Annals of Mathematics, **166** (2007), 347–366

Lehmer's problem for polynomials with odd coefficients

By Peter Borwein, Edward Dobrowolski, and Michael J. Mossinghoff*

Abstract

We prove that if $f(x) = \sum_{k=0}^{n-1} a_k x^k$ is a polynomial with no cyclotomic factors whose coefficients satisfy $a_k \equiv 1 \bmod 2$ for $0 \le k < n$, then Mahler's measure of f satisfies

$$\log \mathrm{M}(f) \ge \frac{\log 5}{4}\left(1 - \frac{1}{n}\right).$$

This resolves a problem of D. H. Lehmer [12] for the class of polynomials with odd coefficients. We also prove that if f has odd coefficients, degree $n-1$, and at least one noncyclotomic factor, then at least one root α of f satisfies

$$|\alpha| > 1 + \frac{\log 3}{2n},$$

resolving a conjecture of Schinzel and Zassenhaus [21] for this class of polynomials. More generally, we solve the problems of Lehmer and Schinzel and Zassenhaus for the class of polynomials where each coefficient satisfies $a_k \equiv 1 \bmod m$ for a fixed integer $m \ge 2$. We also characterize the polynomials that appear as the noncyclotomic part of a polynomial whose coefficients satisfy $a_k \equiv 1 \bmod p$ for each k, for a fixed prime p. Last, we prove that the smallest Pisot number whose minimal polynomial has odd coefficients is a limit point, from both sides, of Salem [19] numbers whose minimal polynomials have coefficients in $\{-1, 1\}$.

1. Introduction

Mahler's measure of a polynomial f, denoted $\mathrm{M}(f)$, is defined as the product of the absolute values of those roots of f that lie outside the unit disk, multiplied by the absolute value of the leading coefficient. Writing $f(x) =$

*The first author was supported in part by NSERC of Canada and MITACS. The authors thank the Banff International Research Station for hosting the workshop on "The many aspects of Mahler's measure," where this research began.

$a\prod_{k=1}^{d}(x-\alpha_k)$, we have

$$\mathrm{M}(f) = |a| \prod_{k=1}^{d} \max\{1, |\alpha_k|\}. \tag{1.1}$$

For $f \in \mathbf{Z}[x]$, clearly $\mathrm{M}(f) \geq 1$, and by a classical theorem of Kronecker, $\mathrm{M}(f) = 1$ precisely when $f(x)$ is a product of cyclotomic polynomials and the monomial x. In 1933, D. H. Lehmer [12] asked if for every $\varepsilon > 0$ there exists a polynomial $f \in \mathbf{Z}[x]$ satisfying $1 < \mathrm{M}(f) < 1 + \varepsilon$. This is known as *Lehmer's problem*. Lehmer noted that the polynomial

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has $\mathrm{M}(\ell) = 1.176280\ldots$, and this value remains the smallest known measure larger than 1 of a polynomial with integer coefficients.

Let f^* denote the *reciprocal polynomial* of f, defined by $f^*(x) = x^{\deg f} f(1/x)$; it is easy to verify that $\mathrm{M}(f^*) = \mathrm{M}(f)$. We say a polynomial f is *reciprocal* if $f = \pm f^*$.

Lehmer's problem has been solved for several special classes of polynomials. For example, Smyth [22] showed that if $f \in \mathbf{Z}[x]$ is nonreciprocal and $f(0) \neq 0$, then $\mathrm{M}(f) \geq \mathrm{M}(x^3 - x - 1) = 1.324717\ldots$. Also, Schinzel [20] proved that if f is a monic, integer polynomial with degree d satisfying $f(0) = \pm 1$ and $f(\pm 1) \neq 0$, and all roots of f are real, then $\mathrm{M}(f) \geq \gamma^{d/2}$, where γ denotes the golden ratio, $\gamma = (1 + \sqrt{5})/2$. In addition, Amoroso and Dvornicich [1] showed that if f is an irreducible, noncyclotomic polynomial of degree d whose splitting field is an abelian extension of $\mathbf{Q}$, then $\mathrm{M}(f) \geq 5^{d/12}$.

The best general lower bound for Mahler's measure of an irreducible, noncyclotomic polynomial $f \in \mathbf{Z}[x]$ with degree d has the form

$$\log \mathrm{M}(f) \gg \left(\frac{\log\log d}{\log d}\right)^3;$$

see [6] or [8].

In this paper, we solve Lehmer's problem for another class of polynomials. Let $\mathcal{D}_m$ denote the set of polynomials whose coefficients are all congruent to 1 mod m,

$$\mathcal{D}_m = \left\{ \sum_{k=0}^{d} a_k x^k \in \mathbf{Z}[x] : a_k \equiv 1 \bmod m \text{ for } 0 \leq k \leq d \right\}. \tag{1.2}$$

The set $\mathcal{D}_2$ thus contains the set of *Littlewood polynomials*, defined as those polynomials f whose coefficients a_k satisfy $a_k = \pm 1$ for $0 \leq k \leq \deg f$. We prove in Corollaries 3.4 and 3.5 of Theorem 3.3 that if $f \in \mathcal{D}_m$ has degree $n-1$

and no cyclotomic factors, then

$$\log \mathrm{M}(f) \geq c_m \left(1 - \frac{1}{n}\right),$$

with $c_2 = (\log 5)/4$ and $c_m = \log(\sqrt{m^2+1}/2)$ for $m > 2$.

We provide in Theorem 2.4 a characterization of polynomials $f \in \mathbf{Z}[x]$ for which there exists a polynomial $F \in \mathcal{D}_p$ with $f \mid F$ and $\mathrm{M}(f) = \mathrm{M}(F)$, where p is a prime number. The proof in fact specifies an explicit construction for such a polynomial F when it exists.

In [21], Schinzel and Zassenhaus conjectured that there exists a constant $c > 0$ such that for any monic, irreducible polynomial f of degree d, there exists a root α of f satisfying $|\alpha| > 1 + c/d$. Certainly, solving Lehmer's problem resolves this conjecture as well: If $\mathrm{M}(f) \geq M_0$ for every member f of a class of monic, irreducible polynomials, then it is easy to see that the conjecture of Schinzel and Zassenhaus holds for this class with $c = \log M_0$. We prove some further results on this conjecture for polynomials in $\mathcal{D}_m$. In Theorem 5.1, we show that if $f \in \mathcal{D}_m$ is monic with degree $n-1$ and $\mathrm{M}(f) > 1$, then there exists a root α of f satisfying $|\alpha| > 1 + c_m/n$, with $c_2 = \log\sqrt{3}$ and $c_m = \log(m-1)$ for $m > 2$. We also prove (Theorem 5.3) that one cannot replace the constant c_m in this result with any number larger than $\log(2m-1)$.

Recall that a *Pisot number* is a real algebraic integer $\alpha > 1$, all of whose conjugates lie inside the open unit disk, and a *Salem number* is a real algebraic integer $\alpha > 1$, all of whose conjugates lie inside the closed unit disk, with at least one conjugate on the unit circle. (In fact, all the conjugates of a Salem number except its reciprocal lie on the unit circle.) In Theorem 6.1, we obtain a lower bound on a Salem number whose minimal polynomial lies in $\mathcal{D}_2$. This bound is slightly stronger than that obtained from our bound on Mahler's measure of a polynomial in this set.

The smallest Pisot number is the minimal value of Mahler's measure of a nonreciprocal polynomial, $\mathrm{M}(x^3 - x - 1) = 1.324717\ldots$. In [4], it is shown that the smallest measure of a nonreciprocal polynomial in $\mathcal{D}_2$ is the golden ratio, $\mathrm{M}(x^2 - x - 1) = \gamma$, and therefore this value is the smallest Pisot number whose minimal polynomial lies in $\mathcal{D}_2$. Salem [19] proved that every Pisot number is a limit point, from both sides, of Salem numbers. We prove in Theorem 6.2 that the golden ratio is in fact a limit point, from both sides, of Salem numbers whose minimal polynomials are also in $\mathcal{D}_2$; in fact, they are Littlewood polynomials.

This paper is organized as follows. Section 2 obtains some preliminary results on factors of cyclotomic polynomials modulo a prime, and describes factors of polynomials in $\mathcal{D}_p$. Section 3 derives our results on Lehmer's problem for polynomials in $\mathcal{D}_m$. The method here requires the use of an auxiliary polynomial, and Section 4 describes two methods for searching for favorable auxiliary polynomials in a particularly promising family. Section 5 proves our

bounds in the problem of Schinzel and Zassenhaus for polynomials in $\mathcal{D}_m$, and Section 6 contains our results on Salem numbers whose minimal polynomials are in $\mathcal{D}_2$.

Throughout this paper, the nth cyclotomic polynomial is denoted by Φ_n. Also, for a polynomial $f(x) = \sum_{k=0}^{d} a_k x^k$, the *length* of f, denoted $L(f)$, is defined as the sum of the absolute values of the coefficients of f,

$$L(f) = \sum_{k=0}^{d} |a_k| , \tag{1.3}$$

and $\|f\|_\infty$ denotes the supremum of $|f(x)|$ over the unit circle.

2. Factors of polynomials in $\mathcal{D}_p$

Let p be a prime number. We describe some facts about factors of cyclotomic polynomials modulo p, and then prove some results about cyclotomic and noncyclotomic parts of polynomials whose coefficients are all congruent to 1 mod p. We begin by recording a factorization of the binomial $x^n - 1$ modulo p.

LEMMA 2.1. *Suppose p is a prime number, and $n = p^k m$ with $p \nmid m$. Then*

$$x^n - 1 \equiv \prod_{d \mid m} \Phi_d^{p^k}(x) \mod p.$$

Proof. Using the standard formula $\Phi_n(x) = \prod_{d \mid n} \left(x^d - 1\right)^{\mu(n/d)}$, where $\mu(\cdot)$ denotes the Möbius function, one obtains the well-known relations

$$\Phi_{pq}(x) = \begin{cases} \Phi_q(x^p), & \text{if } p \mid q, \\ \dfrac{\Phi_q(x^p)}{\Phi_q(x)}, & \text{if } p \nmid q. \end{cases}$$

Thus, if $n = p^k m$ with $p \nmid m$, then $\Phi_n(x) \equiv \Phi_m^{\varphi(p^k)}(x) \mod p$, where $\varphi(\cdot)$ denotes Euler's totient function. Therefore,

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \equiv \prod_{d \mid m} \Phi_d^{\sum_{i=0}^{k} \varphi(p^i)}(x) = \prod_{d \mid m} \Phi_d^{p^k}(x) \mod p,$$

establishing the result. □

Let $\mathbf{F}_p$ denote the field with p elements, where p is a prime number. Cyclotomic polynomials are of course irreducible in $\mathbf{Q}[x]$, but this is not necessarily the case in $\mathbf{F}_p[x]$. However, cyclotomic polynomials whose indices are relatively prime and not divisible by p have no common factors in $\mathbf{F}_p[x]$.

LEMMA 2.2. *Suppose m and n are distinct, relatively prime positive integers, and suppose p is a prime number that does not divide mn. Then $\Phi_n(x)$ and $\Phi_m(x)$ are relatively prime in $\mathbf{F}_p[x]$.*

Proof. Let e denote the multiplicative order of p modulo n. In $\mathbf{F}_p[x]$, the polynomial $\Phi_n(x)$ factors as the product of all monic irreducible polynomials with degree e and order n (see [13, Ch. 3]). Since their factors in $\mathbf{F}_p[x]$ have different orders, we conclude that Φ_n and Φ_m are relatively prime modulo p. □

We next describe the cyclotomic factors that may appear in a polynomial whose coefficients are all congruent to 1 modulo p.

LEMMA 2.3. *Suppose $f(x) \in \mathbf{Z}[x]$ has degree $n-1$ and $\Phi_r \mid f$. If $f \in \mathcal{D}_2$, then $r \mid 2n$; if $f \in \mathcal{D}_p$ for an odd prime p, then $r \mid n$.*

Proof. Suppose $f \in \mathcal{D}_p$ with p prime. Write $n = p^k m$ with $p \nmid m$. By Lemma 2.1, we have

$$(x-1)f(x) \equiv \prod_{d \mid m} \Phi_d^{p^k}(x) \mod p. \tag{2.1}$$

Write $r = p^l s$ with $p \nmid s$. If $l = 0$, then in view of Lemma 2.2, the polynomial Φ_r must appear among the factors Φ_d on the right side of (2.1), so that $r \mid m$. If $l > 0$, then $\Phi_r \equiv \Phi_s^{\varphi(p^l)} \mod p$, so $s \mid m$. If $s > 1$ then we also have $p^k \geq p^l - p^{l-1}$, and so if $p > 2$ then $k \geq l$ and thus $r \mid n$; if $p = 2$ then $k \geq l-1$ and consequently $r \mid 2n$. Last, if $s = 1$ then $p^k \geq p^l - p^{l-1} + 1$ and thus $k \geq l$ and $r \mid n$. □

We now state a simple characterization of polynomials $f \in \mathbf{Z}[x]$ that divide a polynomial with the same measure having all its coefficients congruent to 1 modulo p.

THEOREM 2.4. *Let p be a prime number, and let $f(x)$ be a polynomial with integer coefficients. There exists a polynomial $F \in \mathcal{D}_p$ with $f \mid F$ and $\mathrm{M}(f) = \mathrm{M}(F)$ if and only if f is congruent modulo p to a product of cyclotomic polynomials.*

Proof. Suppose first that $F \in \mathcal{D}_p$ factors as $F(x) = f(x)\Phi(x)$ with $\mathrm{M}(\Phi) = 1$, so that $\Phi(x)$ is a product of cyclotomic polynomials. Since $F \in \mathcal{D}_p$, it is congruent modulo p to a product of cyclotomic polynomials. Using Lemma 2.2 and the fact that $\mathbf{F}_p[x]$ is a unique factorization domain, we conclude that the polynomial f must also be congruent modulo p to a product of cyclotomic polynomials.

For the converse, suppose

$$f(x) \equiv \prod_{p \nmid d} \Phi_d^{e_d}(x) \mod p,$$

with each $e_d \geq 0$. Let $k = \lceil \log_p(\max\{e_1 + 1, \max\{e_d : d > 1, p \nmid d\}\}) \rceil$, $m = \operatorname{lcm}\{d : e_d > 0, p \nmid d\}$, $n = mp^k + 1$, and

$$\Phi(x) = (x-1)^{p^k - e_1 - 1} \prod_{\substack{d \mid m \\ d > 1}} \Phi_d^{p^k - e_d}(x).$$

Then

$$(x-1)f(x)\Phi(x) \equiv \prod_{d \mid m} \Phi_d^{p^k}(x) \equiv x^n - 1 \mod p,$$

and so $F(x) = f(x)\Phi(x)$ has the required properties. □

Theorem 2.4 suggests an algorithm for determining if a given polynomial f with degree d divides a polynomial F in $\mathcal{D}_p$ with the same measure: Construct all possible products of cyclotomic polynomials with degree d, and test if any of these are congruent to f mod p. Using this strategy, we verify that none of the 100 irreducible, noncyclotomic polynomials from [15] representing the smallest known values of Mahler's measure divides a Littlewood polynomial with the same measure. This does not imply, however, that no Littlewood polynomials exist with these measures, since measures are not necessarily represented uniquely by irreducible integer polynomials, even discounting the simple symmetries $\mathrm{M}(f) = \mathrm{M}(\pm f(\pm x^k))$. See [7] for more information on the values of Mahler's measure.

The requirement in Theorem 2.4 that $F(x)$ contain no noncyclotomic factors besides f is certainly necessary. For example, the polynomial $x^{10} - x^7 - x^5 - x^3 + 1$ is not congruent to a product of cyclotomic polynomials mod 2, so no Littlewood polynomial exists having this polynomial as its only noncyclotomic factor. However, the product $(x^{10} - x^7 - x^5 - x^3 + 1)(x^{10} - x^9 + x^5 - x + 1)$ is congruent to Φ_{33} mod 2, and our construction indicates that multiplying this product by $\Phi_1\Phi_3^2\Phi_{11}^2\Phi_{33}$ yields a polynomial with all odd coefficients. (In fact, using the factors $\Phi_2\Phi_3\Phi_6\Phi_{33}\Phi_{44}$ instead yields a Littlewood polynomial.)

We close this section by noting that one may demand stronger conditions on the polynomial F of Theorem 2.4 in certain situations.

COROLLARY 2.5. *Suppose $f \in \mathbf{Z}[x]$ has no cyclotomic factors, and there exists a polynomial $F \in \mathcal{D}_2$ with even degree $2m$ having $f \mid F$ and $\mathrm{M}(f) = \mathrm{M}(F)$. Then there exists a polynomial $G \in \mathcal{D}_2$ with $\deg G = 2m$, $f \mid G$, $\mathrm{M}(f) = \mathrm{M}(G)$, and the additional property that $G(x)$ and $1 + x + x^2 + \cdots + x^{2m}$ have no common factors.*

Proof. Suppose $\Phi_d \mid F$. By Lemma 2.3, we have $d \mid (4m+2)$. If d is odd and $d \geq 3$, so that $\Phi_d(x)$ is a factor of $1 + x + \cdots + x^{2m}$, then we can replace the factor Φ_d in F with Φ_{2d} without disturbing the required properties of F, since $\Phi_{2d}(x) = \Phi_d(-x)$. Let G be the polynomial obtained from F by making this substitution for each factor Φ_d of F with $d \geq 3$ odd. □

3. Lehmer's problem

We derive a lower bound on Mahler's measure of a polynomial that has no cyclotomic factors and whose coefficients are all congruent to 1 modulo m for some fixed integer $m \geq 2$. Our results depend on the bounds on the resultants appearing in the following lemma.

LEMMA 3.1. *Suppose $f \in \mathcal{D}_m$ with degree $n-1$, and let g be a factor of f. If $\gcd(g(x), x^n - 1) = 1$, then*

$$|\mathrm{Res}(g(x), x^n - 1)| \geq m^{\deg g}. \tag{3.1}$$

Further, if $m = 2$, k is a nonnegative integer, and $\gcd(g(x), x^{n2^k} + 1) = 1$, then

$$\left|\mathrm{Res}(g(x), x^{n2^k} + 1)\right| \geq 2^{\deg g}. \tag{3.2}$$

Proof. Define the polynomial $s(x)$ by

$$ms(x) = (x^n - 1) + (1 - x)f(x), \tag{3.3}$$

and note that $s(x) \in \mathbf{Z}[x]$ since $f \in \mathcal{D}_m$. If g has no common factor with $x^n - 1$, then $\gcd(g, s) = 1$, so $|\mathrm{Res}(g, s)| \geq 1$. Thus, by computing the resultant of both sides of (3.3) with g, we obtain (3.1).

Suppose $m = 2$. For $k \geq 0$, define the polynomial $t_k(x)$ by

$$2t_k(x) = (x^{n2^k} + 1) + (1 + x)f(x) \sum_{j=0}^{2^k - 1} x^{jn}.$$

Now, (3.2) follows by a similar argument. □

We also require the following result regarding the length of a power of a polynomial.

LEMMA 3.2. *For any polynomial $f \in \mathbf{C}[x]$, the value of $L(f^k)^{1/k}$ approaches $\|f\|_\infty$ from above as $k \to \infty$.*

Proof. From the triangle and Cauchy-Schwarz inequalities, we have $\|f^k\|_\infty \leq L(f^k) \leq \sqrt{1 + k \deg f}\, \|f^k\|_\infty$, and since $\|f^k\|_\infty = \|f\|_\infty^k$, the result follows immediately. □

Our main theorem in this section provides a lower bound on the measure of a polynomial in $\mathcal{D}_m$ that depends on certain properties of an auxiliary polynomial. For a polynomial $g \in \mathbf{Z}[x]$, let $\nu_k(g)$ denote the multiplicity of the cyclotomic polynomial $\Phi_{2^k}(x)$ in $g(x)$, and let $\nu(g) = \sum_{k\ge 0} \nu_k(g)$.

THEOREM 3.3. *Suppose $f \in \mathcal{D}_m$ with degree $n-1$, and suppose $F \in \mathbf{Z}[x]$ satisfies $\gcd(f(x), F(x^n)) = 1$. Then*

$$\log \mathrm{M}(f) \ge \begin{cases} \dfrac{\nu(F)\log 2 - \log \|F\|_\infty}{\deg F}\left(1 - \dfrac{1}{n}\right), & \text{if } m = 2, \\ \dfrac{\nu_0(F)\log m - \log \|F\|_\infty}{\deg F}\left(1 - \dfrac{1}{n}\right), & \text{if } m > 2. \end{cases}$$

Proof. Suppose $m = 2$. Since $f(x)$ and $F(x^n)$ have no common factors, by Lemma 3.1 each cyclotomic factor Φ_{2^k} of F contributes a factor of 2^{n-1} to their resultant. Thus

$$|\mathrm{Res}(f(x), F(x^n))| \ge 2^{\nu(F)(n-1)}.$$

If α is a root of f, then

$$|F(\alpha^n)| \le L(F) \max\left\{1, |\alpha|^{n \deg F}\right\},$$

so that

$$|\mathrm{Res}(f(x), F(x^n))| \le L(F)^{n-1} \mathrm{M}(f)^{n \deg F}.$$

Therefore

$$2^{\nu(F)(n-1)} \le L(F)^{n-1} \mathrm{M}(f)^{n \deg F},$$

or

$$\log \mathrm{M}(f) \ge \frac{\nu(F)\log 2 - \log L(F)}{\deg F}\left(1 - \frac{1}{n}\right). \tag{3.4}$$

Let k be a positive integer. Since $\nu(F^k) = k\nu(F)$ and $\deg F^k = k \deg F$, we obtain

$$\log \mathrm{M}(f) \ge \frac{\nu(F)\log m - \log L(F^k)^{1/k}}{\deg F}\left(1 - \frac{1}{n}\right).$$

The theorem follows by letting $k \to \infty$ and using Lemma 3.2. The proof for $m > 2$ is similar, with $\nu_0(F)$ in place of $\nu(F)$. □

For example, if f has all odd coefficients and no cyclotomic factors, then we may use $F(x) = x^2 - 1$ in Theorem 3.3 to obtain

$$\log \mathrm{M}(f) \ge \frac{\log 2}{2}\left(1 - \frac{1}{n}\right). \tag{3.5}$$

For $m > 2$, if $f \in \mathcal{D}_m$ has no cyclotomic factors, then we may use $F(x) = x - 1$ to obtain

$$\log \mathrm{M}(f) \geq \log(m/2) \left(1 - \frac{1}{n}\right). \tag{3.6}$$

Section 4 describes a class of polynomials that one might expect to contain some choices for F that improve the bounds (3.5) and (3.6), and describes some algorithms developed to search this set for better auxiliary polynomials. We record here some improved bounds that arose from these searches.

COROLLARY 3.4. *Let f be a polynomial with degree $n-1$ having odd coefficients and no cyclotomic factors. Then*

$$\log \mathrm{M}(f) \geq \frac{\log 5}{4} \left(1 - \frac{1}{n}\right), \tag{3.7}$$

with equality if and only if $f(x) = \pm 1$.

Proof. Let $F(x) = \left(1 + x^2\right)\left(1 - x^2\right)^4$. Since $\nu(F) = 9$, $\deg F = 10$, and

$$\begin{aligned} \|F\|_\infty &= \left\|(1+y)(1-y)^4\right\|_\infty \\ &= 2^5 \max_{0 \leq t \leq 1} \left|\cos(\pi t) \sin^4(\pi t)\right| = \frac{2^9}{25\sqrt{5}}, \end{aligned}$$

using Theorem 3.3 we establish (3.7). Last, if the leading or constant coefficient of f is greater than 1 in absolute value, then $\mathrm{M}(f) \geq 3$; if $n > 1$ and these coefficients are ± 1, then $\mathrm{M}(f)$ is a unit. □

Another auxiliary polynomial yielding the lower bound (3.7) appears in Section 4.

We remark that the bound of $5^{1/4} = 1.495348\ldots$ is not far from the smallest known measure of a polynomial with odd coefficients and no cyclotomic factors: $\mathrm{M}(1 + x - x^2 - x^3 - x^4 + x^5 + x^6) = 1.556030\ldots$. This number is in fact the smallest measure of a reciprocal polynomial with ± 1 coefficients having no cyclotomic factors and degree at most 72; see [4]. Section 6 provides more information on the structure of known small values of Mahler's measure of these polynomials.

For the case $m > 2$, an auxiliary polynomial similar to the one employed in Corollary 3.4 improves (3.6) slightly.

COROLLARY 3.5. *Let $f \in \mathcal{D}_m$ have degree $n-1$ and no cyclotomic factors. Then*

$$\log \mathrm{M}(f) \geq \log \left(\frac{\sqrt{m^2+1}}{2}\right) \left(1 - \frac{1}{n}\right), \tag{3.8}$$

with equality if and only if $f(x) = \pm 1$.

Proof. Let $F(x) = (1+x)(1-x)^{m^2}$. Since $\nu_0(F) = m^2$, $\deg F = m^2+1$, and

$$\begin{aligned}\|F\|_\infty &= 2^{m^2+1} \max_{0\le t\le 1} \left|\cos(\pi t)\sin^{m^2}(\pi t)\right| \\ &= \frac{2^{m^2+1} m^{m^2}}{(m^2+1)^{(m^2+1)/2}},\end{aligned}$$

using Theorem 3.3 we verify (3.8). The argument for the case of equality is similar to that of Corollary 3.4. □

Section 4.3 shows that the bound of $\sqrt{10}/2 = 1.581138\ldots$ for $m = 3$ may be replaced by $1.582495\ldots$ by using the auxiliary polynomial

$$(1-x)^{425}(1-x^2)^{50}(1-x^5).$$

No improvements are known for $m > 3$.

4. Auxiliary polynomials

We obtain nontrivial bounds on the measure of a polynomial $f \in \mathcal{D}_m$ from Theorem 3.3 by using auxiliary polynomials having small degree, small supremum norm, and a high order of vanishing at 1. In this section, we investigate a family of polynomials having precisely these properties and search for auxiliary polynomials yielding good lower bounds.

4.1. *Pure product polynomials.* A *pure product* of size n is a polynomial of the form

$$\prod_{k=1}^{n} (1 - x^{e_k}),$$

with each e_k a positive integer. Let $A(n)$ denote the minimal supremum over the unit disk among all pure products of size n,

$$A(n) = \min\left\{ \left\| \prod_{k=1}^{n} (1-x^{e_k}) \right\|_\infty : e_k \ge 1 \text{ for } 1 \le k \le n \right\}.$$

Erdős and Szekeres studied this quantity in [10], proving that the growth rate of $A(n)$ is subexponential:

$$\lim_{n\to\infty} A(n)^{1/n} = 1.$$

The upper bound on the asymptotic growth rate of $\log A(n)$ has since been greatly improved. Atkinson [2] obtained $O(\sqrt{n}\log n)$, Odlyzko [17] proved $O(n^{1/3}\log^{4/3} n)$, Kolountzakis [11] demonstrated $O(n^{1/3}\log n)$, and Belov and Konyagin [3] showed $O(\log^4 n)$. The best known general lower bound on $A(n)$

is simply $\sqrt{2n}$; strengthening this would provide information on the Diophantine problem of Prouhet, Tarry, and Escott (see for instance [14]). Erdős conjectured [9, p. 55] that in fact $A(n) \gg n^c$ for any $c > 0$.

Since $\nu_0(A(n)) = n$ and $\log A(n) = o(n)$, it follows that there exist pure product polynomials $F(x)$ that yield nontrivial lower bounds in Theorem 3.3. The article [5] exhibits some pure products of size $n \leq 20$ with very small length and degree, and these polynomials yield nontrivial lower bounds in Theorem 3.3. However, these polynomials arise as optimal examples of polynomials with $\{-1, 0, 1\}$ coefficients having a root of prescribed order n at 1 and minimal degree. We obtain better bounds by designing some more specialized searches. We describe two such searches.

4.2. *Hill-climbing.* Our first method employs a modified hill-climbing strategy to search for good auxiliary polynomials $F(x)$, replacing the objective function appearing in Theorem 3.3 with the computationally more attractive function from (3.4). So for each m we wish to find large values of

$$B_m(F) = \begin{cases} \dfrac{\nu(F)\log 2 - \log L(F)}{\deg F}, & \text{if } m = 2, \\ \dfrac{\nu_0(F)\log m - \log L(F)}{\deg F}, & \text{if } m > 2. \end{cases}$$

ALGORITHM 4.1. *Modified hill-climbing for auxiliary polynomials.*

Input. An integer $m \geq 2$, a set E of positive integers, and for each $e \in E$, a nonnegative integer r_e.

Output. A sequence of pure products $\{F_k\}$ with $F_{k-1} \mid F_k$ for each k.

Step 1. Let $F_0(x) = \prod_{e\in E}(1 - x^e)^{r_e}$, let $b_0 = B_m(F_0)$, and set $k = 1$.

Step 2. For each $e \in E$, compute $B_m((1-x^e)F_{k-1}(x))$. If the largest of these $|E|$ values is greater than b_{k-1}, then set $F_k(x) = (1 - x^e)F_{k-1}(x)$ for the optimal choice of e, set $b_k = B_m(F_k)$, print F_k and b_k, increment k, and repeat Step 2. Otherwise, continue with Step 3.

Step 3. For each subset $\{e_1, e_2\}$ of E, compute $B_m((1-x^{e_1})(1-x^{e_2})F_{k-1}(x))$. If the largest of these $\binom{|E|}{2}$ values exceeds b_{k-1}, then set $F_k(x) = (1 - x^{e_1})(1 - x^{e_2})F_{k-1}(x)$ for the optimal choice $\{e_1, e_2\}$, set $b_k = B_m(F_k)$, print F_k and b_k, increment k, and repeat Step 3. Otherwise, set $b_{k-1} = 0$ and perform Step 2. □

Several criteria may be used for termination, for example, a prescribed bound on k or $\deg F_k$, or the appearance of a decreasing sequence of values of b_k of a particular length.

We remark that a pure hill-climbing method would omit the resetting of b_{k-1} to 0 at the end of Step 3 and would terminate as soon as none of the adjustments of Steps 2 or 3 improves the bound. By adding this assignment, we need not stop at local maxima and instead allow our objective value to decrease temporarily in order to continue searching for better values.

We use the revolving door algorithm [16] to enumerate the $\binom{|E|}{2}$ combinations of factors to test in Step 3. This way, each polynomial we test can be constructed from the previous polynomial considered with just one division by a binomial and one multiplication.

We implemented Algorithm 4.1 in C++ and ran it on an Apple PowerPC G4. For $m = 2$, letting $F_0(x) = 1 - x^2$ and choosing E to be a set of small positive integers like $\{1, 2, \ldots, 8\}$, we see that Algorithm 4.1 produces a sequence of polynomials of the form $(1 - x^2)^a(1 - x^4)^b$ with $a \approx 3b$. This suggests the sequence $F_k(x) = ((1 - x^2)^3(1 - x^4))^k$ and hence Corollary 3.4. Despite several variations on the initial values, no better sequence was found with Algorithm 4.1 for $m = 2$.

For several values of m greater than 2, Algorithm 4.1, starting with $F_0(x) = 1 - x$, produces a sequence of auxiliary polynomials of the form $(1 - x)^a(1 - x^2)^b$ with $a \approx (m^2 - 1)b$, suggesting the polynomial employed in Corollary 3.5. Our method also indicates a further improvement for the case $m = 3$. With $E = \{1, 2, 3, 4, 5\}$, Algorithm 4.1 constructs the polynomial

$$F(x) = (1 - x)^{1078}(1 - x^2)^{127}(1 - x^5)^3, \tag{4.1}$$

which has $B_3(F) = 1.581983\ldots > \sqrt{10}/2$. This example is investigated further in our second search method.

4.3. *Special families.* A second method of searching for good auxiliary polynomials in Theorem 3.3 computes $\|F\|_\infty$ directly for certain families of pure products rather than using the quantity $L(F)$ as a bound. For a polynomial F, let $\beta_m(F)$ denote the expression appearing in Theorem 3.3:

$$\beta_m(F) = \begin{cases} \dfrac{\nu(F)\log 2 - \log\|F\|_\infty}{\deg F}, & \text{if } m = 2, \\ \dfrac{\nu_0(F)\log m - \log\|F\|_\infty}{\deg F}, & \text{if } m > 2. \end{cases}$$

Given m and fixing a set of positive integers E, we evaluate

$$\beta_m\left(\prod_{e\in E}(1 - x^e)^{r_e}\right)$$

for a number of selections for the exponents r_e, subject to $\gcd\{r_e : e \in E\} = 1$. For example, for $m = 2$ and $E = \{2, 4, 8\}$, we find no polynomials that yield a bound as good as that of Corollary 3.4. However, using $E = \{2, 4, 6\}$,

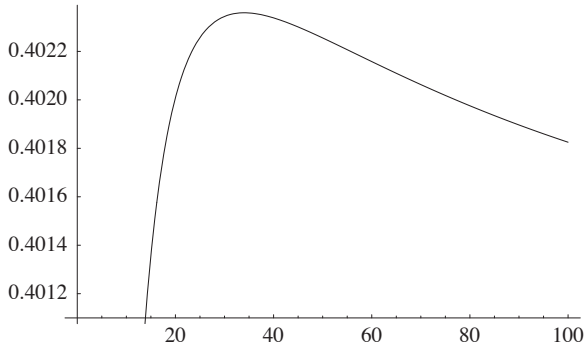

Figure 1: $\beta_2(G_k)$ for $k \le 100$.

we detect an auxiliary polynomial that does just as well. After computing $\beta_2((1-x^2)^a(1-x^4)^b(1-x^6))$ for $1 \le a, b \le 50$, we find that the polynomials

$$G_k(x) = \left(1-x^2\right)^{2k+1}\left(1-x^4\right)^k\left(1-x^6\right)$$

produce values rather close to $(\log 5)/4$, and further that these values are increasing in k over this range. We obtain Figure 1 by computing β_2 for additional polynomials in this sequence. The maximum value occurs at $k = 34$, and

$$\begin{aligned}\|G_{34}\|_\infty &= \left\|(1-y)^{104}(1+y)^{34}(1+y+y^2)\right\|_\infty \\ &= 2^{138}\max_{0\le t\le 1}\left|\sin^{104}(\pi t)\cos^{34}(\pi t)(2\cos(2\pi t)+1)\right| \\ &= \frac{2^{242}}{5^{70}}.\end{aligned}$$

Since $\nu(G_{34}) = 242$ and $\deg G_{34} = 280$, we again obtain (3.7).

For $m = 3$, given (4.1) we investigate polynomials with $E = \{1, 2, 5\}$ and find that we obtain good bounds using $r_1 \approx 8.5r_2$ and $r_3 = 1$. The maximum value of $\beta_3((1-x)^{17k}(1-x^2)^{2k}(1-x^5))$ occurs at $k = 25$, yielding the value $1.582495\ldots$ cited at the end of Section 3.

Similar investigations for larger values of m have not improved the bound of Corollary 3.5. For example, choosing $E = \{1, 2, 5\}$, $r_1 = (2m^2-1)k$, $r_2 = 2k$, $k \ge 1$, and $r_3 = 1$, we obtain a sequence of values under β_m approaching $\log(\sqrt{m^2+1}/2)$ from below, but no polynomial tested improves this bound.

5. The conjecture of Schinzel and Zassenhaus

The lower bounds on $\log \mathrm{M}(f)$ for $f \in \mathcal{D}_m$ of Corollaries 3.4 and 3.5 automatically yield lower bounds on $\max\{|\alpha| : f(\alpha) = 0\}$ for polynomials $f \in \mathcal{D}_m$ having no cyclotomic factors. The following theorem improves these results in the Schinzel-Zassenhaus problem in two ways: weakening the hypotheses and improving the constants.

THEOREM 5.1. *Suppose $f \in \mathcal{D}_m$ is monic with degree $n-1$ having at least one noncyclotomic factor. Then there exists a root α of f satisfying*

$$|\alpha| > \begin{cases} 1 + \dfrac{\log 3}{2n}, & \text{if } m = 2, \\ 1 + \dfrac{\log(m-1)}{n}, & \text{if } m > 2. \end{cases} \tag{5.1}$$

Proof. Let g denote the noncyclotomic part of f, let $d = \deg g$, and let $\alpha_1, \ldots, \alpha_d$ denote the roots of g. Suppose that

$$\max\{|\alpha_k| : 1 \le k \le d\} < 1 + \frac{c}{n}$$

for a positive constant c, so that $|\alpha_k^n| < e^c$ for each k.

Suppose $m = 2$. Since the maximum value of $\left|1 - z^2\right|$ for complex numbers z lying in the disk $\{z : |z| \le r\}$ is $1 + r^2$, with the maximum value occurring at $z = \pm ir$, we have

$$\left|1 - \alpha_k^{2n}\right| < 1 + e^{2c}$$

for each k. Consequently, using Lemma 3.1 with both $x^n + 1$ and $x^n - 1$, we find

$$2^{2d} \le \left|\mathrm{Res}(g(x), 1 - x^{2n})\right| < \left(1 + e^{2c}\right)^d. \tag{5.2}$$

Therefore $1 + e^{2c} > 4$, and the inequality for $m = 2$ follows.

If $m > 2$, in a similar way we obtain

$$m^d \le |\mathrm{Res}(g(x), 1 - x^n)| < (1 + e^c)^d, \tag{5.3}$$

and the theorem follows. □

No better bounds were found by using other auxiliary polynomials in place of $1 - x^{2n}$ and $1 - x^n$ in (5.2) and (5.3). However, for some m we find that the polynomials employed in Corollaries 3.4 and 3.5 do just as well. For example, let $F_{a,b}(x) = (1 - x^2)^a (1 + x^2)^b$, with a and b positive integers. The supremum of $F_{a,b}$ on the disk $\{z \in \mathbf{C} : |z| = r\}$ is

$$\|F_{a,b}\|_{|z|=r} = a^{a/2} b^{b/2} \left(\frac{2(1 + r^4)}{a + b}\right)^{(a+b)/2},$$

and we obtain a lower bound on c from the inequality

$$2^{2a+b} < \|F_{a,b}\|_{|z|=e^c}.$$

The optimal choice of parameters is $a = 4$ and $b = 1$, as in Corollary 3.4, yielding $c \ge (\log 3)/2$. Likewise, for $m > 1$ the optimal choice for a and b in the auxiliary polynomial $(1-x)^a(1+x)^b$ is $a = m^2$ and $b = 1$, but this selection achieves $c \ge \log(m-1)$ only for $m = 3$.

We now show that the constant in Theorem 5.1 for $f \in \mathcal{D}_m$ cannot be replaced with any number larger than $\log(2m-1)$. We first require the following inequality.

LEMMA 5.2. *Suppose* $f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$, *and let* $K = \{k : 0 \le k \le n-1 \text{ and } a_k \neq 0\}$. *For each* $k \in K$, *let* c_k *be a positive number, and suppose that* $\sum_{k\in K} c_k \le 1$. *If* α *is a root of* f, *then*

$$|\alpha| \le \max\left\{ \left(\frac{|a_k|}{c_k}\right)^{\frac{1}{n-k}} : k \in K \right\}.$$

Proof. See [18, part III, problem 20]. □

THEOREM 5.3. *For each* $m \ge 2$, *any* $\varepsilon > 0$, *and all* $n \ge n_0(m,\varepsilon)$, *there exists a polynomial* $f \in \mathcal{D}_m$ *with degree* n *satisfying*

$$1 + \frac{\log m - \varepsilon}{n} < \max_{f(\alpha)=0} |\alpha| < 1 + \frac{\log(2m-1) + \varepsilon}{n}.$$

Proof. Fix $m \ge 2$. Let $f_n(x) = x^n + x^{n-1} + \cdots + x + 1 - m$, so that $(x-1)f_n(x) = x^{n+1} - mx + m - 1$. By Rouché's theorem, f_n has exactly one zero inside the unit disk, and this root is a real number approaching $(m-1)/m$ for large n. Thus f_n^* has a single root outside the unit disk near $m/(m-1)$, so that $\mathrm{M}(f_n) = \mathrm{M}(f_n^*) \to m$ as $n \to \infty$.

If f_n has a reciprocal factor g, then g divides f_n^* as well, and so $g \mid f_n - f_n^* = m(x^n - 1)$. However, $f_n(1) = n + 1 - m$ and $f_n(\zeta) = 1 - m$ for any complex nth root of unity ζ; so f has no reciprocal factor, and hence no roots on the unit circle, if $n \neq m-1$.

Given $\varepsilon > 0$. For sufficiently large n, the polynomial f_n has $n-1$ roots outside the unit circle, and at least one of them must have modulus at least as large as the geometric mean of these roots. Thus,

$$\max_{f_n(\alpha)=0} |\alpha| \ge \mathrm{M}(f_n)^{1/(n-1)} > \left(e^{-\varepsilon} m\right)^{1/(n-1)} > 1 + \frac{\log m - \varepsilon}{n}.$$

For the upper bound, we apply Lemma 5.2 using $f(z) = z^{n+1} - mz + m - 1$, $c_0 = (m-1)/(2m-1)$, and $c_1 = m/(2m-1)$ to obtain

$$\max_{f_n(\alpha)=0} |\alpha| \le (2m-1)^{1/n}.$$

Taking n sufficiently large completes the proof. □

For $m = 2$, the positive real root of the polynomial f_n^* appearing in the proof of Theorem 5.3 is a Pisot number, since all its conjugates lie inside the open unit disk. In the next section we study some properties of Pisot and Salem numbers that appear as roots of Littlewood polynomials.

6. Pisot and Salem numbers

We say a real number $\alpha > 1$ is a *Littlewood-Pisot number* if it is a Pisot number and its minimal polynomial is a Littlewood polynomial, and define a *Littlewood-Salem number* in the same way. The article [4] proves that the minimal value of Mahler's measure of a nonreciprocal polynomial in $\mathcal{D}_2$ is the golden ratio. Thus, this value is the smallest Littlewood-Pisot number.

We first improve Theorem 3.3 slightly for Salem numbers. Since we focus on Littlewood polynomials in this section, we present only the case of polynomials with odd coefficients; an analogous argument improves the bound for Salem numbers whose minimal polynomial lies in $\mathcal{D}_m$ with $m > 2$.

THEOREM 6.1. *Suppose f is a monic, irreducible polynomial in $\mathcal{D}_2$ with degree $n-1$ having exactly one root α outside the unit disk. Then*

$$\log|\alpha| > \frac{\log 5}{4}\left(1 + \frac{1}{10n}\right).$$

Proof. If $F(x)$ is a polynomial with $f(x) \nmid F(x^n)$, then using Lemma 3.1 and the fact that the complex roots of f lie on the unit circle, we obtain

$$2^{\nu(F)(n-1)} \le |\mathrm{Res}(f(x), F(x^n))| \le \|F\|_\infty^{n-3} \left|F(\alpha^n)F(\alpha^{-n})\right|.$$

Choose $F(x) = (1-x^2)^4(1+x^2)$. Then

$$\left|F(\alpha^n)F(\alpha^{-n})\right| = \alpha^{-10n}\left|F(\alpha^n)\right|^2 = \alpha^{-10n}\left(\alpha^{2n}-1\right)^6\left(\alpha^{4n}-1\right)^2 < \alpha^{10n},$$

so that

$$2^{9(n-1)} < \alpha^{10n}\left(\frac{2^9}{5^{5/2}}\right)^{n-3}.$$

Consequently

$$|\alpha| > 5^{1/4}\left(\frac{2^{18}}{5^{15/2}}\right)^{1/10n}.$$

Thus

$$\log|\alpha| > \frac{\log 5}{4} + \frac{9\log 2}{5n} - \frac{3\log 5}{4n} = \frac{\log 5}{4}\left(1 + \frac{c}{n}\right),$$

where

$$c = \frac{36\log 2}{5\log 5} - 3 = .100871\ldots > \frac{1}{10}.$$ □

Our main result of this section concerns a limit point of Littlewood-Salem numbers. It is well-known that every Pisot number is a two-sided limit point of Salem numbers. We prove that more is true for the smallest Littlewood-Pisot number.

THEOREM 6.2. *The smallest Littlewood-Pisot number is a limit point, from both sides, of Littlewood-Salem numbers.*

Proof. We first define two sequences of Littlewood polynomials which have exactly one root outside the unit circle. Let $P_n(x)$ denote the cyclotomic product

$$P_n(x) = \Phi_6(x)\sum_{k=0}^{2n} x^{3k} = \Phi_6(x)\frac{x^{6n+3}-1}{x^3-1} = \Phi_6(x)\prod_{\substack{d|6n+3\\ d>3}} \Phi_d(x),$$

and let

$$p_n(t) = e(-(3n+1)t)P_n(e(t)),$$

where $e(t) = e^{2\pi it}$. Thus, $p_n(t)$ is a real-valued, periodic function with period 1 having simple zeros in the interval $(0, 1/2)$ at the points

$$\left\{\frac{1}{6}\right\} \bigcup \left\{\frac{k}{6n+3} : 1 \le k \le 3n+1, k \ne 2n+1\right\}.$$

Let

$$a_n(t) = 2\cos((6n+2)\pi t)$$

and

$$b_n(t) = -4\sin(\pi t)\sin((6n+1)\pi t).$$

Since

$$\frac{2k-1}{12n+4} < \frac{k}{6n+3} < \frac{2k+1}{12n+4} < \frac{k+1}{6n+3}$$

for $1 \le k \le 3n$, it follows that between two consecutive zeros of $a_n(t)$ in $(0, 1/2)$ there exists exactly one zero of $p_n(t)$, with two exceptions corresponding to the absence of a zero of $p_n(t)$ at $t = 1/3$ and the extra zero at $t = 1/6$. Consequently, the function $a_n(t) - p_n(t)$ has at least $3n-2$ zeros in $(0, 1/2)$. A similar computation verifies that $p_n(t) - b_n(t)$ has at least $3n-2$ zeros in $(0, 1/2)$.

For $n \ge 1$, define the Littlewood polynomials $A_n(x)$ and $B_n(x)$ by

$$A_n(x) = x^{6n} + (1 - x - x^2)\sum_{k=0}^{2n-1} x^{3k} \tag{6.1}$$

and

$$B_n(x) = x^{6n-1} + (1 + x - x^2)\sum_{k=0}^{2n-1} x^{3k}, \tag{6.2}$$

so that $\deg A_n = 6n$ and $\deg B_n = 6n-2$. Since

$$P_n(x) + xA_n(x) = x^{6n+2} + 1$$

and

$$P_n(x) - x^2 B_n(x) = (x-1)(x^{6n+1}-1),$$

it follows that $e(-3nt)A_n(e(t))$ and $e(-(3n-1)t)B_n(e(t))$ each have at least $6n-4$ zeros in $(0,1)$, and thus that $A_n(x)$ and $B_n(x)$ each have at least $6n-4$ zeros on the unit circle. Since $A_n(-1) = 1$, $A_n(1) = 1-2n$, $B_n(-1) = -1$, and $B_n(1) = 1+2n$, it follows that $A_n(x)$ and $B_n(x)$ have one real root in the interval $(-1,1)$, and, since these polynomials are reciprocal, one real root outside the unit disk as well. This accounts for all roots of $B_n(x)$, and all but two roots of $A_n(x)$. These last two roots cannot be real, since evidently $A_n(x)$ has an odd number of roots in $[-1,1]$ and hence its total number of real roots is congruent to 2 mod 4. Also, they must have modulus 1, for otherwise a root α would have distinct conjugates $1/\alpha$, $\overline{\alpha}$, and $1/\overline{\alpha}$.

We next prove that $A_n(x)$ and $B_n(x)$ are irreducible. Let α_n denote the real root of $A_n(x)$ outside the unit disk, and let β_n denote that of $B_n(x)$. If $f \mid A_n$ and $f(\alpha_n) \neq 0$, then by Kronecker's theorem f is a product of cyclotomic polynomials. Suppose then that $\Phi_d \mid A_n$. By Lemma 2.3, we have $d \mid 12n+2$. If $d \mid 6n+1$, then Φ_d divides

$$A_n(x) + \frac{x^{6n+1}-1}{x-1} = 2\frac{x^{6n+3}-1}{x^3-1},$$

so that $d \mid 6n+3$ and thus $d = 1$, but $A_n(1) \neq 0$. If d is an even divisor of $12n+2$, then $\Phi_{d/2}(x) \mid A_n(-x)$. Since

$$\frac{x^{6n+1}-1}{x-1} - A_n(-x) = 2x^2\Phi_3(x)\frac{x^{6n}-1}{x^6-1},$$

we have $d \mid 12n$ as well and again arrive at a contradiction. The proof that $B_n(x)$ is irreducible is similar.

Let γ denote the golden ratio, $\gamma = (1+\sqrt{5})/2$. Since $A_n(1) = 1-2n$ and $A_n(\gamma) = 1$, we have $\alpha_n < \gamma$ for each n. Similarly, we compute $B_n(-2) = (2^{6n-1}-5)/9$ and $B_n(-\gamma) = 1-\gamma$, so that $\beta_n < -\gamma$ for each n. Further,

$$\begin{aligned} A_{n+1}(\alpha_n) &= \alpha_n^{6n+6} - \alpha_n^{6n} + (1-\alpha_n-\alpha_n^2)(\alpha_n^{6n}+\alpha_n^{6n+3}) \\ &= \alpha_n^{6n+1}(\alpha_n^3+1)(\alpha_n^2-\alpha_n-1), \end{aligned}$$

and since $x^2 - x - 1 < 0$ on $(1,\gamma)$, we conclude $A_{n+1}(\alpha_n) < 0$ and thus $\alpha_{n+1} > \alpha_n$. Similarly,

$$B_{n+1}(\beta_n) = \beta_n^{6n-1}(\beta_n^3+1)(\beta_n^2+\beta_n-1) > 0,$$

and so $\beta_{n+1} > \beta_n$. Thus, the sequences $\{\alpha_n\}$ and $\{\beta_n\}$ converge.

Finally, since $A_n(x)$ converges uniformly to $(1-x-x^2)/(1-x^3)$ on any compact subset of $(-1,1)$, it follows that $\lim_{n\to\infty} 1/\alpha_n = 1/\gamma$, and so $\{\alpha_n\}$ converges to γ. Similarly, $\{\beta_n\}$ converges to $-\gamma$. Thus, $A_n(x)$ and $B_n(-x)$ provide the required Littlewood-Salem numbers. □

The root α_1 of $A_1(x)$ in the proof of Theorem 6.2 is the smallest known measure of an irreducible Littlewood polynomial. Moreover, the sequences $\{\alpha_n\}$ and $\{-\beta_n\}$ encompass all known values of Mahler's measure below 1.645 of reciprocal, irreducible Littlewood polynomials (see [15]).

Finally, it is likely that the method of the proof extends, at least in part, to the other Littlewood-Pisot numbers appearing in the proof of Theorem 5.3. Let

$$f_m(x) = x^{m-1} - \sum_{k=0}^{m-2} x^k,$$

and let γ_m denote the Pisot number having $f_m(x)$ as its minimal polynomial. Following (6.1) and (6.2), for each $m \geq 3$ and $n \geq 1$ define the Littlewood polynomials

$$A_{m,n}(x) = x^{2mn} + f_m^*(x) \sum_{k=0}^{2n-1} x^{mk}$$

and

$$B_{m,n}(x) = x^{2mn-1} - f_m(x) \sum_{k=0}^{2n-1} x^{mk}.$$

For each m, it appears that $A_{m,n}(x)$ yields a sequence of Salem numbers approaching γ_m from below. However, while $\mathrm{M}(B_{m,n})$ approaches γ_m as $n \to \infty$, evidently $B_{m,n}(x)$ has $m-2$ roots outside the unit circle.

Added in proof. Since this article was written, some other papers have appeared on the topics treated in this paper. Lower bounds in Lehmer's problem and the Schinzel-Zassenhaus problem for polynomials with coefficients congruent to 1 mod m are developed further in

A. Dubickas and M. J. Mossinghoff, Auxiliary polynomials for some problems regarding Mahler's measure, *Acta Arith.* **119** (2005), 65–79.

Results on Lehmer's problem are generalized in

C. L. Samuels, The Weil height in terms of an auxiliary polynomial, *Acta Arith.* **128** (2007), 209–221.

More information on Littlewood-Pisot and Salem numbers may be found in

K. Mukunda, Littlewood Pisot numbers, *J. Number Theory* **117** (2006), 106–121.

Simon Fraser University, Burnaby, B.C., Canada
E-mail address: pborwein@cecm.sfu.ca

College of New Caledonia, Prince George, B.C., Canada
E-mail address: dobrowolski@cnc.bc.ca

Davidson College, Davidson, N.C., USA
E-mail address: mjm@member.ams.org

References

[1] F. Amoroso and R. Dvornicich, A lower bound for the height in abelian extensions, *J. Number Theory* **80** (2000), 260–272.

[2] F. V. Atkinson, On a problem of Erdős and Szekeres, *Canad. Math. Bull.* **4** (1961), 7–12.

[3] A. S. Belov and S. V. Konyagin, An estimate for the free term of a nonnegative trigonometric polynomial with integer coefficients (Russian), *Mat. Zametki* **59** (1996), 627–629. Translation in *Math. Notes* **59** (1996), 451–453.

[4] P. Borwein, K. G. Hare, and M. J. Mossinghoff, The Mahler measure of polynomials with odd coefficients, *Bull. London Math. Soc.* **36** (2004), 332–338.

[5] P. Borwein and M. J. Mossinghoff, Polynomials with height 1 and prescribed vanishing at 1, *Experiment. Math.* **9** (2000), 425–433.

[6] D. C. Cantor and E. G. Straus, On a conjecture of D. H. Lehmer, *Acta Arith.* **42** (1982), 97–100. Correction, *ibid.* **42** (1983), 327.

[7] J. D. Dixon and A. Dubickas, The values of Mahler measures, *Mathematika* **51** (2005), 131–148.

[8] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.

[9] P. Erdős, Problems and results on diophantine approximations, *Compositio Math.* **16** (1964), 52–65.

[10] P. Erdős and G. Szekeres, On the product $\prod_{k=1}^{n}(1-z^{a_k})$, *Acad. Serbe Sci. Publ. Inst. Math.* **13** (1959), 29–34.

[11] M. N. Kolountzakis, On nonnegative cosine polynomials with nonnegative integral coefficients, *Proc. Amer. Math. Soc.* **120** (1994), 157–163.

[12] D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. of Math.* **34** (1933), 461–479.

[13] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, Cambridge, 1994.

[14] R. Maltby, Pure product polynomials and the Prouhet-Tarry-Escott problem, *Math. Comp.* **66** (1997), 1323–1340.

[15] M. J. Mossinghoff, *Lehmer's Problem*, http://www.cecm.sfu.ca/∼mjm/Lehmer, 2003.

[16] A. Nijenhuis and H. S. Wilf, *Combinatorial Algorithms*, Academic Press, New York, 1975.

[17] A. M. Odlyzko, Minima of cosine sums and maxima of polynomials on the unit circle, *J. London Math. Soc.* **26** (1982), 412–420.

[18] G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, vol. I, Springer-Verlag, New York, 1972.

[19] R. Salem, Power series with integral coefficients, *Duke Math. J.* **12** (1945), 153–172.

[20] A. Schinzel, On the product of the conjugates outside the unit circle of an algebraic number, *Acta Arith.* **24** (1973), 385–399; Addendum, *ibid.* **26** (1975), 329–331.

[21] A. Schinzel and H. Zassenhaus, A refinement of two theorems of Kronecker, *Michigan Math. J.* **12** (1965), 81–85.

[22] C. J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, *Bull. London Math. Soc.* **3** (1971), 169–175.

(Received October 2, 2003)