BULLETIN DE LA S. M. F.

CAMERON L. STEWART

Algebraic integers whose conjugates lie near the unit circle

Bulletin de la S. M. F., tome 106 (1978), p. 169-176
<http://www.numdam.org/item?id=BSMF_1978__106__169_0>

Bull. Soc. math. France,
106, 1978, p. 169-176.

ALGEBRAIC INTEGERS WHOSE CONJUGATES LIE NEAR THE UNIT CIRCLE

BY

CAMERON L. STEWART

[I.H.E.S., Bures-sur-Yvette]

RÉSUMÉ. — Soit α un entier algébrique non nul de degré $D\,(>1)$, et soient $\alpha = \alpha_1, \ldots, \alpha_D$, ses conjugués. Dans cet article, on donne une nouvelle démonstration du résultat suivant de BLANKSBY et MONTGOMERY. Il existe un nombre positif C, tel que si

$$\prod_{i=1}^{D} \max\{1, |\alpha_i|\} < 1+(C D \log D)^{-1},$$

alors α est une racine de l'unité.

ABSTRACT. — Let α be a non-zero algebraic integer of degree $D\,(>1)$, with conjugates $\alpha = \alpha_1, \ldots, \alpha_D$. The purpose of this note is to give a new proof of the following result due to BLANKSBY and MONTGOMERY. There exists a positive number C such that if

$$\prod_{i=1}^{D} \max\{1, |\alpha_i|\} < 1+(C D \log D)^{-1},$$

hen α is a root of unity.

1. Introduction

In 1933 D. H. LEHMER [5], in connexion with a method for discovering large prime numbers, posed the following question. Let α be an algebraic integer of degree D with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_D$, and put

$$M(\alpha) = \prod_{i=1}^{D} \max\{1, |\alpha_i|\}.$$

Is it true that for every positive number ε there exists a non-zero algebraic integer α, not a root of unity, for which $M(\alpha) < 1+\varepsilon$? Plainly $M(\alpha) = 1$ if α is a root of unity; while, by a result of KRONECKER [4], if $M(\alpha) = 1$ and α is non-zero, then α is a root of unity. The smallest value of $M(\alpha)$ larger than 1 which LEHMER found was associated with the roots of the irreducible polynomial

$$x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1.$$

In this case, $M(\alpha) = \alpha_0 = 1.176{,}280{,}81\ldots$; here α_0 is the largest real root of the above equation. We remark that α_0 is a Salem number, a real algebraic integer larger than 1 having one conjugate on the unit circle and all others (¹) on or inside the unit circle. A computer search for small Salem numbers made by BOYD [2] yielded none smaller than α_0. In fact, even in the general case it seems that no algebraic integer α has been found with $1 < M(\alpha) < \alpha_0$.

While Lehmer's question remains open for the Salem numbers it has been answered in the negative for the PV numbers, those real algebraic integers, larger than 1, all of whose conjugates (¹) lie strictly inside the unit circle. If α is a PV number then $M(\alpha) = \alpha$; and, in 1944, SALEM [7] proved that there is a smallest PV number β_0. In the same year, SIEGEL [8] showed that β_0 is the real root of the equation $x^3 - x - 1$, hence $\beta_0 = 1.324{,}717{,}95\ldots$ In 1971, C. J. SMYTH [9] extended the above results considerably by proving, for $\alpha \neq 0,1$, that $M(\alpha) \geqslant \beta_0$ whenever the minimal polynomial $P(z)$ of α is not a reciprocal polynomial, in other words whenever $P(z) \not\equiv z^D P(z^{-1})$ where D is the degree of $P(z)$.

The best result concerning Lehmer's question which applies without restriction is due to BLANKSBY and MONTGOMERY [1]. They proved that if α is a non-zero algebraic integer of degree D which is not a root of unity then

$$M(\alpha) > 1 + (52\, D \log 6\, D)^{-1}. \tag{1}$$

Their proof depends upon the methods of Fourier analysis. The aim of this paper is to prove (1), albeit with a less precise constant, by means of an argument of the sort used in transcendence theory involving the construction of an auxiliary function with a large number of zeros. We prove in this way the following theorem.

THEOREM. — *If α if a non-zero algebraic integer of degree $D\,(> 1)$, and*

$$M(\alpha) < 1 + (10^4\, D \log D)^{-1}, \tag{2}$$

then α is a root of unity.

It follows directly from (1) or (2) that there exists a positive number C such that if α is a non-zero algebraic integer of degree D (> 1), and

$$\overline{|\alpha|} < 1 + (C D^2 \log D)^{-1}, \tag{3}$$

(¹) Here the number itself is understood to be excepted.

then α is a root of unity; here $\lceil\overline{\alpha}\rceil$ denotes the maximum of the absolute values of the conjugates of α. Recently, DOBROWOLSKI [3] obtained a very simple and elegant improvement of (3). He showed that, if α is a non-zero algebraic integer of degree $D\,(> 1)$, and

$$\lceil\overline{\alpha}\rceil < 1+(\log D)/6\,D^2,$$

then α is a root of unity.

In conclusion, I should like to acknowledge the useful conversations concerning this paper which I have had with M. MIGNOTTE and M. WALDSCHMIDT, and to thank A. van der POORTEN for drawing my attention to the problem considered herein.

2. A preliminary lemma

We record here a version of Siegel's lemma concerning solutions of linear equations. Our proof is similar to one given by WALDSCHMIDT in [10] (*see* also [6]).

LEMMA. — *Let b_{ij} $(1 \leqslant i \leqslant N, 1 \leqslant j \leqslant M)$, be algebraic integers, not all of which are zero, in a field K of degree D over the rational numbers, and let $\sigma_1, \sigma_2, \ldots, \sigma_D$ denote the embeddings of K in the complex numbers. If $N \geqslant 2\,MD$, then the system of equations*

$$\textstyle\sum_{i=1}^{N} b_{ij}\,x_i = 0 \qquad (1 \leqslant j \leqslant M),$$

has a solution in rational integers $x_1, x_2, \ldots, x_N$, not all of which are zero, whose absolute values are at most

$$\sqrt{2}\,N\,(\max_{1\leqslant j\leqslant M}\textstyle\prod_{k=1}^{D}(\max_{1\leqslant i\leqslant N}|\sigma_k(b_{ij})|))^{1/D}.$$

Proof. — Let $\sigma_1, \ldots, \sigma_r$ denote the embeddings of K into the real numbers, and let $\sigma_{r+i}, \sigma_{r+s+i}, i = 1, \ldots, s$, be the remaining s conjugate pairs of embeddings. Put $\tau_i = \sigma_i$ for $i = 1, \ldots, r$, and put

$$\tau_{r+i} = \operatorname{Re}\sigma_{r+i} \quad\text{and}\quad \tau_{r+s+i} = \operatorname{Im}\sigma_{r+i} \quad\text{for } i = 1, \ldots, s;$$

here $\operatorname{Re}\sigma_{r+i}(x)$ is just the real part of $\sigma_{r+i}(x)$ while $\operatorname{Im}\sigma_{r+i}(x)$ is the imaginary part. We now set

$$Y = [\sqrt{2}\,N\,(\max_j\textstyle\prod_{k=1}^{D}(\max_i|\sigma_k(b_{ij})|))^{1/D}].$$

For any pair of integers (k, j) with $1 \leqslant k \leqslant D$ and $1 \leqslant j \leqslant M$, the $(Y+1)^N$ different N-tuples $(y_1, \ldots, y_N)$ with $0 \leqslant y_i \leqslant Y$ for $i = 1, \ldots, N$, give rise to $(Y+1)^N$ numbers $\tau_k(\sum_{i=1}^N b_{ij} y_i)$ which all lie in an interval of the real line of length at most $\max_i |\tau_k(b_{ij})| NY$. Put $L = Y(Y+1)$. Note that L is non-zero since the b_{ij} are algebraic integers which are not all zero and hence Y is at least 1. Since $N \geqslant 2\, MD$ and $L < (Y+1)^2$, we have $L^{MD} < (Y+1)^N$. Therefore, by the pigeon-hole principle, two of the N-tuples, $(y_1^{(1)}, \ldots, y_N^{(1)})$ and $(y_1^{(2)}, \ldots, y_N^{(2)})$ say, satisfy

$$(4) \qquad |\tau_k(\textstyle\sum_{i=1}^N b_{ij} y_i^{(1)}) - \tau_k(\sum_{i=1}^N b_{ij} y_i^{(2)})| \leqslant \max_i |\tau_k(b_{ij})| \dfrac{NY}{L},$$

for $k = 1, \ldots, D$ and $j = 1, \ldots, M$. Put $x_i = y_i^{(1)} - y_i^{(2)}$ for $i = 1, ..., N$. Then $\max_i |x_i| \leqslant Y$ and the x_i are not all zero. Therefore, to prove the lemma it suffices to show that

$$\textstyle\sum_{i=1}^N b_{ij} x_i = 0 \qquad \text{for} \quad 1 \leqslant j \leqslant M.$$

From (4), we deduce, for $j = 1, \ldots, M$, that

$$|\sigma_k(\textstyle\sum_{i=1}^N b_{ij} x_i)| \leqslant \max_i |\sigma_k(b_{ij})| \dfrac{NY}{L} \qquad \text{for} \quad k = 1, \ldots, r,$$

and that

$$\begin{aligned} &|\sigma_k(\textstyle\sum_{i=1}^N b_{ij} x_i)\, \sigma_{k+s}(\sum_{i=1}^N b_{ij} x_i)| \\ &\leqslant \{\max_i (\operatorname{Re} \sigma_k(b_{ij}))^2 + \max_i (\operatorname{Im} \sigma_k(b_{ij}))^2\} \left(\dfrac{NY}{L}\right)^2 \\ &\leqslant 2 \max_i |\sigma_k(b_{ij})\, \sigma_{k+s}(b_{ij})| \left(\dfrac{NY}{L}\right)^2, \end{aligned}$$

for $k = r+1, \ldots, r+s$. Therefore

$$|\textstyle\prod_{k=1}^D \sigma_k(\sum_{i=1}^N b_{ij} x_i)| < \left(\dfrac{Y(Y+1)}{L}\right)^D = 1$$

for $j = 1, \ldots, M$. The number on the left hand side of the above expression is the absolute value of the norm from K to Q of $\sum_{i=1}^N b_{ij} x_i$ which, since it is less than 1, is 0. Thus $\sum_{i=1}^N b_{ij} x_i = 0$, for $j = 1, \ldots, M$, as required.

3. Proof of the theorem

We assume that $D \geqslant 4$ since, as is easily checked, the theorem holds for $D \leqslant 3$. Further, we assume, without loss of generality, that $|\alpha| = \overline{|\alpha|}$, the maximum of the absolute values of the conjugates of α. Put

$$(5) \qquad U = [70\, D \log D] \qquad \text{and} \qquad K = 2\, U,$$

and choose K positive integers $r_1 < r_2 < \ldots < r_K$ from the first 13 K positive integers in such a way that

$$\max_{1 \leqslant s \leqslant t \leqslant K} \{ | \operatorname{Im}(\log \alpha^{r_s}) - \operatorname{Im}(\log \alpha^{r_t}) | \} \leqslant 2\pi/13;$$

throughout this paper $\operatorname{Im}(x)$ denotes the imaginary part of x, and $\log x$ denotes the principal value of the logarithm of x taken so that $-\pi < \operatorname{Im}(\log x) \leqslant \pi$. Such a choice is possible by the pigeon-hole principle. Put

$$\theta_1 = \min_{1 \leqslant k \leqslant K} \operatorname{Im}(\log \alpha^{r_k}) \qquad \text{and} \qquad \theta = \theta_1 + \pi/13.$$

We then have

$$\max_{1 \leqslant k \leqslant K} | \operatorname{Im}(\log \alpha^{r_k}) - i\theta | \leqslant \pi/13. \tag{6}$$

We now construct a function $f(z)$ of the form

$$f(z) = \exp(-i\theta z) \sum_{k=1}^{K} \sum_{d=1}^{D} a_{k,d} \alpha^d \exp(\log \alpha^{r_k}) z,$$

where the $a_{k,d}$ are rational integers to be chosen so that $f(u) = 0$ for $u = 1, \ldots, U$. This is equivalent to solving the equations

$$f(u) \exp(i\theta u) = \sum_{k=1}^{K} \sum_{d=1}^{D} a_{k,d} \alpha^{d+r_k u} = 0$$

for $u = 1, \ldots, U$. Since KD, the number of unknowns, is 2 D times U, the number of equations, by the preliminary lemma there exists a solution in rational integers $a_{k,d}$, not all zero, so that

$$\max_{k,d} | a_{k,d} | \leqslant \sqrt{2}\, KD\, M^{13KU+D},$$

where

$$M = (\textstyle\prod_{\sigma \in S} \max\{1, |\sigma\alpha|\})^{1/D} = (M(\alpha))^{1/D};$$

here S denotes the set of embeddings of $Q(\alpha)$ in the complex numbers. Let $f(z)$ be defined by means of these $a_{k,d}$.

We now prove by induction that $f(u) = 0$ for all positive integers u. Accordingly we assume that $f(u) = 0$ for $u \leqslant J$ where $J \geqslant U$, and we prove that $f(J+1) = 0$. Since $f(z)$ is an entire function,

$$F(z) = f(z) / (\textstyle\prod_{u=1}^{J} (z-u))$$

is also entire. By the maximum modulus principle

$$F(J+1) \leqslant \max_{z \in \Gamma} | F(z) |,$$

where $\Gamma = \{ \, | z | = 2J+1 \}$. Thus

$$(7) \qquad |f(J+1)| \leqslant \binom{2J}{J}^{-1} \max_{z \in \Gamma} |f(z)|.$$

It is readily verified that

$$(8) \qquad \max_{z \in \Gamma} |f(z)| \leqslant \sqrt{2}(KD)^2 M^{13KU+D} \, \overline{|\alpha|}^{\,D} \exp(\Delta(2J+1)),$$

where

$$\Delta = \max_{1 \leqslant k \leqslant K} |(\log \alpha^{r_k}) - i\theta|.$$

Further it follows from (6) that $\Delta \leqslant | \, 13\, K \log |\alpha| + i\pi/13 \, |$. Since $|\alpha| = \overline{|\alpha|}$, we may use the fact that $1 \leqslant |\alpha| \leqslant M(\alpha)$, (2) and the inequality

$$(9) \qquad \log(1+x) \leqslant x \qquad \text{for} \quad x \geqslant 0,$$

to show that $0 \leqslant \log |\alpha| \leqslant (10^4 D \log D)^{-1}$. Recalling (5), we see that $0 \leqslant 13\, K \log |\alpha| < \pi/13$ and thus $\Delta(2J+1) < (\log 2)\, J$. Therefore from (7) and (8), we have

$$|f(J+1)| \leqslant \binom{2J}{J}^{-1} 2^J \, \sqrt{2}(KD)^2 M^{13KU+D} \, \overline{|\alpha|}^{\,D},$$

and employing (5) and the estimate $\binom{2J}{J} \geqslant 4^J/2J$, we see that

$$(10) \qquad |f(J+1)| \leqslant J\, 2^{-J} K^4 M^{26KU}.$$

We now estimate $|f(J+1)|$ from below. Put $\beta = f(J+1) \exp(i\theta(J+1))$. Since β is an algebraic integer in $Q(\alpha)$ it is either 0, in which case $f(J+1) = 0$, or the norm from $Q(\alpha)$ to Q of β is at least 1 in absolute value. In the latter case

$$(11) \qquad |f(J+1)| = |\beta| \geqslant \Big(\prod_{\sigma \in S'} |\sigma(\beta)|\Big)^{-1},$$

where S' is the set of embeddings S minus the identity embedding. We have, for all $\sigma \in S'$,

$$(12) \qquad |\sigma(\beta)| \leqslant \sqrt{2}(KD)^2 M^{13KU+D} \max\{1, |\sigma(\alpha)|^{13K(J+1)+D}\}.$$

Since $|\alpha| = \overline{|\alpha|}$,

$$\prod_{\sigma \in S'} \max\{1, |\sigma(\alpha)|\} \leqslant \Big(\prod_{\sigma \in S} \max\{1, |\sigma(\alpha)|\}\Big)^{(D-1)/D} = M^{D-1},$$

and from (11) and (12), we conclude that

$$|f(J+1)| \geqslant (K^4 M^{26K(J+1)})^{-D+1}.$$

Comparing this estimate for $|f(J+1)|$ with the one given by (10), we find that

$$2^J \leqslant JK^{4D} M^{26K(J+1)D}.$$

Taking logarithms and estimating $(J+1)/J$ from above by 27/26 yields

$$\log 2 \leqslant \frac{\log J}{J} + \frac{4 D \log K}{J} + 27 KD \log M.$$

Thus, recall that $M(\alpha) = M^D$, $K = 2U$ and $J \geqslant U$,

$$\log 2 \leqslant \frac{\log U}{U} + \frac{4 D \log 2U}{U} + 54 U \log M(\alpha). \tag{13}$$

Since $U = [70 D \log D]$ and $D \geqslant 4$, we find, after some calculation, that

$$\frac{\log U}{U} + \frac{4 D \log 2U}{U} < .31.$$

And using (2), (9) and (13), we deduce that

$$(\log 2 - .31) 10^4 D \log D < 54 U.$$

This contradicts our choice of U; therefore β, hence also $f(J+1)$, is zero. This completes the induction.

We conclude, on putting $A_k = \sum_{d=1}^{D} a_{k,d} \alpha^d$, that

$$f(u) \exp(i\theta u) = \sum_{k=1}^{K} A_k \alpha^{r_k u} = 0 \tag{14}$$

for all positive integers u. Since α has degree D, $A_k = 0$ if, and only if, $a_{k,1} = \ldots = a_{k,D} = 0$. By construction the $a_{k,d}$'s are not all zero and thus the A_k's are not all zero. Now, as D. BERTRAND observed, it follows from (14) that the polynomial $\sum_{k=1}^{K} A_k z^{r_k}$ vanishes at all points α^u with u a positive integer. Since the polynomial is not identically zero two of these points are the same. Therefore α is a root of unity as required. Alternatively, it is easily seen that (14) cannot hold for all positive integers u unless $|\alpha| \leqslant 1$. By assumption, however, $|\alpha| = \lceil \alpha \rceil$ and so by Kronecker's theorem α is a root of unity. This completes the proof.

REFERENCES

[1] Blanksby (P. E.) and Montgomery (H. L.). — Algebraic integers near the unit circle, *Acta Arithm.*, Warszawa, t. 28, 1971, p. 355-369.

[2] Boyd (D. W.). — Small Salem numbers, *Duke math. J.*, t. 44, 1977, p. 315-328.

[3] Dobrowolski (E.). — On the maximal modulus of conjugates of an algebraic integer, *Bull. Acad. polon. Sc.* (à paraître).

[4] Kronecker (L.). — Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. für reine und angew. Math.*, t. 53, 1857, p. 173-175.

[5] Lehmer (D. H.). — Factorization of certain cyclotomic functions, *Annals of Math.*, Series 2, t. 34, 1933, p. 461-479.

[6] Mignotte (M.) and Waldschmidt (M.). — Linear forms in two logarithms and Schneider's method, *Math. Annalen*, t. 231, 1978, p. 241-267.

[7] Salem (R.). — A remarkable class of algebraic integers. Proof of a conjecture o Vijayaraghavan, *Duke math. J.*, t. 11, 1944, p. 103-108.

[8] Siegel (C. L.). — Algebraic integers whose conjugates lie in the unit circle, *Duke math. J.*, t. 11, 1944, p. 597-602.

[9] Smyth (C. J.). — On the product of the conjugates outside the unit circle of an algebraic integer, *Bull. London math. Soc.*, t. 3, 1971, p. 169-175.

[10] Waldschmidt (M.). — *Nombres transcendants.* — Berlin, Springer-Verlag, 1974 (*Lecture Notes in Mathematics*, 402).

Added in Proof. — E. Dobrowolski has recently proved, again by means of an argument common to transcendence theory, that if α is a non-zero algebraic integer of degree $D(>1)$ which is not a root of unity, then $M(\alpha) > 1+c((\log\log D)/\log D)^3$, where C is a positive constant.

(Texte reçu le 4 octobre 1977.)

Cameron L. Stewart,
I. H.E.S.,
35, route de Chartres,
91440 Bures-sur-Yvette.