Canad. Math. Bull. Vol. **21** (2), 1978

VARIATIONS ON A THEME OF KRONECKER

BY
DAVID W. BOYD

In 1857, Kronecker [10] showed that if $\theta_1, \ldots, \theta_n$ are the roots of the polynomial $P(z) = z^n + c_1 z^{n-1} + \cdots + c_n$, where $c_1, \ldots, c_n$ are integers with $c_n \neq 0$, and if $|\theta_1| \leq 1, \ldots, |\theta_n| \leq 1$, then $\theta_1, \ldots, \theta_n$ are roots of unity. The proof is short and ingenious: Consider the polynomials $P_m(z)$ whose roots are $\theta_1^m, \ldots, \theta_n^m$ for $m = 1, 2, \ldots$. The condition on the size of the roots and the fact that the c_i are integers implies that there can only be a finite number of different P_m. Thus two distinct powers of each root must coincide and this means that each root is a root of unity.

In 1933, Lehmer [11] asked whether the following improvement of Kronecker's theorem might be true: let $\Omega(P)$ denote the product $\prod_i \max(|\theta_i|, 1)$.

(L) Is there a constant $\varepsilon_0 > 0$, independent of n such that if $\Omega(P) < 1 + \varepsilon_0$, then $\theta_1, \ldots, \theta_n$ are roots of unity?

The lack of dependence of ε_0 on n is what makes this suggestion so intriguing. For example, $P_n(z) = z^n - 2$ has its roots arbitrarily close to $|z| = 1$ without being roots of unity; however $\Omega(P_n) = 2$ for all n, so there is no conflict with (L).

Another possible way to improve Kronecker's theorem would be to place a condition on $M(P) = \max_i |\theta_i|$. If (L) is correct then the best possible result would be that

(SZ) There is a constant c such that $M(P) < 1 + c/n$ implies that $\theta_1, \ldots, \theta_n$ are roots of unity.

This is a conjecture made by Schinzel and Zassenhaus [14].

Both of these questions are still unsettled but considerable progress has been made in the recent past, some of which will be described here. For the remainder of the paper we will assume that P is irreducible since it is clear that there is no loss of generality in doing so. Then $\theta = \theta_1, \theta_2, \ldots, \theta_n$ are the conjugates of an algebraic integer of degree n.

If θ is a root of unity and $\theta \neq 1$, then P is a reciprocal polynomial, i.e. $P(z) = z^n P(z^{-1})$. This suggests that the problem may be more accessible for

---

This paper is one of a series of survey papers written at the invitation of the Editors of the Canadian Mathematical Bulletin.

non-reciprocal polynomials and this is indeed the case. In fact, the questions have been answered completely in this situation by Smyth [16]. He showed that $\Omega(P) \geq \theta_0$ and that $M(P) \geq 1 + (\log \theta_0)/n$ when P is a non-reciprocal polynomial. Here $\theta_0 = 1.3247\ldots$ is the real root of $P_0(z) = z^3 - z - 1$, and since $\Omega(P_0) = \theta_0$, Smyth's result concerning $\Omega(P)$ is best possible. The result concerning $M(P)$ improves an earlier result of Cassels [6], that $M(P) \geq 1 + 1/10n$ for non-reciprocal P.

The number θ_0 is the smallest element of the set S of Pisot-Vijayaraghavan numbers, a result due to Siegel [15]. S is the set of algebraic integers $\theta > 1$ whose other conjugates lie strictly within the unit circle. A remarkable property of S, established by Salem [12], is that S is a closed subset of the real line. The fact that $\inf S = \min S > 1$ is an immediate consequence, but of course the exact determination of $\min S$ requires a more detailed study. Dufresnoy and Pisot [9] have gone even further and determined the smallest limit point of S (it is the famous golden section), and have found all points of S less than this limit point. The paper [4] is an elaboration of the ideas of [9].

In view of Smyth's result, it would be interesting to explore the connection between S and the set Ω_1 of values of $\Omega(P)$, as P varies over all the non-reciprocal polynomials. In particular, what is the smallest limit point of Ω_1? That some fairly small limit points exist can be established by a lemma proved in [3]. We showed there that if $p(w, z)$ is a polynomial in two variables then

$$\lim_{n\to\infty} \int_0^1 \log |p(e^{2\pi \mathrm{int}}, e^{2\pi i t})|\, dt = \int_0^1 ds \int_0^1 \log |p(e^{2\pi i s}, e^{2\pi i t})|\, dt. \tag{1}$$

Since Jensen's formula shows that

$$\log \Omega(P) = \int_0^1 \log |P(e^{2\pi i t})|\, dt, \tag{2}$$

it follows from (1) that if $P_n(z) = 1 - z + z^n$ then

$$\log \Omega(P_n) \to (2\pi)^{-2} \int_0^{2\pi} ds \int_0^{2\pi} \log |1 - e^{it} + e^{is}|\, dt. \tag{3}$$

Applying Jensen's formula again to the right member of (3) shows that

$$\Omega(P_n) \to \exp\left\{\pi^{-1} \int_0^{\pi/3} -\log(2 \sin(t/2))\, dt\right\} = 1.38135\ldots. \tag{4}$$

This number does not appear to be algebraic. Are there smaller limit points of Ω_1?

Now we turn to the questions (L) and (SZ) for reciprocal polynomials. The best result in the direction of (L) is due to Blanksby and Montgomery [1], namely that $\Omega(P) < 1 + (52n \log 6n)^{-1}$ implies that θ is a root of unity. As a

corollary, one obtains the result that $M(P)<1+(30n^2\log 6n)^{-1}$ implies that θ is a root of unity. Their result was obtained by an analysis using multiple Fourier series. Recently, Stewart [17] has obtained their result, with a slightly worse constant, by using Baker's extrapolation method.

The result concerning $M(P)$ has recently been improved by Dobrowolski [8]. He has been able to show that

$$M(P)<1+(\log n)/6n^2 \tag{5}$$

implies that θ is a root of unity. His strikingly elementary proof is reminiscent of Kronecker's original proof of his theorem. He observes that if

$$S_k=\theta_1^k+\cdots+\theta_n^k,$$

then $S_{kp}\equiv S_k \pmod p$, for any prime p. Choosing a prime which satisfies $3n<p<6n$, he is able to show that (5) implies $|S_{kp}-S_k|<p$ and hence $S_{kp}=S_k$ for $k=1,2,\ldots,n$. But then θ and θ^p are roots of the same irreducible polynomial, and this implies that θ is a root of unity.

By analogy with Smyth's result, one might expect that $\Omega(P)$ would be smallest for polynomials having exactly one root outside the unit circle. In fact, the smallest known value of $\Omega(P)>1$ is attained for such a polynomial, first exhibited by Lehmer in [11]:

$$P(z)=z^{10}+z^9-z^7-z^6-z^5-z^4-z^3+z+1. \tag{6}$$

This has exactly one root $\sigma_1>1$ outside $|z|=1$, and thus $\Omega(P)=\sigma_1=1.1762808\ldots$.

The set of $\sigma>1$ which satisfy a reciprocal polynomial all of whose remaining roots lie in $|z|\le 1$ is denoted T, and called the set of Salem numbers. For such a polynomial, one has $\Omega(P)=\sigma$, so an immediate consequence of an affirmative answer to (L) would be that $\inf T>1$, but even this is not known.

In fact, basically the only fact known about the distribution of T is due to Salem [13], who showed that each point of S is a limit point of T. To do this, he showed that if P is the minimal polynomial of θ in S (with $P\neq z^2-qz+1$, $q\ge 3$), and if

$$Q_m^{\pm}(z)=x^mP(z)\pm z^nP(z^{-1}), \tag{7}$$

then $Q_m^{\pm}$ has at most one root $\theta_m^{\pm}>1$ outside the unit circle, and that $\theta_m^{\pm}\to\theta$ as $m\to\infty$. The number $\theta_m^{\pm}$ is thus either a Salem number, or is of the form $(q+(q^2-4)^{1/2})/2$, with $q\ge 2$, and so (7) can be thought of as a construction for producing members of T from members of S.

We recently showed [2] that, in fact, all Salem numbers are produced in this way. The study of the set T thus reduces to the study of $\{\theta_m^{\pm}: m\ge 1\}$. We have been able to show that if $m\ge 2$, then $\theta_m^{\pm}\to\infty$ as $\theta\to\infty$. Also, there is a finite algorithm for determining all $\theta_m^{\pm}$, $m\ge 2$ which lie in an interval disjoint from

$\{1\} \cup S$. For example, there are 41 Salem numbers of the form $\theta_2^{\pm}$ in [9/8, 13/10], the smallest of which is σ_1 [4].

The situation is quite different for $\theta_1^{\pm}$, and any σ in T is represented infinitely often in the form $\theta_1^{\pm}$ for arbitrarily large $\theta \in S$, and with $Q_1^{\pm}$ having an arbitrary "extraneous" factor $K(z)$ whose roots are simple roots of unity. Thus, the connection between S and T is, at this time, not sufficient to establish that $\inf T > 1$. Intuitively, it seems to suggest that the set $S \cup T$ is closed.

Returning to the general question (L), it seems plausible to me that $\inf \Omega(P) = \inf T$, although there is very little evidence to support this. Stewart and te Riele carried out a complete survey of reciprocal polynomials with coefficients ± 1 or 0, with degrees ≤ 20 and $1.175 < \Omega(P) < 1.25$, without finding a smaller value of $\Omega(P)$ than σ_1, and incidentally without finding any Salem numbers which are not on the list given in [2]. (There are four further numbers to add to the list in [2] which may be found in [4]).

If the feelings expressed in [2] are correct, then $\theta_0 = \inf S$ should be the smallest limit point of T. The same cannot be said of the set Ω_2 of values of $\Omega(P)$, as P varies over all reciprocal polynomials (with integer coefficients of course). For example, if $P_n = z^{2n} - z^{n+1} - z^n - z^{n-1} + 1$, then

$$\begin{aligned} \lim \Omega(P_n) &= \exp\left\{ \pi^{-1} \int_0^{\pi/3} \log(b(t) + (b(t)^2 - 1)^{1/2})\, dt \right\} \\ &= 1.2857348 \ldots < \theta_0, \end{aligned} \tag{8}$$

where $b(t) = (\frac{1}{2}) + \cos t$. This limit point was discovered independently by the author and C. J. Smyth (who considered instead $P_n = z^{2n} - z^{2n-1} - z^n - z + 1$). The result (8) can be proved in the same way as (4). An even smaller limit point is obtained from $P_n = z^{2n} - z^{2n-1} - z^{n+1} + z^n - z^{n-1} - z + 1$ for which $\Omega(P_n) \to 1.255425 \ldots$ (an approximate numerical value of an expression similar to (8)).

To conclude, let me suggest some problems for the reader. Let $\Omega_{1,k}$ be the set of numbers $\Omega(P)$ where P is non-reciprocal, has exactly k roots outside the unit circle, and is not of the form $Q(z^r)$ for any $r > 1$. Is $\Omega_{1,k}$ a closed set? Let $\inf \Omega_{1,k} = b_{1,k}$. Is $b_{1,k}$ an increasing sequence? The work of Cantor [5] on PV k-tuples should be useful here. The work of Chamfy [7] on the Schur-Dufresnoy-Pisot algorithm may also have some bearing on these questions.

Let $\Omega_{2,k}$ be the corresponding set with P required to be reciprocal rather than non-reciprocal, and let $b_{2,k} = \inf \Omega_{2,k}$. Is $\Omega_{1,k} \cup \Omega_{2,k}$ closed? Is $b_{2,k}$ increasing? Since $\Omega_{1,1} = S$ and $\Omega_{2,1} = T$ the first question is unanswered even for $k = 1$. It appears that completely new methods will be needed to answer these questions.

ACKNOWLEDGMENT. I would like to thank C. J. Smyth and C. L. Stewart for sending me some of their unpublished results, and informing me of the work of Dobrowolski.

This work was supported in part by N.R.C. grant A8128.

References

1. P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. **18** (1971), 355–369.

2. D. W. Boyd, *Small Salem numbers*, Duke Math. Jour. **44** (1977), 315–328.

3. ——, *Pisot numbers and the width of meromorphic functions*, privately circulated manuscript.

4. ——, *Pisot and Salem numbers in intervals of the real line*, Math. of Comp., (to appear in October 1978).

5. D. G. Cantor, *On sets of algebraic integers whose remaining conjugates lie in the unit circle*, Trans. Amer. Math. Soc. **105** (1962), 391–406.

6. J. W. S. Cassels, *On a problem of Schinzel and Zassenhaus*, Jour. Math. Sci. **1** (1966), 1–8.

7. C. Chamfy, *Fonctions méromorphes dans le cercle-unité et leurs séries de Taylor*, Ann. Inst. Fourier (Grenoble) **8** (1958), 211–251.

8. E. Dobrowolski, *On the maximal modulus of conjugates of an algebraic integer*, Acta Arith. (to appear).

9. J. Dufresnoy and Ch. Pisot, *Étude de certaines fonctions méromorphes bornées sur le cercle unité. Application à un ensemble fermé d'entiers algébriques*, Ann. Sc. Éc. Norm. Sup (3) **72** (1955), 69–92.

10. L. Kronecker, *Zwei sätze über gleichungen mit Ganzzahligen coefficienten*, J. fur Reine und Angew. Math. **53** (1857), 173–175.

11. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) **34** (1933), 461–479.

12. R. Salem, *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan*, Duke Math. Jour. **11** (1944), 103–108.

13. ——, *Power series with integral coefficients*, Duke Math. Jour. **12** (1945), 153–172.

14. A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. Jour. **12** (1965), 81–85.

15. C. L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*, Duke Math. Jour. **11** (1944), 597–602.

16. C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. Lond. Math. Soc. **3** (1971), 169–175.

17. C. L. Stewart, *Algebraic integers whose conjugates lie near the unit circle*, Bull. Soc. Math. France, (to appear).

Department of Mathematics
The University of British Columbia
Vancouver, Canada
V6T 1W5