MATH. SCAND. 21 (1967), 177–189

ON THE IRREDUCIBILITY OF THE TRINOMIALS $x^m \pm x^n \pm 4$.

ARNE T. JONASSEN

1.

The object of this paper is to prove the following

THEOREM. *Let m and n denote any natural numbers, $m > n$, and let $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. The polynomials*

$$f(x) = x^m + \varepsilon_1 x^n + 4\varepsilon_2 \tag{1}$$

are then irreducible over the field of rationals with the exception of

(i) $x^{3t} + \varepsilon_1 x^{2t} + 4\varepsilon_1 = (x^t + 2\varepsilon_1)(x^{2t} - \varepsilon_1 x^t + 2)$
(ii) $x^{5t} + \varepsilon_1 x^{2t} - 4\varepsilon_1 = (x^{3t} + \varepsilon_1 x^{2t} - x^t - 2\varepsilon_1)(x^{2t} - \varepsilon_1 x^t + 2)$
(iii) $x^{11t} + \varepsilon_1 x^{4t} + 4\varepsilon_1 = (x^{5t} - x^{3t} - \varepsilon_1 x^{2t} + 2\varepsilon_1)(x^{6t} + x^{4t} + \varepsilon_1 x^{3t} + x^{2t} + 2)$,

where $t = (m,n)$ and the factors in these decompositions are irreducible.

Assuming reducibility of $f(x)$, let

$$f(x) = \varphi_r(x)\, \psi_s(x), \qquad r + s = m \,, \tag{2}$$

where $\varphi_r(x)$ and $\psi_s(x)$ are monic polynomials with integral coefficients of positive degrees r and s, respectively. Both $\varphi_r(x)$ and $\psi_s(x)$ have a constant term of modulus 2. For suppose the converse. Then one of them, say $\varphi_r(x)$, has a constant term of modulus 1. This implies that one of the zeros of $f(x)$ has modulus not greater than 1, hence the inequality $|-4\varepsilon_2| \leqq 1 + 1 = 2$ which is impossible.

Both $\varphi_r(x)$ and $\psi_s(x)$ are irreducible over the field of rationals. Assume this to be false. The reducibility of one of these polynomials shows that there must exist a zero of $f(x)$ with modulus not greater than 1, a contradiction.

The method of proof is a refinement of that used by W. Ljunggren in [1]. The proof depend on 10 lemmas, which will be proved in sections 2–9.

Received August 1, 1967.

2.

Putting

$$f_1(x) = x^r \varphi_r(x^{-1}) \psi_s(x) = \sum_{j=0}^{m} c_j x^{m-j}, \tag{3}$$

and

$$f_2(x) = x^s \psi_s(x^{-1}) \varphi_r(x) = \sum_{j=0}^{m} c_{m-j} x^{m-j} \tag{4}$$

we get

$$f_1(x) f_2(x) = x^m f(x) f(x^{-1}). \tag{5}$$

Writing

$$S_{m-k} = \sum_{j=0}^{k} c_j c_{j+m-k}, \qquad 0 \leqq k \leqq m, \tag{6}$$

we obtain, after neglecting the terms in (5) having exponents less than m, and then canceling by x^m

$$\sum_{j=0}^{m} S_{m-j} x^{m-j} = 4\varepsilon_2 x^m + \varepsilon_1 x^{m-n} + 4\varepsilon_1\varepsilon_2 x^n + 18. \tag{7}$$

Since $\varphi_r(x)$ and $\psi_s(x)$ have constant terms with modulus 2, and

$$S_0 = \sum_{j=0}^{m} c_j^2 = 18, \qquad S_m = C_0 C_m = 4\varepsilon_2,$$

we get

$$c_0 = 2\delta_0, \quad c_m = 2\delta_0\varepsilon_2 \quad \text{and} \quad \sum_{j=1}^{m-1} c_j^2 = 10, \quad \delta_0 = \pm 1, \tag{8}$$

giving the following lemma:

LEMMA 1. *There are the following four possibilities for the set* $\mathcal{M} = \{c_i\}$, $i = 1, 2, \ldots, m-1$:

1° *One element of* $\mathcal{M}$ *has modulus* 3 *and one has modulus* 1.
2° *Two elements of* $\mathcal{M}$ *have modulus* 2 *and two have modulus* 1.
3° *One element of* $\mathcal{M}$ *has modulus* 2 *and six have modulus* 1.
4° *Ten elements of* $\mathcal{M}$ *have modulus* 1.

In all of the four cases the remaining elements of $\mathcal{M}$ *are equal to zero.*

From (7) it is seen that

$$\begin{aligned} S_i &= 0 \quad \text{if} \quad 0 < i < m,\ i \neq n-m,\ i \neq n \\ S_{m-n} &= \varepsilon_1 \text{ and } S_n = 4\varepsilon_1\varepsilon_2 \quad \text{if} \quad n \neq \tfrac{1}{2}m \\ S_n &= 4\varepsilon_1\varepsilon_2 + \varepsilon_1 \quad \text{if} \quad n = \tfrac{1}{2}m. \end{aligned} \tag{9}$$

In what follows δ_x, x being some index, always is a member of the set $\{\pm 1\}$. We also define

$$c_j = 0 \quad \text{if} \quad j > m \text{ or } j < 0 .$$

3.

In this section we prove three lemmas.

LEMMA 2.

$$c_i \equiv c_{m-i} \equiv 0 \pmod 2, \qquad 0 < i < \tfrac{1}{2}n ,$$
$$n \equiv 0 \pmod 2, \qquad c_{\frac{1}{2}n} \equiv c_{m-\frac{1}{2}n} \equiv 1 \pmod 2 .$$

PROOF. Suppose c_i even for $0 \leqq i < h < \frac{1}{2}n, c_h$ odd and c_{m-j} even for $0 \leqq j < k < \frac{1}{2}n, c_{m-k}$ odd. If $k < h$ we get $S_{m-k} \equiv 2$, (mod 4), and if $k > h$ we find $S_{m-h} \equiv 2$, (mod 4), which is impossible on account of (9). If $k = h$ we get

$$S_{m-2k} \equiv c_k c_{m-k} \equiv 1 \pmod 2 ,$$

contradicting (9) since $k < \frac{1}{2}n$. Hence

$$c_i \equiv c_{m-i} \equiv 0 \pmod 2, \qquad 0 \leqq i < \tfrac{1}{2}n .$$

If $(n, 2) = 1$

$$S_{m-n} \equiv c_{\frac{1}{2}(n-1)} c_{m-\frac{1}{2}(n+1)} + c_{\frac{1}{2}(n+1)} c_{m-\frac{1}{2}(n-1)} \equiv 0 \pmod 2 ,$$

which also contradicts (9). Hence n even and

$$S_{m-n} \equiv c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} \equiv \varepsilon_1 \equiv 1 \pmod 2$$

This completes the proof of lemma 2.

LEMMA 3. *Case* 1° *in lemma* 1 *can only occur if* $n = \frac{2}{3}m$ *and* $\varepsilon_2 = \varepsilon_1$.

PROOF. Lemmas 1 and 2 imply either $c_{\frac{1}{2}n} = \pm 1$, $c_{m-\frac{1}{2}n} = \pm 3$ or $c_{\frac{1}{2}n} = \pm 3$, $c_{m-\frac{1}{2}n} = \pm 1$, the other c_i's being equal to zero. Since

$$|S_{m-\frac{1}{2}n}| = |c_0 c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_m| = |\pm 2 \pm 6| \geqq 4 ,$$

we get by (9) that $m - \frac{1}{2}n = n$, that is, $n = \frac{2}{3}m$, and further

$$c_0 c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_m = 4\varepsilon_1 \varepsilon_2 , \tag{10}$$

or

$$c_m c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_0 = 4\varepsilon_1 , \tag{11}$$

multiplying (10) by ε_2 and utilizing $c_0 = \varepsilon_2 c_m$ from (8). Equation (10) implies

$$c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} + \varepsilon_2 \equiv 2 \pmod 4, \qquad \text{that is,} \qquad c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} = -3\varepsilon_2 .$$

By means of (11) we then obtain

$$S_{m-n} = \varepsilon_1 = c_0 c_{\frac{1}{2}n} + c_m c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} = 4\varepsilon_1 - 3\varepsilon_2 ,$$

giving $\varepsilon_2 = \varepsilon_1$. Our lemma is proved.

LEMMA 4. *Case 2° in lemma 1 can only occur if $n = \frac{2}{5}m$ and $\varepsilon_1 = -\varepsilon_2$.*

PROOF. On account of lemmas 1 and 2 we have

$$(12) \quad c_{m-\frac{1}{2}n} = \delta_1, \quad c_{\frac{1}{2}n} = \delta_2, \quad c_{k_1} = 2\delta_3, \quad c_{k_2} = 2\delta_4 , \quad m > k_1 > k_2 > 0 .$$

At first we prove that $k_1 = m - k_2$. Suppose contrary and define $h_1 = \max\{k_1, m-k_2\}$. Then $h_1 > \frac{1}{2}m$ and $c_0 c_{h_1} + c_{m-h_1} c_m = \pm 4$, since

$$c_{h_1}^2 + c_{m-h_1}^2 = 4 ,$$

the last relation following from the fact that

$$h_1 \gtreqless k_1 > k_2 \geqq m - h_1, \quad h_1 \neq m - \tfrac{1}{2}n, \quad m - h_1 \neq m - \tfrac{1}{2}n .$$

Now it is seen to be possible to determine $\delta_x = \pm 1$ in such a way that

$$(c_0 + \delta_x c_{h_1})^2 + (c_{m-h_1} + \delta_x c_m)^2 = 20 .$$

Then we get

$$\sum_{j=0}^{m-h_1} (c_j + \delta_x c_{j+h_1})^2 = 2\delta_x S_{h_1} + 12 + T ,$$

where $T = 0$ if $h_1 < m - \frac{1}{2}n$ and $T = c_{\frac{1}{2}n}^2 + c_{m-\frac{1}{2}n}^2 = 2$ if $h_1 > m - \frac{1}{2}n$. Consequently $20 \leqq 14 + 2|S_{h_1}|$, that is $|S_{h_1}| \geqq 3$ which implies $S_{h_1} = \pm 4$ and $h_1 = n$. Considering

$$S_{\frac{1}{2}n} = c_0 c_{\frac{1}{2}n} + c_{\frac{1}{2}n} c_{h_1} + c_{m-h_1} c_{m-\frac{1}{2}n} + c_{m-\frac{1}{2}n} c_m ,$$

we find $S_{\frac{1}{2}n} \equiv 2 \pmod 4$, which is impossible. Hence $k_1 + k_2 = m$.

Then we shall prove that $c_0 c_{k_1} + c_{m-k_1} c_m = 0$. Suppose the contrary. Then $c_0 c_{k_1} + c_{m-k_1} c_m = \pm 8$, giving $S_{k_1} = \pm 8 + T$, where T now denotes the remaining part of the sum S_{k_1}. The part T contains at most one term $\neq 0$, namely $c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} = \pm 1$, giving $|S_{k_1}| \geqq 7$, a contradiction, and our assertion is proved. This formula implies $\delta_4 = -\delta_3 \varepsilon_2$. Inserting this in the identity (5) and treating it as a congruence mod 4, we find $\delta_2 = \varepsilon_1 \delta_1$.

If $\varepsilon_1 = \varepsilon_2$, (5) reduces to

$$(13) \quad 4\delta_0 \delta_1 x^{2m-\frac{1}{2}n} + 4\delta_0 \delta_1 \varepsilon_2 x^{m+\frac{1}{2}n} - 4\varepsilon_1 x^{2k_1} \equiv 4x^{m+n} .$$

Since $m + \frac{1}{2}n \notin \{2m - \frac{1}{2}n, m+n\}$, the identity (13) implies $2k_1 = \frac{1}{2}n + m$ and $m + n = 2m - \frac{1}{2}n$, giving $k_1 = m - \frac{1}{2}n$ which is impossible.

If $\varepsilon_1 = -\varepsilon_2$, (5) reduces to

$$(14) \qquad -4\delta_1\delta_3\varepsilon_1 x^{m+k_1-\frac{1}{2}n} + 4\delta_1\delta_3 x^{2m-k_1-\frac{1}{2}n} + 4\varepsilon_1 x^{2k_1} \equiv -4x^{m+n}, \quad k_1 < m - \tfrac{1}{2}n ,$$

$$(15) \qquad -4\delta_1\delta_3\varepsilon_1 x^{m+k_1-\frac{1}{2}n} + 4\delta_1\delta_3 x^{k_1+\frac{1}{2}n} + 4\varepsilon_1 x^{2k_1} \equiv -4x^{m+n}, \quad k_1 > m - \tfrac{1}{2}n .$$

It is easily seen that (15) cannot occur, while (14) is satisfied only by putting $m+k_1-\frac{1}{2}n = m+n$ and $2m-k_1-\frac{1}{2}n = 2k_1$, hence $n = \frac{2}{5}m$. This completes the proof of lemma 4.

4.

Here we prove a lemma which shall be frequently used in the following sections:

LEMMA 5. *In cases* 4° *and* 3° *in lemma* 1 *we have*

$$S_{m-i} = c_0 c_{m-i} + c_i c_m \quad \text{if} \quad 0 < i < n, \; n \leqq \tfrac{2}{3}m ,$$
$$c_i = c_{m-i} = 0 \quad \text{if} \quad 0 < i < \tfrac{1}{2}n, \; i \neq m-n ,$$

the restriction $i \neq m-n$, $n \leqq \frac{2}{3}m$, *being necessary only in case* 3°. *In case* 3°, $n > \frac{2}{3}m$ *implies* $c_n^2 + c_{m-n}^2 = 4$.

From Lemma 2 it is obvious that $c_i = c_{m-i} = 0$, $0 < i < \frac{1}{2}n$, for the case 4°. Let $0 < i < n$, $0 < t < i$. If $0 < t < \frac{1}{2}n$ then $c_t = 0$. If $\frac{1}{2}n \leqq t < i$ then $m - \frac{1}{2}n < m - i + t < m$ so that $c_{m-i+t} = 0$. This gives

$$S_{m-i} = \sum_{t=0}^{i} c_t c_{m-i+t} = c_0 c_{m-i} + c_i c_m, \qquad 0 < i < n ,$$

proving the lemma for the case 4°.

Again from lemma 2, but now in the case 3°, it follows that at most one of c_i, c_{m-i}, $0 < i < \frac{1}{2}n$, can be nonzero. Let $i = k$ give one such. Then obviously $c_k^2 + c_{m-k}^2 = 4$ and $S_{m-k} = \pm 4$. This gives $k = m - n < \frac{1}{2}n$, that is, $n > \frac{2}{3}m$, proving the first formula for the case 3°, and the last statement.

The second formula for the case 3° follows as for case 4°, ending the proof of lemma 5.

5.

LEMMA 6. *The cases* 3° *and* 4° *in lemma* 1 *are both impossible if* $n \geqq \frac{1}{2}m$.

PROOF. Suppose $n = \frac{1}{2}m$.

We get from the first formula in lemma 5, on account of (9), that

$$S_n = c_0 c_n + c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} + c_n c_m = 4\varepsilon_1\varepsilon_2 + \varepsilon_1 .$$

If $c_n = 0$ or $c_n = \pm 2$, we find $S_n \equiv \pm 1 \pmod 8$, which is impossible. If $c_n = \pm 1$ there are an odd number of terms of modulus 1 in the set $\mathscr{M}$, defined in lemma 1, but this is also impossible.

Suppose then $\frac{1}{2}m < n \leqq \frac{2}{3}m$. The second formula in lemma 5 gives

$$S_n = c_0 c_n + c_{m-n} c_m = 4\varepsilon_1\varepsilon_2$$

or

$$(18) \qquad c_m c_n + c_0 c_{m-n} = 4\varepsilon_1 .$$

We conclude that

$$S_{m-n} = \varepsilon_1 = c_0 c_{m-n} + c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} + c_n c_m ,$$

hence

$$S_{m-n} = 4\varepsilon_1 + \delta_1\delta_2 = \varepsilon_1 ,$$

which is impossible.

Suppose at last $n > \frac{2}{3}m$. In case 4° we find $S_n = 0$, contrary to (9). In case 3° we obtain from lemma 5

$$(19) \qquad S_{\frac{1}{2}n} = c_0 c_{\frac{1}{2}n} + c_{m-n} c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_n + c_{m-\frac{1}{2}n} c_m = 0$$

By (19) we get

$$(20) \qquad c_{m-n} c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_n = 0 ,$$

utilizing

$$S_{m-\frac{1}{2}n} = c_0 c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_m = c_0 c_{\frac{1}{2}n} + c_{m-\frac{1}{2}n} c_m = 0 .$$

Since (20) contradicts $c_{m-n}^2 + c_n^2 = 4$, our lemma is proved.

6.

LEMMA 7. *If $n < \frac{1}{2}m$ the cases 3° and 4° in lemma 1 results in, either*

$$\text{(A)} \qquad \begin{aligned} &c_i = c_{m-i} = 0, \quad 0 < i < \tfrac{3}{4}n,\ i \neq \tfrac{1}{2}n; \\ &c_{m-\frac{1}{2}n} = \delta_1, \quad c_{\frac{1}{2}n} = -\varepsilon_2\delta_1, \quad c_{m-\frac{3}{4}n} = \delta_2, \quad c_{\frac{3}{4}n} = -\delta_2\varepsilon_2; \\ &\varepsilon_2 = \varepsilon_1, \quad c_{m-n} \not\equiv c_n \pmod 2 , \end{aligned}$$

or

$$\text{(B)} \qquad \begin{aligned} &c_i = c_{m-1} = 0, \quad 0 < i < n,\ i \neq \tfrac{1}{2}n; \\ &c_{m-\frac{1}{2}n} = \delta_1, \quad c_{\frac{1}{2}n} = -\varepsilon_2\delta_1, \quad c_{m-n} = \delta_2, \quad c_n = -\delta_2\varepsilon_2; \\ &\varepsilon_2 = -\varepsilon_1, \quad c_{m-\frac{1}{2}3n} \not\equiv c_{\frac{1}{2}3n} \pmod 2 . \end{aligned}$$

PROOF. Since $n < \frac{1}{2}m < \frac{2}{3}m$ it follows from lemma 5 that $c_i = c_{m-i} = 0, 0 < i < \frac{1}{2}n$ and $c_0 c_{m-i} + c_i c_m = 0, 0 < i < n$. Consequently, $c_i \equiv c_{m-i} \pmod 2$,

$0<i<n$. It is obvious that none of these c_i's can be equal to ± 2. From lemma 5 it further follows

$$S_{m-\frac{1}{2}n} = c_0 c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_n = 0 . \tag{21}$$

Putting $c_{m-\frac{1}{2}n}=\delta_1$, equation (21) implies $c_{\frac{1}{2}n}=-\varepsilon_2\delta_1$.

Suppose that there exist indices i, $\frac{1}{2}n<i<n$, such that $c_i^2+c_{m-i}^2 \neq 0$, and let k be the smallest of these. As in the proofs of lemmas 2 and 5 we get $c_i=c_{m-i}=0$, $\frac{1}{2}n<i<k$, and $c_k \equiv c_{m-k} \equiv 1 \pmod 2$. We have

$$S_{m-2k} = c_0 c_{m-2k} + c_{\frac{1}{2}n} c_{m-2k+\frac{1}{2}n} + c_k c_{m-k} + c_{2k-\frac{1}{2}n} c_{m-\frac{1}{2}n} + c_{2k} c_m .$$

Here $S_{m-2k}=0$ or $4\varepsilon_1\varepsilon_2$ on account of (9) since $m-2k<m-n$. The relation $c_k c_{m-k} \equiv 1 \pmod 2$ shows that

$$c_{m-2k+\frac{1}{2}n} \not\equiv c_{2k-\frac{1}{2}n} \pmod 2 .$$

Now we shall prove that $m-2k+\frac{1}{2}n=m-n$, that is, $k=\frac{3}{4}n$. Suppose the contrary. Then

$$S_{m-2k+\frac{1}{2}n} = c_0 c_{m-2k+\frac{1}{2}n} + c_{2k-\frac{1}{2}n} c_m \equiv 2 \pmod 4 ,$$

which is impossible since $S_{m-2k+\frac{1}{2}n} \equiv 0 \pmod 4$. From

$$S_{m-k} = c_0 c_{m-k} + c_k c_m$$

it follows, putting $c_{m-\frac{3}{4}n}=\delta_2$, that $c_{\frac{3}{4}n}=-\varepsilon_2\delta_2$. At last we remark that

$$c_{m-n} = c_{m-2k+\frac{1}{2}n} \not\equiv c_{2k-\frac{1}{2}n} = c_n \pmod 2 ,$$

giving $\varepsilon_1=S_{m-n}\equiv 2-\varepsilon_2 \pmod 4$, and hence $\varepsilon_2=\varepsilon_1$, giving us the case (A).

Suppose that $c_i=0$, $\frac{1}{2}n<i<n$. We conclude that $c_i=c_{m-i}=0$ for these i. Suppose further $c_{m-n} \not\equiv c_n \pmod 2$. Then

$$S_{m-\frac{1}{2}3n} \equiv c_{\frac{1}{2}n} c_{m-n} + c_n c_{m-\frac{1}{2}n} \equiv 1 \pmod 2 ,$$

which is impossible since $m-\frac{3}{2}n \neq m-n$. Hence $c_{m-n} \equiv c_n \pmod 2$.

We shall prove that $c_{m-n} \equiv c_n \equiv 1 \pmod 2$. Assume the contrary. Then $c_n \equiv c_{m-n} \equiv 0 \pmod 2$, from which we conclude $c_n^2+c_{m-n}^2=0$ or 4. Considering

$$S_{m-n} = c_0 c_{m-n} + c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} + c_n c_m$$

as a congruence mod 8, the second possibility implies

$$\varepsilon_1 = S_{m-n} \equiv \pm 3 \pmod 8 ,$$

and hence

$$c_n = c_{m-n} = 0 .$$

Let $k>n$ be the smallest index i such that $c_i \neq 0$ (such an index must exist). As in case (A) we find

$$c_i = c_{m-i} = 0, \quad n<i<k \quad \text{and} \quad c_k \equiv c_{m-k} \equiv 1 \pmod 2 .$$

Putting $c_{m-k}=\delta_2$ we get $c_k=-\delta_2\varepsilon_2$. Since $m-k-\frac{1}{2}n \neq m-n$, $n \neq \frac{1}{2}m$, we have

$$S_{m-k-\frac{1}{2}n} = c_0 c_{m-k-\frac{1}{2}n} + c_{\frac{1}{2}n} c_{m-k} + c_k c_{m-\frac{1}{2}n} + c_{k+\frac{1}{2}n} c_m \equiv 0 \pmod 4 .$$

Now $c_{\frac{1}{2}n} c_{m-k} + c_k c_{m-\frac{1}{2}n} = -2\delta_1\delta_2\varepsilon_2$, and consequently

$$c_{k+\frac{1}{2}n} \not\equiv c_{m-k-\frac{1}{2}n} \pmod 2 .$$

Further we have

$$S_{m-n-k} \equiv c_{\frac{1}{2}n} c_{m-k-\frac{1}{2}n} + c_{k+\frac{1}{2}n} c_{m-\frac{1}{2}n} \equiv 1 \pmod 2 ,$$

which is impossible on account of (9) since $n \neq \frac{1}{2}m$. Then we have proved that

$$c_n \equiv c_{m-n} \equiv 1 \pmod 2 .$$

From

$$S_{m-n} = c_0 c_{m-n} + c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} + c_n c_m = \varepsilon_1$$

we conclude $2\delta_0(c_{m-n}+\varepsilon_2 c_n)=\varepsilon_1+\varepsilon_2$, that is, $\varepsilon_2=-\varepsilon_1$, and further, putting $c_{m-n}=\delta_2$, that $c_m=-\delta_2\varepsilon_2$. Considering

$$S_{m-\frac{1}{2}3n} = c_0 c_{m-\frac{1}{2}3n} + c_{\frac{1}{2}n} c_{m-n} + c_n c_{m-\frac{1}{2}n} + c_{\frac{1}{2}3n} c_m \equiv 0 \pmod 4$$

on account of (9), infering $c_{m-\frac{1}{2}3n} \not\equiv c_{\frac{1}{2}3n} \pmod 2$, we have case B. This completes the proof of lemma 7.

7.

LEMMA 8. *When $n<\frac{1}{2}m$, the case 3° in lemma 1 can only occur if $\varepsilon_2=\varepsilon_1$ and $n=\frac{4}{11}m$.*

PROOF. Let $m>k_1>k_2>k_3>k_4>k_5>k_6>0$, the k_i's denoting natural numbers. Let further c_{k_i} be the six values of c_j in (3) with modulus 1 and put $c_{k_7}=2\delta_7$. By lemma 2, $k_6=m-k_1=\frac{1}{2}n$. Comparing both sides of the identity (5) modulo 2 we get

$$\begin{aligned} & x^{k_2-k_6} + x^{k_3-k_6} + x^{k_4-k_6} + x^{k_5-k_6} + \\ + & x^{k_1-k_5} + x^{k_2-k_5} + x^{k_3-k_5} + x^{k_4-k_5} + \\ + & x^{k_1-k_4} + x^{k_2-k_4} + x^{k_3-k_4} + \\ + & x^{k_1-k_3} + x^{k_2-k_3} + \\ + & x^{k_1-k_2} \qquad \equiv 0 \pmod 2 . \end{aligned}$$

Now $k_2-k_6=k_1-k_5$, giving $k_1-k_2=k_5-k_6$. Suppose $k_3-k_6=k_1-k_4$, implying $k_1-k_3=k_4-k_6$. However, this is impossible, since then k_2-k_5

would be greater than all the remaining exponents. We conclude that there are the following two possibilities:

(a) $k_3 - k_6 = k_2 - k_5 > k_1 - k_4$,
(b) $k_1 - k_4 = k_2 - k_5 > k_3 - k_6$.

From (a) we get $k_4 - k_5 > k_1 - k_2 = k_2 - k_3 = k_5 - k_6$. If $k_2 - k_3 \neq k_3 - k_4$ we would obtain $h = \min\{k_2 - k_3, k_3 - k_4\}$ smaller than all the remaining exponents, which is impossible. Hence $k_2 - k_3 = k_3 - k_4$, and we get $k_1 - k_3 = k_2 - k_4$, $k_1 - k_4 = k_4 - k_5$ and $k_3 - k_5 = k_4 - k_6$. Solving these equations we find

$$k_6 = \tfrac{1}{2}n, \quad k_5 = \tfrac{1}{14}(2m+5n), \quad k_4 = \tfrac{1}{14}(8m-n), \quad k_3 = \tfrac{1}{14}(10m-3n)\,,$$
$$k_2 = \tfrac{1}{14}(12m-5n), \quad k_1 = m - \tfrac{1}{2}n.$$

The case (b) is symmetrical to (a) and gives

$$k_6 = \tfrac{1}{2}n, \quad k_5 = \tfrac{1}{14}(2m+5n), \quad k_4 = \tfrac{1}{14}(4m+3n), \quad k_3 = \tfrac{1}{14}(6m+n)\,,$$
$$k_2 = \tfrac{1}{14}(12m-5n), \quad k_1 = m - \tfrac{1}{2}n\,.$$

Lemma 7 implies, either

$$\text{(A)} \qquad \varepsilon_2 = \varepsilon_1, \quad k_2 = m - \tfrac{3}{4}n = \tfrac{1}{14}(12m-5n)\,,$$

hence $n = \frac{4}{11}m$, our exceptional case, or

$$\text{(B)} \qquad \varepsilon_2 = -\varepsilon_1, \quad k_2 = \tfrac{1}{14}(12m-5n) = m-n\,,$$

giving $n = \frac{2}{9}m$.

Then we shall show that the last case cannot occur. Let $h = \{\max k_7, m - k_7\}$ and assume $h = \frac{1}{2}m$. Since

$$\tfrac{1}{2}(m-n) \notin \{\tfrac{1}{2}n, n, k_3, m-k_3, k_4, m-k_4, \tfrac{1}{2}m\}$$

we must have

$$\tfrac{1}{2}(m-n), \tfrac{1}{2}(m+n) \notin \{0, k_1, k_2, k_3, k_4, k_5, k_6, m\}\,,$$

and hence $c_{\frac{1}{2}(m-n)} = c_{\frac{1}{2}(m+n)} = 0$. Since $c_{\frac{1}{2}m} = c_{k_7} = \pm 2$,

$$S_{\frac{1}{2}m} = c_0 c_{\frac{1}{2}m} + c_{\frac{1}{2}m} c_m = 0$$

implies $c_0 + c_m = 0$ and hence $\varepsilon_2 = -1$. Further we get

$$S_{\frac{1}{2}(m-n)} = c_{\frac{1}{2}n} c_{\frac{1}{2}m} + c_{\frac{1}{2}m} c_{m-\frac{1}{2}n} = \pm 2\delta_1(1-\varepsilon_2) = \pm 4\,,$$

which contradicts (9). Hence $h > \frac{1}{2}m$ and $h \neq m - \frac{1}{2}n$, $h \neq m - n$. Assuming $c_h c_{m-h} = 0$, we can find a δ_x such that

$$(c_0 + \delta_x c_h)^2 + (c_{m-h} + \delta_x c_m)^2 = 20\,.$$

Then we get

$$20 \leqq \sum_{j=0}^{m-h} (c_j + \delta_x c_{j+h})^2 \leqq 18 + 2S_h \delta_x = 18 ,$$

which is clearly impossible. Consequently $c_h c_{m-h} \neq 0$, and we must have either $k_7 = m - k_4$ or $k_7 = m - k_3$.

In order to complete the proof we introduce

$$h_3 = \max\{k_3, m-k_4\} = \tfrac{6}{9}m, \qquad h_4 = \max\{k_4, m-k_3\} = \tfrac{5}{9}m ,$$

separating two cases.

1°. $k_7 = m - k_3$. Using the equations

$$c_0 c_{h_3} + c_{\frac{1}{2}n} c_{m-n} + c_n c_{m-\frac{1}{2}n} + c_{m-h_3} c_m = S_{h_3} = 0 ,$$
$$c_0 c_{h_4} + c_{\frac{1}{2}n} c_{h_3} + c_n c_{m-n} + c_{m-h_3} c_{m-\frac{1}{2}n} + c_{m-h_4} c_m = S_{h_4} = 0$$

we get the following two possibilities:

(i) $c_{m-\frac{1}{2}n} = -\delta_7, \quad c_{m-n} = -\varepsilon_2 \delta_0, \quad c_{m-\frac{1}{2}3n} = 2\delta_7, \quad c_{m-2n} = 0 ,$
$c_{\frac{1}{2}n} = \delta_7 \varepsilon_2, \quad c_n = \delta_0, \quad c_{\frac{1}{2}3n} = -\delta_7 \varepsilon_2, \quad c_{2n} = -\delta_0;$

(ii) $c_{m-\frac{1}{2}n} = \delta_7 \varepsilon_2, \quad c_{m-n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{2}3n} = -\delta_7 \varepsilon_2, \quad c_{m-2n} = -\delta_0 \varepsilon_2 ,$
$c_{\frac{1}{2}n} = -\delta_7, \quad c_n = -\delta_0, \quad c_{\frac{1}{2}3n} = 2\delta_7, \quad c_{2n} = 0 .$

Both cases result in

$$S_{m-\frac{1}{2}5n} = \sum_{j=0}^{5} c_{\frac{1}{2}jn} c_{m-\frac{1}{2}5n+\frac{1}{2}jn} \equiv 2 \pmod 4 ,$$

which contradicts (9).

2°. $k_7 = m - k_4$ is shown to be impossible in the same way, using S_{m-3n} instead of $S_{m-\frac{1}{2}5n}$. Then we have proved lemma 8.

8.

LEMMA 9. *The case* 4° *in lemma* 1 *together with case* A *in lemma* 7 *is impossible if* $n \neq \frac{4}{11}m$.

PROOF. As in the proof of lemma 7, we find

$$c_i \equiv c_{m-i} \pmod 2 \qquad \text{for} \qquad \tfrac{3}{4}n < i < n, \qquad n < i < \tfrac{5}{4}n,$$

giving

(22) $c_i = c_{m-i} = 0, \quad \frac{3}{4} < i < n; \qquad c_{m-\frac{1}{4}5n} \not\equiv c_{\frac{1}{4}5n},\ c_{m-\frac{1}{2}3n} \not\equiv c_{\frac{1}{2}3n} \pmod 2 .$

We have also

$$c_{m-i} \equiv c_i \pmod 2, \qquad n < i < \tfrac{3}{2}n,\ i \neq \tfrac{5}{4}n .$$

These relations imply the equations:

$$S_{m-n} = c_0 c_{m-n} - \varepsilon_2 + c_n c_m = \varepsilon_1$$
$$S_{m-\frac{1}{4}5n} = c_0 c_{m-\frac{1}{4}5n} - 2\delta_1 \delta_2 \varepsilon_2 + c_{\frac{1}{4}5n} c_m = 0 \qquad (23)$$

$$S_{m-\frac{1}{2}3n} = c_0 c_{m-\frac{1}{2}3n} + c_{m-n}(-\delta_1 \varepsilon_2) - \varepsilon_2 + c_n \delta_1 + c_{\frac{1}{2}3n} c_m = 0,$$

because $m > 3n$, as seen from the following.

One member in each pair (c_x, c_{m-x}), $x = n, \frac{5}{4}n, \frac{3}{2}n$, must be equal to ± 1. If $\frac{3}{2}n \neq m-n$ and $\frac{3}{2}n \neq m-\frac{5}{4}n$ we get *new* odd coefficients. But these inequalities are satisfied, since $\frac{3}{2}n = m-n$ gives $m-\frac{5}{4}n = \frac{5}{4}n$ which is impossible, and $\frac{3}{2}n = m-\frac{5}{4}n$ is the case excluded. Since $x < m-x$ we have $\frac{3}{2}n < m-\frac{3}{2}n$, that is, $m > 3n$.

Suppose first $c_{m-n} \equiv c_{m-\frac{1}{4}5n} \equiv 1 \pmod 2$. Then by (23)

$$\begin{gathered} c_{m-\frac{1}{2}n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4}3n} = \delta_2, \quad c_{m-n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4}5n} = \delta_2, \\ c_{\frac{1}{2}n} = -\delta_0, \quad c_{\frac{3}{4}n} = -\delta_2 \varepsilon_2, \quad c_n = 0, \quad c_{\frac{1}{4}5n} = 0, \\ c_0 c_{m-\frac{1}{2}3n} + c_{\frac{1}{2}3n} c_m = 2\varepsilon_2 . \end{gathered} \tag{24}$$

We define

$$T = \sum_{i=1}^{5} (c_{\frac{1}{4}in} c_{\frac{1}{4}n+\frac{1}{4}in} + c_{m-\frac{1}{4}n-\frac{1}{4}in} c_{m-\frac{1}{4}in})$$

Now

$$S_{\frac{1}{4}n} = T + R + c_0 c_{\frac{1}{4}n} + c_{m-\frac{1}{4}n} c_m ,$$

where R denotes the rest of the elements in $S_{\frac{1}{4}n}$. We have $c_0 c_{\frac{1}{4}n} + c_{m-\frac{1}{4}n} c_m = 0$. The part $R+T$ contain at most 10 elements of the types ± 1, and T alone seven of these.

If $c_{\frac{1}{2}3n} = 0$ we find $T = 5\delta_0 \delta_2 \varepsilon_2$, and if $c_{m-\frac{1}{2}3n} = 0$ we find $T = 4\delta_0 \delta_2 \varepsilon_2$, utilizing (24). Since $|R| \leqq 3$, this contradicts $R = -T$, $S_{\frac{1}{4}n}$ being zero.

The possibilities $c_{m-n} = c_{m-\frac{1}{4}5n} = 0$ and $c_{m-n} \equiv c_{\frac{1}{4}5n} \equiv c_{\frac{1}{2}3n} \pmod 2$ can be excluded in exactly the same way, and hence

$$c_{m-n} \equiv c_{\frac{1}{4}5n} \equiv c_{m-\frac{1}{2}3n} \pmod 2 .$$

If we solve the equations (23), we get, either

$$\begin{gathered} c_{m-\frac{1}{2}n} = -\delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4}3n} = \delta_2, \quad c_{m-n} = 0, \quad c_{m-\frac{1}{4}5n} = -\delta_2, \\ c_{m-\frac{1}{2}3n} = 0 , \\ c_{\frac{1}{2}n} = \delta_0, \quad c_{\frac{1}{4}3n} = -\delta_2 \varepsilon_2, \quad c_n = \delta_0, \quad c_{\frac{1}{4}5n} = 0, \quad c_{\frac{1}{2}3n} = \delta_0 , \end{gathered} \tag{25}$$

or

$$\begin{gathered} c_{m-\frac{1}{2}n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4}3n} = \delta_2, \quad c_{m-n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4}5n} = 0 , \\ c_{m-\frac{1}{2}3n} = \delta_0 \varepsilon_2 , \\ c_{\frac{1}{2}n} = -\delta_0, \quad c_{\frac{1}{4}3n} = -\delta_2 \varepsilon_2, \quad c_n = 0, \quad c_{\frac{1}{4}5n} = \delta_2 \varepsilon_2, \quad c_{\frac{1}{2}3n} = 0 . \end{gathered} \tag{26}$$

We define

$$\begin{aligned} u_j &= (c_j - c_{j+\frac{1}{4}n} \delta_0 \delta_2 \varepsilon_2 + c_{j+\frac{1}{2}n})^2, \\ v_j &= (c_j + c_{j+\frac{1}{4}n} \delta_0 \delta_2 \varepsilon_2 + c_{j+\frac{1}{2}n})^2, \end{aligned} \qquad -\tfrac{1}{4}n \leqq j \leqq m .$$

A calculation shows that

$$\begin{aligned} U = \sum_{j=-\frac14 n}^{m-\frac14 n} u_j &= \sum_{j=-\frac14 n}^{m-\frac14 n} (c_j^2 + c_{j+\frac14 n}^2 + c_{j+\frac12 n}^2) - 4\delta_0\delta_2\varepsilon_2 \sum_{j=0}^{m-\frac14 n} c_j c_{j+\frac14 n} + 2 \sum_{j=0}^{m-\frac12 n} c_j c_{j+\frac12 n} \\ &= 2\sum_{j=0}^{m} c_j^2 + \sum_{j=0}^{m-\frac14 n} c_j^2 - \sum_{j=0}^{\frac14 n-1} c_j^2 - 4\delta_0\delta_2\varepsilon_2 S_{m-\frac14 n} + 2S_{m-\frac12 n} \\ &= 36 + 14 - 4 = 46 , \end{aligned}$$

noticing that $S_{m-\frac14 n} = S_{m-\frac12 n} = 0$. In a similar way is found that

$$V = \sum_{j=-\frac14 n}^{m-\frac14 n} v_j = 46 .$$

Inserting the values from (25) in the sum U, and the values from (26) in V, we obtain

$$\sum_{j=-1}^{4} (u_{\frac14 jn} + u_{m-\frac54 n+\frac14 jn}) = 48 \leqq U = 46, \qquad 48 \leqq V = 46 ,$$

a contradiction. This completes the proof of lemma 9.

9.

In this section we prove our last lemma:

LEMMA 10. *The case 4° in lemma 1 together with case B in lemma 6 is impossible.*

PROOF. With arguments similar to those used in lemma 9 we get $c_{\frac12 3n} \not\equiv c_{m-\frac12 3n} \pmod 2$. As in the proof of lemma 7 we find $c_i = c_{m-i} = 0$ for $n < i < \frac32 n$ and $c_i \equiv c_{m-i} \pmod 2$ for $\frac32 n < i < 2n$. From this we obtain $c_{m-2n} \not\equiv c_{2n} \pmod 2$, $m > 3n$, and $c_{m-\frac12 5n} \not\equiv c_{\frac12 5n} \pmod 2$. This gives further $m-2n > 2n$. By lemma 7, case (B):

$$\begin{aligned} S_{m-\frac12 3n} &= c_0 c_{m-\frac12 3n} - 2\delta_1\delta_2\varepsilon_2 + c_{\frac12 3n} c_m = 0 \\ S_{m-2n} &= c_0 c_{m-2n} - \delta_1\varepsilon_2 c_{m-\frac12 3n} - \varepsilon_2 + c_{\frac12 3n}\delta_1 + c_{2n} c_m = 0 \\ S_{m-\frac12 5n} &= c_0 c_{m-\frac12 5n} - \delta_1\varepsilon_2 c_{m-2n} - \delta_2\varepsilon_2 c_{m-\frac12 3n} + c_{\frac12 3n}\delta_2 + c_{2n}\delta_1 + \\ &\quad + c_{\frac52 n} c_m = 0 \end{aligned} \tag{27}$$

Suppose $c_{\frac12 3n} = c_{m-2n} = 0$. Then $c_{m-\frac12 3n} = \delta_1\delta_2\varepsilon_2\delta_0$, $c_{2n} = \delta_0$, and $c_{\frac12 n} c_{m-\frac12 3n} = -\varepsilon_2$, giving $\delta_2 = \delta_0\varepsilon_2$ and $c_{m-\frac12 3n} = \delta_1$. Hence $S_{m-\frac12 5n} \equiv 2 \pmod 4$, which contradicts (9). The cases $c_{m-\frac12 3n} = c_{2n} = 0$ and $c_{m-2n} \not\equiv c_{m-\frac12 5n} \pmod 2$ give impossibilities in the same way, in the last case by considering S_{m-3n} and $S_{m-\frac72 n}$ instead of $S_{m-\frac12 5n}$. Hence

$$c_{m-\frac12 3n} \equiv c_{m-2n} \equiv c_{m-\frac12 5n} \pmod 2 ,$$

and from (27) we get the two cases:

(i) $c_{m-n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{2}3n} = \delta_1, \quad c_{m-2n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{2}5n} = \delta_1 ,$
$c_n = -\delta_0, \quad c_{\frac{1}{2}3n} = c_{2n} = c_{\frac{1}{2}5n} = 0 ,$

(ii) $c_{m-n} = -\delta_0 \varepsilon_2, \quad c_{m-\frac{1}{2}3n} = c_{m-2n} = c_{m-\frac{1}{2}5n} = 0 ,$
$c_n = \delta_0, \quad c_{\frac{1}{2}3n} = -\delta_1 \varepsilon_2, \quad c_{2n} = \delta_0, \quad c_{\frac{1}{2}5n} = -\delta_1 \varepsilon_2 .$

In both cases $c_{m-\frac{1}{2}n} = \delta_1$, $c_{\frac{1}{2}n} = -\delta_1 \varepsilon_2$.

The final phase in the proof is quite similar to that in the previous section. We put

$$W = \sum_{j=0}^{m-n} (c_j + c_{j+n})^2 = \sum_{j=0}^{m-n} c_j^2 + 2 \sum_{j=0}^{m-n} c_j c_{j+n} + \sum_{j=n}^{m} c_j^2 = 18 .$$

Since in both cases

$$\sum_{j=0}^{3} (c_{m-\frac{1}{2}jn} + c_{m-n-\frac{1}{2}jn})^2 + \sum_{j=0}^{3} (c_{\frac{1}{2}jn} + c_{n+\frac{1}{2}jn})^2 = 24 \leqq W = 18 ,$$

we have proved lemma 10.

10.

The ten lemmas which we have proved in section 2–9 tell us that $f(x)$ is irreducible, apart from the cases:

$$n = \tfrac{3}{2}m \text{ and } \varepsilon_2 = \varepsilon_1; \qquad n = \tfrac{2}{5}m \text{ and } \varepsilon_2 = -\varepsilon_1; \qquad n = \tfrac{4}{11}m \text{ and } \varepsilon_2 = \varepsilon_1 .$$

It is easily shown that these exceptions give rise to exactly the listed identities, and our theorem is proved.

A further development of the ideas in [1], although in another direction, is given in papers [2] and [3]. According to a general result due to A. Schinzel in [3] it is for instance possible effectively to compute a constant C such that $m/(m,n) < C$. However, his investigations are quite complicated, and the value of C seems to be only of theoretical interest. The method used in this paper is elementary and can be used to prove other theorems of irreducibility.

REFERENCES

1. W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials,* Math. Scand. 8 (1960), 65–70.
2. J. Mikusiński et A. Schinzel, *Sur la réductibilité de certains trinomes,* Acta Arith. 9 (1964), 91–96.
3. A. Schinzel, *On the reducibility of polynomials and in particular of trinomials,* Acta Arith. 11 (1965), 1–33.

UNIVERSITY OF OSLO, NORWAY