MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 145–153

A Necessary and Sufficient Condition for Transcendency

By K. Mahler

To D. H. Lehmer in friendship on his 70th birthday

Abstract. As has been known for many years (see, e.g., K. Mahler, *J. Reine Angew. Math.*, v. 166, 1932, pp. 118–150), a real or complex number ζ is transcendental if and only if the following condition is satisfied.

To every positive number ω there exists a positive integer n and an infinite sequence of distinct polynomials $\{p_r(z)\} = \{p_{r_0} + p_{r_1}z + \cdots + p_{r_n}z^n\}$ at most of degree n with integral coefficients, such that

$$0 < |p_r(\zeta)| \leqslant \{p_{r_0}^2 + p_{r_1}^2 + \cdots + p_{r_n}^2\}^{-\omega} \quad \textit{for all } r.$$

In the present note I prove a simpler test which makes the transcendency of ζ depend on the approximation behaviour of a *single sequence* of distinct polynomials of arbitrary degrees with integral coefficients.

1. If

$$p(z) = \sum_{h=0}^{n} p_h z^h = p_n \prod_{h=1}^{n} (z - \alpha_h), \quad \text{where } p_n \neq 0,$$

is any polynomial with real or complex coefficients, of the exact degree n, and with the zeros $\alpha_1, \cdots, \alpha_n$, put

$$\partial(p) = n, \qquad M(p) = \exp\left(\int_0^1 \log|p(e^{2\pi it})|\,dt\right), \qquad m(p) = +\sqrt{\sum_{h=0}^{n} |p_h|^2}.$$

It is well known that

$$(1) \qquad M(p) = |p_n| \prod_{h=1}^{n} \max(1, |\alpha_h|), \qquad M(p) \leqslant m(p).$$

Next, if ζ is any real or complex number, put

$$\sigma(\zeta) = \begin{cases} 1 & \text{if } \zeta \text{ is real,} \\ 2 & \text{otherwise,} \end{cases}$$

and denote by $\mathfrak{P}(\zeta)$ the set of all polynomials $p(z)$ with integral coefficients that satisfy the inequality $p(\zeta) \neq 0$.

Received January 23, 1974.
AMS (MOS) subject classifications (1970). Primary 10F35.

In particular, let ζ be an algebraic number, say of the exact degree N. There exists then just one primitive irreducible polynomial

$$P(z) = \sum_{k=0}^{N} P_k z^k, \quad \text{where } P_N > 0,$$

with integral coefficients, that vanishes for $z = \zeta$. In terms of this polynomial we use the notations

$$\partial(\zeta) = \partial(P) = N, \qquad M(\zeta) = M(P), \qquad m(\zeta) = m(P).$$

Then, by (1),

$$M(\zeta) = P_N \prod_{k=1}^{N} \max(1, |\zeta_k|), \qquad M(\zeta) \leqslant m(\zeta),$$

where now $\zeta_1 = \zeta, \zeta_2, \cdots, \zeta_N$ are the algebraic conjugates of ζ, thus the zeros of $P(z)$. If, in particular, $\sigma(\zeta) = 2$, let the notation be such that ζ_2 is that algebraic conjugate of ζ which is also complex conjugate to ζ.

We wish to investigate how small $|p(\zeta)|$, as a function of the parameters $\sigma(\zeta)$, $\partial(\zeta)$, $m(\zeta)$, $\partial(p)$, and $m(p)$, can be made when $p(z)$ runs over the elements of $\mathfrak{P}(\zeta)$.

2. If ζ is algebraic, the following result holds which is essentially due to R. Güting (*Michigan Math. J.*, v. 8, 1961, pp. 149–159).

THEOREM 1. *If ζ is algebraic, and if $p(z) \in \mathfrak{P}(\zeta)$, then*

$$|p(\zeta)| \geqslant \max(1, |\zeta|)^{\partial(p)} m(\zeta)^{-\partial(p)/\sigma(\zeta)} \{\sqrt{\partial(p)+1}\; m(p)\}^{-(\partial(\zeta)/\sigma(\zeta)-1)}.$$

Proof. By the hypothesis, $p(\zeta) \neq 0$, but $P(\zeta) = 0$, where $P(z)$ is the primitive irreducible polynomial defined in Section 1 that belongs to ζ. It follows that $p(z)$ and $P(z)$ are relatively prime, so that their resultant R is distinct from zero. From its representation as a determinant in the coefficients of $p(z)$ and $P(z)$, R is an integer, and hence

(2) $$|R| \geqslant 1.$$

Also R may be written as the product

(3) $$R = P_N^n \prod_{k=1}^{N} p(\zeta_k).$$

Here

$$|p(\zeta_k)|^2 = \left|\sum_{h=0}^{n} p_h \zeta_k^h\right|^2 \leqslant \left(\sum_{h=0}^{n} p_h^2\right)\left(\sum_{h=0}^{n} |\zeta_k|^{2h}\right)$$

and

$$\sum_{h=0}^{n} |\zeta_k|^{2h} \leqslant (n+1) \max(1, |\zeta_k|)^{2n},$$

and therefore

$$|p(\zeta_k)| \leqslant \sqrt{\partial(p)+1}\, m(p) \max(1, |\zeta_k|)^n. \tag{4}$$

If $\sigma(\zeta) = 2$, then in addition $|p(\zeta_2)| = |p(\zeta)|$ because the numbers $p(\zeta)$ and $p(\zeta_2)$ are now complex conjugate.

Therefore

$$M(\zeta) = P_N \max(1, |\zeta|)^{\sigma(\zeta)} \prod_{k=\sigma(\zeta)+1}^{N} \max(1, |\zeta_k|) \leqslant m(\zeta).$$

Hence, from (2), (3), and (4),

$$1 \leqslant |R| \leqslant P_N^n |p(\zeta)|^{\sigma(\zeta)} \prod_{k=\sigma(\zeta)+1}^{N} \{\sqrt{\partial(p)+1}\, m(p) \max(1, |\zeta_k|)^n\}$$

$$\leqslant |p(\zeta)|^{\sigma(\zeta)} \{\sqrt{\partial(p)+1}\, m(p)\}^{N-\sigma(\zeta)} m(\zeta)^n \max(1, |\zeta|)^{-n\sigma(\zeta)}.$$

From this, the assertion follows at once.

3. When ζ is transcendental, or at least *not* algebraic of degree $\leqslant n$, it is necessary to determine polynomials $p(z)$ in $\mathfrak{P}(\zeta)$ for which $|p(\zeta)|$ is small. This construction is based on the following elementary lemma.

LEMMA 1. *Let*

$$F(x_0, x_1, \cdots, x_n) = \sum_{h=0}^{n} \sum_{k=0}^{n} F_{hk} x_h x_k \qquad (F_{hk} = F_{kh})$$

be a positive definite quadratic form in $n+1$ *variables, and let*

$$D = \begin{vmatrix} F_{00} & F_{01} & \cdots & F_{0n} \\ F_{10} & F_{11} & \cdots & F_{1n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ F_{n0} & F_{n1} & \cdots & F_{nn} \end{vmatrix} > 0$$

be its discriminant. Then integers $p_0, p_1, \cdots, p_n$ *not all zero exist such that*

$$F(p_0, p_1, \cdots, p_n) \leqslant (n+1) D^{1/(n+1)}.$$

Proof. Write F as a sum

$$F(x_0, x_1, \cdots, x_n) = \sum_{h=0}^{n} L_h(x_0, x_1, \cdots, x_n)^2$$

of the squares of $n+1$ linear forms $L_0, L_1, \cdots, L_n$ in $x_0, x_1, \cdots, x_n$ with real coefficients. The determinant of these linear forms is equal to $\mp\sqrt{D}$. Hence, by Minkowski's theorem on linear forms, there exist integers $p_0, p_1, \cdots, p_n$ not all zero for which

$$L_h(p_0, p_1, \cdots, p_n) \leqslant D^{1/2(n+1)} \qquad (h = 0, 1, \cdots, n),$$

and so these integers satisfy the assertion.

It is well known that one can prove stronger results than Lemma 1, of the form

$$F(p_0, p_1, \cdots, p_n) \leqslant c(n+1)D^{1/(n+1)},$$

where $c > 0$ stands for certain constants less than 1. However, Lemma 1 has the advantage of simplicity and suffices for our purpose.

The following lemma is nearly trivial, and its proof is therefore left to the reader.

LEMMA 2. *The positive definite quadratic form*

$$F(x_0, x_1, \cdots, x_n) = \left(\sum_{h=0}^{n} f_h x_h\right)^2 + \sum_{h=0}^{n} x_h^2$$

has the discriminant $D = 1 + \Sigma_{h=0}^{n} f_h^2$, *and the positive definite quadratic form*

$$F(x_0, x_1, \cdots, x_n) = \left(\sum_{h=0}^{n} f_h x_h\right)^2 + \left(\sum_{h=0}^{n} g_h x_h\right)^2 + \sum_{h=0}^{n} x_h^2$$

has the discriminant

$$D = 1 + \sum_{h=0}^{n} (f_h^2 + g_h^2) + \sum_{0 \leqslant h < k \leqslant n} (f_h g_k - f_k g_h)^2.$$

4. Let now ζ be any real or complex number and n an integer satisfying $n \geqslant \sigma(\zeta)$. We assume that ζ is either transcendental, or that it is algebraic of a degree greater than n.

First let ζ be a real number, and let s and t be two parameters such that

(5) $s \geqslant \max(1, |\zeta|)^{-n/(n+1)}, \qquad t = (n+1)^{1/2}(n+2)^{1/2(n+1)} \max(1, |\zeta|)^{n/(n+1)} s.$

The expression

$$F(x_0, x_1, \cdots, x_n) = s^{2(n+1)}\left(\sum_{h=0}^{n} x_h \zeta^h\right)^2 + \sum_{h=0}^{n} x_h^2$$

is a positive definite quadratic form in $x_0, x_1, \cdots, x_n$ which, by Lemma 2, has the discriminant

$$D = 1 + s^{2(n+1)} \sum_{h=0}^{n} \zeta^{2h}.$$

Here

$$\sum_{h=0}^{n} \zeta^{2h} \leqslant (n+1) \max(1, |\zeta|)^{2n},$$

and hence

$$D \leqslant s^{2(n+1)} \max(1, |\zeta|)^{2n} + s^{2(n+1)}(n+1) \max(1, |\zeta|)^{2n}$$
$$= s^{2(n+1)}(n+2) \max(1, |\zeta|)^{2n}.$$

Therefore, by Lemma 1, there exist integers $p_0, p_1, \cdots, p_n$ not all zero for which

$$F(p_0, p_1, \cdots, p_n) \leqslant (n+1)s^2(n+2)^{1/(n+1)} \max(1, |\zeta|)^{2n/(n+1)}. \tag{6}$$

Denote now by

$$p(z) = \sum_{h=0}^{n} p_h z^h$$

the polynomial which has these integers as coefficients; from the hypothesis,

$$p(z) \in \mathfrak{P}(\zeta). \tag{7}$$

The inequality (6) is equivalent to

$$s^{2(n+1)}p(\zeta)^2 + m(p)^2 \leqslant (n+1)s^2(n+2)^{1/(n+1)} \max(1, |\zeta|)^{2n/(n+1)},$$

and so it implies that

$$|p(\zeta)| \leqslant \frac{(n+1)^{1/2}(n+2)^{1/2(n+1)} \max(1, |\zeta|)^{n/(n+1)}}{s^n},$$

$$m(p) \leqslant (n+1)^{1/2}(n+2)^{1/2(n+1)} \max(1, |\zeta|)^{n/(n+1)}s.$$

In terms of t, this may instead be written as

$$|p(\zeta)| \leqslant \frac{(n+1)^{(n+1)/2}(n+2)^{1/2} \max(1, |\zeta|)^n}{t^n}, \qquad m(p) \leqslant t. \tag{8}$$

5. Secondly, let

$$\zeta = \xi + \eta i, \quad \text{where} \quad \eta \neq 0,$$

be a nonreal complex number. The powers of ζ may be split into their real and imaginary parts, say $\zeta^h = \xi_h + i\eta_h$, and then

$$\xi_h^2 + \eta_h^2 = |\zeta|^{2h}, \tag{9}$$

while by Cauchy's inequality

$$|\xi_h\eta_k - \xi_k\eta_h| \leqslant |\zeta|^{h+k}. \tag{10}$$

Denote now by s and t two parameters such that

$$\begin{aligned} &s \geqslant \max(1, |\zeta|)^{-2n/(n+1)}, \\ &t = (n+1)^{1/2}(n+2)^{1/(n+1)} \max(1, |\zeta|)^{2n/(n+1)}s. \end{aligned} \tag{11}$$

The expression

$$F(x_0, x_1, \cdots, x_n) = s^{n+1}\left|\sum_{h=0}^{n} x_h\zeta^h\right|^2 + \sum_{h=0}^{n} x_h^2$$

can be written as the positive definite quadratic form

$$F(x_0, x_1, \cdots, x_n) = s^{n+1}\left(\sum_{h=0}^{n} x_h\xi_h\right)^2 + s^{n+1}\left(\sum_{h=0}^{n} x_h\eta_h\right)^2 + \sum_{h=0}^{n} x_h^2,$$

which, by Lemma 2, has the discriminant

$$D = 1 + s^{n+1}\sum_{h=0}^{n}(\xi_h^2 + \eta_h^2) + s^{2(n+1)}\sum_{0\leqslant h<k\leqslant n}(\xi_h\eta_k - \xi_k\eta_h)^2.$$

Here, by (9),

$$\sum_{h=0}^{n}(\xi_h^2 + \eta_h^2) = \sum_{h=0}^{n}|\zeta|^{2h} \leqslant (n+1)\max(1, |\zeta|)^{2n},$$

and by (10),

$$\sum_{0\leqslant h<k\leqslant n}(\xi_h\eta_k - \xi_k\eta_h)^2 < \sum_{h=0}^{n}\sum_{k=0}^{n}|\zeta|^{2(h+k)} \leqslant (n+1)^2\max(1, |\zeta|)^{4n}.$$

Hence, from (11),

$$D \leqslant s^{2(n+1)}\{1 + (n+1) + (n+1)^2\}\max(1, |\zeta|)^{4n}$$

$$< s^{2(n+1)}(n+2)^2\max(1, |\zeta|)^{4n}.$$

With this estimate for D, we apply again Lemma 1. It follows that there exist integers $p_0, p_1, \cdots, p_n$ not all zero for which

(12) $$F(p_0, p_1, \cdots, p_n) < (n+1)\cdot s^2(n+2)^{2/(n+1)}\max(1, |\zeta|)^{4n/(n+1)}.$$

As in the first case, denote by

$$p(z) = \sum_{h=0}^{n} p_h z^h$$

the polynomial with these integers as coefficients; then $p(z) \in \mathfrak{P}(\zeta)$. From (12),

$$s^{n+1}|p(\zeta)|^2 + m(p)^2 < (n+1)(n+2)^{2/(n+1)}\max(1, |\zeta|)^{4n/(n+1)}s^2$$

and hence

$$|p(\zeta)| < \frac{(n+1)^{1/2}(n+2)^{1/(n+1)}\max(1, |\zeta|)^{2n/(n+1)}}{s^{(n-1)/2}},$$

$$m(p) < (n+1)^{1/2}(n+2)^{1/(n+1)}\max(1, |\zeta|)^{4n/(n+1)}s.$$

Thus, on changing over to the parameter t,

(13) $$|p(\zeta)| < \frac{(n+1)^{(n+1)/4}(n+2)^{1/2}\max(1, |\zeta|)^n}{t^{(n-1)/2}}, \quad m(p) < t.$$

6. In both estimates (8) and (13), $p(\zeta) \neq 0$ because $p(z)$ is an element of $\mathfrak{P}(\zeta)$. On combining the results just proved we arrive therefore at the following theorem.

THEOREM 2. *Let ζ be a real or complex number, and let n be an integer not less than $\sigma(\zeta)$. Assume that ζ is either transcendental, or that $\partial(\zeta) > n$. Further* *denote by* t *any real number satisfying*

$$t \geqslant (n+1)^{1/2}(n+2)^{1/(n+1)\sigma(\zeta)}.$$

Then there exists a polynomial $p(z) \not\equiv 0$ *with integral coefficients and such that* $\partial(p) \leqslant n$, $m(p) \leqslant t$ *and*

$$0 < |p(\zeta)| \leqslant \frac{(n+1)^{(n+1)/2\sigma(\zeta)}(n+2)^{1/2} \max(1, |\zeta|)^n}{t^{(n+1)/\sigma(\zeta)-1}}.$$

To this theorem we add the following remark.

The estimates (6) and (12) in the proof of Theorem 2 may be written as

$$\frac{1}{n+1}\left\{s^{2(n+1)}p(\zeta)^2 + n\cdot\frac{m(p)^2}{n}\right\} \leqslant s^2(n+2)^{1/(n+1)} \max(1, |\zeta|)^{2n/(n+1)}$$

and

$$\frac{1}{n+1}\left\{2s^{n+1}|p(\zeta)|^2 + (n-1)\cdot\frac{2m(p)^2}{n-1}\right\} \leqslant 2s^2(n+2)^{2/(n+1)} \max(1, |\zeta|)^{4n/(n+1)}$$

respectively. Thus, by the theorem on the arithmetic and geometric means, it follows that

$$\left\{p(\zeta)^2\frac{m(p)^{2n}}{n^n}\right\}^{1/(n+1)} \leqslant (n+2)^{1/(n+1)} \max(1, |\zeta|)^{2n/(n+1)}$$

and

$$\left\{|p(\zeta)|^4\left(\frac{2}{n-1}\right)^{n-1} m(p)^{2(n-1)}\right\}^{1/(n+1)} \leqslant 2(n+2)^{2/(n+1)} \max(1, |\zeta|)^{4n/(n+1)},$$

respectively. On simplifying and combining these two estimates we arrive then at the following result.

COROLLARY. *The polynomial* $p(z)$ *in Theorem* 2 *has the additional property that*

$$0 < |p(\zeta)| \leqslant \frac{(n-\sigma(\zeta)+1)^{(n+1)/2\sigma(\zeta)-1/2}\{\sigma(\zeta)(n+2)\}^{1/2} \max(1, |\zeta|)^n}{m(p)^{(n+1)/\sigma(\zeta)-1}}.$$

7. We say that a real or complex number ζ has the property (A) if there exist

(i) an infinite sequence of *distinct* polynomials $\{p_1(z), p_2(z), p_3(z), \cdots\}$ with integral coefficients, and

(ii) a sequence of positive numbers $\{\omega_1, \omega_2, \omega_3, \cdots\}$ tending to ∞, with the property that

$$0 < |p_r(\zeta)| \leqslant \{e^{\partial(p_r)}m(p_r)\}^{-\omega_r} \quad \text{for all } r.$$

From Theorems 1 and 2 we derive now the following test for transcendency.

THEOREM 3. *The real or complex number* ζ *is transcendental if, and only if, it has the property* (A).

Proof. (i) First, assume that ζ has the property (A), but that it is algebraic. Then, by this hypothesis and by Theorem 1,

$$\max(1, |\zeta|)^{\partial(p_r)} m(\zeta)^{-\partial(p_r)/\sigma(\zeta)} \{\sqrt{\partial(p_r)+1}\, m(p_r)\}^{-(\partial(\zeta)/\sigma(\zeta)-1)}$$

$$\leqslant |p_r(\zeta)| \leqslant \{e^{\partial(p_r)} m(p_r)\}^{-\omega_r}.$$

Here, on the left-hand side, the two numbers

$$m(\zeta)^{-1/\sigma(\zeta)} \quad \text{and} \quad \partial(\zeta)/\sigma(\zeta) - 1$$

are independent of r; and it is also obvious that

$$\sqrt{\partial(p_r)+1} \leqslant e^{\partial(p_r)}.$$

Hence there exists a positive number c independent of r such that

$$\max(1, |\zeta|)^{\partial(p_r)} m(\zeta)^{-\partial(p_r)/\sigma(\zeta)} \{\sqrt{\partial(p_r)+1}\, m(p_r)\}^{-(\partial(\zeta)/\sigma(\zeta)-1)}$$

$$\geqslant \{e^{\partial(p_r)} m(p_r)\}^{-c}.$$

By hypothesis, all the polynomials $p_r(z)$ are distinct, and so

$$\lim_{r\to\infty} e^{\partial(p_r)} m(p_r) = \infty,$$

because there cannot be more than finitely many polynomials $p_r(z)$ for which both $\partial(p_r)$ and $m(p_r)$ are below given bounds. Hence, as soon as r is so large that $\omega_r > c$, a contradiction arises. The hypothesis was therefore false, and ζ was transcendental.

(ii) Secondly, assume that ζ is transcendental. Denote by $\{n_1, n_2, n_3, \cdots\}$ a sequence of positive integers tending to infinity, by ϵ a positive constant, and by $\{t_1, t_2, t_3, \cdots\}$ a sequence of positive numbers satisfying

$$t_r \geqslant (n_r + 2)^{1/2+\epsilon} \quad \text{for all } r. \tag{14}$$

We now apply Theorem 2 to ζ, with the parameters $n = n_r$ and $t = t_r$. This may be done as soon as r is sufficiently large, because then

$$t_r \geqslant (n_r+2)^{1/2+\epsilon} \geqslant (n_r+1)^{1/2}(n_r+2)^{1/(n_r+1)\sigma(\zeta)}.$$

It follows that there exists for $r \geqslant r_0$ a polynomial $p_r(z)$ with integral coefficients such that

$$\partial(p_r) \leqslant n_r, \qquad m(p_r) \leqslant t_r$$

and

$$0 < |p_r(\zeta)| \leqslant \frac{(n_r+2)^{(1/2+\sigma(\zeta)/2(n_r+1))(n_r+1)/\sigma(\zeta)} \max(1, |\zeta|)^{n_r}}{t_r^{(n_r+1)/\sigma(\zeta)-1}}.$$

Here, for $r \geqslant r_1$,

$$\frac{\sigma(\zeta)}{2(n_r+1)} < \frac{\epsilon}{4}, \qquad \max(1, |\zeta|)^{n_r} < (n_r+2)^{\epsilon n_r/4}, \qquad t_r < (n_r+2)^{\epsilon n_r/4},$$

and therefore

$$0 < |p_r(\zeta)| \leqslant \frac{(n_r+2)^{(1/2+\epsilon/4+\epsilon/4+\epsilon/4)(n_r+1)/\sigma(\zeta)}}{t_r^{(n_r+1)/\sigma(\zeta)}}.$$

Now, by (14),

$$n_r + 2 \leqslant t_r^{2/(1+2\epsilon)},$$

and hence

$$0 < |p_r(\zeta)| \leqslant t_r^{-((n_r+1)/\sigma(\zeta))\{1-(2/(1+2\epsilon))(1/2+3\epsilon/4)\}} = t_r^{-(\epsilon/(2+4\epsilon))(n_r+1)/\sigma(\zeta)}.$$

On the other hand, $e^{\partial(p_r)}m(p_r) \leqslant e^{n_r}t_r, = t_r^{\lambda_r}$ say, where

$$\lambda_r = 1 + \frac{n_r}{\log t_r} = o(n_r).$$

Hence, on writing

$$t_r^{(\epsilon/(2+4\epsilon))(n_r+1)/\sigma(\zeta)} = \{e^{\partial(p_r)}m(p_r)\}^{\omega_r},$$

the number ω_r so defined has the property $\lim_{r\to\infty}\omega_r = \infty$, whence the assertion.

In the second part of this proof it was assumed that the sequence $\{n_r\}$ tended to infinity. *This hypothesis cannot be avoided,* as follows at once from the existence of S-numbers. With regard to the choice of the sequence $\{t_r\}$ by (14), it would have some interest to decide whether t_r could be chosen as a smaller function of n_r. Naturally, this might require an entirely different proof.

Mathematics Department
Institute of Advanced Studies
Australian National University
Canberra, A.C.T., Australia