MATH. SCAND. 57 (1985), 44–50

THE FACTORIZATION OF CERTAIN QUADRINOMIALS

W. H. MILLS

In this paper we study the factorizations of those quadrinomials over the field of rationals that are of the form $x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, where $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are ± 1. We can always write such a polynomial as $A(x)B(x)$ where every root of $A(x)$ is a root of unity, and no root of $B(x)$ is a root of unity. Of course either $A(x)$ or $B(x)$ may be a constant. The polynomial $A(x)$ is easily found and factored, while $B(x)$ is usually, but not always, irreducible.

Selmer [2], Ljunggren [1], and Tverberg [3] have solved the corresponding problem for trinomials. Ljunggren applied his method to quadrinomials, but overlooked a number of cases, so that there are counter-examples to his theorem. In the present paper we apply Ljunggren's methods to factor $B(x)$ when possible.

1. Preliminaries.

Wilhelm Ljunggren [1] considered the factorization over the field of rationals of quadrinomials of the form

$$F(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3, \tag{1}$$

where $n > m > p > 0$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are all ± 1. He asserted that $F(x)$ is the product of two factors, of which one has only roots of unity as zeros and the other is irreducible. The factorization

$$x^8 + x^4 + x^2 - 1 = (x^2 + 1)(x^3 + x^2 - 1)(x^3 - x^2 + 1)$$

is a counter-example to his theorem. However his methods are sound and we apply them.

If $E(x) = e_n x^n + \ldots + e_2 x^2 + e_1 x + e_0$ is a polynomial with $e_n \neq 0$ and $e_0 \neq 0$, then we let $E^*(x)$ denote the polynomial

$$E^*(x) = x^n E(x^{-1}) = e_0 x^n + e_1 x^{n-1} + e_2 x^{n-2} + \ldots + e_n.$$

The roots of $E^*(x)$ are the reciprocals of the roots of $E(x)$.

If $F(x)$ is any polynomial that factors, say $F(x) = C(x)D(x)$, then we can write $G(x) = C(x)D^*(x)$ and we have

Received August 1, 1984.

$$G(x)G^*(x) = F(x)F^*(x). \tag{2}$$

Ljunggren's method is to determine all polynomials $G(x)$ that satisfy (2). From this a complete factorization of $F(x)$ can usually be obtained.

LEMMA 1. (Ljunggren) *If $F(x)$ is of the form* (1) *and if $G(x)$ is a polynomial with integer coefficients such that* (2) *holds, then $G(x)$ has exactly four non-zero coefficients and these coefficients are all ± 1.*

PROOF. Clearly $G(x)$ has degree n, so that

$$G(x) = \sum_{i=0}^{n} g_i x^i.$$

The coefficient of x^n in $F(x)F^*(x)$ is

$$1 + \varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2 = 4,$$

while the coefficient of x^n in $G(x)G^*(x)$ is

$$\sum_{i=0}^{n} g_i^2.$$

Since $G(x)$ cannot be a monomial, it follows that $G(x)$ has exactly four non-zero coefficients, and these coefficients are all ± 1.

2. Solution of $G(x)G^*(x) = F(x)F^*(x)$.

We start with a polynomial $F(x)$ of the form (1). The factorization of $F(x)$ and $F^*(x)$ are equivalent problems. Replacing $F(x)$ by $\varepsilon_3 F^*(x)$ if necessary, we can cuppose that $n \geqq m+p$, and that if $n = m+p$ then $\varepsilon_1 \geqq \varepsilon_2\varepsilon_3$.

Now let $G(x)$ be a polynomial with integer coefficients such that (2) holds. By Lemma 1, $G(x)$ has exactly four non-zero coefficients and these are all ± 1. If we multiply $G(x)$ by -1 then (2) still holds, so that we can suppose that the leading coefficient of $G(x)$ is 1. Then we have

$$G(x) = x^n + \delta_1 x^s + \delta_2 x^t + \delta_3, \tag{3}$$

where $n > s > t > 0$ and $\delta_1, \delta_2, \delta_3$ are ± 1.

Replacing $G(x)$ by $\delta_3 G^*(x)$ leaves $G(x)G^*(x)$ unchanged. Making this replacement if necessary, we can assume that $n \geqq s+t$, and that if $n = s+t$ then $\delta_1 \geqq \delta_2\delta_3$.

THEOREM 1. *Suppose that $F(x)$ is of the form* (1) *and that $G(x)$ is of the form* (3). *Suppose that $n \geqq m+p$, and that if $n = m+p$ then $\varepsilon_1 \geqq \varepsilon_2\varepsilon_3$. Suppose that $n \geqq s+t$, and that if $n = s+t$ then $\delta_1 \geqq \delta_2\delta_3$. If $F(x)F^*(x)$*

$= G(x)G^*(x)$, *then either* (i) $F(x) = G(x)$, *or* (ii) n *is divisible by* 8 *and one of* $F(x)$, $G(x)$ *is*

$$x^{8r} + z^{7r} + x^r - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1),$$

and the other is

$$x^{8r} + x^{4r} + x^{2r} - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^{2r} + 1),$$

where $n = 8r$.

PROOF. We have

$$F(x)F^*(x) = \varepsilon_3 x^{2n} + \varepsilon_2 x^{2n-p} + \varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_2\varepsilon_3 x^{n+p} + \varepsilon_1\varepsilon_2 x^{n+m-p} + f(x)$$

and

$$G(x)G^*(x) = \delta_3 x^{2n} + \delta_2 x^{2n-t} + \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n+s-t} + g(x),$$

where $f(x)$ and $g(x)$ are polynomials of degree n. We see at once that $\delta_3 = \varepsilon_3$ and

$$\varepsilon_2 x^{2n-p} + \varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_2\varepsilon_3 x^{n+p} + \varepsilon_1\varepsilon_2 x^{n+m-p} = \delta_2 x^{2n-t} + \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n+s-t}. \tag{4}$$

We have $2n-p > 2n-m$, $2n-p \geqq n+m$, $n+m > n+p$, and $n+m > n+m-p$. Therefore to determine the term of largest degree on the left hand side of (4) we must look at the two terms $\varepsilon_2 x^{2n-p}$ and $\varepsilon_1\varepsilon_3 x^{n+m}$. Either these two terms cancel or the degree of the left hand side of (4) is $2n-p$.

Similarly either $\delta_2 x^{2n-t}$ and $\delta_1\delta_3 x^{n+s}$ cancel, or the degree of the right hand side of (4) is $2n-t$.

CASE 1. $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} = 0$ and $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} = 0$. In this case we must have $n = m+p = s+t$, $\varepsilon_2 + \varepsilon_1\varepsilon_3 = 0$, and $\delta_2 + \delta_1\delta_3 = 0$. These last two equalities give us $\varepsilon_1 = -\varepsilon_2\varepsilon_3$ and $\delta_1 = -\delta_2\delta_3$. By assumption we have $\varepsilon_1 \geqq \varepsilon_2\varepsilon_3$ and $\delta_1 \geqq \delta_2\delta_3$. Therefore $\varepsilon_1 = \delta_1 = 1$ and $\varepsilon_2\varepsilon_3 = \delta_2\delta_3 = -1$. Since $\varepsilon_3 = \delta_3$ we also get $\varepsilon_2 = \delta_2$. The left hand side of (4) reduces to $\varepsilon_2 x^{n+m-p}$ and the right hand side to $\delta_2 x^{n+s-t}$. It follows that $m-p = s-t$. Since we already have $m+p = s+t$ this gives us $m = s$, $p = t$, and therefore $F(x) = G(x)$.

CASE 2. Exactly one of $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m}$ and $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s}$ vanishes. Without loss of generality we suppose $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} = 0$ and $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} \neq 0$. Here again $n = m+p$ and $\varepsilon_2 + \varepsilon_1\varepsilon_3 = 0$. This

implies that $\varepsilon_1 + \varepsilon_2\varepsilon_3 = 0$, $\varepsilon_1 = 1$, $\varepsilon_2\varepsilon_3 = -1$, and the left hand side of (4) becomes $\varepsilon_2 x^{n+m-p}$.

There are six terms left of (4) and these must cancel in pairs. The only way this can happen is

$$\varepsilon_2 x^{n+m-p} = \delta_2 x^{2n-t},\ \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} = 0,\ \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n+s-t} = 0,$$

so that $n+m-p = 2n-t$, $2n-s = n+s$, and $n+t = n+s-t$. These yield $s = n/2$, $t = s/2 = n/4$, and $m-p = 3n/4$. Since $n = m+p$, we get $m = 7n/8$ and $p = n/8$. We also have $\delta_2 = \varepsilon_2$, $\delta_3 = -1$, and $\delta_1 + \delta_3 = 0$, so that $\delta_1 = 1$, $\varepsilon_3 = \delta_3 = -1$, and $\delta_2 = \varepsilon_2 = 1$. Here n is divisible by 8. Setting $n = 8r$ we get

$$F(x) = x^{8r} + x^{7r} + x^r - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1)$$

and

$$G(x) = x^{8r} + x^{4r} + x^{2r} - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^{2r} + 1).$$

CASE 3. $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} \neq 0$ and $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} \neq 0$. Since the terms of maximal degree on the two sides of (4) must be equal we have

$$\varepsilon_2 x^{2n-p} = \delta_2 x^{2n-t},$$

so that $\varepsilon_2 = \delta_2$ and $p = t$. We also have $\varepsilon_3 = \delta_3$. Here $\varepsilon_2\varepsilon_3 x^{n+p} = \delta_2\delta_3 x^{n+t}$ and (4) becomes

(5)
$$\varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_1\varepsilon_2 x^{n+m-p} = \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_1\delta_2 x^{n+s-t}.$$

If either

(6) $$\varepsilon_1 x^{2n-m} = \delta_1 x^{2n-s}$$

or

(7) $$\varepsilon_1\varepsilon_3 x^{n+m} = \delta_1\delta_3 x^{n+s}$$

or

(8) $$\varepsilon_1\varepsilon_2 x^{n+m-p} = \delta_1\delta_2 x^{n+s-t},$$

then we must have $m = s$ and $\varepsilon_1 = \delta_1$ so that $F(x) = G(x)$. Thus we can suppose that (6), (7), and (8) do not hold. Moreover if no pair of terms on the left hand side of (5) cancels, then the three terms on the left hand side are equal to the three terms on the right hand side in some order, so that

$$2n-m+n+m+n+m-p = 2n-s+n+s+n+s-t$$

and

$$\varepsilon_1\varepsilon_1\varepsilon_3\varepsilon_1\varepsilon_2 = \delta_1\delta_1\delta_3\delta_1\delta_2.$$

These equalities imply that $m-p = s-t$ and $\varepsilon_1\varepsilon_2\varepsilon_3 = \delta_1\delta_2\delta_3$, and again we have $m = s$, $\varepsilon_1 = \delta_1$, and $F(x) = G(x)$. Therefore we can suppose that two terms on the left side of (5) cancel. This implies that two terms on the right side of (5) cancel. The last two terms on a side of (5) cannot cancel because they have different degrees. Since none of (6), (7), and (8) can hold we can suppose, without loss of generality, that the first and third terms on the left hand side of (5) cancel, and that the first and second terms on the right hand side of (5) cancel. Hence we have

$$\varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_2 x^{n+m-p} = 0 \tag{9}$$

and

$$\delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} = 0. \tag{10}$$

Here (5) becomes

$$\varepsilon_1\varepsilon_3 x^{n+m} = \delta_1\delta_2 x^{n+s-t}. \tag{11}$$

Now (9) yields $2n-m = n+m-p$ or $n = 2m-p$, while (10) yields $n = 2s$. These two imply that $s < m$. On the other hand (11) gives us $n+m = n+s-t$, which implies that $m < s$. This is a contradiction. Thus in Case 3 we always have $F(x) = G(x)$, which completes the proof of the theorem.

3. The factorization.

We need the following result in order to prove our main result.

LEMMA 2. (Ljunggren) *If $F(x)$ is of the form* (1), *and if both λ and λ^{-1} are roots of $F(x)$, then λ is a root of unity. Indeed we must have one of the following three possibilities:*

(a) $\lambda^n = -\varepsilon_3$ *and* $\lambda^{m-p} = -\varepsilon_1\varepsilon_2$,

(b) $\lambda^m = -\varepsilon_1\varepsilon_3$ *and* $\lambda^{n-p} = -\varepsilon_2$,

(c) $\lambda^p = -\varepsilon_2\varepsilon_3$ *and* $\lambda^{n-m} = -\varepsilon_1$.

PROOF. Since λ is a root of $F(x)$ we have

$$\lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0.$$

Since λ^{-1} is a root of $F(x)$ we have

$$\lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3 = 0.$$

It follows that

$$\varepsilon_1\lambda^m + \varepsilon_2\lambda^p = \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m},$$

which can be written in the form

$$(\varepsilon_1\lambda^m + \varepsilon_2\lambda^p)(1 - \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m-p}) = 0.$$

It follows that either $\lambda^p = -\varepsilon_1\varepsilon_2\lambda^m$ or $\lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}$. In the first case substitution in $F(\lambda) = 0$ gives us $\lambda^n = -\varepsilon_3$, so that (a) holds. In the second case substitution in $F(\lambda) = 0$ gives us

$$(\lambda^m + \varepsilon_1\varepsilon_3)(\lambda^{n-m} + \varepsilon_1) = 0.$$

Here we see that either (b) or (c) must hold, which completes the proof.

Now let $F(x)$ be a quadrinomial of the form (1) that we wish to factor. Since it is sufficient to factor $F^*(x)$, we can suppose that $n \geqq m+p$, and that if $n = m+p$ then $\varepsilon_1 \geqq \varepsilon_2\varepsilon_3$. We can write $F(x) = A(x)B(x)$, where every root of $A(x)$ is a root of unity, and no root of $B(x)$ is a root of unity. Of course either $A(x)$ or $B(x)$ may be a constant. Then $A^*(x) = \pm A(x)$ and by Lemma 2 no root of $B(x)$ is a root of $B^*(x)$. It follows that $A(x)$ is the greatest common divisor of $F(x)$ and $F^*(x)$.

Suppose that $B(x)$ is reducible, say $B(x) = B_1(x)B_2(x)$, where both $B_1(x)$ and $B_2(x)$ have positive degree. Then

$$F(x) = A(x)B_1(x)B_2(x),$$

and we set

$$G(x) = A(x)B_1(x)B_2^*(x).$$

We have $F(x)F^*(x) = G(x)G^*(x)$.

If $G(x) = \pm F(x)$, then $B_2^*(x) = \pm B_2(x)$ which is impossible. Therefore we have $G(x) \neq \pm F(x)$.

If $G(x) = \pm F^*(x)$, then

$$A(x)B_1(x) = \pm A^*(x)B_1^*(x) \text{ and } B_1^*(x) = \pm B_1(x),$$

which is also impossible. Therefore $G(x) \neq \pm F^*(x)$.

We now apply Lemma 1 and Theorem 1 to conclude that n is divisible by 8, and that $F(x)$ is one of the two polynomials

$$x^{8r} + x^{7r} + x^r - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1)$$

and

$$x^{8r} + x^{4r} + x^{2r} - 1 = (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^{2r} + 1),$$

where $n = 8r$. In this case the other of these two polynomials must be either $\pm G(x)$ or $\pm G^*(x)$. Therefore $A(x) = x^{2r} + 1$ and the factors of $B(x)$ can be immediately deduced. Thus we have the following result.

THEOREM 2. *Suppose that $F(x)$ is a polynomial over the rationals of the form*

$$F(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3,$$

where $n > m > p > 0$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are all ± 1. Let $F(x) = A(x)B(x)$ where every root of $A(x)$ and no root of $B(x)$ is a root of unity. Then $A(x)$ is the greatest common divisor of $F(x)$ and $F^*(x)$. The second factor $B(x)$ is irreducible except when $F(x)$ is of one of the following four forms:

$$\begin{aligned}
x^{8r} + x^{7r} + x^r - 1 &= (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1),\\
x^{8r} - x^{7r} - x^r - 1 &= (x^{2r}+1)(x^{3r} - x^{2r} + 1)(x^{3r} - x^r - 1),\\
x^{8r} + x^{4r} + x^{2r} - 1 &= (x^{2r}+1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^{2r} + 1),\\
x^{8r} - x^{6r} - x^{4r} - 1 &= (x^{2r}+1)(x^{3r} - x^r - 1)(x^{3r} - x^r + 1).
\end{aligned}$$

In these cases the factors of degree $3r$ are irreducible.

In any particular case the factorization of $A(x)$ present no difficulty, since each of its roots must satisfy (a), (b), or (c) of Lemma 2.

As an immediate consequence of Theorem 2 we have the following corrected version of Ljunggren's Lemma 2.

COROLLARY. *If $F(x) = \varphi(x)\psi(x)$, where $\varphi(x)$ and $\psi(x)$ are monic polynomials with integral coefficients, then either* (i) *at least one of the two factors is a reciprocal polynomial, or* (ii) *$F(x)$ is of one of the four special forms of Theorem 2.*

REFERENCES

1. Wilhelm Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), 65–70.
2. Ernst S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.
3. Helge Tverberg, *On the irreducibility of the trinomials $x^n \pm x^m \pm 1$*, Math. Scand. 8 (1960), 121–126.

INSTITUTE FOR DEFENSE ANALYSES
THANET ROAD
PRINCETON, NEW JERSEY 08540
U.S.A.