ACTA ARITHMETICA
LXXVIII.3 (1997)

Irreducible polynomials with many roots of equal modulus

by

RONALD FERGUSON (Vancouver, B.C.)

Introduction. Let $f(x) \in \mathbb{Z}[x]$ be irreducible. Suppose that $f(x)$ has m roots on the circle $|z| = c$, at least one of which is real. We will show that $f(x)$ is of the form $g(x^m)$, where $g(x) \in \mathbb{Z}[x]$ and $g(x)$ has no more than one real root on any circle with centre at the origin in $\mathbb{C}$.

David Boyd [1] proves this result in case the circle $|z| = c$ contains roots of maximum or minimum modulus. In a seminar given at the University of British Columbia, he presented this theorem. In a discussion with the author afterwards, he suggested that the result should hold where the circle is of intermediate modulus. The purpose of this note is to give a proof of this extension.

THEOREM. *Suppose that the irreducible polynomial $f(x) \in \mathbb{Z}[x]$ has m roots, at least one real, on the circle $|z| = c$. Then $f(x) = g(x^m)$ where $g(x)$ has no more than one real root on any circle in $\mathbb{C}$.*

Proof. Let $\mathcal{K}$ be the splitting field of f. As in [1] we use induction on m. If $m = 1$ the result is clear.

If m is even, then both c and $-c$ are roots of $f(x)$. Since f is irreducible, it must be even, that is, $f(x)$ is of the form $h(x^2)$. h now has $m/2$ roots of equal modulus, one being real. By induction $h(x) = g(x^{m/2})$ and $f(x) = g(x^m)$.

We now move to the case where m is odd. The following lemma gives an important bridge:

LEMMA. *If $\alpha_1, \alpha_2, \alpha_3$ are roots of the irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and $\alpha_1^2 = \alpha_2\alpha_3$, then α_1/α_2 is a root of unity.*

Proof. Let $\gamma_1, \ldots, \gamma_n$ be the set of roots of f of largest modulus. For $1 \le i \le n$ there is some automorphism σ_i of $\mathcal{K}$ such that $\sigma_i(\alpha_1) = \gamma_i$. Since then

$$\gamma_i^2 = \sigma_i(\alpha_2)\sigma_i(\alpha_3),$$

$\sigma_i(\alpha_1)$ and $\sigma_i(\alpha_2)$ must be of maximum modulus as well. This can be translated into a linear equation in the arguments of the γ_i's, represented in the following matrix form:

$$\begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} & \cdots & 0 \\ * & 1 & * & & * \\ * & * & 1 & & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & & 1 \end{pmatrix} \begin{pmatrix} \arg(\gamma_1) \\ \arg(\gamma_2) \\ \vdots \\ \arg(\gamma_n) \end{pmatrix} = \begin{pmatrix} 0 \text{ or } \pm\pi \\ 0 \text{ or } \pm\pi \\ \vdots \\ 0 \text{ or } \pm\pi \end{pmatrix},$$

where the ordering is chosen so that the matrix on the left has entries of 1's along the diagonal. Each row has two other entries of $-\frac{1}{2}$ with all the other entries being 0. Not all rows are linearly independent since the row sums are 0.

Suppose that the first k (but not the first $k+1$) rows of this matrix are linearly independent. We use row reduction as described below on the first k rows in the above equation to obtain the identity matrix in the first $k \times k$ block. After each stage in the reduction each row will have one positive entry of 1 in the diagonal position with all other entries ≤ 0 and summing to -1. If, in the reduction, any row is left with only two non-zero entries 1 and -1, then, as described in (3) below, we have proved the result.

Assume then that we have reduced to a stage where we have the matrix $M = (m_{ij})$ on the left and we wish to reduce an entry m_{ij} with $-1 \leq m_{ij} < 0$. We multiply the jth row by $-m_{ij}$ and add this to this ith row. We thus reduce the entry in the ijth position to zero, but add non-positive values to each other entry in the row. The diagonal entry in the ith row now becomes $1 - m_{ij}m_{ji}$. The only way this can be zero is for $m_{ij} = m_{ji} = -1$, in which case the ith row is the negative of the jth row, contradicting linear independence. Thus $1 - m_{ij}m_{ji} > 0$ and we can divide the ith row by this value. The diagonal value on this row is now 1 again, all other entries are between -1 and 0 and the row sum is still zero. If we have not achieved the result at some stage along the way, we eventually produce a matrix $A = (a_{ij})$ of the following form:

$$\begin{array}{r} \\ \\ \\ \\ k\text{th row} \\ \\ \\ \end{array} \left(\begin{array}{cccccccc|c} 1 & 0 & 0 & & 0 & * & \cdots & & r_1\pi \\ 0 & 1 & 0 & & 0 & * & \cdots & & \vdots \\ 0 & 0 & 1 & & 0 & * & \cdots & & \\ & & & \ddots & & & & & \\ 0 & 0 & 0 & & 1 & * & \cdots & & r_k\pi \\ * & * & * & & * & 1 & \cdots & & 0 \text{ or } \pm\pi \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & & \vdots \end{array}\right)$$

with the r_i's being rational. The $(k+1)$th row remains unchanged, i.e. it has only 3 non-zero entries of $1, -\frac{1}{2}, -\frac{1}{2}$.

Consider the following cases:

(1) *All the entries before the diagonal in the* $(k+1)$*th row are* 0. Then the first $k+1$ rows are linearly independent, contradicting our original choice.

(2) *For one column i with $i \le k$, $a_{k+1,i} = -\frac{1}{2}$.* But then this row must be a multiple, by $-\frac{1}{2}$, of the ith row. However, this is impossible since

$$a_{k+1,k+1} = 1 \neq -\tfrac{1}{2} a_{i,k+1}$$

since $-1 < a_{i,k+1} \le 0$.

(3) *Two entries $a_{k+1,i}$ and $a_{k+1,j}$ before the diagonal in the* $(k+1)$*th row have the value* $-\frac{1}{2}$. Since then

$$a_{k+1,k+1} = 1 = -\tfrac{1}{2}(a_{i,k+1} + a_{j,k+1}),$$

we must have $a_{i,k+1} = a_{j,k+1} = -1$. But then the ith (or jth for that matter) row has only two non-zero entries of 1 and -1.

From our choice of the σ_i's, $\sigma_{k+1}(\alpha_1) = \gamma_{k+1}$, and $\sigma_{k+1}(\alpha_2) = \gamma_i$ or γ_j, say γ_i. Then from the above

$$\arg(\gamma_{k+1}) - \arg(\gamma_i) = r\pi$$

for some $r \in \mathbb{Q}$. Thus $\omega = \gamma_{k+1}/\gamma_i$ is a root of unity and $\omega \in \mathcal{K}$. Now

$$\alpha_1 = \sigma_{k+1}^{-1}(\omega\gamma_i) = \sigma_{k+1}^{-1}(\omega)\alpha_2.$$

Since $\sigma_{k+1}^{-1}(\omega)$ is a root of unity, the result follows. ∎

Continuation of proof of Theorem. Let $C = \{\alpha_1, \ldots, \alpha_m\}$ be the roots of $f(x)$ on $|z| = c$ with α_1 real and $\alpha_{2i+1} = \overline{\alpha}_{2i}$, $1 \le i \le (m-1)/2$. Hence we have

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

and consequently

$$\alpha_1^m = \alpha_1 \cdot (\alpha_1^2)^{(m-1)/2} = \alpha_1\alpha_2 \ldots \alpha_{m-1}\alpha_m.$$

By the Lemma α_j/α_1 is a root of unity for $1 \le j \le m$. Hence every automorphism τ_i satisfying $\tau_i(\alpha_1) = \alpha_i$ permutes the elements of C.

Thus we get

$$\alpha_i^m = \tau_i(\alpha_i^m) = \tau_i(\alpha_1) \ldots \tau_i(\alpha_m) = \alpha_1 \ldots \alpha_m = \alpha_1^m,$$

i.e. α_i/α_1 is a root of unity, and, for $i = 1, \ldots, m$, we get all mth roots of unity.

Consequently, $f(\zeta_m^i \alpha_1) = 0$ for $i = 1, \ldots, m$. Thus, we have

$$\frac{1}{m}(f(x) + f(\zeta_m x) + \ldots + f(\zeta_m^{m-1})) = g(x^m),$$

for some $g \in \mathbb{Q}[x]$, by the orthogonality relations for the mth roots of unity. Evidently, $\deg(g(x^m)) \le \deg(f(x))$.

Hence $g(x^m) = f(x)$, since both polynomials are monic, have a common zero, α_1, and f is irreducible. ■

Notes. 1. The Lemma would hold as well when relations of the form

$$\alpha_1^n = \alpha_2^{n_2}\alpha_3^{n_3}\ldots\alpha_k^{n_k}$$

hold between conjugate roots where the n_i's are positive integers and $\sum_{i=1}^{k} n_i = n$. However, there are limits on what relation will work. Results stated in Smyth [3] illustrate cases where relations of the form

$$\alpha_1^{n_1}\alpha_2^{n_2}\ldots\alpha_k^{n_k} = 1$$

hold between conjugates where the n_i's are integers but no quotient of two roots is a root of unity. In Lemma 1 of [2], Smyth gives a different proof of the lemma in this paper using Dirichlet's Theorem.

2. Having two roots differing by a root of unity is not sufficient to effect the reduction. Consider the polynomial $x^4 - 2x^3 + 4x^2 - 3x + 1$ which has roots $\frac{1}{2}(1+\sqrt{5})\zeta_5$, $\frac{1}{2}(1-\sqrt{5})\zeta_5^2$, $\frac{1}{2}(1-\sqrt{5})\zeta_5^3$, $\frac{1}{2}(1+\sqrt{5})\zeta_5^4$, where $\zeta_5 = \exp(2\pi i/5)$.

3. There are other cases where the relation $\alpha_1^2 = \alpha_2\alpha_3$ holds between conjugate roots where the polynomial has no real roots, but the reduction occurs. Take for example $x^6 + x^3 + 1$, which gives the primitive ninth roots of unity. We have $\zeta_9^2 = \zeta_9^4\zeta_9^7$.

However, in the case of the primitive fifteenth roots of unity the polynomial is $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ and there is the relation $\zeta_{15}^2 = \zeta_{15}^4\zeta_{15}^{13}$.

There is even no need for a circle to contain what might be thought of as a "set" of roots which occupy positions corresponding to some set of primitive roots. Consider the twelfth degree polynomial $x^{12} - 6x^{11} + 23x^{10} - 73x^9 + 191x^8 - 405x^7 + 766x^6 - 1164x^5 + 1368x^4 - 1539x^3 + 1863x^2 - 1701x + 729$, having as roots the conjugates of $\frac{1}{2}(1+\sqrt{13})\zeta_{13}$. Six of the roots are on the circle $|z| = \frac{1}{2}(1+\sqrt{13})$ and six on $|z| = \frac{1}{2}(\sqrt{13}-1)$. For $\alpha_1 = \frac{1}{2}(1+\sqrt{13})\zeta_{13}$, $\alpha_2 = \frac{1}{2}(1+\sqrt{13})\zeta_{13}^3$, $\alpha_3 = \frac{1}{2}(1+\sqrt{13})\zeta_{13}^{12}$, we have $\alpha_1^2 = \alpha_2\alpha_3$.

I would like to acknowledge the referee for the simplification which is incorporated into the final steps in the proof of the Theorem.

References

[1] D. W. Boyd, *Irreducible polynomials with many roots of maximal modulus*, Acta Arith. 68 (1994), 85–88.

[2] C. J. Smyth, *Conjugate algebraic numbers on conics*, ibid. 40 (1982), 333–346.

[3] C. J. Smyth, *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Theory 23 (1986), 243–254.

Department of Mathematics
University of British Columbia
Vancouver, Canada V6T 1Z2
E-mail: ferguson@math.ubc.ca

Received on 16.8.1995
and in revised form on 26.1.1996 (2844)