AN EXTENSION OF A THEOREM OF LJUNGGREN

Michael Filaseta and Junior Solan*

1. Introduction

E.S. Selmer [5] studied the irreducibility over the rationals of polynomials of the form $x^n + \varepsilon_1 x^m + \varepsilon_2$ where $n \geq m$ and each $\varepsilon_j \in \{-1, 1\}$. He obtained complete solutions in the case $m = 1$ and partial results for $m > 1$. Ljunggren [1] later extended the problem to polynomials of the form $x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$ where again each $\varepsilon_j \in \{-1, 1\}$. He established

Theorem (Ljunggren). *For any distinct positive integers n, m, and p, and for any choice of $\varepsilon_j \in \{-1, 1\}$, the polynomial*

$$x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3,$$

with its cyclotomic factors removed, either is the identity 1 or is irreducible over the integers.

The analogous theorem also holds for the case of the trinomials studied by Selmer with $n \geq m \geq 0$. Similar studies and related problems can be found in [2], [3] and [4]. For example, in [2], Mikusinski and Schinzel proved that if p is an odd prime then there is only a finite number of ratios n/m for which $f(x) = x^n \pm px^m \pm 1$ is reducible; and in [3], Schinzel proved that for $n > m$ the polynomial

$$g(x) = \frac{x^n - 2x^m + 1}{x^{(n,m)} - 1}$$

is irreducible unless (n, m) is $(7k, 2k)$ or $(7k, 5k)$ in which case

$$g(x) = (x^{3k} + x^{2k} - 1)(x^{3k} + x^k + 1) \quad \text{and} \quad (x^{3k} + x^{2k} + 1)(x^{3k} - x^k - 1),$$

respectively.

Consider now

$$f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3 x^q + \varepsilon_4, \qquad \text{with each } \varepsilon_j \in \{-1, 1\}. \tag{1}$$

*Both authors were supported by NSF Grant DMS-9400937. Research of the second author was done as partial fulfillment of the Ph.D. requirement at the University of South Carolina.

If we remove the cyclotomic factors of $f(x)$, must the resulting polynomial be 1 or irreducible? This is in fact not the case. A simple example is given by

$$x^7 + x^5 + x^3 + x^2 - 1 = \left(x^3 + x - 1\right)\left(x^4 + x + 1\right).$$

An infinite set of examples is given by

$$f(x) = (x^n - x^2 + 1)(x^{n-2} + x^2 + 1) = x^{2n-2} + x^{n+2} + x^{n-2} - x^4 + 1$$

where n represents any integer ≥ 5 with $n \not\equiv 0, 3, 4, 6,$ or $9 \pmod{12}$; here, Ljunggren's result for trinomials can be used to establish $x^n - x^2 + 1$ and $x^{n-2} + x^2 + 1$ are both irreducible. In fact, these examples show that if $f(x)$ has five terms as above, it may be reducible and still not have "reciprocal" factors (a factor $g(x) \in \mathbb{Z}[x]$ satisfying $g(x) = \pm x^{\deg g} g(1/x)$). Nevertheless, it is reasonable still to consider $f(x)$ as in (1) with added restrictions. Our main result is the following five term version of Ljunggren's theorem.

Theorem 1. *Let $f(x) = x^n + x^m + x^p + x^q + 1$ be a polynomial with $n > m > p > q > 0$. Then $f(x)$ with its irreducible reciprocal factors removed either is the identity 1 or is irreducible over the integers.*

We do not know if the same result holds with the role of irreducible reciprocal factors replaced by cyclotomic factors. We were able to show that such a replacement is possible in the special case that n is exactly one of $2m$, $2q$, $2p$, $m+p$, $p+q$, or $m+q$. We also have the following examples:

$$x^{11} + x^8 + x^6 + x^2 + x + 1 = (x^5 - x^3 + 1)(x^6 + x^4 + x^3 + x^2 + x + 1)$$

and

$$x^{12} + x^{11} + 2x^7 + 1 = (x^5 + x^4 - x^3 - x^2 + 1)(x^7 + x^5 + x^3 + x^2 + 1).$$

The first of these shows that Theorem 1 cannot be extended to polynomials with six non-zero terms with coefficients 1. The second example illustrates that we need $p \neq q$ (and reciprocal considerations would imply we need $m \neq p$).

A more general theorem than Theorem 1 exists, and its proof would follow easily from the arguments given below. We emphasize Theorem 1 mainly because of its simplicity. The more general result replaces the condition that the coefficients of $f(x)$ in (1) are positive with the condition that when the product of the polynomial and its reciprocal polynomial is expanded there are no cancellation in terms. More precisely, we can show

Theorem 2. *Let $f(x) = x^n + \epsilon_1 x^m + \epsilon_2 x^p + \epsilon_3 x^q + \epsilon_4$ be a polynomial with $n > m > p > q > 0$ and each $\epsilon_j = \pm 1$. Suppose that the sum of the absolute values of the coefficients in the product*

$$\left(x^n + \epsilon_1 x^m + \epsilon_2 x^p + \epsilon_3 x^q + \epsilon_4\right)\left(\epsilon_4 x^n + \epsilon_3 x^{n-q} + \epsilon_2 x^{n-p} + \epsilon_1 x^{n-m} + 1\right)$$

is equal to 25. If $f(x) = \Omega(x)\Psi(x)$ where $\Omega(x)$ and $\Psi(x)$ are polynomials with integer coefficients, then at least one of $\Omega(x)$ and $\Psi(x)$ is a reciprocal polynomial.

Schinzel in [4] gives a general result which shows that any theorem similar to those stated above can be effectively established. Using this result directly involves performing a tremendous number of computations; we estimated establishing Theorem 1 directly in this manner would require over 10^{200} steps. Nevertheless, Schinzel's result is quite general giving a method of determining how all polynomials factor with Euclidean norm less than a prescribed amount.

The methods used in this paper are essentially the same as those of Ljunggren. He presented some key ideas introducing reciprocal polynomials into the problem of determining how polynomials with small Euclidean norm factor. The proof he gave of his theorem above involved consideration of several cases depending on the relative sizes of the exponents n, m, and p. In the case of Theorem 1 (or Theorem 2), we were able to bypass considering as many cases, mainly because the coefficients are more restrictive. We make no pretense here, however, of developing new approaches; this paper is merely a note that a five term version of Ljunggren's theorem does in fact exist. We give a proof of Theorem 1 below; a proof of Theorem 2 can be made with very few changes.

2. Proof of Theorem 1

Suppose $f(x) = \Omega(x)\Psi(x)$ where $\Omega(x)$ and $\Psi(x)$ are polynomials with integer coefficients. We show that at least one of $\Omega(x)$ and $\Psi(x)$ is a reciprocal polynomial. We explain first why this will imply Theorem 1. Suppose this has been established and $f(x)$ has more than two non-reciprocal irreducible factors (not necessarily distinct). Let $u(x)$ denote one of these. The polynomial $w(x) = x^{\deg u}u(1/x)$ will also be a non-reciprocal irreducible polynomial. If $w(x)|f(x)$, then we consider $\Omega(x)$ and $\Psi(x)$ such that $f(x) = \Omega(x)\Psi(x)$, $u(x) \nmid \Psi(x)$, and $w(x) \nmid \Omega(x)$. If α is a root of $u(x)$, then $\Omega(\alpha) = 0$ and $\Omega(1/\alpha) \neq 0$ so that $\Omega(x)$ is a non-reciprocal polynomial. Similarly, $\Psi(x)$ is non-reciprocal, and we arrive at a contradiction to what we are about to show. If $w(x) \nmid f(x)$, we consider a second non-reciprocal irreducible factor of $f(x)$, say $v(x)$, where possibly $v(x) = u(x)$ if $u(x)^2|f(x)$. If $w(x) = x^{\deg v}v(1/x)$ divides $f(x)$, then we can repeat the above argument replacing the role of $u(x)$ with $v(x)$. So suppose now that both $x^{\deg u}u(1/x)$ and $x^{\deg v}v(1/x)$ are not factors of $f(x)$. In this case, we consider $\Omega(x)$ and $\Psi(x)$ such that $f(x) = \Omega(x)\Psi(x)$, $u(x)|\Omega(x)$, and $v(x)|\Psi(x)$. As before, we deduce that each of $\Omega(x)$ and $\Psi(x)$ is non-reciprocal, leading to a contradiction.

Now, let $r = \deg \Omega$ and $s = \deg \Psi$. Write

$$f_1(x) = x^r\Omega(x^{-1})\Psi(x) = \sum_{i=0}^{n} c_i x^i \quad \text{and} \quad f_2(x) = x^s\Psi(x^{-1})\Omega(x).$$

We have

$$f_2(x) = x^n f_1(x^{-1}) = \sum_{i=0}^{n} c_i x^{n-i}$$

and

$$\begin{aligned} (2) \qquad f_1(x)f_2(x) &= \Omega(x)\Psi(x)\left(x^n\Omega(x^{-1})\Psi(x^{-1})\right) \\ &= (x^n + x^m + x^p + x^q + 1)\left(x^n + x^{n-q} + x^{n-p} + x^{n-m} + 1\right). \end{aligned}$$

On the other hand,

$$(3) \qquad f_1(x)f_2(x) = \left(\sum_{i=0}^{n} c_i x^i\right)\left(\sum_{i=0}^{n} c_i x^{n-i}\right).$$

Equating the coefficients of x^{2n} and x^n in the two expressions for $f_1(x)f_2(x)$ we find

$$c_0 c_n = 1 \qquad \text{and} \qquad c_0^2 + c_1^2 + \cdots + c_n^2 = 5.$$

Thus,

$$c_0 c_n = 1 \qquad \text{and} \qquad c_1^2 + c_2^2 + \cdots + c_{n-1}^2 = 3.$$

We deduce that three of the c_i's with $i \in \{1, 2, \ldots, n-1\}$, say c_{k_1}, c_{k_2} and c_{k_3} with $k_1 < k_2 < k_3$, must be ± 1 and the other c_i's are equal to 0. Furthermore,

$$(c_n + c_{k_3} + c_{k_2} + c_{k_1} + c_0)^2 = f_1(1)f_2(1) = 25$$

so that

$$c_0 = c_{k_1} = c_{k_2} = c_{k_3} = c_n = 1 \quad \text{or} \quad c_0 = c_{k_1} = c_{k_2} = c_{k_3} = c_n = -1.$$

We may suppose the former occurs and do so. Thus,

$$f_1(x) = x^n + x^{k_3} + x^{k_2} + x^{k_1} + 1 \quad \text{and} \quad f_2(x) = x^n + x^{n-k_1} + x^{n-k_2} + x^{n-k_3} + 1.$$

We suppose as we may that $n \geq m+q$, since otherwise we may replace $f(x)$ with $x^n f(1/x)$ (so that the role of m gets replaced by $n-q$, the role of p gets replaced by $n-p$, and the role of q gets replaced by $n-m$). It suffices also to take $n \geq k_1 + k_3$, since otherwise we can interchange the role of $f_1(x)$ and $f_2(x)$ (replacing k_3 with $n-k_1$, k_2 with $n-k_2$, and k_1 with $n-k_3$). From (2), we deduce that

$$(4) \qquad \begin{aligned} f_1(x)f_2(x) = x^{2n} &+ x^{2n-q} + x^{2n-p} + x^{2n-m} + x^{n+m} + x^{n+p} \\ &+ x^{n+q} + x^{n+m-q} + x^{n+m-p} + x^{n+p-q} + 5x^n + \cdots. \end{aligned}$$

From (3), we obtain

$$(5) \qquad \begin{aligned} f_1(x)f_2(x) = x^{2n} &+ x^{2n-k_1} + x^{2n-k_2} + x^{2n-k_3} + x^{n+k_3} + x^{n+k_2} \\ &+ x^{n+k_1} + x^{n+k_3-k_1} + x^{n+k_3-k_2} + x^{n+k_2-k_1} + 5x^n + \cdots. \end{aligned}$$

In (4) and (5), the terms shown are those having an exponent of x being at least n.

The condition $n \geq m+q$ implies that the second largest exponent in (4) is $2n-q$. The condition $n \geq k_1 + k_3$ implies that the second largest exponent in (5) is $2n - k_1$. It follows that $k_1 = q$.

The sum of the exponents greater than n in the expanded product of $f_1(x)f_2(x)$ given in (4) is $14n + 2m - 2q$. The sum of those exponents greater than n in the expanded product of $f_1(x)f_2(x)$ given in (5) is $14n + 2k_3 - 2k_1$. We deduce that $k_3 - k_1 = m - q$. Since $k_1 = q$, we obtain $k_3 = m$.

Making the substitutions $k_1 = q$ and $k_3 = m$ in (5) and comparing the resulting exponents with (4), we see that

$$\{2n - p, n + p, n + m - p, n + p - q\} = \{2n - k_2, n + k_2, n + k_3 - k_2, n + k_2 - k_1\}.$$

The largest element in the representation of the set given on the left is either $2n - p$ or $n + p$, and similarly the largest element on the right is either $2n - k_2$ or $n + k_2$. So one of $2n - p$ and $n + p$ must equal one of $2n - k_2$ and $n + k_2$.

If $2n - p = 2n - k_2$ or $n + p = n + k_2$, then $k_2 = p$. In this case, we obtain $\langle k_1, k_2, k_3 \rangle = \langle q, p, m \rangle$. Thus,

$$f_1(x) = x^n + x^m + x^p + x^q + 1 = f(x)$$

so that

$$\langle k_1, k_2, k_3 \rangle = \langle q, p, m \rangle \quad \Longrightarrow \quad \Omega(x) = x^r \Omega(x^{-1}). \tag{6}$$

If $2n - p = n + k_2$ or $n + p = 2n - k_2$, then $k_2 = n - p$. Comparing exponents in (4) and (5) with this additional substitution, we deduce that

$$\{n + m - p, n + p - q\} = \{n + k_3 - k_2, n + k_2 - k_1\} = \{m + p, 2n - p - q\}.$$

If $n + m - p = m + p$, then $n = 2p$ so that $k_2 = n - p = p$, and we can apply (6). If $n + m - p = 2n - p - q$, then $n = m + q$ so that $k_3 = m = n - q$ and $k_1 = q = n - m$. Thus, $\langle k_1, k_2, k_3 \rangle = \langle n - m, n - p, n - q \rangle$. An argument analogous to the argument for (6) gives in this case that $\Psi(x) = x^s \Psi(x^{-1})$.

This completes the proof of the theorem.

References

1. W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.
2. J. Mikusinski and A. Schinzel, *Sur la réductibilité de certains trinômes*, Acta Arith. **9** (1964), 91–95.
3. A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationels*, Colloq. Math. **9** (1962), 291–296.
4. A. Schinzel, *Reducibility of lacunary polynomials I*, Acta Arith. **16** (1969/70), 123–159.
5. E. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.