ACTA ARITHMETICA
128.3 (2007)

The Weil height in terms of an auxiliary polynomial

by

CHARLES L. SAMUELS (Austin, TX)

1. Introduction. Let K be a number field and v a place of K dividing the place p of $\mathbb{Q}$. Let K_v and $\mathbb{Q}_p$ denote the respective completions. We write $\|\cdot\|_v$ to denote the unique absolute value on K_v extending the p-adic absolute value on $\mathbb{Q}_p$ and let $|\cdot|_v = \|\cdot\|_v^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]}$. Define the logarithmic *Weil height* of $\alpha \in K$ by

$$h(\alpha) = \sum_v \log^+ |\alpha|_v$$

where the sum is taken over all places v of K. By the way we have normalized our absolute values, this definition does not depend on K, and therefore, h is a well-defined function on $\overline{\mathbb{Q}}$. By Kronecker's theorem, $h(\alpha) \geq 0$ with equality precisely when α is zero or a root of unity.

For $f \in \mathbb{Z}[x]$ having roots $\alpha_1, \ldots, \alpha_d$ define the logarithmic *Mahler measure* of f by

$$\mu(f) = \sum_{k=1}^{d} h(\alpha_k).$$

It is also worth noting that if f is irreducible then $\mu(f) = \deg \alpha \cdot h(\alpha)$.

Certainly $\mu(f) \geq 0$ with equality precisely when the only roots of f are 0 and roots of unity. In 1933, D. H. Lehmer [7] asked if there is a constant $c > 0$ such that $\mu(f) \geq c$ in all other cases. He noted that

$$\mu(x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1) = .1623\ldots$$

and this remains the smallest known Mahler measure greater than 0. The best known unconditional result toward answering Lehmer's problem is a theorem of Dobrowolski [5] where he proves that if f has positive Mahler measure then

$$\mu(f) \gg \left(\frac{\log\log\deg f}{\log\deg f}\right)^3.$$

2000 *Mathematics Subject Classification*: Primary 11R04, 11R09.
Key words and phrases: Weil height, Mahler measure, Lehmer's problem.

An affirmative answer to Lehmer's problem has been given in certain special cases. A polynomial f is said to be *reciprocal* if whenever α is a root of f then α^{-1} is also a root. Breusch [4] proved that there exists a positive constant c such that if f is not reciprocal then $\mu(f) \geq c$. Smyth [11] later showed that we may take $c = \mu(x^3 - x + 1)$. Borwein, Hare and Mossinghoff [3] improved the constant found by Smyth in the special case that f has odd coefficients. They showed that if f is a non-reciprocal polynomial over $\mathbb{Z}$ having odd coefficients, then $\mu(f) \geq \mu(x^2 - x - 1)$.

Borwein, Dobrowolski and Mossinghoff [2] relaxed the assumption that f not be reciprocal and still obtained an absolute lower bound on $\mu(f)$. They used properties of the resultant to prove that if f has no cyclotomic factors and coefficients congruent to 1 mod m then

$$\mu(f) \geq c_m \frac{\deg f}{1 + \deg f}$$

where $c_2 = (\log 5)/4$ and $c_m = \log(\sqrt{m^2+1}/2)$ for all $m > 2$. These results appear in [2] as Corollaries 3.4 and 3.5 to Theorem 3.3. This theorem gives a lower bound of the form

$$\mu(f) \geq c_m(T) \frac{\deg f}{1 + \deg f} \tag{1.1}$$

where f has no cyclotomic factors and coefficients congruent to 1 mod m. Here, $c_m(T)$ is a positive constant depending on both m and an auxiliary polynomial $T \in \mathbb{Z}[x]$. The corollaries follow by making an appropriate choice of T.

Extending the techniques of [2], Dubickas and Mossinghoff [6] improved inequality (1.1) by finding a lower bound of the form

$$\mu(g) \geq b_m(T) \frac{\deg g}{1 + \deg f} \tag{1.2}$$

where $b_m(T) \geq c_m(T)$. Here, g has no cyclotomic factors and is a factor of a polynomial f having coefficients congruent to 1 mod m. Moreover, they produced an algorithm which generates a sequence of polynomials $\{T_k\}$ such that the sequence $\{b_m(T_k)\}$ is increasing and $b_m(T_k) > c_m$ for sufficiently large k.

In a slightly different direction, Schinzel [10] proved that if α is a totally real algebraic integer, not 0 or ± 1, then $h(\alpha) \geq \frac{1}{2}\log\frac{1+\sqrt{5}}{2}$. Bombieri and Zannier [1] proved that if α is a totally p-adic algebraic number, not 0 or a root of unity, then $h(\alpha) \geq \frac{\log p}{2(p+1)}$.

If, in addition, α is an algebraic unit, Petsche [9] gave the improved lower bound

$$h(\alpha) \geq \frac{c_p}{p-1} \tag{1.3}$$

where $c_2 = \log\sqrt{2}$ and $c_p = \log(p/2)$ for all primes $p > 2$. Dubickas and Mossinghoff [6] introduced an auxiliary polynomial to this problem as well, giving the lower bound

$$h(\alpha) \geq \frac{b_p(T)}{p-1} \tag{1.4}$$

where $b_p(T)$ is the same as in (1.2). They showed how to find a sequence of auxiliary polynomials that further improved (1.3).

As we have remarked, the well-known lower bounds (1.1), (1.2) and (1.4) all rely on an auxiliary polynomial T. However, each of these bounds requires an assumption on α. Our main result, Theorem 2.2, shows that if $\alpha \in \overline{\mathbb{Q}}$ then $h(\alpha)$ can be written in terms of an auxiliary polynomial. In Section 3, we show that this theorem naturally contains the results of [6]. Finally, in Sections 4 and 5 we deduce two other interesting consequences of our main result.

2. Main results. Let Ω_v be the completion of an algebraic closure of K_v. We define the logarithmic *local supremum norm* of $T \in \Omega_v[x]$ on the unit circle by

$$\nu_v(T) = \log\sup\{|T(z)|_v : z \in \Omega_v \text{ and } |z|_v = 1\}.$$

For $\alpha \in \Omega_v$ and $N \in \mathbb{Z}$ such that $\deg T \leq N$ define

$$U_v(N, \alpha, T) = \inf\{\nu_v(T - f) : f \in \Omega_v[x],\ f(\alpha) = 0 \text{ and } \deg f \leq N\}.$$

We now obtain the following lemma which relates $U_v(N, \alpha, T)$ to more familiar functions.

LEMMA 2.1. *Let $N \in \mathbb{Z}$ and $\alpha \in \Omega_v$. If $T \in \Omega_v[x]$ is such that* $\deg T \leq N$ *then*

$$\begin{aligned} U_v(N, \alpha, T) &= \log|T(\alpha)|_v + U_v(N, \alpha, 1) \\ &= \log|T(\alpha)|_v - N\log^+|\alpha|_v. \end{aligned} \tag{2.1}$$

Proof. If $T(\alpha) = 0$ then all parts of equations (2.1) equal $-\infty$, so we assume that $T(\alpha) \neq 0$. Let us first verify the left hand equation. For simplicity define the set

$$S_v(\alpha, N) = \{f \in \Omega_v[x] : f(\alpha) = 0 \text{ and } \deg f \leq N\}.$$

It is clear that

$$\begin{aligned} U_v(N, \alpha, T) &= \inf\{\nu_v(T(x) - f(x)) : f \in S_v(\alpha, N)\} \\ &= \inf\{\nu_v(T(x) - (T(x) - T(\alpha) + f(x))) : f \in S_v(\alpha, N)\} \\ &= \inf\{\nu_v(T(\alpha) - f(x)) : f \in S_v(\alpha, N)\} \\ &= \inf\{\nu_v(T(\alpha)(1 - f(x))) : f \in S_v(\alpha, N)\}. \end{aligned}$$

Since ν_v is the logarithm of a norm, we may factor $T(\alpha)$ out of the infimum to see that

$$\begin{aligned} U_v(N,\alpha,T) &= \log|T(\alpha)|_v + \inf\{\nu_v(1-f(x)) : f \in S_v(\alpha,N)\} \\ &= \log|T(\alpha)|_v + U_v(N,\alpha,1), \end{aligned}$$

which establishes the left hand equality.

In order to establish the right hand equality we must show that $U_v(N,\alpha,1) = -N\log^+|\alpha|_v$. We first claim that if $N \in \mathbb{Z}$ then

$$\log|F(\alpha)|_v \le \nu_v(F) + N\log^+|\alpha|_v \tag{2.2}$$

for all $F \in \Omega_v[x]$ with $\deg F \le N$. To see this, write $F(x) = \sum_{k=0}^{\deg F} a_k x^k$. If v is non-Archimedean then we have

$$\nu_v(F) = \log\max\{|a_k|_v : 0 \le k \le \deg F\} \tag{2.3}$$

and (2.2) follows from the strong triangle inequality. We now assume that v is Archimedean. If $|\alpha|_v \le 1$ then the inequality follows from the maximum principle. If $|\alpha|_v > 1$ then we obtain

$$\log|\alpha^{-\deg F}F(\alpha)|_v \le \nu_v(x^{\deg F}F(x^{-1})) = \nu_v(F)$$

and (2.2) follows.

Now suppose that $f \in S_v(\alpha,N)$. Therefore, $\deg(1-f) \le N$ and inequality (2.2) implies that

$$0 = \log|1-f(\alpha)|_v \le \nu_v(1-f) + N\log^+|\alpha|_v.$$

This inequality holds for all polynomials $f \in S_v(\alpha,N)$ so that the right hand side may be replaced by its infimum over all such f. That is, we obtain $0 \le U_v(N,\alpha,1) + N\log^+|\alpha|_v$ so we find that

$$U_v(N,\alpha,1) \ge -N\log^+|\alpha|_v. \tag{2.4}$$

We will now establish the opposite direction of (2.4) by making specific choices for f to give upper bounds on $U_v(N,\alpha,1)$. By taking $f \equiv 0$ we see easily that $U_v(N,\alpha,1) \le 0$. Similarly, by taking $f(x) = 1-(x/\alpha)^N$ we obtain

$$U_v(N,\alpha,1) \le \nu_v(x/\alpha)^N = -N\log|\alpha|_v.$$

Hence

$$U_v(N,\alpha,1) \le \min\{0, -N\log|\alpha|_v\} = -N\log^+|\alpha|_v. \ \blacksquare \tag{2.5}$$

If $\alpha \in K$ and $T \in K[x]$ are such that $T(\alpha) \ne 0$ then Lemma 2.1 implies that $U_v(N,\alpha,T) = 0$ for all but finitely many places v of K. Hence, in this situation we may define

$$U(N,\alpha,T) = \sum_v U_v(N,\alpha,T)$$

where v runs over the places of K. We note that this definition does not depend on K, so that U is a well-defined function on $\{(\alpha, T) \in \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}[x] : T(\alpha) \neq 0\}$. We are now prepared to state and prove our main result.

THEOREM 2.2. *Let $N \in \mathbb{Z}$ and $\alpha \in \overline{\mathbb{Q}}$. If $T \in \overline{\mathbb{Q}}[x]$ is such that* $\deg T \leq N$ *and $T(\alpha) \neq 0$ then*

$$U(N, \alpha, T) = U(N, \alpha, 1) = -Nh(\alpha).$$

Proof. Assume that K is a number field containing α and the coefficients of T, and v is a place of K. We know that the absolute value $|\cdot|_v$ satisfies the product formula $\prod_v |\beta|_v = 1$ for all $\beta \in K^\times$. Hence, summing the equation of Lemma 2.1 over all places v of K we get

$$U(N, \alpha, T) = U(N, \alpha, 1) = -Nh(\alpha), \tag{2.6}$$

which establishes the theorem. ∎

3. Polynomials near $x^n - 1$. As we have remarked, Theorem 2.2 naturally generalizes the results of Dubickas and Mossinghoff in [6]. We will give a single result that contains both their bound on the Mahler measure of a polynomial having coefficients congruent to 1 mod m and their bound on the height of a totally p-adic algebraic unit.

Let us begin by reconstructing the situation of [6]. For an auxiliary polynomial $T \in \mathbb{Z}[x]$ and a positive integer m define

$$\omega_m(T) = \log \gcd \left\{ \frac{m^k T^{(k)}(1)}{k!} : 0 \leq k \leq \deg T \right\}. \tag{3.1}$$

Also assume that f is a polynomial of degree $n-1$ with integer coefficients congruent to 1 mod m. The authors prove (Theorem 2.2 of [6]) that if g is a factor of f over $\mathbb{Z}$ satisfying $\gcd(g(x), T(x^n)) = 1$ then

$$\mu(g) \geq \frac{\omega_m(T) - \nu_\infty(T)}{\deg T} \cdot \frac{\deg g}{n}. \tag{3.2}$$

Later they prove (Theorem 4.2 of [6]) that if α is a totally p-adic algebraic unit then

$$h(\alpha) \geq \frac{\omega_p(T) - \nu_\infty(T)}{(p-1)\deg T}. \tag{3.3}$$

Our goal is to produce a generalization of (3.2) where T and f are allowed to have algebraic coefficients. Our version also contains (3.3) as a corollary.

Before we begin, we make one final trivial remark regarding the hypotheses of [6]. The assumption that f have degree $n-1$ and coefficients congruent to 1 mod m is equivalent to the assumption that $(x-1)f(x) \equiv x^n - 1 \bmod m$. Therefore, we can make a slightly stronger conclusion by hypothesizing instead that $f(x) \equiv x^n - 1 \bmod m$ and bounding the Mahler measure of all factors g of f.

We will require a version of $\omega_m(T)$ defined in (3.1) that allows m to be a general algebraic number and T to have any algebraic coefficients. If K is a number field, $m \in K$ and $T \in K[x]$ define

$$\omega_m(T) = -\sum_{v\nmid\infty} \log\max\left\{\left|\frac{m^k T^{(k)}(1)}{k!}\right|_v : 0 \le k \le \deg T\right\} \tag{3.4}$$

where the sum is taken over places v of K. By the way we have normalized our absolute values, this definition does not depend on K. Moreover, if $m \in \mathbb{Z}$ and $T \in \mathbb{Z}[x]$ then (3.4) is the same as the definition (3.1).

If $\alpha, \beta, m \in K$, then we write $\alpha \equiv \beta \bmod m$ if $|\alpha - \beta|_v \le |m|_v$ for all $v \nmid \infty$. Similarly, if $f, g \in K[x]$ we write $f \equiv g \bmod m$ if $\nu_v(f-g) \le \log|m|_v$ for all $v \nmid \infty$. Neither definition depends on K and both generalize the usual notions of congruence in $\mathbb{Z}$. If $T \in K[x]$ we often write $\nu_\infty(T) = \sum_{v\mid\infty} \nu_v(T)$ where v runs over places of K. This notation again does not depend on K.

It will also be convenient for this section and future applications to define $U_v(\alpha, T) = U_v(\deg T, \alpha, T)$ and $U(\alpha, T) = U(\deg T, \alpha, T)$.

Using the definitions above, we obtain our generalized version of the results of [6].

THEOREM 3.1. *Let m be an algebraic number. Suppose that $f \in \overline{\mathbb{Q}}[x]$ has degree n and $f(x) \equiv x^n - 1 \bmod m$. If α is a root of f and $T \in \overline{\mathbb{Q}}[x]$ is such that $T(\alpha^n) \ne 0$ then*

$$h(\alpha) \ge \frac{\omega_m(T) - \nu_\infty(T)}{n \deg T}.$$

Proof. Let K be a number field containing α and the coefficients of T and let v index the places of K. Using Theorem 2.2 with $N = \deg T$ and the definition of U_v we have

$$-n \deg T \cdot h(\alpha) \le \sum_{v\nmid\infty} U_v(\alpha, T(x^n)) + \nu_\infty(T) \tag{3.5}$$

so we must show that $\sum_{v\nmid\infty} U_v(\alpha, T(x^n)) \le -\omega_m(T)$. Let $v \nmid \infty$. Writing T in its Taylor expansion at 1 and using the binomial theorem we find that

$$\begin{aligned} U_v(\alpha, T(x^n)) &= U_v\left(\alpha, \sum_{k=0}^{\deg T} \frac{T^{(k)}(1)}{k!}(x^n - 1)^k\right) \\ &\le \nu_v\left(\sum_{k=0}^{\deg T} \frac{T^{(k)}(1)}{k!}(x^n - 1 - f(x))^k\right). \end{aligned}$$

Then using the strong triangle inequality for ν_v we obtain

$$U_v(\alpha, T(x^n)) \le \max\left\{\log\left|\frac{T^{(k)}(1)}{k!}\right|_v + k\nu_v(x^n - 1 - f(x)) : 0 \le k \le \deg T\right\}.$$

Since $f(x) \equiv x^n - 1 \bmod m$ we have $\nu_v(x^n - 1 - f(x)) \le \log|m|_v$. Consequently,

$$\sum_{v\nmid\infty} U_v(\alpha, T(x^n)) \le \sum_{v\nmid\infty} \log\max\left\{\left|\frac{m^k T^{(k)}(1)}{k!}\right|_v : 0 \le k \le \deg T\right\} = -\omega_m(T)$$

and the theorem follows from (3.5). ∎

If we assume that f and T have integer coefficients and m is a positive integer then we recover Theorem 2.2 of [6].

Corollary 3.2. *Let $f \in \mathbb{Z}[x]$ have degree n and $f(x) \equiv x^n - 1 \bmod m$. If g is a factor of f and $T \in \mathbb{Z}[x]$ is such that $\gcd(g(x), T(x^n)) = 1$ then*

$$\mu(g) \ge \frac{\omega_m(T) - \nu_\infty(T)}{\deg T} \cdot \frac{\deg g}{n}.$$

Proof. Apply Theorem 3.1 to each root α of g and the result follows. ∎

We also recover Theorem 4.2 of [6] giving a lower bound on the height of a totally p-adic algebraic unit.

Corollary 3.3. *If α is a totally p-adic algebraic unit and $T \in \mathbb{Z}[x]$ is such that $T(\alpha^{p-1}) \ne 0$ then*

$$h(\alpha) \ge \frac{\omega_p(T) - \nu_\infty(T)}{(p-1)\deg T}.$$

Proof. For a general number field K and a non-Archimedean place v of K dividing the place p of $\mathbb{Q}$, let $O_v = \{x \in K_v : |x|_v \le 1\}$ denote the ring of v-adic integers in K_v and let π_v be a generator of its unique maximal ideal $M_v = \{x \in K_v : |x|_v < 1\}$. Let $d_v = [K_v : \mathbb{Q}_p]$ denote the local degree and $d = [K : \mathbb{Q}]$ the global degree. We also define the residue degree f_v by $p^{f_v} = |O_v/M_v|$ and note that $|\pi_v|_v = \|p\|_v^{f_v/d}$. If K is a totally p-adic field then we have $f_v = d_v = 1$ for all $v \mid p$.

Now assume that K is the totally p-adic field $\mathbb{Q}(\alpha)$. If v is a place of K dividing p then

$$|\alpha^{p-1} - 1|_v \le |\pi_v|_v = \|p\|_v^{f_v/d} = \|p\|_v^{d_v/d} = |p|_v,$$

and if v does not divide p or ∞ then

$$|\alpha^{p-1} - 1|_v \le 1 = |p|_v.$$

Hence $x^{p-1} - 1 \equiv x^{p-1} - \alpha^{p-1} \bmod p$. Now we may apply Theorem 3.1 with $m = p$ and $f(x) = x^{p-1} - \alpha^{p-1}$ and the result follows. ∎

4. Polynomials near $(x^n - 1)^r$. In this section, we apply Theorem 2.2 in order to examine the Mahler measure of any factor of a polynomial f satisfying $f(x) \equiv (x^n - 1)^r \bmod m$. In particular, we obtain the following explicit lower bound.

THEOREM 4.1. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr, $m \geq 2$ is an integer, and $f(x) \equiv (x^n - 1)^r \bmod m$. If g is a factor of f over $\mathbb{Z}$ having no cyclotomic factors then*

$$\mu(g) \geq c\,\frac{\deg g}{n2^r}$$

where c is the unique positive number satisfying $ce^{c/2}\log 3 = \log(3/2)\log 2$. (Note that $c = .22823\ldots$.)

As an application, let T be a product of cyclotomic polynomials of degree $2N$. Then we may apply Theorem 4.1 with $g(x) = T(x) + mx^N$ where $|m| \geq 2$. In this situation, r is the maximum multiplicity of the cyclotomic polynomials in the factorization of T over $\mathbb{Z}$. These types of polynomials have been studied extensively (see, for example, [8]) and our results yield a lower bound on any such g, although it is not absolute for this entire class of polynomials.

Of course, Theorem 4.1 is not helpful when g is a product of cyclotomic polynomials with the middle coefficient shifted by only 1. Numerical evidence presented in [8] suggests that these polynomials form a relatively rich collection of polynomials of small Mahler measure. Hence it would be useful to have a method for giving a lower bound on their Mahler measure. However, we are unable to do so in this paper.

We also note that Theorem 4.1 is weaker than Corollaries 3.3 and 3.4 of [2] when $r = 1$. In this situation, we may appeal to [6] or the results of Section 3 to obtain the sharpest known bounds.

The proof of Theorem 4.1 will require three lemmas as well as some additional notation. Suppose that g and T are polynomials over any field K. As $K[x]$ is a unique factorization domain, we may write $\lambda_g(T)$ to denote the multiplicity of g in the factorization of T. If G is a collection of polynomials over K, then let $\lambda_G(T) = \sum_{g\in G}\lambda_g(T)$.

Our first lemma is a direct generalization of Theorem 3.3 of [2].

LEMMA 4.2. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr and $f(x) \equiv (x^n - 1)^r \bmod m$. If g is a factor of f over $\mathbb{Z}$ and $T \in \mathbb{Q}[x]$ is relatively prime to g then*

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T)\log m - r\nu_\infty(T)}{r\deg T}\deg g. \tag{4.1}$$

Moreover, if $2 \mid m$ then

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T)\log m + \lambda_{G_n}(T)\log 2 - r\nu_\infty(T)}{r\deg T}\deg g \tag{4.2}$$

where $G_n = \{x^{n2^j} + 1 : j \geq 0\}$.

Proof. Suppose that α is a root of f, K is a number field containing α, and v indexes the places of K. First observe that if $F_1, F_2 \in \Omega_v[x]$ then $\nu_v(F_1F_2) \le \nu_v(F_1) + \nu_v(F_2)$. This yields the multiplicativity relation

$$U_v(\alpha, F_1F_2) \le U_v(\alpha, F_1) + U_v(\alpha, F_2). \tag{4.3}$$

Theorem 2.2 implies that

$$-r \deg T \cdot h(\alpha) \le \sum_{v \nmid \infty} U_v(\alpha, T^r) + r\nu_\infty(T). \tag{4.4}$$

Suppose that $T_0 \in \mathbb{Z}[x]$ is such that $T(x)^r = (x^n-1)^{r\lambda_{x^n-1}(T)}T_0(x)$. We know that since T_0 has integer coefficients, $U_v(\alpha, T_0) \le \nu_v(T_0) \le 0$. Then (4.3) implies that

$$U_v(\alpha, T^r) \le \lambda_{x^n-1}(T)U_v(\alpha, (x^n-1)^r) \le \lambda_{x^n-1}(T)\nu_v((x^n-1)^r - f(x)).$$

Since f has integer coefficients and satisfies $f(x) \equiv (x^n-1)^r \bmod m$ we know that $\sum_{v \nmid \infty} \nu_v((x^n-1)^r - f(x)) \le -\log m$. It follows that

$$-r \deg T \cdot h(\alpha) \le -\lambda_{x^n-1}(T) \log m + r\nu_\infty(T). \tag{4.5}$$

Applying (4.5) to each root α of g, we obtain (4.1).

Next, assume that $2 \mid m$. In this situation, write

$$T(x)^r = T_0(x)(x^n-1)^{r\lambda_{x^n-1}(T)} \prod_{j\ge 0} (x^{n2^j}+1)^{r\lambda_{x^{n2^j}+1}(T)}$$

for some $T_0 \in \mathbb{Z}[x]$. In addition to the congruence $f(x) \equiv (x^n-1)^r \bmod m$, for each $j \ge 0$ there exists $b_j \in \mathbb{Z}[x]$ such that $f(x)b_j(x) \equiv (x^{n2^j}+1)^r \bmod 2$. Hence,

$$\sum_{v \nmid \infty} \nu_v(x^{n2^j} + 1 - f(x)b_j(x)) \le -\log 2$$

for all $j \ge 0$. Now we find that

$$\begin{aligned} U_v(\alpha, T^r) \le{}& \lambda_{x^n-1}(T)\nu_v((x^n-1)^r - f(x)) \\ &+ \sum_{j \ge 0} \lambda_{x^{n2^j}+1}(T)\nu_v(x^{n2^j} + 1 - f(x)b_j(x)) \end{aligned}$$

for all $v \nmid \infty$. Therefore, (4.4) yields

$$-r \deg T \cdot h(\alpha) \le -\lambda_{x^n-1}(T) \log m - \lambda_{G_n}(T) \log 2 + r\nu_\infty(T),$$

and the result follows by a similar argument to the above. ∎

Note that the right hand sides of the inequalities of Lemma 4.2 are less than 0 when r is large compared to m. Hence, it may appear that these bounds are useful only when r is small. However, a simple consequence of Lemma 4.2 allows us to give non-trivial lower bounds when r is large.

Lemma 4.3. *Let p be prime and q be a power of p such that* $\deg f = nq$ *and* $f(x) \equiv (x^n - 1)^q \bmod p$. *If g is a factor of f over $\mathbb{Z}$ and $T \in \mathbb{Q}[x]$ is such that* $\gcd(T(x^q), g(x)) = 1$ *then*

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T)\log p - \nu_\infty(T)}{q \deg T}\deg g. \tag{4.6}$$

Moreover, if $p = 2$ then

$$\mu(g) \geq \frac{(\lambda_{x^n-1}(T) + \lambda_{G_n}(T))\log 2 - \nu_\infty(T)}{q \deg T}\deg g \tag{4.7}$$

where $G_n = \{x^{n2^j} + 1 : j \geq 0\}$.

Proof. We know that $f(x) \equiv (x^n - 1)^q \equiv x^{nq} - 1 \bmod p$. Therefore, we may apply Lemma 4.2 with $m = p$, $r = 1$ and $T(x^q)$ in place of $T(x)$. We obtain

$$\begin{aligned}\mu(g) &\geq \frac{\lambda_{x^{nq}-1}(T(x^q))\log p - \nu_\infty(T(x^q))}{q \deg T}\deg g\\ &= \frac{\lambda_{x^n-1}(T)\log p - \nu_\infty(T)}{q \deg T}\deg g.\end{aligned}$$

Inequality (4.7) follows from a similar argument. ∎

In the hypotheses of Lemma 4.2 we are given $f(x) \equiv (x^n - 1)^r \bmod m$, so we may also apply Lemma 4.3 with p a prime dividing m and $q = p^{\lceil \log_p r \rceil}$. We know that $(x^n - 1)^{q-r} f(x) \equiv (x^n - 1)^q \bmod p$ so that Lemma 4.3 still applies to any factor g of f.

As we have noted, this method allows us to deduce non-trivial lower bounds on the Mahler measure even when r is large. There is the disadvantage that q is potentially much larger than r, making the inequalities of Lemma 4.3 weaker than those of Lemma 4.2 in some cases. Furthermore, if m has many prime factors, p will be significantly smaller than m, again making the inequalities of Lemma 4.3 weaker than those of Lemma 4.2.

As a general rule, we will use Lemma 4.2 when r is small and Lemma 4.3 when r is large to obtain the best universal results. We see this strategy in the proof of our next lemma.

Lemma 4.4. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr and* $f(x) \equiv (x^n - 1)^r \bmod m$. *If g is a factor of f over $\mathbb{Z}$ having no cyclotomic factors then*

$$\mu(g) \geq \log\left(\frac{m}{2^r}\right) \cdot \frac{\deg g}{nr}. \tag{4.8}$$

If p is a prime dividing m then

$$\mu(g) \geq \frac{1}{p}\log\left(\frac{p}{2}\right) \cdot \frac{\deg g}{nr} \tag{4.9}$$

and if 2 divides m then

$$\mu(g) \geq \frac{\log 2}{4} \cdot \frac{\deg g}{nr}. \tag{4.10}$$

Proof. To prove (4.8), we apply Lemma 4.2 with $T(x) = x^n - 1$ and the inequality follows immediately.

To prove (4.9), we let p be a prime dividing m and set $q = p^{\lceil \log_p r \rceil}$. Therefore q is an integer greater than or equal to r so that $(x^n - 1)^{q-r} f(x) \equiv (x^n - 1)^q \bmod p$. Using $T(x) = x^n - 1$ with inequality (4.6) of Lemma 4.3 we find that

$$\mu(g) \geq \log\left(\frac{p}{2}\right) \cdot \frac{\deg g}{nq}.$$

But we also know that $q = p^{\lceil \log_p r \rceil} < p^{1+\log_p r} = pr$ so that

$$\mu(g) \geq \log\left(\frac{p}{2}\right) \cdot \frac{\deg g}{npr},$$

which is the desired inequality.

Finally, to prove (4.10), suppose that $2 \mid m$ and $q = 2^{\lceil \log_2 r \rceil}$. Use $T(x) = x^{2n} - 1$ in inequality (4.7) of Lemma 4.3 to obtain the desired result. ∎

Proof of Theorem 4.1. Let $c_0 = c/(2 \log 2)$. We distinguish the following three cases:

(i) $m \geq 2^{r+c_0}$,
(ii) $m < 2^{r+c_0}$ and $2 \mid m$,
(iii) $m < 2^{r+c_0}$ and $2 \nmid m$.

If $m \geq 2^{r+c_0}$ then we use inequality (4.8) of Lemma 4.4 to find that

$$\mu(g) \geq c_0 \log 2 \cdot \frac{\deg g}{nr} \geq 2c_0 \log 2 \cdot \frac{\deg g}{n2^r} = c\,\frac{\deg g}{n2^r}.$$

If $m < 2^{r+c_0}$ and $2 \mid m$ then inequality (4.10) implies that

$$\mu(g) \geq \frac{\log 2}{4} \cdot \frac{\deg g}{nr} \geq \frac{\log 2}{2} \cdot \frac{\deg g}{n2^r} \geq c\,\frac{\deg g}{n2^r}.$$

If $m < 2^{r+c_0}$ and $p \neq 2$ is a prime dividing m then we apply inequality (4.9) to find that

$$\begin{aligned}\mu(g) &\geq \frac{1}{p} \log\left(\frac{p}{2}\right) \cdot \frac{\deg g}{nr} \geq \left(1 - \frac{\log 2}{\log p}\right) \cdot \frac{\log p}{p} \cdot \frac{\deg g}{nr} \\ &\geq \frac{\log(3/2)}{\log 3} \cdot \frac{\log p}{p} \cdot \frac{\deg g}{nr}.\end{aligned}$$

However, the function $(\log x)/x$ is decreasing for $x \geq e$. Since $p \leq m < 2^{r+c_0}$, we conclude that

$$\frac{\log p}{p} > \frac{(r + c_0) \log 2}{2^{r+c_0}} > \frac{r \log 2}{2^{r+c_0}},$$

and hence,

$$\mu(g) \geq \frac{\log(3/2) \log 2}{2^{c_0} \log 3} \cdot \frac{\deg g}{n2^r}.$$

We know that $2^{c_0} = e^{c/2}$ so that by our definition of c we obtain

$$\mu(g) \geq c\,\frac{\deg g}{n2^r},$$

which establishes the theorem in the final case. ∎

5. Polynomials near polynomials of low Archimedean supremum norm. Suppose that m is a non-zero algebraic number. We now examine the situation where f and T are polynomials over $\overline{\mathbb{Q}}$ of the same degree with $f \equiv T \bmod m$. If K is a number field containing m with v indexing the places of K, let

$$N(m) = \sum_{v\mid\infty} \log|m|_v = -\sum_{v\nmid\infty} \log|m|_v.$$

Note that this definition does not depend on K and the second equality follows from the product formula. Recall that we write $\nu_\infty(T) = \sum_{v\mid\infty} \nu_v(T)$ and we say that $f \equiv T \bmod m$ if $\nu_v(T - f) \leq \log|m|_v$ for all $v \nmid \infty$.

Theorem 5.1. *Suppose that f and T are polynomials over $\overline{\mathbb{Q}}$ of the same degree such that $f \equiv T \bmod m$. If α satisfies $f(\alpha) = 0$ and $T(\alpha) \neq 0$ then*

$$\deg T \cdot h(\alpha) \geq N(m) - \nu_\infty(T).$$

Proof. Let K be a number field containing α, m, the coefficients of T and the coefficients of f. By Theorem 2.2 we find that

$$-\deg T \cdot h(\alpha) \leq \sum_{v\nmid\infty} U_v(\alpha, T) + \nu_\infty(T).$$

If $v \nmid \infty$ then $U_v(\alpha, T) \leq \nu_v(T - f) \leq \log|m|_v$ and the result follows. ∎

Clearly, in order for Theorem 5.1 to yield a non-trivial lower bound, we must have $N(m) > \nu_\infty(T)$, which justifies the title of this section. That is, if f is sufficiently close to T at enough non-Archimedean places of K, the positive contribution from $N(m)$ will overcome the negative contribution from $\nu_\infty(T)$. We also note the special case of Theorem 5.1 where $m \in \mathbb{Z}$ and $f, T \in \mathbb{Z}[x]$.

Corollary 5.2. *Suppose that f and T are polynomials over $\mathbb{Z}$ of the same degree and m is a positive integer such that $f \equiv T \bmod m$. If g is a factor of f relatively prime to T then*

$$\deg f \cdot \mu(g) \geq \deg g \cdot (\log m - \nu_\infty(T)).$$

Proof. Apply Theorem 5.1 to each root α of g and the corollary follows. ∎

Corollary 5.3. *Suppose that f and T are polynomials over $\mathbb{Z}$ of the same degree and m is a positive integer such that $f \equiv T \bmod m$. If f is relatively prime to T then*

$$\mu(f) \geq \log m - \nu_\infty(T).$$

Proof. Apply Corollary 5.2 with $g = f$ and the result is immediate. ∎

Acknowledgments. The author wishes to thank J. Garza for noticing that the language of heights and places yields a more easily generalized proof of the results of [2]. We also thank F. Rodriguez-Villegas for remarking that the hypothesis that f have coefficients congruent to 1 mod m may be replaced by a hypothesis giving a more general congruence relation in $\mathbb{Z}$. We thank M. J. Mossinghoff for his many useful suggestions, in particular, the inclusion of [4] in the introduction. Finally, we thank J. D. Vaaler for noticing that equality occurs in Theorem 2.2 for all auxiliary polynomials T along with many other ideas.

References

[1] 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.

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

[3] 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.

[4] R. Breusch, *On the distribution of the roots of a polynomial with integral coefficients*, Proc. Amer. Math. Soc. 2 (1951), 939–941.

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

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

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

[8] M. J. Mossinghoff, C. G. Pinner and J. D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. 67 (1998), 1707–1726.

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

[10] 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.

[11] 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
University of Texas at Austin
1 University Station C1200
Austin, TX 78712, U.S.A.
E-mail: csamuels@math.utexas.edu

Received on 20.8.2006
and in revised form on 16.11.2006 (5266)