ACTA ARITHMETICA
119.1 (2005)

Auxiliary polynomials for some problems regarding Mahler's measure

by

Artūras Dubickas (Vilnius) and
Michael J. Mossinghoff (Davidson, NC)

1. Introduction. In this paper, we describe an iterative method of constructing some favorable auxiliary polynomials used to obtain lower bounds in some problems of algebraic number theory. With this method we improve a lower bound on Mahler's measure of a polynomial with no cyclotomic factors whose coefficients are all congruent to 1 modulo m for some integer $m \geq 2$, raise a lower bound in the problem of Schinzel and Zassenhaus on the largest root of such a polynomial, and improve a lower bound on the absolute Weil height of an algebraic unit whose minimal polynomial splits completely over a p-adic field.

Recall that *Mahler's measure* of a polynomial $f(x) = a\prod_{k=1}^{\deg f}(x-\alpha_k)$ is defined by

$$M(f) = |a| \prod_{k=1}^{\deg f} \max\{1, |\alpha_k|\}.$$

Clearly $M(f) \geq 1$ for $f \in \mathbb{Z}[x]$, and a well known result of Kronecker implies that equality occurs precisely when f is a product of cyclotomic polynomials and a power of the monomial x. In 1933, D. H. Lehmer [9] found that the polynomial

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

has $M(\ell) = 1.176280\ldots$, and this remains the smallest known value larger than 1 of the measure of a polynomial with integer coefficients. *Lehmer's problem* asks if there exist polynomials in $\mathbb{Z}[x]$ with measure arbitrarily close to 1.

2000 *Mathematics Subject Classification*: Primary 11R09; Secondary 11C08, 12D05.

Key words and phrases: Lehmer's problem, Schinzel–Zassenhaus conjecture, Mahler's measure, Weil height, Littlewood polynomials.

The research of the first author was partially supported by the Lithuanian State Science and Studies Foundation.

Lehmer's problem has been resolved in some special cases. For example, let f^* denote the polynomial obtained from f by reversing its sequence of coefficients, so $f^*(x) = x^{\deg f} f(1/x)$. We say f is *reciprocal* if $f = \pm f^*$. Smyth [14] proved that if f is nonreciprocal and $f(0) \neq 0$, then $M(f) \geq M(x^3 - x - 1) = 1.324717\ldots$. Recently, Lehmer's problem was resolved for another class of polynomials. For a positive integer $m \geq 2$, let $\mathcal{D}_m$ denote the set of polynomials whose coefficients are all congruent to 1 modulo m:

$$\mathcal{D}_m = \Big\{ f(x) = \sum_{k=0}^{\deg f} a_k x^k \in \mathbb{Z}[x] : a_k \equiv 1 \bmod m \text{ for } 0 \leq k \leq \deg f \Big\}.$$

The set $\mathcal{D}_2$ is precisely the set of polynomials with odd coefficients, so it contains the frequently studied set of *Littlewood polynomials*, whose coefficients are all ± 1. In [4], it is shown that if $f \in \mathcal{D}_m$ has degree $n-1$ and no cyclotomic factors, then

$$\log M(f) \geq \begin{cases} \dfrac{\log 5}{4}\left(1 - \dfrac{1}{n}\right) & \text{if } m = 2, \\ \log\left(\dfrac{\sqrt{m^2+1}}{2}\right)\left(1 - \dfrac{1}{n}\right) & \text{if } m > 2. \end{cases} \tag{1}$$

The proof requires constructing some auxiliary polynomials with certain favorable properties, and the polynomials employed there were found by searching certain promising families. In Section 2 we describe a method for constructing better auxiliary polynomials directly, and use this technique to improve the bounds in (1) (see Theorem 2.4).

A problem related to Lehmer's was posed by Schinzel and Zassenhaus in 1965 [13]. They conjectured that there exists a positive constant c so that every monic, irreducible polynomial of degree d has a root α satisfying $|\alpha| > 1 + c/d$. It is easy to verify that answering Lehmer's question resolves this problem as well: if $M(f) \geq M_0$ for each f in a particular set of monic polynomials, then one may take $c = \log M_0$ in the problem of Schinzel and Zassenhaus for this same set. However, the best known results in this problem are often stronger than those inherited in this way from corresponding inequalities in Lehmer's problem. For example, it is shown in [7] that one may take $c = 0.3096\ldots$ for the case of nonreciprocal polynomials, strengthening the bound inherited from Smyth's theorem. Likewise, in [4] it is shown that if $f \in \mathcal{D}_m$ is monic with degree $n-1$ and has at least one noncyclotomic factor, then there exists a root α of f satisfying

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

Our method allows us to improve the bounds in these inequalities. This problem is treated in Section 3 (see Theorem 3.1).

The *logarithmic Weil height* of an algebraic number α is defined by

$$h(\alpha) = \frac{\log M(\alpha)}{\deg(\alpha)},$$

where $M(\alpha)$ denotes Mahler's measure of the minimal polynomial for α. A result of Schinzel [12] implies that if α is totally real and $\alpha \notin \{-1, 0, 1\}$ then $h(\alpha) \geq (\log \gamma)/2$, where γ denotes the golden ratio, $\gamma = (1 + \sqrt{5})/2$; a simple proof of this fact appears in [8]. Bombieri and Zannier [2] extended Schinzel's result to local fields. We say an algebraic number α is *totally p-adic* if the minimal polynomial $f \in \mathbb{Z}[x]$ for α splits completely in the field $\mathbb{Q}_p$ of p-adic numbers, or equivalently, if the prime p splits completely in the field $\mathbb{Q}(\alpha)$. For a prime number p, define the quantity σ_p by

$$\sigma_p = \inf\{h(\alpha) : \alpha \in \overline{\mathbb{Q}} \text{ is totally } p\text{-adic and } M(\alpha) > 1\}.$$

Bombieri and Zannier proved that $\sigma_p > 0$ for each prime p. Recently, Petsche [11] obtained explicit lower bounds for $h(\alpha)$ for the case when α is an algebraic unit, that is, when both α and α^{-1} are algebraic integers. Define the quantity τ_p by

$$\tau_p = \inf\{h(\alpha) : \alpha \in \overline{\mathbb{Q}} \text{ is a totally } p\text{-adic algebraic unit and } M(\alpha) > 1\},$$

so clearly $\sigma_p \leq \tau_p$. Petsche established that

$$\tau_p \geq \begin{cases} \log(\sqrt{2}) & \text{if } p = 2, \\ \dfrac{\log(p/2)}{p-1} & \text{if } p > 2. \end{cases} \tag{3}$$

We use our method to improve these bounds for every prime p in Section 4; see (13) and (14).

Throughout this article, let $\mathrm{Res}(f(x), g(x))$ denote the resultant of the polynomials $f(x)$ and $g(x)$.

2. Lehmer's problem. We first study the problem of obtaining a lower bound on the measure of a polynomial $f \in \mathcal{D}_m$ that is not a product of cyclotomic polynomials. We require the following lemma.

LEMMA 2.1. *Suppose $f \in \mathcal{D}_m$ is monic with degree $n-1$, and let α be a root of f. Suppose also that $G \in \mathbb{Z}[x]$ satisfies $m \,|\, G(1)$. Then $G(\alpha^n)/m$ is an algebraic integer. Further, if g is a factor of f with degree d and $\gcd(g(x), G(x^n)) = 1$, then*

$$|\mathrm{Res}(g(x), G(x^n))| \geq m^d.$$

Proof. Since $f \in \mathcal{D}_m$, the polynomial $s(x)$ defined by

$$s(x) = \frac{x^n - 1 - (x-1)f(x)}{m}$$

has integer coefficients, so $s(\alpha) = (\alpha^n - 1)/m$ is an algebraic integer. Writing $G(x) \equiv (x-1)q(x) \bmod m$ for some integer polynomial q, we see that $G(\alpha^n)/m$ is an algebraic integer. For the second part, suppose α is a root of g, and let K denote the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Since $G(\alpha^n) \neq 0$, we have

$$|N_{K/\mathbb{Q}}(G(\alpha^n))| \geq m^{[K:\mathbb{Q}]},$$

and raising both sides to the power $d/[K:\mathbb{Q}]$ yields the final inequality. ∎

For an auxiliary polynomial $F \in \mathbb{Z}[x]$, let $\nu_m(F)$ denote the number of irreducible factors G of F satisfying $m \mid G(1)$. Also, if $\deg F = r$, define the quantity $\omega_m(F)$ by

$$\omega_m(F) = \gcd(F(1), mF'(1), m^2F''(1)/2, \ldots, m^rF^{(r)}(1)/r!). \tag{4}$$

Let $c_k = m^kF^{(k)}(1)/k!$ for $0 \leq k \leq r$, so each c_k is an integer divisible by $\omega_m(F)$. Suppose α, f, and g are as in the statement of Lemma 2.1. Since $F(x) = \sum_{k=0}^{r} c_k((x-1)/m)^k$, using the argument of the lemma we see that $F(\alpha^n)/\omega_m(F)$ is an algebraic integer, and so $\omega_m(F)^d \mid \mathrm{Res}(g(x), F(x^n))$. Note also that $\omega_m(G_1G_2) \geq \omega_m(G_1)\omega_m(G_2)$ for any integer polynomials G_1 and G_2, and that consequently $\omega_m(F) \geq m^{\nu_m(F)}$.

Finally, we define for an integer polynomial F the quantity

$$B_m(F) = \frac{\log \omega_m(F) - \log\|F\|_\infty}{\deg F}, \tag{5}$$

where $\|F\|_\infty$ stands for the maximum of $|F(x)|$ on the unit circle. We now establish the following lower bound on Mahler's measure of a factor of a polynomial in $\mathcal{D}_m$.

THEOREM 2.2. *Suppose $f \in \mathcal{D}_m$ has degree $n-1$, $g \in \mathbb{Z}[x]$ is a factor of f with degree d, and $F \in \mathbb{Z}[x]$ satisfies $\gcd(g(x), F(x^n)) = 1$. Then*

$$\log M(g) \geq B_m(F)d/n.$$

Proof. From the discussion above, we have

$$|\mathrm{Res}(g(x), F(x^n))| \geq \omega_m(F)^d,$$

and, since $|F(x)| \leq \|F\|_\infty \max\{1, |x|\}^{\deg F}$, we find

$$|\mathrm{Res}(g(x), F(x^n))| \leq \|F\|_\infty^d M(g)^{n \deg F}.$$

The result follows by combining these inequalities. ∎

We aim then to optimize the lower bound in the theorem by constructing favorable auxiliary polynomials. Throughout the rest of this section, we consider only auxiliary polynomials F having all their roots on the unit

circle. Hence, if g is a monic, irreducible, noncyclotomic factor of f, then the condition $\gcd(g(x), F(x^n)) = 1$ of the theorem is automatically satisfied. By Siegel's lemma (see, e.g., [1] or [10]), if $g \in \mathbb{Z}[x]$ is an irreducible polynomial with degree d and $M(g) < 2$, then there exists a polynomial f with $\{-1, 0, 1\}$ coefficients such that $g \mid f$ and $\deg f < n$, where n satisfies $(n^{d/2} M(g)^{n-1})^{1/(n-d)} < 2$. Suppose that $M(g) < 2 - \varepsilon$, with ε a fixed small positive number. Then g is a divisor of a polynomial f with $\{-1, 0, 1\}$ coefficients and degree less than $n = \kappa_\varepsilon d \log d$, where κ_ε is a positive constant depending only on ε. If, by chance, the polynomial f is a Littlewood polynomial, then Theorem 2.2 with $m = 2$ implies that for such g we have $\log M(g) > c_\varepsilon / \log d$, for a positive constant c_ε. This is better than the bound of Dobrowolski [6], which asserts that $\log M(g) > c(\log\log d / \log d)^3$ for every irreducible, noncyclotomic polynomial $g \in \mathbb{Z}[x]$ of degree d. This raises an interesting question: which polynomials of small measure are divisors of Littlewood polynomials? A partial answer appears in [4]: for any prime number p, a polynomial $g \in \mathbb{Z}[x]$ is the noncyclotomic part of some polynomial $f \in \mathcal{D}_p$ precisely when g is congruent modulo p to a product of cyclotomic polynomials. Measures of Littlewood polynomials are studied further in [5].

In [4], two methods are used to search for auxiliary polynomials that produce a good lower bound on the measure of a polynomial in $\mathcal{D}_m$ having no cyclotomic factors. Both of them consider polynomials of the form $F(x) = \prod_{k=1}^{n} (x^{e_k} - 1)$, with each e_k a positive integer: one of them employs a greedy strategy; the other tests certain specific families. In that paper, the quantity $m^{\nu_m(F)}$ is in essence used in place of $\omega_m(F)$. Here, we find improvements not only by introducing $\omega_m(F)$, but, more importantly, by observing that given one auxiliary polynomial F_0 with $B_m(F_0) > 0$, we may often use it to construct another auxiliary polynomial F_1 with $B_m(F_1) > B_m(F_0)$. We propose then an iterative algorithm for constructing a sequence of favorable auxiliary polynomials directly, and we obtain improved lower bounds on the measure of polynomials in $\mathcal{D}_m$ by using this method. More precisely, note that $B_m(F^a)$ is constant for all positive integers a, so if Q denotes a polynomial that has a zero where F achieves its maximum over the unit circle, then for some a we may find that $B_m(F^a Q)$ exceeds $B_m(F)$, particularly if $\omega_m(Q) > 1$. This raises another interesting problem: find $\sup\{B_m(F) : F \in \mathbb{Z}[x]\}$, where $B_m(F)$ is defined in (5).

ALGORITHM 2.3. *Construction of auxiliary polynomials.*

Input. An integer $m \geq 2$.

Output. A sequence of polynomials $\{F_k\}$ for which $\{B_m(F_k)\}$ is increasing.

Step 1. Set $k = 0$, and let $F_0(x) = x - 1$.

Step 2. Let Q_k denote an irreducible polynomial that has a zero at a point where $|F_k|$ attains its maximum over the unit disk. Select an integer a_k so that $B_m(F_k^{a_k}Q_k)$ is maximized. Set $F_{k+1} = F_k^{a_k}Q_k$.

Step 3. If $B_m(F_{k+1}) > B_m(F_k)$, increment k by 1 and repeat Step 2. ∎

2.1. *The case* $m = 2$. We apply this method for the case $m = 2$. We clearly have $\omega_2(F_0) = \omega_2(x-1) = 2$, so $B_2(F_0) = 0$ and $Q_0(x) = x+1$. Similarly, $\omega_2((x-1)^{a_0}(x+1)) = 2^{a_0+1}$. Since

$$\|(x-1)^{a_0}(x+1)\|_\infty = 2^{a_0+1} \max_{0\le t\le\pi} |(\sin t)^{a_0}\cos t| = \frac{2^{a_0+1}a_0^{a_0/2}}{(a_0+1)^{(a_0+1)/2}},$$

we find that

$$B_2((x-1)^{a_0}(x+1)) = \frac{(a_0+1)\log(a_0+1) - a_0\log a_0}{2(a_0+1)},$$

and this expression is maximized by choosing $a_0 = 1$. We thus take $F_1(x) = x^2-1$, so $Q_1(x) = x^2+1$, and

$$B_2(F_1) = \frac{\log 2}{2} = 0.3465735902\ldots.$$

In the next iteration, we verify that $\omega_2(F_1^{a_1}Q_1) = 2^{2a_1+1}$, and since $\|F_1^{a_1}Q_1\|_\infty = \|(x-1)^{a_1}(x+1)\|_\infty$, we obtain

$$B_2((x^2-1)^{a_1}(x^2+1)) = \frac{2a_1\log 2 + (a_1+1)\log(a_1+1) - a_1\log a_1}{4(a_1+1)}.$$

A short calculation verifies that this expression is maximized when $a_1 = 4$, so we take $F_2(x) = (x^2-1)^4(x^2+1)$, and find that

$$B_2(F_2) = \frac{\log 5}{4} = 0.4023594781\ldots.$$

This is the best bound obtained for the case $m = 2$ in [4]; we now improve this value with further iterations.

As $F_2(x)$ attains its maximum over the unit circle when $x^2 = (-3\pm 4i)/5$, we set $Q_2(x) = 5x^4+6x^2+5$. Certainly $\nu_2(Q_2) = 1$, but the expansion

$$Q_2(x) = 5(x-1)^4 + 20(x-1)^3 + 36(x-1)^2 + 32(x-1) + 16$$

shows that $\omega_2(Q_2) = 16$. Hence $\omega_2(F_2^{a_2}Q_2) \ge 2^{9a_2+4}$, and one may verify easily that in fact equality occurs. The maximum value of $|F_2(e^{i\theta})^{a_2}Q_2(e^{i\theta})|$ occurs when $y = \cos(2\theta)$ satisfies

$$(25a_2+10)y^2 + 30a_2y + 9a_2 - 10 = 0, \tag{6}$$

and we compute that $B_2(F_2^{a_2}Q_2)$ is maximized when $a_2 = 3.9764\ldots$. Choosing $F_3(x) = (x^2-1)^{16}(x^2+1)^4(5x^4+6x^2+5)$ yields $\omega_2(F_3) = 2^{40}$ and

$$B_2(F_3) = 0.4161410261\ldots.$$

Another iteration improves this value still further. Substituting $a_2 = 4$ and $y = (x^2 + x^{-2})/2$ in (6) and normalizing, we compute

$$Q_3(x) = 55x^8 + 120x^6 + 162x^4 + 120x^2 + 55.$$

Expanding $Q_3(x)$ in powers of $x - 1$, we find that $\omega_2(Q_3) = 64$, hence $\omega_2(F_3^{a_3}Q_3) \geq 2^{40a_3+6}$. An easy computation shows that again we have equality. The maximum modulus of this polynomial over the unit circle occurs when $y = \cos(2\theta)$ satisfies

$$275(11a_3 + 2)y^4 + 30(220a_3 + 21)y^3 + 10(503a_3 - 37)y^2 + 30(52a_3 - 21)y + 169a_3 - 180 = 0, \tag{7}$$

and we compute that the optimal value of $B_2(F_3^{a_3}Q_3)$ occurs at $a_3 = 133.291\ldots$. Setting $F_4 = F_3^{133}Q_3$, we obtain

$$B_2(F_4) = 0.4162307204\ldots.$$

It appears that further iterations of this procedure yield additional, though small, improvements to this value. For example, from (7) we determine

$$Q_4(x) = 402875(x^{16} + 1) + 1756860x^2(x^{12} + 1) + 4285980x^4(x^8 + 1) + 6925380x^6(x^4 + 1) + 8122962x^8,$$

and we compute that $\omega_2(F_4^{a_4}Q_4) = 2^{5326a_4+12}$. Choosing $a_4 = 33264$ yields

$$B_2(F_5) = 0.4162307230\ldots.$$

2.2. *The case of odd $m > 2$.* We describe the behavior of Algorithm 2.3 for a fixed odd integer $m \geq 3$. Since $\omega_m(x - 1) = m$, we begin by noting that

$$B_m(F_0) = \log(m/2).$$

With $Q_0(x) = x + 1$, we compute

$$B_m(F_0^{a_0}Q_0) = \frac{2a_0 \log m - 2(a_0 + 1)\log 2 - a_0 \log a_0 + (a_0 + 1)\log(a_0 + 1)}{2(a_0 + 1)},$$

which is maximized by selecting $a_0 = m^2$. Setting $F_1(x) = (x-1)^{m^2}(x+1)$, we find

$$B_m(F_1) = \log\left(\frac{\sqrt{m^2+1}}{2}\right) = \log(m/2) + \frac{1}{2m^2} - \frac{1}{4m^4} + O\left(\frac{1}{m^6}\right).$$

This is the value obtained in [4] for all $m > 2$.

In the next iteration, we find that F_1 attains its maximum modulus over the unit circle where $\cos\theta = (1 - m^2)/(1 + m^2)$, so

$$Q_1(x) = (m^2+1)(x^2+1)+2(m^2-1)x = (m^2+1)(x-1)^2+4m^2(x-1)+4m^2.$$

Since m is odd, we find that $\omega_m(Q_1) = 2m^2$, and verify that $\omega_m(F_1^{a_1}Q_1) = 2m^{a_1m^2+2}$. Noting that the maximum modulus of $F_1^{a_1}Q_1$ over the unit circle

occurs when $y = \cos\theta$ satisfies

$$(m^2+1)(a_1(m^2+1)+2)y^2 + 2a_1(m^4-1)y + a_1(m^2-1)^2 - 2(m^2+1) = 0,$$

we may then compute the optimal choice of a_1 for any fixed value of m. We find empirically that this value is always near $3/2$; for example, for $m = 3$, 5, 7, 9, and 101, the optimal choices are respectively $a_1 = 1.42644\ldots$, $1.47264\ldots$, $1.48591\ldots$, $1.49144\ldots$, and $1.49993\ldots$. Setting $a_1 = 3/2$ and

$$F_2(x) = (x-1)^{3m^2}(x+1)^3((m^2+1)(x^2+1)+2(m^2-1)x)^2,$$

we compute

$$\begin{aligned}(8)\quad B_m(F_2) &= (2(3m^2+4)\log m + (3m^2+7)\log(3m^2+7)\\ &\quad + 3(m^2+1)\log(m^2+1) - 2(3m^2+7)\log 2\\ &\quad - 3m^2\log((m^2+1)(3m^2+2) - 2\sqrt{(m^2+1)(4m^2+1)})\\ &\quad - 4\log(m^2-1+\sqrt{(m^2+1)(4m^2+1)})\\ &\quad - 3\log(5(m^2+1)+2\sqrt{(m^2+1)(4m^2+1)}))/(6m^2+14)\\ &= \log(m/2) + \frac{3-\log 3}{2m^2} - \frac{27-14\log 3}{12m^4} + O\left(\frac{1}{m^6}\right).\end{aligned}$$

A third iteration produces further, though small, improvements. Using

$$\begin{aligned}Q_2(x) &= (3m^2+7)(m^2+1)(x^4+1) + 12x(m^4-1)(x^2+1)\\ &\quad + (9m^4-10m^2+5)x^2\\ &= (3m^7+7)(m^2+1)(x-1)^4 + 8(m^2+1)(3m^2+2)(x-1)^3\\ &\quad + 8(9m^4+5m^2+2)(x-1)^2 + 96m^4(x-1) + 48m^4,\end{aligned}$$

we find that $\omega_m(Q_2) = 16m^2$. Hence, for any fixed odd integer m, we may compute the optimal value of a_2 to find F_3. For odd m ranging from $m = 3$ to $m = 11$, and choosing $a_2 = 41$, 267, 968, 2570, and 5654 respectively, we

Table 1. Values of $B_m(F_k)$

m	$B_m(F_0)$	$B_m(F_1)$	$B_m(F_2)$	$B_m(F_3)$
3	0.4054651	0.4581453	0.5006408	0.5010266
4	0.6931471	0.8047189	0.8322820	0.8324614
5	0.9162907	0.9359010	0.9528456	0.9528692
6	1.0986122	1.1512925	1.1658631	1.1658844
7	1.2527629	1.2628643	1.2717720	1.2717754
8	1.3862943	1.4166066	1.4253654	1.4253697
9	1.5040773	1.5102124	1.5156691	1.5156698
10	1.6094379	1.6290482	1.6348355	1.6348367
11	1.7047480	1.7088633	1.7125396	1.7125398

obtain the values shown in the last column of Table 1. For comparison, this table also lists the values of the bounds from previous rounds for these m. Each value here is truncated (not rounded) at the seventh decimal place.

We note that the best bound obtained for $m = 3$ is $0.5010266\ldots$ and exceeds the value of 0.459003 derived in [4] by using the auxiliary polynomial $(1-x)^{425}(1-x^2)^{50}(1-x^5)$.

2.3. *The case of even $m > 2$.* We obtain better bounds using Algorithm 2.3 for the case of an even integer $m \geq 4$. Again, $B_m(F_0) = \log(m/2)$ and $Q_0(x) = x+1$, but since

$$(x-1)^{a_0}(x+1) = (x-1)^{a_0+1} + 2(x-1)^{a_0},$$

we find that $\omega_m((x-1)^{a_0}(x+1)) = 2m^{a_0}$. Noting that the maximum value of $B_m((x-1)^{a_0}(x+1))$ occurs at $a_0 = m^2/4$, we set $F_1(x) = (x-1)^{m^2/4}(x+1)$, and compute

$$B_m(F_1) = \log\left(\frac{\sqrt{m^2+4}}{2}\right) = \log(m/2) + \frac{2}{m^2} - \frac{4}{m^4} + O\left(\frac{1}{m^6}\right).$$

We then find that

$$Q_1(x) = (m^2+4)(x^2+1)+2(m^2-4)x = (m^2+4)(x-1)^2+4m^2(x-1)+4m^2,$$

so $\omega_m(Q_1) = 4m^2$. The maximum value of $|F_1^{a_1}Q_1|$ on the unit circle occurs when $y = \cos\theta$ satisfies

$$(m^2+4)(a_1(m^2+4)+8)y^2 + 2a_1(m^4-16)y + a_1(m^2-4)^2 - 8(m^2+4) = 0,$$

and we may again compute the optimal value of a_1 for any even m. We find that the optimal value is always near 4 (for example, for $m = 4$, 6, 8, and 100, we obtain $3.97641\ldots$, $3.98593\ldots$, $3.99125\ldots$, and $3.99993\ldots$, respectively). Setting $a_1 = 4$ and

$$F_2(x) = (x-1)^{m^2}(x+1)^4((m^2+4)(x^2+1)+2(m^2-4)x),$$

we compute

$$\begin{aligned}(9)\qquad B_m(F_2) &= (2(m^2+2)\log m + (m^2+4)\log(m^2+4)\\ &\quad + (m^2+6)\log(m^2+6) - 2m^2\log 2\\ &\quad - m^2\log((m^2+1)(m^2+4) - \sqrt{(m^2+4)(9m^2+4)})\\ &\quad - 2\log(m^2-4+\sqrt{(m^2+4)(9m^2+4)})\\ &\quad - 4\log(5(m^2+4)+\sqrt{(m^2+4)(9m^2+4)}))/(2m^2+12)\\ &= \log(m/2) + \frac{4-\log 4}{m^2} - \frac{16-12\log 2}{m^4} + O\left(\frac{1}{m^6}\right).\end{aligned}$$

Again, we obtain further improvements with a third iteration. With

$$\begin{aligned} Q_2(x) &= (m^2+4)(m^2+6)(x^4+1) + 4x(m^4-16)(x^2+1) \\ &\quad + 2(3m^4-10m^2+40)x^2 \\ &= (m^2+4)(m^2+6)(x-1)^4 + 8(m^2+1)(m^2+4)(x-1)^3 \\ &\quad + 8(3m^4+5m^2+4)(x-1)^2 + 32m^4(x-1) + 16m^4, \end{aligned}$$

we have $\omega_m(Q_2) = 32m^2$, and selecting $a_2 = 133$, 575, 1697, and 4005 for $m = 4$, 6, 8, and 10 respectively, we obtain the values shown in Table 1 for $B_m(F_3)$.

2.4. *Conclusion.* The following statement summarizes our improvements to (1).

THEOREM 2.4. *Suppose $f \in \mathcal{D}_m$ has degree $n-1$ and no cyclotomic factors. Then*

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

where

$$c_m = \begin{cases} 0.4162307230\ldots > 77/185 & \text{if } m = 2, \\ \log(m/2) + (3-\log 3)/2m^2 + O(1/m^4) & \text{if } m \geq 3 \text{ is odd}, \\ \log(m/2) + (4-\log 4)/m^2 + O(1/m^4) & \text{if } m \geq 4 \text{ is even}, \end{cases}$$

and bounds for $m \geq 3$ are given explicitly in (8) *and* (9).

Proof. The preceding arguments require that f is monic and has no common factor with the appropriate auxiliary polynomial. However, our auxiliary polynomials have all their roots on the unit circle, so any non-cyclotomic factor of such a polynomial $F(x^n)$ is necessarily not monic. Thus, if f is monic, then the required condition is automatically satisfied, and if $f \in \mathcal{D}_m$ is not monic, then the inequality is satisfied, because $M(f) \geq \max\{2, m-1\}$. ∎

Since the only cyclotomic factors of the auxiliary polynomials $F(x)$ which occur in our constructions are $x-1$, $x+1$, and, when $m = 2$, x^2+1, the condition that $f \in \mathcal{D}_m$ has no cyclotomic factors may be replaced by the hypothesis that $\gcd(f(x), x^{2n}-1) = 1$, or $\gcd(f(x), x^{4n}-1) = 1$ when $m = 2$. However, in [4] (see also [3]) it is shown that every cyclotomic factor of a polynomial $f \in \mathcal{D}_2$ with degree $n-1$ must divide $x^{2n}-1$, and every cyclotomic factor of a polynomial $f \in \mathcal{D}_p$ with degree $n-1$, where p is an odd prime, must divide x^n-1. Thus, these conditions are equivalent when the modulus m is prime.

We remark that for $m = 2$ the condition that f have no cyclotomic factors cannot be removed: the polynomial $h(x) = x^{12}+x^{11}-x^8-x^6-x^4+x+1$ has $\log M(h) = 0.40327\ldots$, and for each $k \geq 1$ this polynomial occurs

as the noncyclotomic part of a polynomial in $\mathcal{D}_2$ having degree $20k-1$. Indeed,

$$h_k(x) = h(x)(x+1)(x^2+1)(x^4-x^3+x^2-x+1)(x^{20(k-1)}+\cdots+x^{20}+1)$$

is a Littlewood polynomial of degree $20k-1$ for every $k \geq 1$ and $M(h_k) = M(h)$. Note that this is not a counterexample to the previous lower bound $(\log 5)/4 = 0.402359\ldots$ (which is just smaller than $0.40327\ldots$) found in [4], so the advantage of Theorem 2.4 over (1) is not only quantitative but also qualitative!

We note also that the smallest known value of Mahler's measure of a polynomial in $\mathcal{D}_2$ with no cyclotomic factors is $\log M(x^6+x^5-x^4-x^3-x^2+x+1) = 0.44213\ldots$, so there is still room for improvement in the constant c_2.

3. The problem of Schinzel and Zassenhaus. This method of constructing auxiliary polynomials also allows us to improve the result obtained in [4] on the problem of Schinzel and Zassenhaus for polynomials in $\mathcal{D}_m$. We review first the method for obtaining a lower bound in this problem, given an auxiliary polynomial F.

Given a monic polynomial $f \in \mathcal{D}_m$ of degree $n-1$, let g be a factor of f of degree d, and assume that $\gcd(g(x), F(x^n)) = 1$. If c is selected so that each root α of g satisfies $|\alpha| \leq 1 + c/n$, then $|\alpha^n| < e^c$ for each α. Therefore,

$$|\mathrm{Res}(g(x), F(x^n))| < \|F\|^d_{|x|=e^c}, \tag{10}$$

where $\|F\|_{|x|=e^c}$ denotes the supremum of F over the circle of radius e^c centered at the origin. This quantity is an expression involving e^c, and combining this with the inequality from Lemma 2.1,

$$|\mathrm{Res}(g(x), F(x^n))| \geq \omega_m(F)^d, \tag{11}$$

one obtains a lower bound on c.

Consider first the case $m = 2$. Using $F(x) = x^2 - 1$ as in [4], we compute $\|F\|_{|x|=e^c} = 1 + e^{2c}$ and $\omega_2(F) = 4$, and conclude that $c > (\log 3)/2$ as in (2). Now the maximum value of $|F(x)|$ on $|x| = \sqrt{3}$ occurs at $\pm i\sqrt{3}$, so this suggests investigating polynomials of the form $(x^2-1)^a(x^2+3)$, with a a positive integer. We compute

$$\|(x^2-1)^a(x^2+3)\|^2_{|x|=r} = \left(\frac{a}{3}\right)^a \left(\frac{4(r^4+3)}{a+1}\right)^{a+1},$$

and since $x^2+3 = (x-1)^2+2(x-1)+4$, we find that $\omega_2(x^2+3) = 4$. Hence $\omega_2((x^2-1)^a(x^2+3)) = 2^{2a+2}$ and, with $r = e^c$, inequalities (10) and (11) yield

$$e^{4c} + 3 > 4(a+1)\left(\frac{3}{a}\right)^{a/(a+1)}.$$

The right side is maximized at $a = 3$, producing $c > (\log 13)/4$.

Next, suppose that $m > 2$. Using $F(x) = x - 1$, we obtain from (10) and (11) the bound $c > \log(m-1)$ of (2). Clearly, the maximum value of $x-1$ on the circle $|x| = m-1$ occurs at $1-m$, so we next consider auxiliary polynomials of the form $(x-1)^a(x+m-1)$. We compute that

$$\|(x-1)^a(x+m-1)\|^2_{|x|=r} = \left(\frac{a}{m-1}\right)^a \left(\frac{m(r^2+m-1)}{a+1}\right)^{a+1},$$

and since $\omega_m((x-1)^a(x+m-1)) = m^{a+1}$, we obtain from (10) and (11) the inequality

$$e^{2c} + m - 1 > m(a+1)\left(\frac{m-1}{a}\right)^{a/(a+1)}.$$

Choosing $a = m-1$, we conclude that $c > (\log(m^2-m+1))/2$. We then obtain the following theorem.

THEOREM 3.1. *Suppose $f \in \mathcal{D}_m$ is monic with degree $n-1$ and is not a product of cyclotomic polynomials. Then there exists a root α of f satisfying*

$$|\alpha| > \begin{cases} 1 + \dfrac{\log 13}{4n} & \text{if } m = 2, \\ 1 + \dfrac{\log(m^2-m+1)}{2n} & \text{if } m > 2. \end{cases} \tag{12}$$

Proof. Suppose $f \in \mathcal{D}_m$ is monic with degree $n-1$. The preceding analysis establishes these inequalities in the case that the noncyclotomic part of f has no common factor with the appropriate auxiliary polynomial $F(x^n)$. We need to establish (12) under the weaker hypothesis that f merely contain a noncyclotomic factor.

In the case $m = 2$, this is immediate, since the polynomial $x^{2n} + 3$ is irreducible by Eisenstein's criterion, and clearly this polynomial cannot divide f. However, for $m > 2$ the polynomial $x^n + m - 1$ may be reducible and may in fact have a common factor with f. (Consider for example $m = 5$ and $f(x) = x^3 + x^2 - 4x + 6 = (x+3)(x^2 - 2x + 2)$; the second factor divides $x^4 + 4$.) Suppose then that every irreducible noncyclotomic factor g of f has a common zero with $x^n - m + 1$. Then each root of g has modulus $(m-1)^{1/n}$, hence $|f(0)| = (m-1)^{s/n}$, where s is the degree of the noncyclotomic part of f. But $1 \le s \le n-1$ implies that $1 < |f(0)| < m-1$, so $f \notin \mathcal{D}_m$, a contradiction. ∎

Note that to obtain Theorem 3.1, we applied the method of Algorithm 2.3 twice beginning with $F_0(x) = x - 1$ for the case $m = 2$, but only once for $m > 2$. A second iteration of this method allows us to improve the general case as well, at least with an asymptotic formula. Since the polynomial $F_1(x) = (x-1)^{m-1}(x+1)$ achieves its maximum value over the circle $|x| = \sqrt{m^2-m+1}$ at the roots of $Q(x) = (x-1)^2 + m(x-1) + m^2$, we investigate

$\|F_1(x)^a Q(x)\|_{|x|=e^c}$ and compare this quantity with $\omega_m(F_1^a Q) = m^{am+2}$. We find empirically that the optimal choice for a approaches 4 as m grows large, and using this value we compute that the expression $(\log(m^2-m+1))/2$ of Theorem 3.1 may be replaced by

$$\frac{\log(m^2-m+1)}{2} + \frac{1-\log 2}{2m} + \frac{2-\log 2}{8m^2} - \frac{34-53\log 2+26(\log 2)^2}{96m^3} + O\left(\frac{1}{m^4}\right).$$

The proof of the theorem may be modified to account for the additional factor Q. Suppose every noncyclotomic factor g of f has a common root with either x^n-m+1 or $Q(x^n)$. Then $|f(0)| = (m-1)^{s/n}(m^2-m+1)^{t/2n}$ for some nonnegative integers s and t satisfying $0 < s+t < n$. Thus $|f(0)| < m$, and so the only possibility is $f(0) = 1-m$. In this case, we have $(m-1)^{2(n-s)} = (m^2-m+1)^t$, and we obtain a contradiction by reducing modulo $m-1$.

We add that it is established in [4] that the value of the bound for $f \in \mathcal{D}_m$ in Theorem 3.1 cannot exceed $\log(2m-1)$.

4. Totally p-adic polynomials. We now turn to the problem of bounding the logarithmic Weil height of a totally p-adic algebraic unit. We require first the following result, which is very similar to Lemma 2.1.

LEMMA 4.1. *Suppose $g \in \mathbb{Z}[x]$ is a monic polynomial of degree d with $g(0) = \pm 1$, and suppose that g splits completely in the field $\mathbb{Q}_p$, for some prime p. Suppose also that $G \in \mathbb{Z}[x]$ satisfies $p \,|\, G(1)$. Then*

$$p^d \mid \operatorname{Res}(g(x), G(x^{p-1})).$$

Proof. Let $\alpha \in \mathbb{Q}_p$ be a root of g. Since g is monic with constant term ± 1, it follows that $|\alpha|_p = 1$, so $|\alpha^{p-1}-1|_p \le p^{-1}$. Next, because $p \,|\, G(1)$, there exist integer polynomials $Q(x)$ and $R(x)$ such that $G(x) = (x-1)Q(x) + pR(x)$, so

$$|G(\alpha^{p-1})|_p \le \max\{|(\alpha^{p-1}-1)Q(\alpha^{p-1})|_p, |pR(\alpha^{p-1})|_p\} \le p^{-1}.$$

Finally, since g splits completely in $\mathbb{Q}_p$, the assertion follows. ∎

Given $F \in \mathbb{Z}[x]$, let $\omega_p(F)$ be as in Section 2. Note that since p is prime, the value of $\omega_p(F)$ is a power of p if the coefficients of F have no common divisor. Expanding $F(x^{p-1})$ in powers of $x^{p-1}-1$ and using the lemma, we deduce that $\omega_p(F)^d \mid \operatorname{Res}(g(x), F(x^{p-1}))$ for every totally p-adic monic polynomial g of degree d having constant term ± 1. Thus, setting as above

$$B_p(F) = \frac{\log \omega_p(F) - \log\|F\|_\infty}{\deg F},$$

we obtain the following lower bound on the height of a totally p-adic algebraic unit.

THEOREM 4.2. *Suppose α is a totally p-adic algebraic unit, and suppose $F \in \mathbb{Z}[x]$ satisfies $F(\alpha^{p-1}) \neq 0$. Then*

$$h(\alpha) \geq \frac{B_p(F)}{p-1}.$$

Proof. Let $g \in \mathbb{Z}[x]$ denote the minimal polynomial of α, and let d denote the degree of g. Since $F(\alpha^{p-1}) \neq 0$, the discussion above yields

$$|\mathrm{Res}(g(x), F(x^{p-1}))| \geq \omega_p(F)^d,$$

and, as in the proof of Theorem 2.2, we find

$$|\mathrm{Res}(g(x), F(x^{p-1}))| \leq \|F\|_\infty^d M(g)^{(p-1)\deg F}.$$

Thus

$$h(\alpha) = \frac{\log M(g)}{d} \geq \frac{\log \omega_p(F) - \log\|F\|_\infty}{(p-1)\deg F} = \frac{B_p(F)}{p-1}. \quad \blacksquare$$

We may now use the values of $B_p(F)$ computed in Section 2. For $p = 2$, since the only algebraic units that are roots of F_5 are roots of unity, we obtain

$$\tau_2 \geq 0.4162307230\ldots > 77/185, \tag{13}$$

improving the value in (3). Likewise, for $p > 2$, choosing

$$F(x) = (x-1)^{p^2}(x+1)$$

produces the inequality

$$\tau_p \geq \frac{\log(\sqrt{p^2+1}) - \log 2}{p-1},$$

which already improves (3). Selecting

$$F(x) = (x-1)^{3p^2}(x+1)^3((p^2+1)(x^2+1) + 2(p^2-1)x)^2$$

yields an expression corresponding to (8), so

$$\tau_p \geq \frac{\log(p/2)}{p-1} + \frac{3 - \log 3}{2p^2(p-1)} + O\left(\frac{1}{p^5}\right). \tag{14}$$

Numerical values obtained from a third iteration of Algorithm 2.3 for some small primes p are shown in Table 2, together with the value from (3), and an upper bound on τ_p. Petsche [11] notes that the upper bound

$$\tau_p \leq \frac{\log(p + \sqrt{p^2+4}) - \log 2}{p-1}$$

for $p \geq 3$ may be obtained by considering the totally p-adic polynomial $x^{p-1} - px^{(p-1)/2} - 1$. Of course, for particular p one may find slightly better bounds; the values in the third column of Table 2 arise by considering the polynomials x^2+8x-1, x^2+3x-1, x^4+5x-1, x^6+7x^4-1, and $x^{10}+11x^4-1$, respectively.

Finally, we remark that the polynomial $f(x) = x^2 + x + 2$ is totally 2-adic and has Mahler's measure 2, so $\sigma_2 \leq (\log 2)/2 = 0.34657\ldots$, and

Table 2. Bounds on τ_p

p	Original lower bound	New lower bound	Upper bound
2	0.34657359	0.41623072	1.04735627
3	0.20273255	0.25051330	0.59738160
5	0.22907268	0.23821731	0.40275725
7	0.20879382	0.21196257	0.32382886
11	0.17047480	0.17125398	0.23978828

consequently $\sigma_2 < \tau_2$. It would be of interest to find all p for which $\sigma_p = \tau_p$, or to prove that no such p exists.

References

[1] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. 73 (1983), 11–32; Addendum, ibid. 75 (1984), 377.

[2] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. 12 (2001), 5–14.

[3] P. Borwein and K.-K. S. Choi, *On cyclotomic polynomials with* ± 1 *coefficients*, Experiment. Math. 8 (1999), 399–407.

[4] P. Borwein, E. Dobrowolski, and M. J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, preprint, 2003.

[5] 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.

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

[7] A. Dubickas, *The maximal conjugate of a non-reciprocal algebraic integer*, Lithuanian Math. J. 37 (1997), 129–133.

[8] G. Höhn et N.-P. Skoruppa, *Un résultat de Schinzel*, J. Théor. Nombres Bordeaux 5 (1993), 185.

[9] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) 34 (1933), 461–479.

[10] M. Mignotte, *Sur un théorème de M. Langevin*, Acta Arith. 54 (1989), 81–86.

[11] C. J. Petsche, *The height of algebraic units in local fields*, preprint, 2003.

[12] 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.

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

[14] 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.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24, LT-03225 Vilnius, Lithuania
E-mail: arturas.dubickas@maf.vu.lt

Department of Mathematics
Davidson College
Davidson, NC 28035-6996, U.S.A.
E-mail: mjm@member.ams.org

Received on 22.9.2004 (4852)