $c_1(\epsilon) > 0$ such that, for any integers $a > b > 0$,*

$$\prod_{d|n} V_d(a,b) < c_1(\epsilon)(ab)^{1+\epsilon} a^{\epsilon n}.$$

Proof. This is essentially Lemma 7 in [19]. For the sake of completenesss, we shall briefly review the proof.

Apply the ABC conjecture and we get, for every $\epsilon > 0$ there exists an absolute constant $c_0(\epsilon) > 0$ such that

$$a^n = \max(a^n, b^n, a^n - b^n) < c_0(\epsilon)\Big(\prod_{p|ab(a^n-b^n)} p\Big)^{1+\epsilon}.$$

Since the square-free part of $V_d(a,b)$ is $\leq \sqrt{V_d(a,b)}$, this becomes

$$\begin{aligned}a^n &< c_0(\epsilon)(ab)^{1+\epsilon}\Big(\prod_{d|n} U_d(a,b)\sqrt{V_d(a,b)}\Big)^{1+\epsilon} \\ &< c_0(\epsilon)(ab)^{1+\epsilon} a^{n(1+\epsilon)}\Big(\prod_{d|n} V_d(a,b)\Big)^{-(1+\epsilon)/2}.\end{aligned}$$

Rearrange the terms and we are done. □

Proof of Theorem 2. Lemma 1 shows that, under the ABC conjecture,

$$\prod_{d|n} U_d(a,b) = \frac{a^n - b^n}{\prod_{d|n} V_d(a,b)} \gg_\epsilon (a^n - b^n)a^{-n\epsilon} > a^{n-1-n\epsilon} = a^{n(1-\epsilon)-1}.$$

For any d, we have the trivial estimate $U_d(a,b) < \Phi_d(a,b) < a^d$. For any $z \geq 1$, we have

$$a^{n(1-\epsilon)} \ll_{\epsilon,a} \prod_{\substack{d|n \\ d\leq z}} U_d(a,b) \prod_{\substack{d|n \\ d>z}} U_d(a,b) \ll_{\epsilon,a} \prod_{\substack{d|n \\ d\leq z}} a^d \prod_{\substack{d|n \\ d>z}} U_d(a,b).$$

Since $\sum_{d|n} 1 \ll_\epsilon n^\epsilon$, upon letting $z = n^{1-2\epsilon}$,

$$a^{n(1-\epsilon)} \ll_{\epsilon,a} n^\epsilon a^{n^{1-\epsilon}} \prod_{\substack{d|n \\ d>z}} U_d(a,b),$$

whence

$$a^{n(1-2\epsilon)} \ll_{\epsilon,a} \prod_{\substack{d|n \\ d>z}} U_d(a,b). \tag{7}$$

Now, U_d is the square-free part of the value of the homogeneous d-th cyclotomic polynomial, so that if $p \not| ab$ divides $U_d(a,b)$ then $p \equiv 1 \pmod d$. Now, suppose that $P(a^n - b^n) \leq N := n^{2-5\epsilon}$. Then for $d > z$, the Brun-Titchmarsh theorem [23, p. 73] gives

$$\begin{aligned} U_d(a,b) \ll_{a,b} \prod_{\substack{p\leq N \\ p\equiv 1(d)}} p \ll_{a,b,\epsilon} \exp(2N/\varphi(d)) &\ll \exp(2N \log\log d/d) \\ &\leq \exp(n^{1-3\epsilon} \log\log n), \end{aligned}$$

upon using $\varphi(d) \gg d/\log\log d$. Combine this with (7), we get

$$a^{n(1-\epsilon)} \ll_{\epsilon,a,b} \prod_{\substack{d|n \\ d>z}} \exp(n^{1-3\epsilon} \log\log n).$$

Taking logs on both sides and we get

$$n(1-\epsilon) \ll_{\epsilon,a,b} \sum_{\substack{d|n \\ d>z}} n^{1-3\epsilon} \log\log n \ll_{\epsilon,a,b} n^{1-2\epsilon},$$

a contradiction if $n \gg_{\epsilon,a,b} 1$. □

Proof of Theorem 5. The ABC conjecture gives

$$n! \ll_\epsilon \left(\prod_{p|(n!)(n!+1)} p \right)^{1+\epsilon} \ll_\epsilon \left(e^n \prod_{\substack{p|(n!+1) \\ p>n}} p \right)^{1+\epsilon}.$$

Taking logs and applying the Stirling approximation, we get

$$(n+1/2)\log n - n \leq (1+\epsilon)\Big(n + \sum_{\substack{p|(n!+1) \\ p>n}} \log p\Big),$$

and the theorem follows. □

5. Heuristics for Erdös' conjecture

For any prime p and any integer a not divisible by p, denote by $f_a(p)$ the order of $a \pmod p$. Define

$$P_x = \max_{n \leq x} P(a^n - 1).$$

Under the ABC conjecture, the argument for Lemma 1 shows that $a^n - 1 = u_n v_n$ with u_n square-free and $v_n \ll_{a,\epsilon} a^{\epsilon n}$. Thus

$$\sum_{\substack{p \leq P_x \\ f_a(p) \leq x}} [x/f_a(p)] \log p \sim \frac{1}{2} x^2 \log a,$$

whence

$$(\log P_x) \sum_{p : f_p(a) < x} [x/f_p(a)] \geq \frac{1}{2} x^2 \log a.$$

On the other hand,

$$\sum_{\substack{p \leq P_x \\ f_a(p) \leq x}} [x/f_p(a)] = \sum_{n \leq x} v(a^n - 1), \tag{8}$$

where $v(m)$ denotes the number of distinct prime divisors of m. A classical result of Hardy and Ramanujan [8] says that the average order of $v(m)$ is $\log\log m$. If we assume that $v(a^n - 1)$ behaves like this, then it follows that $a^n - 1$ usually has $O(\log n)$ prime divisors, in which case the sum on the right side of (8) behaves like $x \log x$. This gives a more precise form of (5):

$$P_x \geq a^{x/2\log x}.$$

In fact, we can do even better. The Hardy-Ramanujan result is based on the heuristic that the probability a prime divides n is $1/p$. Thus the

number of prime divisors of n should be roughly

$$\sum_{p \le n} \frac{1}{p} \sim \log\log n.$$

In our case, $a^n - 1 = \prod_{d|n} \phi_d(a)$, so we should really be looking at prime divisors of $\phi_d(a)$. But then all prime divisors are $\equiv 1 \pmod{d}$, so the average number of prime divisors of $\phi_d(a)$ should be

$$\sum_{\substack{p \le a^d \\ p \equiv 1 \pmod{d}}} \frac{1}{p} \sim \frac{\log d}{\phi(d)}.$$

This slightly improves the heuristic above to

$$P_x \ge a^{cx}$$

for some constant $c > 0$.

6. Prime divisors of polynomials

The following result was noted independently by Langevin [10] and Granville [6].

Theorem 7. *Assume the ABC conjecture. Suppose that $g \in \mathbf{Z}[x]$ has distinct roots. Then for any $\epsilon > 0$ there exists a constant $c(\epsilon, g) > 0$ such that for any integer m,*

$$\prod_{p | g(m)} p \le c(\epsilon, g) |m|^{\deg g - 1 - \epsilon}.$$

□

Proof of Theorem 4. Suppose that $P(f(n)) \ll_{\epsilon,f} (\deg(f) - 1 - \epsilon)\log n$ for $n \gg_{\epsilon,f} 1$. Then under the ABC conjecture, Theorem 7 gives

$$\big(\deg(f) - 1 - \frac{\epsilon}{2}\big)\log n \ll_{\epsilon,f} \sum_{p | f(n)} \log p \ll \sum_{p < (\deg f - 1 - \epsilon)\log n} \log p$$

$$\ll (\deg f - 1 - \epsilon)\log n$$

for n sufficiently large, a contradiction. □

7. Compositeness of $2^q - 1$

Denote, by $f_a(p)$ the order of $a \pmod{p}$, as before.

Proof of Theorem 6. Define a set of primes (with $\eta > 0$)

$$S = \{p \leq x : p - 1 = 2l_1 \text{ or } 2l_1 l_2, l_2 > x^{1/2-\eta} > l_1 > x^{1/4-\eta}\},$$

where 2 is a quadratic residue mod p. If the set of primes $p \in S$ with $p-1 = 2l_1$ is infinite, then Artin's conjecture holds for index 2. So now suppose that all the primes $p \in S$ are of the form $2l_1 l_2$ with l_1, l_2 as indicated in S. Then, the order of 2 mod p for $p \in S$ is either l_1 or l_2. In either case, $2^{l_1} - 1$ or $2^{l_2} - 1$ is divisible by p and hence composite since each of these numbers is larger than p. This completes the proof. □

A similar argument can be applied to show that if it is not the case that 2 is a primitive root for infinitely many primes p then $(2^p + 1)/3$ is composite for infinitely many primes p. We leave the details to the interested reader.

References

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra.* Addison-Wesley, 1969.

[2] A. Baker, A sharpening of the bounds for linear forms in logarithms I, II, III. *Acta Arith.* **21** (1972) 117-129; **24** (1973) 33-36; **27** (1975) 247-252.

[3] P. Erdös, Some recent advances and current problems in number theory. In: *Lectures on modern mathematics, III* (edited by T. L. Saaty), 196-244. John Wiley & Sons, 1965.

[4] P. Erdös and C. L. Stewart, On the greatest and least prime factors of $n! + 1$. *J. London Math. Soc.* (2) **13** (1976) no. 3, 513-519.

[5] G. Frey, On ternary equations of Fermat type and relations with elliptic curves, in: *Modular forms and Fermat's last theorem*, 527-548. Springer-Verlag, 1997.

[6] A. Granville, *ABC* allows us to count squarefrees. *Inter. Math. Research Notices* (1998) 991-1009.

[7] R. Gupta and R. Murty, A remark on Artin's conjecture. *Invent. Math.* **78** (1984) 127-130.

[8] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n. *Quarterly J. Math.* **48** (1920) 76-92.

[9] Hinz, Jürgen and M. Lodemann, On Siegel zeros of Hecke-Landau zeta-functions. *Monatsh. Math.* **118** (1994) 231-248.

[10] M. Langevin, Cas d'egalité pour le théorème de Mason et applications de la conjecture (abc). *C. R. Acad. Sci. Paris* Ser. I Math **317** (1993) 441-444.

[11] R. Murty, On Artin's conjecture. *J. Number Theory* **16** (1983) 147-168.

[12] R. Murty and S. Srinivasan, Some remarks on Artin's conjecture, *Canad. Math. Bulletin* **30** (1987) no. 1, 80-85.

[13] A. Nitaj, La conjecture *abc*. *Enseign. Math.* (2) **42** (1996) 1-24.

[14] J. Oesterlé, Nouvelles approches du théorème de Fermat, in: *Séminaire Bourbaki* exposé 694, 1987-88.

[15] G. Pólya, Zur arithmetischen Untersuchung der Polynome. *Math. Zeitschrift* **1** (1918) 143-148.

[16] P. Ribenboim and G. Walsh, The *ABC* conjecture and the powerful part of terms in binary recurring sequences. *J. Number Theory* **74** (1999) 134-147.

[17] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gelfond-Baker method to Diophantine equations. In: *Transcendence theory: advances and applications.* (edited by A. Baker and D. W. Masser), 59-77. Academic Press, 1977.
[18] C. L. Siegel, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921) 173-213.
[19] J. Silverman, Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988) 226-237.
[20] C. L. Stewart, *Divisor properties of arithmetic sequences*, Ph. D. thesis, University of Cambridge, 1976.
[21] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. *Proc. London Math. Soc.* (3) **35** (1977) 425-477.
[22] C. L. Stewart, Primitive divisors of Lucas and Lehmer numbers. In: *Transcendence theory: advances and applications* (edited by A. Baker and D. W. Masser), 79-92. Academic Press, 1977.
[23] G. Tenenbaum, *Introduction to analytic and probabilistic number theory.* Cambridge Univ. Press, 1995.
[24] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. reine angew. Math.* **135** (1909) 284-305.
[25] H. C. Williams, *Edouard Lucas and primality testing.* Wiley, 1998.

Department of Mathematics, Queen's University. Kingston, Ontario K7L 3N6. Canada

Department of Mathematics, University of Massachusetts. Amherst, MA 01003. USA

E-mail address: murty@mast.queensu.ca, siman@math.umass.edu