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

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

\[
M(F) > 1 + \frac{\log 2e}{2e} \frac{1}{(k+1)^k}
\]

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

\[
\ell(F) < k^{k+1}
\]

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 of cyclotomic polynomials then

\[
M(g) > 1 + \frac{1}{\exp_{k+1}{2k^2}}
\]

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 \( \mathbf{x} \), \( \ell(\mathbf{x}) \) denotes the sum of absolute values of coordinates of \( \mathbf{x} \).

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

\[
\prod_{i,j=1}^{n} (\alpha_i^p - \alpha_j^p) > p^n
\]
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 \( e \ell(f) < p < 2e \ell(f) \). Suppose that \( f \) is not a cyclotomic polynomial and let \( \alpha_1, \alpha_2, \ldots, \alpha_{\ell(f)} \) be its zeros. Lemma 1 gives

\[
\ell(f) \frac{M(f)}{\ell(f)} > \prod_{i=1}^{\ell(f)} |f(\alpha_i)| > p |f|
\]

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 \( \ell(a) > (NB)^N + 1 \) and \( B > 1 \) be a real number. Then there exist vectors \( c \in \mathbb{Z}^N \) and \( \mathbf{x} \in \mathbb{Q}^N \) and a rational number \( q \) such that

(i) \( a = \mathbf{x} + q \mathbf{c} \)

(ii) \( 0 \neq \ell(\mathbf{c}) < (NB)^N + B^{-1} \)

(iii) \( q > B \cdot \ell(\mathbf{c}) \)

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

Proof: Let \( Q > 1 \) be a real number. By Dirichlet's theorem there exist a rational integer \( t, 1 < t < Q^N \), 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 \( Q = NB \) and define \( q = \frac{\ell(a)}{t} \). Define the vector \( \mathbf{c} = (c_1, c_2, \ldots, c_N) \) by the conditions

\[
\|t \frac{a_i}{\ell(a)} - c_i\| = |t - \frac{a_i}{\ell(a)} - c_i|, \quad c_i \in \mathbb{Z} \quad \text{for} \quad i = 1, 2, \ldots, N
\]
and the vector $\xi = (r_1, r_2, \ldots, r_N)$ by $\xi = a - q \cdot c$. Then (i) holds trivially. For (ii)
note the inequality

$$
|t - \sum |c_i| | = | \sum \left( \frac{1}{\xi(a)} - |c_i| \right) | < \sum \frac{1}{\xi(a)} |c_i| < NQ^{-1} < 1.
$$

Thus $t > 1$ implies that $c \not= 0$. On the other hand

$$
\xi(\xi) = \sum \frac{a_i}{\xi(a)} + |c_i| < (NB)^N + B^{-1}.
$$

Finally

$$
\xi(\xi) = \sum \frac{a_i - q \cdot c_i}{|c_i|} = q \sum \frac{a_i}{\xi(a)} - |c_i| < qB^{-1}
$$

which proves (iii).

**Proof of Theorem 1**: Let $F(z) = \sum a_i z^i \in \mathbb{Z}[z]$. 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
$a(z) = \sum a_i z^i$ and conversely. If $\xi(F) \leq (k+1)^k$ then the assertion of the
theorem holds by Lemma 2. Otherwise, let $F \in \mathbb{Z}^k$ be the vector corresponding to
$F$. Then

$$
\xi(F) = \xi(F) > kB^k + 1 \quad \text{with} \quad B > 1 + \frac{\log 2e}{2e} \left( \frac{1}{(k+1)^k} \right).
$$

By Lemma 3 $F = r + q \cdot c$ with $r \in \mathbb{Q}^k$ and $c \in \mathbb{Z}^k$. Further $q > B$. $\xi(\xi)$ and $F \not= c$.
If $F, r, c$ are the corresponding polynomials then $F \not= c$ implies that $r \not= 0$ and
$(F, c) = 1$ because of the irreducibility of $F$. Hence

$$
\begin{bmatrix}
F(a) = 0 \\
F(a) = 0
\end{bmatrix} \quad \begin{bmatrix}
(-q \cdot c(a))
\end{bmatrix}
$$

and
ON A QUESTION OF LEHMER

\[ \ell(r) |F| \frac{M(F) |F|}{|F|} = q^{|F|} \]

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

Proof of Corollary 1: Assume that \( \ell(F) > k^k + 1 \). 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

\[ 0 \neq \prod_{f(a)=0} r(a) = \prod_{f(a)=0} (-q.c(a)) \]

and

\[ \ell(r) |f| \frac{M(f) |F|}{|F|} = q^{|F|} \]

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

References


