E. Dobrowolski

On a question of Lehmer


<http://www.numdam.org/item?id=MSMF_1980_2_2__35_0>
Let $f$ be a polynomial with integral coefficients. Define the measure of $f$ by

$$M(f) = a \prod_{i=1}^{n} \max(1, |\alpha_i|)$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeros of $f$ listed with proper multiplicity and $a$ is the leading coefficient. D. H. Lehmer [5] asked whether for every $\epsilon > 0$ there exists a monic polynomial $f$ such that $1 < M(f) < 1 + \epsilon$.

P. E. Blanksby and H. L. Montgomery [1] and the present writer [2] obtained lower bounds for $M(f)$ in terms of the degree of $f$. In this paper we give a lower bound for $M(f)$ in terms of the number of non-zero coefficients of the polynomial $f$. The existence of such a bound (but not its form) has been announced by W. Lawton [4].
Theorem 1: If \( F(z) \in \mathbb{Z}[z] \) is an irreducible non-cyclotomic polynomial, \( F(z) \neq \pm z \), then
\[
M(F) \geq 1 + \frac{\log_2 e + 1}{2e} - \frac{1}{(k+1)^k}
\]
where \( k \) is the number of non-zero coefficients of \( F \).

The argument used in the proof gives the following corollary.

Corollary 1: If \( F \) is a product of different cyclotomic polynomials and \( F \) has at most \( k \) non-zero coefficients then
\[
\ell(F) \leq k^k + 1
\]
where \( \ell(F) \) denotes the sum of absolute values of the coefficients of \( F \).

The omission of the assumption of irreducibility of the polynomial \( F \) in Theorem 1 leads to a more complicated situation. In the general case the present writer, W. Lawton and A. Schinzel [3] obtained the following result.

Theorem 2: If \( g(z) \in \mathbb{Z}[z] \) is a monic polynomial with \( g(0) \neq 0 \) that is not a product a cyclotomic polynomials then
\[
M(g) \geq 1 + \exp_{k+1} \frac{1}{2k^2}
\]
where \( k \) is the number of non-zero coefficients of \( g \).
(Here, \( \exp_{k+1} \) denotes the \( (k+1) \)-th iterate of the exponential function).

In the proof we use notation of \( \ell(f) \) and \( M(f) \) as above. Further \( |f| \) denotes the degree of \( f \). For a vector \( x \), \( \ell(x) \) denotes the sum of absolute values of coordinates of \( x \).

Lemma 1: If \( \alpha \) is a non-zero algebraic integer of degree \( n \) which is not a root of unity, and if \( p \) is a prime number, then
\[
\prod_{i,j=1}^{n} (\alpha_i^p - \alpha_j) \geq p^n
\]
Proof : This is Lemma 1 of [2].

Lemma 2 : If \( f(z) \in \mathbb{Z}[z] \) is an irreducible polynomial and

\[
M(f) < 1 + \frac{\log 2e}{2e} \frac{1}{\ell(f)}
\]

then \( f \) is a cyclotomic polynomial or \( f(z) = \pm z \).

Proof : Let \( p \) be a prime number in the interval \( \ell(f) < p < 2\ell(f) \). Suppose that \( f \) is not a cyclotomic polynomial and let \( a_1, a_2, \ldots, a_{\ell(f)} \) be its zeros. Lemma 1 gives

\[
\ell(f)^{\ell(f)} |f|^{\ell(f)} P |f| > \prod_{i=1}^{\ell(f)} |f(a_i)| > p^{|f|}
\]

which is inconsistent with the inequality assumed in the Lemma. This Lemma was also proved with \( \frac{1}{6} \) in place of \( \frac{\log 2e}{2e} \) by C. L. Stewart, M. Mignotte and M. Waldschmidt, see [6].

Lemma 3 : Let \( a \in \mathbb{Z}^N \) be a vector with \( \ell(a) \geq (\text{NB})^N + 1 \) and \( B > 1 \) be a real number. Then there exist vectors \( c \in \mathbb{Z}^N \) and \( r \in \mathbb{Q}^N \) and a rational number \( q \) such that

(i) \( a = r + q c \)
(ii) \( 0 \neq \ell(c) < (\text{NB})^N + B^{-1} \)
(iii) \( q > B \cdot \ell(g) \)

(Note that \( \ell(a) > \ell(c) \) so \( a \neq c \)).

Proof : Let \( Q > 1 \) be a real number. By Dirichlet's theorem there exist a rational integer \( t, 1 \leq t \leq Q^N \), such that

\[
\|t \frac{1}{\ell(a)}\| < Q^{-1} \quad \text{for} \quad i = 1, 2, \ldots, N
\]

where \( a = (a_1, a_2, \ldots, a_N) \) and \( \| \| \) denotes the distance to the nearest integer. Take \( Q = \text{NB} \) and define \( q \frac{\ell(a)}{t} \). Define the vector \( c = (c_1, c_2, \ldots, c_N) \) by the conditions

\[
\|t \frac{a_i}{\ell(a)}\| = |t \frac{1}{\ell(a)} - c_i|, \quad c_i \in \mathbb{Z} \quad \text{for} \quad i = 1, 2, \ldots, N
\]
E. DOBROWOLSKI

and the vector \( \mathbf{r} = (r_1, r_2, \ldots, r_N) \) by \( \mathbf{z} = a - q \mathbf{c} \). Then (i) holds trivially. For (ii) note the inequality

\[
|t - \sum |c_i| | = | \sum (t \frac{1}{h(a)} - |c_i|) | < \sum |t \frac{1}{h(a)} - |c_i| | < N q^{-1} < 1.
\]

Thus \( t > 1 \) implies that \( c \neq 0 \). On the other hand

\[
\ell(z) = \sum \frac{a_i}{h(a)} - \sum q |c_i| < \frac{a_i}{h(a)} + q^{-1} < (N)^N + B^{-1}.
\]

Finally

\[
\ell(z) = \sum |a_i - q c_i| = q \sum |t \frac{1}{h(a)} - c_i| < q B^{-1}
\]

which proves (iii).

Proof of Theorem 1: Let \( F(z) = \sum_{i=1}^{k} a_i z^i \in \mathbb{Z}[z] \). If the exponents \( n_1, n_2, \ldots, n_k \) are fixed, then, with each vector \( a = (a_1, a_2, \ldots, a_k) \), we can associate the polynomial \( a(z) = \sum_{i=1}^{k} a_i z^{n_i} \) and conversely. If \( \ell(F) < (k+1)^k \) then the assertion of the theorem holds by Lemma 2. Otherwise, let \( F \in \mathbb{Z}^k \) be the vector corresponding to \( F \). Then

\[
\ell(F) = \ell(F) > k B^k + 1 \quad \text{with} \quad B > 1 + \frac{\log 2 e - 1}{2 e (k+1)^k}.
\]

By Lemma 3 \( F = r + q \mathbf{c} \) with \( r \in \mathbb{Q}^k \) and \( \mathbf{c} \in \mathbb{Z}^k \). Further \( q > B \). \( \ell(z) \) and \( F \neq \mathbf{c} \). If \( F, r, c \) are the corresponding polynomials then \( F \neq c \) implies that \( r \neq 0 \) and \( (F, c) = 1 \) because of the irreducibility of \( F \). Hence

\[
\mathbf{F}(a) = \mathbf{F}(a) - (q c(a))
\]

and
ON A QUESTION OF LEHMER

\[ \ell(r) \mid F \mid M(F) \mid F \mid > q \mid F \mid \]

So \( M(F) > B \).

Proof of Corollary 1: Assume that \( \ell(F) > k^r + 1 \). Then \( \ell(F) > kB^k + 1 \) with some \( B > 1 \) and, by Lemma 3, \( F = r + q.c \) with \( c(z) \in \mathbb{Z}[z] \) and \( q > B \ell(r) \). Further \( \ell(c) < \ell(F) \) and \( |c| < |F| \). So \( F \) does not divide \( c \) and there exists a cyclotomic polynomial \( f \) dividing \( F \) and not dividing \( c \). Hence

\[ r(\alpha) = \sum_{f(\alpha) = 0} (-q.c(\alpha)) \]

and

\[ \ell(r) \mid f \mid M(f) \mid F \mid > q \mid f \mid \]

which gives the contradiction \( 1 = M(f) > B > 1 \).

References


