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

\[ f(x) = x^m + \varepsilon_1 x^n + 4 \varepsilon_2 \]

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

\[ f(x) = \varphi_r(x) \psi_s(x), \quad r + s = m, \]

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 \(| -4 \varepsilon_1 | \leq 1 + 1 = 2 \) 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

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

and

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

we get

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

Writing

$$S_{m-k} = \sum_{j=0}^{k} c_j c_{j+m-k}, \quad 0 \leq k \leq m,$$

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

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

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

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

we get

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

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

$$S_i = 0 \quad \text{if} \quad 0 < i < m, \quad i \neq n - m, \quad i \neq n$$

$$S_{m-n} = \varepsilon_1 \text{ and } S_n = 4\varepsilon_1 \varepsilon_2 \quad \text{if} \quad n \neq \frac{1}{2} m$$

$$S_n = 4\varepsilon_1 \varepsilon_2 + \varepsilon_1 \quad \text{if} \quad n = \frac{1}{2} m.$$
In what follows $\delta_x$, $x$ being some index, always is a member of the set \{\pm 1\}. We also define
\[ c_j = 0 \quad \text{if} \quad j > m \quad \text{or} \quad j < 0 . \]

3.

In this section we prove three lemmas.

**Lemma 2.**
\[ c_i \equiv c_{m-i} \equiv 0 \pmod{2}, \quad 0 < i < \frac{1}{2} n , \]
\[ n \equiv 0 \pmod{2}, \quad c_{\frac{1}{2} n} \equiv c_{m-\frac{1}{2} n} \equiv 1 \pmod{2}. \]

**Proof.** Suppose $c_i$ even for $0 \leq i < \frac{1}{2} n$, $c_k$ odd and $c_{m-j}$ even for $0 \leq j < k < \frac{1}{2} n$, $c_{m-k}$ odd. If $k < h$ we get $S_{m-k} \equiv 2, \pmod{4}$, and if $k > h$ we find $S_{m-h} \equiv 2, \pmod{4}$, 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
\[ c_i \equiv c_{m-i} \equiv 0 \pmod{2}, \quad 0 \leq i < \frac{1}{2} n . \]

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 $n = \frac{3}{2} m$ 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
\[ |S_{m-\frac{1}{2} n}| = |c_0 c_{m-\frac{1}{2} n} + c_{\frac{1}{2} n} c_m| = |\pm 2 \pm 6| \geq 4 , \]
we get by (9) that $m - \frac{1}{2} n = n$, that is, $n = \frac{3}{2} m$, and further
\[ c_0 c_{m-\frac{1}{2} n} + c_{\frac{1}{2} n} c_m = 4 \varepsilon_1 \varepsilon_2 , \quad (10) \]
or
\[ c_m c_{m-\frac{1}{2} n} + c_{\frac{1}{2} n} c_0 = 4 \varepsilon_1 , \quad (11) \]
multiplying (10) by $\varepsilon_2$ and utilizing $c_0 = \varepsilon_2 c_m$ from (8). Equation (10) implies
\[ c_{\frac{1}{2} n} c_{m-\frac{1}{2} n} + \varepsilon_2 \equiv 2 \pmod{4}, \quad \text{that is}, \quad c_{\frac{1}{2} n} c_{m-\frac{1}{2} n} = -3 \varepsilon_2 . \]
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 \( n = \frac{3}{2}m \) and \( \varepsilon_1 = -\varepsilon_2 \).

**Proof.** On account of lemmas 1 and 2 we have
\[ c_{m-\frac{1}{2}n} = \delta_1 , \quad c_{\frac{1}{2}n} = \delta_2 , \quad c_{k_1} = 2\delta_3 , \quad c_{k_2} = 2\delta_4 , \quad m > k_1 > k_2 > 0 . \]
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
\[ h_1 \leq k_1 > k_2 \geq m - h_1 , \quad h_1 \pm m - \frac{1}{2}n , \quad m - h_1 \pm m - \frac{1}{2}n . \]
Now it is seen to be possible to determine \( \delta_2 = \pm 1 \) 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 \( 20 \leq 14 + 2|S_{h_1}| \), that is \( |S_{h_1}| \geq 3 \) 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 \( |S_{k_1}| \geq 7 \), a contradiction, and our assertion is proved. This formula implies \( \delta_2 = -\delta_3 \varepsilon_2 \). Inserting this in the identity (5) and treating it as a congruence mod 4, we find \( \delta_2 = \varepsilon_1 \delta_4 \).

If \( \varepsilon_1 = \varepsilon_2 \), (5) reduces to
\[ 4\delta_0 \delta_1 x^{2m-\frac{1}{2}n} + 4\delta_0 \delta_1 \varepsilon_2 x^{m+\frac{1}{2}n} - 4\varepsilon_1 x^{2k_1} \equiv 4x^{m+n} . \]
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

\[
4\delta_1 \delta_3 \varepsilon_1 x^{m+k_1-\frac{1}{2}n} + 4\delta_1 \delta_3 x^{2m-k_1-\frac{1}{2}n} + 4\varepsilon_1 x^{2k_1} \equiv -4x^{m+n},
\]
\[k_1 < m - \frac{1}{2}n,\]

\[
4\delta_1 \delta_3 \varepsilon_1 x^{m+k_1-\frac{1}{2}n} + 4\delta_1 \delta_3 x^{k_1+\frac{1}{2}n} + 4\varepsilon_1 x^{2k_1} \equiv -4x^{m+n},
\]
\[k_1 > m - \frac{1}{2}n.\]

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 \( n = \frac{3}{2}m \). 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

\[
S_{m-i} = c_0 c_{m-i} + c_i c_m \quad \text{if} \quad 0 < i < n, \quad n \leq \frac{3}{2}m,
\]

\[
c_i = c_{m-i} = 0 \quad \text{if} \quad 0 < i < \frac{1}{2}n, \quad i \neq m - n,
\]

the restriction \( i \neq m - n, \ n \leq \frac{3}{2}m \), being necessary only in case 3°. In case 3°, \( n > \frac{3}{2}m \) 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 \( \frac{1}{2}n \leq t < i \) then \( m - \frac{1}{2}n < m - i + t < m \) so that \( c_{m-i+t} = 0 \). This gives

\[
S_{m-i} = \sum_{t=0}^{i} c_tC_{m-i+t} = c_0 c_{m-i} + c_i c_m, \quad 0 < i < n,
\]

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, \( n > \frac{3}{2}m \), 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 \( n \geq \frac{1}{2}m \).

**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 \( \mathcal{M} \), defined in lemma 1, but this is also impossible.

Suppose then \( \frac{1}{2}m < n \leq \frac{3}{2}m \). The second formula in lemma 5 gives
\[ S_n = c_0 c_n + c_{m-n} c_m = 4\varepsilon_1 \varepsilon_2 \]
or
\[ (18) \quad c_m c_n + c_0 c_{m-n} = 4\varepsilon_1. \]

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 \( n > \frac{3}{2}m \). In case 4° we find \( S_n = 0 \), contrary to (9).

In case 3° we obtain from lemma 5
\[ (19) \quad S_{\frac{1}{2}n} = c_0 c_{\frac{1}{2}n} + c_{m-n} c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_n + c_{m-\frac{1}{2}n} c_m = 0 \]

By (19) we get
\[ (20) \quad c_{m-n} c_{m-\frac{1}{2}n} + c_{\frac{1}{2}n} c_n = 0, \]

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

(A) \( c_i = c_{m-i} = 0, \quad 0 < i < \frac{3}{2}n, \quad i \equiv \frac{1}{2}n; \)

\[ c_{m-\frac{1}{2}n} = \delta_1, \quad c_{\frac{1}{2}n} = -\varepsilon_2 \delta_1, \quad c_{m-\frac{1}{2}n} = \delta_2, \quad c_{\frac{1}{2}n} = -\delta_2 \varepsilon_2; \]

\[ \varepsilon_2 = \varepsilon_1, \quad c_{m-n} \equiv c_n \pmod{2}, \]

or

(B) \( c_i = c_{m-i} = 0, \quad 0 < i < n, \quad i \equiv \frac{1}{2}n; \)

\[ c_{m-\frac{1}{2}n} = \delta_1, \quad c_{\frac{1}{2}n} = -\varepsilon_2 \delta_1, \quad c_{m-\frac{1}{2}n} = \delta_2, \quad c_n = -\delta_2 \varepsilon_2; \]

\[ \varepsilon_2 = -\varepsilon_1, \quad c_{m-\frac{1}{3}n} \equiv c_{\frac{1}{3}n} \pmod{2}. \]

**Proof.** Since \( n < \frac{1}{2}m < \frac{3}{2}n \) 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

\[
S_{m-n} = c_0 c_{m-n} + c_1 c_n = 0.
\]

Putting \( c_{m-n} = \delta_1 \), equation (21) implies \( c_1 = -\epsilon_2 \delta_1 \).

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 \( c_k \equiv c_{m-k} \equiv 1 \) (mod 2). We have

\[
S_{m-2k} = c_0 c_{m-2k} + c_1 c_{m-2k} + c_k c_{m-k} + c_{2k} c_{m-1} + c_{2k-1} c_{m-n} + c_{2k} c_m.
\]

Here \( S_{m-2k} = 0 \) or \( 4 \epsilon_1 \epsilon_2 \) on account of (9) since \( m - 2k < m - n \). The relation \( c_k c_{m-k} \equiv 1 \) (mod 2) shows that

\[ c_{m-2k+1} + c_2 \equiv c_{2k-1} \equiv (mod 2) .
\]

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

\[
S_{m-2k+1} = c_0 c_{m-2k+1} + c_{2k-1} c_m \equiv 2 \pmod{4},
\]

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

\[
S_{m-k} = c_0 c_{m-k} + c_k c_m
\]

it follows, putting \( c_{m-n} = \delta_2 \), that \( c_1 = -\epsilon_2 \delta_2 \). At last we remark that

\[
c_{m-n} = c_{m-2k+1} + c_{2k-1} \equiv c_n (mod 2),
\]

giving \( \epsilon_1 = S_{m-n} \equiv 2 - \epsilon_2 \pmod{4} \), and hence \( \epsilon_2 = \epsilon_1 \), 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 \( c_{m-n} \equiv c_n \) (mod 2). Then

\[
S_{m-n} = c_1 c_{m-n} + c_n c_{m-n} \equiv 1 \pmod{2},
\]

which is impossible since \( m - \frac{3}{2} n + m - n \). Hence \( c_{m-n} \equiv c_n \) (mod 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 \( c_i^2 + c_{m-n}^2 = 0 \) or 4. Considering

\[
S_{m-n} = c_0 c_{m-n} + c_n c_{m-n} + c_n c_m
\]

as a congruence mod 8, the second possibility implies

\[
\epsilon_1 = S_{m-n} \equiv \pm 3 \pmod{8},
\]

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 \( m - k - \frac{1}{2}n \equiv m - n, \ n \equiv \frac{1}{2}m, \) we have

\[ S_{m-k-\frac{1}{2}n} = c_0c_{m-k-\frac{1}{2}n} + c_1c_{m-k} + c_kc_{m-\frac{1}{2}n} + c_{k+\frac{1}{2}n}c_m \equiv 0 \pmod{2}. \]

Now \( c_1c_{m-k} + c_kc_{m-\frac{1}{2}n} = -2\delta_1\delta_2\varepsilon_2 \), and consequently

\[ c_{k+\frac{1}{2}n} \equiv c_{m-k-\frac{1}{2}n} \pmod{4}. \]

Further we have

\[ S_{m-n-k} = c_1c_{m-k-\frac{1}{2}n} + c_{k+\frac{1}{2}n}c_{m-\frac{1}{2}n} \equiv 1 \pmod{2}, \]

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

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

From

\[ S_{m-n} = c_0c_{m-n} + c_1c_{m-\frac{1}{2}n} + c_nc_m = \varepsilon_1 \]

we conclude \( 2\delta_0(c_{m-n} + \varepsilon_2c_n) = \varepsilon_1 + \varepsilon_2 \), that is, \( \varepsilon_2 = -\varepsilon_1 \), and further, putting \( c_{m-n} = \delta_2 \), that \( c_m = -\delta_2 \varepsilon_2 \). Considering

\[ S_{m-\frac{1}{2}m} = c_0c_{m-\frac{1}{2}m} + c_1c_{m-n} + c_nc_{m-\frac{1}{2}n} + c_{\frac{1}{2}m}c_m \equiv 0 \pmod{4} \]

on account of (9), noferring \( c_{m-\frac{1}{2}m} \equiv c_{\frac{1}{2}m} \pmod{2} \), 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 \( c_{k_i} = 2\delta_7 \). By lemma 2, \( k_6 = m - k_1 = \frac{1}{2}n \). Comparing both sides of the identity (5) modulo 2 we get

\[
\begin{align*}
&x^{k_2-k_6} + x^{k_3-k_6} + x^{k_4-k_6} + x^{k_5-k_6} + \\
&+ x^{k_1-k_5} + x^{k_2-k_5} + x^{k_3-k_5} + x^{k_4-k_5} + \\
&+ x^{k_1-k_4} + x^{k_2-k_4} + x^{k_3-k_4} + \\
&+ x^{k_1-k_3} + x^{k_2-k_3} + \\
&+ x^{k_1-k_2} \equiv 0 \pmod{2}.
\end{align*}
\]

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

\[
\begin{align*}
  k_6 &= \frac{1}{2}n, \quad k_5 = \frac{1}{14}(2m+5n), \quad k_4 = \frac{1}{14}(8m-n), \quad k_3 = \frac{1}{14}(10m-3n), \\
  k_2 &= \frac{1}{14}(12m-5n), \quad k_1 = m - \frac{1}{2}n.
\end{align*}
\]

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

\[
\begin{align*}
  k_6 &= \frac{1}{2}n, \quad k_5 = \frac{1}{14}(2m+5n), \quad k_4 = \frac{1}{14}(4m+3n), \quad k_3 = \frac{1}{14}(6m+n), \\
  k_2 &= \frac{1}{14}(12m-5n), \quad k_1 = m - \frac{1}{2}n.
\end{align*}
\]

Lemma 7 implies, either

(A) \[ \epsilon_2 = \epsilon_1, \quad k_2 = m - \frac{3}{2}n = \frac{1}{14}(12m-5n), \]

hence \( n = \frac{11}{3}m \), our exceptional case, or

(B) \[ \epsilon_2 = -\epsilon_1, \quad k_2 = \frac{1}{14}(12m-5n) = m - n, \]

giving \( n = \frac{7}{3}m \).

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

\[ \frac{1}{2}(m-n) \notin \{\frac{1}{2}n, n, k_3, m - k_3, k_4, m - k_4, \frac{1}{2}m\} \]

we must have

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

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 \( \epsilon_2 = -1 \). Further we get

\[ S_{\frac{1}{2}(m-n)} = c_{\frac{1}{2}n} c_{\frac{1}{2}m} + c_{\frac{1}{2}m} c_{m-\frac{1}{2}n} = \pm 2 \delta_1(1 - \epsilon_2) = \pm 4, \]

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

\[ (c_0 + \delta_x c_h)^2 + (c_{m-h} + \delta_x c_m)^2 = 20. \]
Then we get
\[ 20 \leq \sum_{j=0}^{m-h} (c_j + \delta_x c_{j+h})^2 \leq 18 + 2S_h \delta_x = 18, \]
which is clearly impossible. Consequently \( c_h c_{m-h} \neq 0 \), and we must have either \( k_7 = m-k \) or \( k_7 = m-k_3 \).

In order to complete the proof we introduce
\[ h_3 = \max \{k_3, m-k_3\} = \frac{5}{8} m, \quad h_4 = \max \{k_4, m-k_3\} = \frac{5}{8} m, \]
separating two cases.

1°. \( k_7 = m-k_3 \). Using the equations
\[ c_0 c_{h_3} + c_{\frac{1}{4} n} c_{m-n} + c_n c_{m-\frac{1}{4} n} + c_{m-h_3} c_m = S_{h_3} = 0, \]
\[ c_0 c_{h_4} + c_{\frac{1}{4} n} c_{h_3} + c_n c_{m-n} + c_{m-h_3} c_{m-\frac{1}{4} n} + c_{m-h_4} c_m = S_{h_4} = 0 \]
we get the following two possibilities:

(i) \( c_{m-\frac{1}{4} n} = -\delta_7, \quad c_{m-n} = -\varepsilon_2 \delta_0, \quad c_{m-\frac{1}{4} 3n} = 2\delta_7, \quad c_{m-2n} = 0, \)
\[ c_{\frac{1}{4} n} = \delta_7 \varepsilon_2, \quad c_n = \delta_0, \quad c_{\frac{1}{4} 3n} = -\delta_7 \varepsilon_2, \quad c_{2n} = -\delta_0; \]
(ii) \( c_{m-\frac{1}{4} n} = \delta_7 \varepsilon_2, \quad c_{m-n} = \delta_0 \varepsilon_2, \quad c_{m-\frac{1}{4} 3n} = -\delta_7 \varepsilon_2, \quad c_{m-2n} = -\delta_0 \varepsilon_2, \)
\[ c_{\frac{1}{4} n} = -\delta_7, \quad c_n = -\delta_0, \quad c_{\frac{1}{4} 3n} = 2\delta_7, \quad c_{2n} = 0. \]

Both cases result in
\[ S_{m-\frac{1}{4} 5n} = \sum_{j=0}^{5} c_{\frac{1}{4} j n} c_{m-\frac{1}{4} 5n + \frac{1}{4} j n} \equiv 2 \pmod{4}, \]
which contradicts (9).

2°. \( k_7 = m-k_4 \) is shown to be impossible in the same way, using \( S_{m-3n} \) instead of \( S_{m-\frac{1}{4} 5n} \). 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 \( n \neq \frac{1}{4} m \).

**Proof.** As in the proof of lemma 7, we find
\[ c_i \equiv c_{m-i} \pmod{2} \quad \text{for} \quad \frac{3}{4} n < i < n, \quad n < i < \frac{5}{4} n, \]
giving
\[ c_i = c_{m-i} = 0, \quad \frac{1}{4} i < i < \frac{5}{4} n; \quad c_{m-\frac{1}{4} 5n} \equiv c_{\frac{1}{4} 5n}, \quad c_{m-\frac{1}{4} 3n} \equiv c_{\frac{1}{4} 3n} \pmod{2}. \]

We have also
\[ c_{m-i} \equiv c_i \pmod{2}, \quad n < i < \frac{3}{2} n, \quad i \neq \frac{5}{4} n. \]

These relations imply the equations:
\[ S_{m-n} = c_0 c_{m-n} - \varepsilon_2 + c_n c_m = \varepsilon_1 \]
\[ S_{m-\frac{1}{4} 5n} = c_0 c_{m-\frac{1}{4} 5n} - 2\delta_1 \delta_2 \varepsilon_2 + c_{\frac{1}{4} 5n} c_m = 0 \]
(23)
\[ S_{m-\frac{1}{3}n} = c_0 c_{m-\frac{1}{3}n} + c_{m-n} (-\delta_1 e_2) - e_2 + c_n \delta_1 + c_{\frac{1}{3}n} c_m = 0, \]
because \( m > 3n \), as seen from the following.

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

Suppose first \( c_{m-n} \equiv c_{m-\frac{1}{3}n} \equiv 1 \ (\text{mod} \ 2) \). Then by (23)
\[
\begin{align*}
c_{m-\frac{1}{3}n} &= \delta_0 e_2, \\
c_{\frac{1}{3}n} &= -\delta_0, \\
c_{\frac{2}{3}n} &= -\delta_2 e_2, \\
c_n &= 0, \\
c_{\frac{5}{3}n} &= 0, \\
c_0 c_{m-\frac{1}{3}n} + c_{\frac{1}{3}n} c_m &= 2e_2.
\end{align*}
\]

We define
\[ T = \sum_{i=1}^{5} (c_{\frac{1}{6}n} c_{\frac{1}{6}n+i\frac{1}{6}n} + c_{m-\frac{1}{6}n-i\frac{1}{6}n} c_{m-\frac{1}{6}n}) \]
Now
\[ S_{\frac{1}{6}n} = T + R + c_0 c_{\frac{1}{6}n} + c_{m-\frac{1}{6}n} c_m, \]
where \( R \) denotes the rest of the elements in \( S_{\frac{1}{6}n} \). We have \( c_0 c_{\frac{1}{6}n} + c_{m-\frac{1}{6}n} c_m = 0 \). The part \( R + T \) contain at most 10 elements of the types \( \pm 1 \), and \( T \) alone seven of these.

If \( c_{\frac{1}{6}n} = 0 \) we find \( T = 5\delta_0 \delta_2 e_2 \), and if \( c_{m-\frac{1}{6}n} = 0 \) we find \( T = 4\delta_0 \delta_2 e_2 \), utilizing (24). Since \(|R| \leq 3\), this contradicts \( R = -T \), \( S_{\frac{1}{6}n} \) being zero.

The possibilities \( c_{m-n} \equiv c_{m-\frac{1}{3}n} \equiv 0 \) and \( c_{m-n} \equiv c_{\frac{1}{3}n} \equiv c_{\frac{5}{3}n} \ (\text{mod} \ 2) \) can be excluded in exactly the same way, and hence
\[ c_{m-n} \equiv c_{\frac{1}{3}n} \equiv c_{m-\frac{1}{3}n} \ (\text{mod} \ 2). \]

If we solve the equations (23), we get, either
\[
\begin{align*}
c_{m-\frac{1}{3}n} &= -\delta_0 e_2, \\
c_{m-\frac{1}{3}n} &= \delta_2, \\
c_{m-n} &= 0, \\
c_{m-\frac{1}{3}n} &= -\delta_2, \\
c_{\frac{1}{3}n} &= \delta_0, \\
c_{\frac{2}{3}n} &= -\delta_2 e_2, \\
c_n &= 0, \\
c_{\frac{5}{3}n} &= 0, \\
\text{or}
\end{align*}
\]
\[
\begin{align*}
c_{m-\frac{1}{3}n} &= \delta_0 e_2, \\
c_{m-\frac{1}{3}n} &= \delta_2, \\
c_{m-n} &= \delta_0 e_2, \\
c_{m-\frac{1}{3}n} &= 0, \\
c_{\frac{1}{3}n} &= -\delta_0, \\
c_{\frac{2}{3}n} &= -\delta_2 e_2, \\
c_n &= 0, \\
c_{\frac{5}{3}n} &= \delta_2 e_2, \\
c_{\frac{5}{3}n} &= 0.
\end{align*}
\]

We define
\[
\begin{align*}
u_j &= (c_j - c_{j+\frac{1}{3}n} \delta_0 \delta_2 e_2 + c_{j+\frac{1}{3}n})^2, \\
v_j &= (c_j + c_{j+\frac{1}{3}n} \delta_0 \delta_2 e_2 + c_{j+\frac{1}{3}n})^2, \\
-\frac{1}{3}n &\leq j \leq m.
\end{align*}
\]
A calculation shows that
\[
U = \sum_{j=-\frac{1}{2}n}^{m-\frac{1}{2}n} u_j = \sum_{j=-\frac{1}{2}n}^{m-\frac{1}{2}n} (c_j^2 + c_{j+\frac{1}{2}n}^2 + c_{j+\frac{1}{2}n}^2) - 4\delta_0 \delta_2 \varepsilon_2 \sum_{j=0}^{m-\frac{1}{2}n} c_j c_{j+\frac{1}{2}n} + 2 \sum_{j=0}^{m-\frac{1}{2}n} c_j c_{j+\frac{3}{2}n}
\]
\[
= 2 \sum_{j=0}^{m} c_j^2 + \sum_{j=0}^{m-\frac{1}{2}n} c_j^2 - \sum_{j=0}^{m-\frac{1}{2}n-1} c_j^2 - 4\delta_0 \delta_2 \varepsilon_2 S_{m-\frac{1}{2}n} + 2S_{m-\frac{1}{2}n}
\]
\[
= 36 + 14 - 4 = 46
\]
noticing that \( S_{m-\frac{1}{2}n} = S_{m-\frac{1}{2}n} = 0 \). In a similar way is found that
\[
V = \sum_{j=-\frac{1}{2}n}^{m-\frac{1}{2}n} v_j = 46
\]
Inserting the values from (25) in the sum \( U \), and the values from (26) in \( V \), we obtain
\[
\sum_{j=-1}^{4} (u_{\frac{1}{2}n} + u_{m-\frac{n}{2}n+\frac{1}{2}n}) = 48 \leq U = 46, \quad 48 \leq V = 46
\]
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 \( c_{\frac{1}{2}n} \equiv c_{m-\frac{1}{2}n} \pmod{2} \). As in the proof of lemma 7 we find \( c_i = c_{m-i} = 0 \) for \( n < i < \frac{3}{2}n \) and \( c_i \equiv c_{m-i} \pmod{2} \) for \( \frac{3}{2}n < i < 2n \). From this we obtain \( c_{m-2n} \equiv c_{2n} \pmod{2} \), \( m > 3n \), and \( c_{m-45n} \equiv c_{45n} \pmod{2} \). This gives further \( m-2n > 2n \). By lemma 7, case (B):

\[
S_{m-3n} = c_0 c_{m-3n} - 2\delta_1 \delta_2 \varepsilon_2 + c_{\frac{1}{2}n} c_m = 0
\]
\[
S_{m-2n} = c_0 c_{m-2n} - \delta_1 \varepsilon_2 c_{m-\frac{1}{2}n} - \varepsilon_2 + c_{\frac{1}{2}n} \delta_1 + c_{2n} c_m = 0
\]
\[
S_{m-\frac{1}{2}n} = c_0 c_{m-\frac{1}{2}n} - \delta_1 \varepsilon_2 c_{m-2n} - \delta_2 \varepsilon_2 c_{m-\frac{3}{2}n} + c_{\frac{1}{2}n} \delta_2 + c_{2n} \delta_1 + c_{\frac{1}{2}n} c_m = 0
\]
Suppose \( c_{\frac{1}{2}n} = c_{m-2n} = 0 \). Then \( c_{m-3n} = \delta_1 \delta_2 \varepsilon_2 \delta_0, c_{2n} = \delta_0, \) and \( c_{\frac{1}{2}n} c_{m-\frac{1}{2}n} = -\varepsilon_2 \), giving \( \delta_2 = \delta_0 \varepsilon_2 \) and \( c_{m-\frac{3}{2}n} = \delta_1 \). Hence \( S_{m-\frac{1}{2}n} = 2 \pmod{4} \), which contradicts (9). The cases \( c_{m-\frac{1}{2}n} = c_{2n} = 0 \) and \( c_{m-2n} \equiv c_{m-\frac{1}{2}n} \pmod{2} \) give impossibilities in the same way, in the last case by considering \( S_{m-3n} \) and \( S_{m-\frac{3}{2}n} \) instead of \( S_{m-\frac{1}{2}n} \). Hence
\[
c_{m-\frac{1}{2}n} \equiv c_{m-2n} \equiv c_{m-\frac{1}{2}n} \pmod{2}
\]
and from (27) we get the two cases:

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

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

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

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

\[
3 \sum_{j=0}^{3} (c_{m-\frac{1}{2} j n} + c_{m-\frac{3}{2} j n})^2 + 3 \sum_{j=0}^{3} (c_{\frac{1}{2} j n} + c_{n+\frac{1}{2} j n})^2 = 24 \leq W = 18,
\]

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:

\[ n = \frac{2}{3} m \text{ and } \varepsilon_2 = \varepsilon_1; \quad n = \frac{2}{3} m \text{ and } \varepsilon_2 = -\varepsilon_1; \quad n = \frac{4}{11} m \text{ and } \varepsilon_2 = \varepsilon_1. \]

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


UNIVERSITY OF OSLO, NORWAY