ACTA ARITHMETICA
LXVIII.1 (1994)

# Irreducible polynomials with many roots of maximal modulus

by

David W. Boyd (Vancouver, B.C.)

**Introduction.** There are a number of interesting results connecting the geometry of the roots of a polynomial with integer coefficients with algebraic properties of the roots. The best known is Kronecker's famous result which states that if a polynomial with integer coefficients has all its zeros on the unit circle then these must all be roots of unity [1].

One cannot extend this too far, as the existence of Salem numbers shows: a *Salem polynomial* $f(x)$ is a monic irreducible polynomial with integer coefficients which has one positive root outside the unit circle, one inside the circle and the remainder on the circle. The roots on the unit circle are obviously not roots of unity since $f$ is irreducible. In fact, there are no nontrivial multiplicative relations between these roots, as shown by Pisot (see [3, p. 32]).

Another related result, due to Smyth [4], is that if $f(x)$ is a Pisot polynomial then it has no two conjugates of equal modulus, except for pairs of complex conjugate roots. A *Pisot polynomial* is a monic polynomial with integer coefficients with a single positive root outside the unit circle and the rest inside. A generalization of this due to Mignotte [2] is that there is no nontrivial multiplicative relation between the zeros of a Pisot polynomial.

An obvious way to construct polynomials with roots of equal modulus is to take $f(x)$ to be of the form $g(x^m)$, so the roots of $f$ are all of the $m$th roots of the roots of $g$. Of course, even if $g$ is irreducible, $f$ may or may not be irreducible.

Michael Hollander asked the author for an example of an irreducible $f(x)$ with a positive root $\alpha_1$ of largest modulus and $m-1$ other roots of modulus $\alpha_1$ but which is not of this form. The purpose of this note is to show that such examples do not exist.

This research was supported in part by NSERC.

THEOREM. *Let $f(x)$ be an irreducible polynomial of degree $n$ with integer coefficients. Let $\alpha_j$, $j = 1, \ldots, n$, be the roots of $f$ listed in order of decreasing modulus. Assume that $\alpha_1 > 0$ and that $|\alpha_j| = \alpha_1$, for $j = 1, \ldots, m$, for some $m \le n$ and that $|\alpha_j| < \alpha_1$ if $j > m$. Then $m$ divides $n$ and there is an irreducible polynomial $g$ of degree $n/m$ with integer coefficients such that $f(x) = g(x^m)$.*

Proof. We will use induction on $m$. Clearly the result is true if $m = 1$.

If $m$ is even then $-\alpha_1$ must be a root of $f(x)$ and hence, being irreducible, $f$ must be even and hence of the form $h(x^2)$. Clearly $h$ has $m/2$ roots of equal modulus, one being $\alpha_1^2 > 0$ and hence by induction $h(x) = g(x^{m/2})$ so $f(x) = g(x^m)$.

To illustrate the main ideas, we next treat the case $m = 3$. Now $\alpha_2$ and $\alpha_3$ are complex conjugates and hence we have

$$\alpha_1^2 = \alpha_2\alpha_3. \tag{1}$$

Since $f$ is irreducible its Galois group $G$ is transitive so there is an automorphism $\sigma \in G$ taking $\alpha_1$ to $\alpha_2$. Applying this to (1) gives an equation of the form $\alpha_2^2 = \alpha_i\alpha_j$ where $\alpha_i$ and $\alpha_j$ are roots of $f(x)$. Since $\alpha_2$ is of maximal modulus, neither $\alpha_i$ nor $\alpha_j$ can have smaller modulus so they must in fact be $\alpha_1$ and $\alpha_3$, i.e.

$$\alpha_2^2 = \alpha_1\alpha_3. \tag{2}$$

Combining (1) and (2), we find that $\alpha_2^3 = \alpha_1^3$ and by complex conjugation that $\alpha_3^3 = \alpha_1^3$ so that $\alpha_1$, $\alpha_2$ and $\alpha_3$ are the three cube roots of $\alpha_1^3$ and hence $f(x) = g(x^3)$ where $g$ is the minimal polynomial of $\alpha_1^3$. (For more details, see the argument below.)

Now we treat the general case of $m$ odd. Number the roots so that $\alpha_{2i}$ and $\alpha_{2i+1}$ are complex conjugates. As in (1) we have

$$\alpha_1^2 = \alpha_2\alpha_3 = \ldots = \alpha_{m-1}\alpha_m. \tag{3}$$

Given $i = 2, \ldots, m$, there is a Galois automorphism taking $\alpha_1$ to $\alpha_i$, and from (3) we obtain $[m/2]$ equations of the form

$$\alpha_i^2 = \alpha_j\alpha_k, \tag{4}$$

where $j, k \le m$ by the observation made in the case $m = 3$. The subscripts appearing in these equations are a permutation of $\{1, \ldots, m\}$ so each $j \ne i$ with $j \le m$ appears in the right member of exactly one of these equations. So, for each $1 \le i, j \le m$, there is a $k$ with $1 \le k \le m$ such that $\alpha_i^2\alpha_j^{-1} = \alpha_k$. In other words, the set $S = \{\alpha_1, \ldots, \alpha_m\}$ is closed under the operation

$$(a, b) \to a^2b^{-1}. \tag{5}$$

Define $\omega_i = \alpha_i/\alpha_1$ for $i = 1, \ldots, m$, so $|\omega_i| = 1$, and let $W = \{1, \omega_2, \ldots$ $\ldots, \omega_m\}$. Then $W$ is also closed under the operation (5). Clearly $W$ is also closed under $a \to a^{-1}$. We will show that $W$ is the set of $m$th roots of 1.

Let $\omega \in W$, $\omega \neq 1$. Then one may build up all powers of $\omega$ by repeated squaring and multiplication by $\omega$ (as is familiar to computational number theorists). That is, if we know that $\omega^k \in W$ then taking $a = \omega^k$ and $b = 1$ or $b = \omega^{-1}$ in (5), we see that $\omega^{2k}$ and $\omega^{2k+1}$ are in $W$. Hence all powers of $\omega$ lie in $W$. Since $W$ is finite, two of these powers must be equal so $\omega$ must be a root of unity, say of order $s$. Thus $\alpha_1\omega^k$ are roots of $f(x)$ for $k = 0, \ldots, s-1$ and hence $f(x) = h(x^s)$ for some polynomial $h$ with integer coefficients. Explicitly, $(f(x) + f(\omega x) + \ldots + f(\omega^{s-1}x))/s$ is a polynomial with zeros $\alpha_1\omega^k$ for $k = 0, \ldots, s-1$ which is of the form $h(x^s)$ by the familiar orthogonality relations involving roots of unity. Here $h$ is of degree $n/s$ and has $m/s$ roots of largest modulus. If $s = m$, we are finished. Otherwise apply induction as in the case of even $m$.

R e m a r k s. 1. The proof goes through without change if "maximal modulus" is replaced by "minimal modulus". Or one may simply apply the theorem to the reciprocal polynomial of $f(x)$.

2. If all conditions of the theorem hold except that $\alpha_1 > 0$ is replaced by $\alpha_1 < 0$ then one obtains $f(x) = g(-x^m)$.

3. The assumption that there be a real root of maximal modulus is necessary. This is clear if $m = 2$ since a pair of complex conjugate roots will rarely have their ratio a root of unity. It is also easy to construct examples with larger $m$. For example, let $f(x) = x^6 + x^5 + x^4 + 2x^3 + x^2 + 1$ the roots of which are the products of the roots of $x^3 + x^2 - 1$ and the primitive 6th roots of unity. This has $m = 4$. The ratios of certain, but not all, pairs of roots of maximal modulus are roots of unity.

4. The referee has observed that the final induction step in the proof can be avoided by observing that $-1 \notin W$ so $s$ is odd and hence we can write $\omega\zeta^{-1} = (\omega^{(s+1)/2})^2\zeta^{-1}$. Thus $W$ is closed under $(\omega, \zeta) \to \omega\zeta^{-1}$. Hence $W$ is a finite subgroup of the unit circle and thus is the set of $m$th roots of unity.

## References

[1] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[2] M. Mignotte, *Sur les conjugées des nombres de Pisot*, C. R. Acad. Sci. Paris Sér. I Math. 298 (1984), 21.

[3] R. Salem, *Algebraic Numbers and Fourier Analysis*, D. C. Heath and Co., Boston, 1963.

[4] C. Smyth, *The conjugates of algebraic integers*, Advanced Problem 5931, Amer. Math. Monthly 82 (1975), 86.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, CANADA V6T 1Z2

*Received on 10.2.1994* (2562)