MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 171
JULY 1985, PAGES 243-249

The Maximal Modulus of an Algebraic Integer

By David W. Boyd*

Abstract. The maximal modulus of an algebraic integer is the absolute value of its largest conjugate. We compute the minimum of the maximal modulus of all algebraic integers of degree d which are not roots of unity, for d at most 12. The computations suggest that the minimum is never attained for a reciprocal algebraic integer. The truth of this conjecture would show that the conjecture of Schinzel and Zassenhaus follows from a theorem of Smyth. We further test our conjecture by computing the minimum of the maximal modulus of all reciprocal algebraic integers of degree d which are not roots of unity, for d at most 16. Our computations strongly suggest that the best constant in the conjecture of Schinzel and Zassenhaus is 1.5 $\log \theta_0$, where θ_0 is the smallest P.V. number. They also shed some light on a recent conjecture of Lind concerning the Perron numbers.

1. Introduction. Let α be an algebraic integer of degree d, with conjugates $\alpha_1, \ldots, \alpha_d$. As usual, let $\overline{|\alpha|} = \max|\alpha_i|$ denote the maximal modulus of α. Clearly, $\overline{|\alpha|} \geqslant 1$, and a theorem of Kronecker [4] tells us that $\overline{|\alpha|} = 1$ if and only if α is a root of unity. Schinzel and Zassenhaus [9] have made the following conjecture:

CONJECTURE (SZ). There is a constant $c_1 > 0$ such that if α is not a root of unity, then $\overline{|\alpha|} \geqslant 1 + c_1/d$.

In this paper we describe the computation of the minimum of $\overline{|\alpha|}$ for α of degree d, with $d \leqslant 12$. The results suggest a conjecture which, when combined with a result of Smyth [10], implies (SZ). Our results also suggest that the best constant c_1 in (SZ) should be $\frac{3}{2} \log \theta_0$, where $\theta_0 = 1.3247\ldots$ is the smallest Pisot number (the real zero of $x^3 - x - 1$).

The results also shed some light on a conjecture of Lind concerning the "Perron numbers" introduced in [6] and [7].

2. Conjectures Implying (SZ). The best results to date concerning (SZ) have been obtained as corollaries to results on a question of Lehmer. Let $M(\alpha) = \prod_{i=1}^{d} \max(|\alpha_i|, 1)$ denote the Mahler measure of α. Lehmer [5] asked:

(L) Does there exist a constant $c_0 > 1$ so that $M(\alpha) \geqslant c_0$ for all α not roots of unity?

A positive answer to (L) would prove (SZ), for, if ν is the number of α_i satisfying $|\alpha_i| > 1$, then clearly $M(\alpha) \leqslant \overline{|\alpha|}^{\nu}$. Thus,

$$\overline{|\alpha|} \geqslant M(\alpha)^{1/\nu} \geqslant M(\alpha)^{1/d} \geqslant c_0^{1/d} \geqslant 1 + c_1/d.$$

Received July 10, 1984.
1980 *Mathematics Subject Classification*. Primary 12-04, 12A15.
Key words and phrases. Algebraic integer, maximal modulus, Schinzel-Zassenhaus conjecture, Perron numbers, Smyth's theorem, Newton's formulas.
*This research ws supported in part by NSERC.

TABLE 1

Extreme values of $\overline{|\alpha|}$ for fixed degree d. The minimum $m(d)$ is attained for α with minimal polynomial $P_d(x)$ having ν roots outside the unit circle.

d	ν	$m(d)$	$P_d(x)$
1	1	2	$x - 2$
2	2	$2^{1/2} = 1.4142135624$	$x^2 - 2, x^2 + x + 2$ or $x^2 + 2x + 2$
3	2	$\theta_0^{1/2} = 1.1509639253$	$x^3 + x - 1$
4	2	1.1837518186	$x^4 + x^3 + 1$ or $x^4 + x + 1$
5	4	1.1216451786	$x^5 - x^3 + x^2 + x - 1$
6	4	$\theta_0^{1/4} = 1.0728298678$	$P_3(x^2)$
7	4	1.0928455996	$x^7 + x^6 + x^3 - x - 1$
n8	6	1.0756204773	$x^8 + x^7 + x^4 - x^2 + 1$
9	6	$\theta_0^{1/6} = 1.0479821944$	$P_3(x^3)$
10	8	1.0590775130	$P_5(x^2)$
11	8	1.0571248570	$x^{11} + x^{10} + x^7 + x^6 - x^4 + x^2 - 1$
12	8	$\theta_0^{1/8} = 1.0357750083$	$P_3(x^4)$

However, it is conceivable that (SZ) could be true, and yet the answer to (L) could be negative.

Smyth [10] proved that if α is nonreciprocal (i.e., α_i^{-1} is not a conjugate of α for any i), then $M(\alpha) \geqslant \theta_0$. Hence, $\overline{|\alpha|} \geqslant 1 + (\log \theta_0)/d$ for nonreciprocal α. Smyth also pointed out that the α with minimal polynomial $x^{3k} + x^{2k} - 1$ (so $d = 3k$), has $\overline{|\alpha|} = \theta_0^{1/(2k)} = \theta_0^{3/(2d)}$, so one cannot improve this beyond $\overline{|\alpha|} \geqslant 1 + \frac{3}{2}(\log \theta_0)/d$.

On the other hand, it is known that, for reciprocal α, one can definitely have $1 < M(\alpha) < \theta_0$. Indeed, Lehmer [5] provided an example α_0 with $d = 10$ for which $M(\alpha_0) = 1.17628\ldots < \theta_0$. It is widely felt that α_0 may be the best constant in (L). There are many other examples in [1]. For reciprocal α, Dobrowolski [3] has shown that

$$M(\alpha) \geqslant 1 + c_2\left(\frac{\log\log d}{\log d}\right)^3,$$

from which a result slightly weaker than (SZ) follows.

It should be pointed out that the known reciprocal α with small measure (as listed in [1], for example) do not have $\overline{|\alpha|}$ particularly small, since ν is too small. For example, Lehmer's 10th degree α_0 has $\nu = 1$ and, hence, $\overline{|\alpha_0|} = M(\alpha_0) = 1.17628\ldots$. Even the naive guess $\alpha = \sqrt[10]{2}$ has $\overline{|\alpha|} = 1.07177\ldots$, while the minimum of $\overline{|\alpha|}$ for degree 10 is $1.05907\ldots$, which is considerably smaller (see Table 1).

Let $m(d)$ denote the minimum of $\overline{|\alpha|}$ over α of degree d which are not roots of unity. It is easy to see that this is an attained minimum. Let an α attaining $m(d)$ be called extremal. Then our computations, as summarized in Tables 1 and 2 suggest the following:

CONJECTURE (A). Extremal α are always nonreciprocal.

CONJECTURE (B). If $d = 3k$, then the extremal α has minimal polynomial $x^{3k} + x^{2k} - 1$ (or $x^{3k} - x^{2k} - 1$).

CONJECTURE (C). The extremal α of degree d have $\nu \sim \frac{2}{3}d$ as $d \to \infty$.

TABLE 2

Extreme values of $\overline{|\alpha|}$ *for reciprocal* α *of even degree* d. *The minimum* $m_R(d)$ *is attained for an* α *with minimal polynomial* $R_d(x)$ *having* ν *roots outside the unit circle.*

d	ν	$m_R(d)$	$R_d(x)$
2	1	2.6180339887	1 -3 1
4	2n	1.5392223384	1 1 3 1 1
6	2	1.3216631562	1 2 2 1 2 2 1
8	2	1.1692830298	1 0 0 1 1 1 0 0 1
10	2	1.1257148215	1 0 1 1 0 1 0 1 1 0 1
12	2	1.1080548536	1 1 1 0 -1 -1 -1 -1 -1 0 1 1 1
14	4	1.0939016857	1 0 0 0 1 1 0 1 0 1 1 0 0 0 1
16	4	1.0813339123	$R_8(x^2)$

Perhaps (C) seems far-fetched on the basis of Table 1. However, the evidence for (B) is clear, and it does appear that $\nu(d)$ is monotone. These would imply (C).

Note that (A) implies (SZ) with $c_1 = \log\theta_0$, while (C) implies that the best constant is $c_1 = \frac{3}{2}\log\theta_0$.

Since the computation for $d = 12$ was rather lengthy, it is not feasible to extend it to $d \geqslant 13$. However, we were able to test (A) up to $d = 16$ by computing $m_R(d)$, the minimum of $\overline{|\alpha|}$ over *reciprocal* α of degree d which are not roots of unity. Since $m_R(2k) > m(k)^{1/2} \geqslant m(2k)$ for $k \leqslant 8$, we thus have verified (A) for $d \leqslant 16$.

3. Perron Numbers. Lind [6] has defined a Perron number to be a real algebraic integer $\alpha = \alpha_1$ such that $\alpha_1 > |\alpha_i|$ for $i \geqslant 2$.

By the Perron-Frobenius theorem, if A is a matrix with nonnegative integer entries and such that A^k has positive entries for some k, then the dominant eigenvalue α of A is a Perron number. Lind has proved the converse [6], [7]. (Note that the dimension of A may have to be larger than $\deg(\alpha)$, e.g., if α has negative trace.)

In private correspondence, Lind conjectured that the smallest Perron number of degree $d \geqslant 2$ should have minimal polynomial $x^d - x - 1$. This turns out to be true if $d = 2, 3, 4, 6, 7, 8, 10, 12$, but false if $d > 3$ and $d \equiv 3$ or $5 \pmod 6$. A slight modification of the conjecture is true up to degree 12.

The reason for the modification is the following: It is known [8] that if $(n, m) = 1$, then $x^n - x^m - 1$ is either irreducible or the product of $x^2 - x + 1$ and an irreducible polynomial. (One can now derive this in a few lines from Smyth's theorem [10] and the fact that $M(x^n - x^m - 1) \leqslant \sqrt{3} < \theta_0^2$.) For $(n, m) = 1$, $x^n - x^m - 1$ can have the factor $x^2 - x + 1$ only if $n \equiv 1$ or $5 \pmod 6$ and $m + n \equiv 3 \pmod 6$. Let us now compare the size of α, the positive root of $x^d - x - 1$, with β, the positive root of $x^{d+2} - x^m - 1$. If $d > 3$ and $m \leqslant 4$, then

$$\alpha^{d+2} - \alpha^m - 1 \geqslant \alpha^{d+2} - \alpha^4 - 1 = \alpha^2(\alpha + 1) - \alpha^4 - 1$$
$$= -(\alpha - 1)(\alpha^3 - \alpha - 1) > 0,$$

since $\alpha^3 - \alpha - 1 < \alpha^d - \alpha - 1 = 0$. Thus $\beta < \alpha$.

On the other hand, if $m \geqslant 5$, then

$$\alpha^{d+2} - \alpha^m - 1 \leqslant \alpha^{d+2} - \alpha^5 - 1 = \alpha^2(\alpha + 1) - \alpha^5 - 1$$
$$= -(\alpha^2 - 1)(\alpha^3 - 1) < 0;$$

so $\beta > \alpha$.

Thus, if $m \leqslant 4$ and $x^{d+2} - x^m - 1$ is divisible by $x^2 - x + 1$, then β is of degree d, and $\lceil\beta\rceil = \beta < \lceil\alpha\rceil = \alpha$. This occurs exactly when $d \equiv 5 \pmod 6$, and $m = 2$ or $d \equiv 3 \pmod 6$, and $m = 4$.

This suggests the following modification of Lind's conjecture. It has been verified for $d \leqslant 12$:

CONJECTURE (D). The smallest Perron number of degree $d \geqslant 2$ has minimal polynomial

$$\begin{array}{ll} x^d - x - 1 & \text{if } d \not\equiv 3, 5 \pmod 6, \\ (x^{d+2} - x^4 - 1)/(x^2 - x + 1) & \text{if } d \equiv 3 \pmod 6, \\ (x^{d+2} - x^2 - 1)/(x^2 - x + 1) & \text{if } d \equiv 5 \pmod 6. \end{array}$$

($N.B.\ x^5 - x^4 - 1 = (x^2 - x + 1)(x^3 - x - 1)$.)

4. The Computations. The method is based on similar principles to those used in [1], but is somewhat simpler. Given a bound $B > 1$, we wish to generate the set R of polynomials of degree d all of whose zeros are at most B in modulus. From this finite set we will eliminate the cyclotomic polynomials and the reducible polynomials. If B has been chosen sufficiently large, the remaining set will be nonempty and will contain the minimal polynomials of the extremal α for $\lceil\alpha\rceil$ and the smallest Perron number of degree d. For $d \geqslant 3$, the choice $B = (2 + 1/d)^{1/d}$ suffices, since $B^d - B - 1 > 0$ and $B^d - 2 > 0$. In practice we chose B to be a "round" number approximately equal to this value.

Let $P(x) = x^d + a_1x^{d-1} + \cdots + a_d$ have zeros $\alpha_1, \ldots, \alpha_d$, and let $S_k = \sum_{i=1}^d \alpha_i^k$ for $k = 1, 2, \ldots$. If all $|\alpha_i| \leqslant B$, then, clearly,

$$|S_k| \leqslant dB^k, \qquad k = 1, 2, \ldots. \tag{1}$$

In addition, we have [1, Lemma 1]

$$-dB^{k/2} + (2/d)S_{k/2} \leqslant S_k, \qquad k = 2, 4, \ldots. \tag{2}$$

By Newton's identities, the S_k and a_k are related by

$$S_k + a_1S_{k-1} + \cdots + a_{k-1}S_1 + ka_k = 0, \qquad k \geqslant d, \tag{3}$$

$$S_k + a_1S_{k-1} + \cdots + a_dS_{k-d} = 0, \qquad k > d. \tag{4}$$

According to (3), $(S_1, \ldots, S_k)$ is uniquely determined from $(a_1, \ldots, a_k)$ and vice versa for $k \leqslant d$. If the a_i are integers, then $a_1, \ldots, a_{k-1}$ determine $S_k \pmod k$. Hence, the number of P satisfying (1) for $k \leqslant d$ is approximately

$$N_d = \prod_{k=1}^{d} \frac{2dB^k}{k} \sim (2eB^{d/2})^d \sim (2e\sqrt{2})^d$$

if $B \sim 2^{1/d}$.

If we apply (2) for $k \leqslant d$, then we reduce this by a factor of approximately $(2/3)^{d/2}$. To see this, note that, e.g., the number of pairs (S_1, S_2) which satisfy (1) and (2) is approximately

$$\int_{-dB}^{dB} \left(2dB^2 - \left(\frac{2}{d}\right)x^2\right) dx = \frac{2}{3}(2dB)(2dB^2).$$

The factor $(2/3)^{n-1}$ is not quite correct for n-tuples $(S_1, S_2, S_4, \ldots, S_m)$ with $m = 2^{n-1}$. For triples (S_1, S_2, S_4), the correct factor, for example, should be

$(2/3) \cdot (24/35)$, since

$$\int_{-dB}^{dB} dx \int_{-dB^2+(2/d)x^2}^{dB^2} \left(2dB^4 - \left(\frac{2}{d}\right)y^2\right) dy = \frac{2}{3} \cdot \frac{24}{35}(2dB)(2dB^2)(2dB^4).$$

However, the approximation is good enough for these purposes.

Thus, we are ultimately faced with investigating about $(4e/\sqrt{3})^d \sim (6.28)^d$ polynomials, so it is apparent that only relatively small d will be feasible.

Of course, one can use some symmetry and insist that $S_1 \geqslant 0$. For $d = 12$ and $B = 1.063$, the size of the set is thus predicted to be about

$$\frac{1}{2}\left(\frac{2}{3}\right)^6 N_{12} \approx 3.93 \times 10^8.$$

The exact size of the set was in fact 451 682 220.

If we use no other information than (1) and (2) for $k \leqslant d$, then it is clear that all polynomials which appear in this set must be investigated further. Thus the size of this set does play a critical role in determining the running time of the algorithm. However, it is clear that one should not simply solve all such P to determine whether P is in R. The inequalities (1) for $k > d$ provide further tests which should provide the same sort of information more inexpensively.

Let us denote by R_d the set of P satisfying $S_1 \geqslant 0$ and (1) and (2) for $k \leqslant d$. For $n > d$, let R_n denote the set of P in R_d satisfying $a_d \neq 0$ and (1) for $k \leqslant n$. Clearly, the R_n are nested, and their intersection is R, since

$$\limsup\,(\log|S_k|/k) = \log \overline{|\alpha|}.$$

Thus for sufficiently large N, the set R_N is not much larger than R, and we can afford simply to solve all P in R_N. The optimal choice of N depends on the rate of decay $|R_n|$ and on the time t_1 for applying the test (1) for a given $k = n$ relative to the time t_2 for solving P. Clearly, $t_1 \ll t_2$. Of course, since we naturally generate the P's one at a time without storing them, we do not know the values of $|R_n|$ until after the computation is complete. Thus, optimizing the choice of N is not feasible, but $N = 3d$ worked well in practice.

As a sample of the numbers involved, for $d = 12$, $B = 1.063$ we have

$$\begin{array}{lll} |R_{12}| = 451{,}682{,}220, & |R_{23}| = 37{,}019, & |R_{35}| = 4931, \\ |R_{13}| = 23{,}746{,}503, & |R_{24}| = 28{,}277, & |R_{36}| = 4435. \\ |R_{14}| = 4{,}987{,}914, & & \end{array}$$

In fact, $|R| = 867$, of which 811 are cyclotomic, 26 are reducible, and 30 are irreducible.

The algorithm then is simply to generate each P in R_d and apply the sequence of tests (1) sequentially for $k = d + 1, \ldots, N$. The surviving P are in R_N. We then test for small cyclotomic factors (of order 7 or less) and then solve P using the QR-algorithm. Using the ideas in [2], one can get a priori lower bounds on $\overline{|\alpha|}$ for noncyclotomic P, so we can reject any P which have $\overline{|\alpha|} \leqslant 1.0005$ or $\overline{|\alpha|} > B$. The remaining P are generally irreducible, but reducibility is easily checked, since we apply the algorithm in order of increasing d, so we have a list of possible factors.

To save time in generating R_d, the bounds in (1) and (2) are precomputed so that, for example, the test (2) simply requires testing $S_k \geqslant C(k/2, S_{k/2})$, where $C(i, j)$ is a precomputed array. Thus, only integer arithmetic is required when applying (1) and (2).

For reciprocal P of even degree, since $a_{d-k} = a_k$, P is determined completely by $S_1, \ldots, S_{d/2}$. Writing $m = d/2$, we see that the initial set R_m contains approximately

$$\frac{1}{2}\frac{(4m)^m B^{m^2/2}}{m!}\left(\frac{2}{3}\right)^{m/2}$$

polynomials. For $d = 16$ and $B = 1.09$, this is about 4.25×10^7. The actual number generated was 46,345,943.

The same choice $N = 3d$ was made and the same procedure followed in processing the set R_N. In this case, a number of reducible polynomials of the form QQ^* appeared, where $Q^*(x) = \pm x^{d/2}Q(x^{-1})$. These correspond to α of degree $d/2$ with $\overline{|\alpha^{-1}|} \leqslant \overline{|\alpha|}$.

The running time was essentially proportional to the size of the initial set of polynomials. For example, the case $d = 12$, $B = 1.063$ required 4.69 hours of CPU time on an Amdahl 470 V7A.

5. The Tables. Tables 3 and 4 appear as an appendix in the supplements section of this issue. If $P_1(x) = Q(x^s)$ and $P_2(x) = \pm Q(-x^s)$ for some $s \geqslant 1$, then we say P_1 and P_2 are equivalent. Since $\overline{|\alpha|}$ is the same for P_1 and P_2, only one of such a pair is listed in the tables. Generally, it is the one in which the first nonvanishing a_i is positive, except when an α_i attaining $\overline{|\alpha|}$ is real, in which case we choose the sign so $\alpha_i > 0$.

All the tables exhibit $\alpha_i = \overline{|\alpha|}e^{i\phi}$, where ϕ is given in degrees and chosen minimally so that $0 \leqslant \phi < 180$. The minimal polynomial of α is exhibited as a vector $a_1 \cdots a_d$ except in Table 1.

Table 1 gives a list of extrema for $\overline{|\alpha|}$ for degrees $1 \leqslant d \leqslant 12$. Table 2 gives the corresponding list for reciprocal polynomials of even degrees $2 \leqslant d \leqslant 16$.

Table 3 gives a complete list of inequivalent α of degree d with $\overline{|\alpha|}$ smaller than the given bound B. Perron numbers are indicated by a "P" in the column preceding ν. Table 4 gives the corresponding lists for reciprocal polynomials. (Perron numbers are not marked.)

Department of Mathematics
University of British Columbia
Vancouver, B.C., Canada V6T 1Y4

1. D. W. BOYD, "Reciprocal polynomials having small measure," *Math. Comp.*, v. 35, 1980, pp. 1361–1377.

2. E. DOBROWOLSKI, "On the maximal modulus of conjugates of an algebraic integer," *Bull. Acad. Polon. Sci.*, v. 26, 1978, pp. 291–292.

3. E. DOBROWOLSKI, "On a question of Lehmer and the number of irreducible factors of a polynomial," *Acta Arith.*, v. 34, 1979, pp. 391–401.

4. L. KRONECKER, "Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten," *J. Reine Angew. Math.*, v. 53, 1857, pp. 173–175.

D. H. LEHMER, "Factorization of certain cyclotomic functions," *Ann. of Math.* (2), v. 34, 1933, pp. 461–479.

6. D. LIND, "Entropies and factorizations of topological Markov shifts," *Bull. Amer. Math. Soc. (N.S.)*, v. 9, 1983, pp. 219–222.

7. D. LIND, "The entropies of topological Markov shifts and a related class of algebraic integers," *Ergodic Theory Dynamical Systems*, v. 4, 1984, pp. 283–300.

8. W. LJUNDGGREN, "On the irreducibility of certain trinomials and quadrinomials," *Math. Scand.*, v. 8, 1960, pp. 65–70.

9. A. SCHINZEL & H. ZASSENHAUS, "A refinement of two theorems of Kronecker," *Michigan Math. J.*, v. 12, 1965, pp. 81–84.

10. C. J. SMYTH, "On the product of the conjugates outside the unit circle of an algebraic integer," *Bull London Math. Soc.*, v. 3, 1971, pp. 169–175.