

## ON THE REDUCIBILITY OF CERTAIN QUADRINOMIALS

JONAS JANKAUSKAS

Vilnius University, Lithuania

ABSTRACT. In 2007 West Coast Number Theory conference Walsh asked to determine all irreducible polynomials of the form  $P(x) = x^i + x^j + x^k + 4$  with integer exponents  $i > j > k > 0$ , such that for some positive integer  $l$  the polynomial  $P(x^l)$  is reducible in  $\mathbb{Z}[x]$ . In this paper we prove that such polynomials are quadrinomials  $x^{4m} + x^{3m} + x^{2m} + 4$ , where  $m$  is an odd positive integer. In addition, Walsh asked for the examples of reducible quadrinomials  $x^i + x^j + x^k + n$ ,  $n > 4$  with no linear or quadratic factors. We compute the examples of reducible polynomials of the form above with non-trivial factors and negative coefficient  $n$ .

### 1. INTRODUCTION

Let  $P(x)$  be a polynomial with integer coefficients. The polynomial  $P(x)$  is called *primitive*, if one cannot write  $P(x) = P_1(x^l)$  for some polynomial  $P_1 \in \mathbb{Z}[x]$  and integer  $l > 1$ . The *reciprocal* polynomial  $x^{\deg P} P(1/x)$  of the polynomial  $P(x)$  is denoted by  $P^*(x)$ . Through the paper, *reducibility* shall always mean reducibility in  $\mathbb{Z}[x]$ .

The following question was posed by Walsh ([9]) in 2007 at West Coast Number Theory conference (Problem 007 : 14). Let  $i > j > k$  be positive integers. Does there exist an irreducible polynomial  $P(x) = x^i + x^j + x^k + 4$  of degree  $\deg P > 17$ , such that for some integer  $l > 1$ , the polynomial  $P(x^l)$  factors in  $\mathbb{Z}[x]$ ?

In addition, Walsh asked for the examples of reducible primitive quadrinomials of the form  $x^i + x^j + x^k + n$  with integer constant coefficient  $n > 4$ , which have no linear or quadratic factors. He gave one such example  $x^7 + x^5 + x^3 + 8 = (x^3 - x^2 - x + 2)(x^4 + x^3 + 3x^2 + 2x + 4)$ .

---

2010 *Mathematics Subject Classification.* 12E05.

*Key words and phrases.* Reducibility, quadrinomials.

The choice of the constant coefficient 4 in the polynomial  $x^i + x^j + x^k + 4$  is not accidental. A similar example is the binomial  $x^2 + 4$  which factors after the change of variable  $x$  to  $x^2$ . The polynomials  $x^{4m} + 4b^4$  are the exceptional case in the theorem of Capelli ([12]) on the reducibility of binomials. In the trinomial case, all reducible polynomials of the form  $x^i \pm x^j \pm 4$  were completely determined by Jonassen ([6]). By the theorem given in his paper [6], there are no irreducible trinomials  $P(x) = x^i \pm x^j \pm 4$ , such that for some positive integer  $l$ , the polynomial  $P(x^l)$  is reducible. In contrast, there exist quadrinomials  $P(x) = x^i + x^j + x^k + 4$  which have this property. In Section 2, we shall give a complete description of such quadrinomials.

The questions on the reducibility of trinomials and quadrinomials have received a lot of interest. The reducible trinomials and quadrinomials with all non-zero coefficients equal to 1 or  $-1$  were investigated by Selmer ([13]) and Ljunggren ([7]). The missing cases in Ljunggren's work were settled by Mills ([8]). Many important results and generalizations were established by Schinzel in the long series of papers starting with [10, 11]. In 1972 Fried and Schinzel ([5]) proved a deep result on the reducibility of quadrinomials. Theorems 2 and 3 in [5] state that for the fixed integers  $a, b, c, d$ , any reducible quadrinomial  $P(x) = ax^i + bx^j + cx^k + d$  either factors into the product of certain polynomials of standard shape, or such polynomial has the form  $P(x) = P_1(x^l)$ ,  $l \in \mathbb{Z}$ ,  $l > 0$ , where  $P_1 \in \mathbb{Z}[x]$  is primitive reducible quadrinomial of degree less or equal to the effectively computable constant  $C(a, b, c, d)$ . Unfortunately, this constant is too large for almost any practical applications: in our case,  $C(1, 1, 1, 4) > 2^{8045222}$ . In the present paper, we shall use Ljunggren's method ([7]) to determine all such exceptional quadrinomials  $x^i + x^j + x^k + 4$  which appear in the question of Walsh. See [1, 4] for a good exposition on the Ljunggren's method. More recent results on reducibility of trinomials can be found in [3]. For efficient factoring algorithms, we refer to [2].

## 2. MAIN RESULTS

The following theorem gives an answer to the first question of Walsh. We note that in this paper we do not use the same terminology as in [9].

**THEOREM 2.1.** *The only primitive irreducible polynomial  $P \in \mathbb{Z}[x]$  of the form  $P(x) = x^i + x^j + x^k + 4$ ,  $i > j > k > 0$ , such that the polynomial  $P(x^l)$  for some positive integer  $l$  factors in  $\mathbb{Z}[x]$ , is the polynomial  $P(x) = x^4 + x^3 + x^2 + 4$ . More precisely, for  $l = 2$ ,*

$$P(x^2) = x^8 + x^6 + x^4 + 4 = (x^4 - x^3 + x^2 - 2x + 2)(x^4 + x^3 + x^2 + 2x + 2).$$

Indeed, if the polynomial  $P(x) = x^i + x^j + x^k + 4$  has the property asked in the Problem 007 : 14, then  $P(x) = P_1(x^m)$  for some primitive polynomial  $P_1(x)$  and some positive integer  $m$ . By Theorem 2.1,  $P_1(x) = x^4 + x^3 + x^2 + 4$ .

In Lemma 2.2 below, we prove that  $P(x^l)$  is reducible only for even values  $l = 2g$ ; in this case the polynomial  $P(x^l)$  splits into two irreducible factors  $x^{4g} - x^{3g} + x^{2g} - 2x^g + 2$  and  $x^{4g} + x^{3g} + x^{2g} + 2x^g + 2$ .

LEMMA 2.2. *Let  $P(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0$  be a monic integer polynomial, such that  $|a_0| = p^2 > |a_1| + |a_2| + \dots + |a_{d-1}| + 1$ , where  $p$  is a prime. Let  $l > 1$  be a positive integer, such that  $P(x^l)$  is reducible in  $\mathbb{Z}[x]$  but  $P(x^m)$  is irreducible for any positive integer  $m < l$  which divides  $l$ . Then  $l$  is even and  $P(x^l) = \pm Q(x)Q(-x)$ ,  $Q \in \mathbb{Z}[x]$ . Moreover, for any integer  $r \geq 1$ , both factors  $Q(\pm x^r) \in \mathbb{Z}[x]$  are irreducible.*

In Lemma 2.3 we shall determine all the possible forms the product polynomial  $PP^*$  can take. This will be used in the proof of Theorem 2.1.

LEMMA 2.3. *Let  $P$  be a quadrinomial  $P(x) = x^i + x^j + x^k + 4$  with the integer exponents  $i > j > k > 0$ . Then the polynomial  $PP^*$  takes one of the following forms:*

- 1)  $4x^{2i} + x^{2i-k} + x^{2i-j} + x^{i+j-k} + 4x^{i+j} + 4x^{i+k} + 19x^i + 4x^{i-k} + 4x^{i-j} + x^{i-j+k} + x^j + x^k + 4$ ,  
if  $i \neq 2j$ ,  $i \neq 2k$ ,  $j \neq 2k$ ,  $i+k \neq 2j$ ,  $i \neq j+k$ ;
- 2)  $4x^{2i} + x^{2i-k} + 5x^{2i-j} + x^{i+j-k} + 4x^{i+k} + 19x^i + 4x^{i-k} + x^{i-j+k} + 5x^j + x^k + 4$ ,  
if  $i = 2j$ ,  $i \neq 2k$ ,  $j \neq 2k$ ,  $i+k \neq 2j$ ,  $i \neq j+k$ ;
- 3)  $4x^{2i} + 5x^{2i-k} + x^{2i-j} + x^{i+j-k} + 4x^{i+j} + 19x^i + 4x^{i-j} + x^{i-j+k} + x^j + 5x^k + 4$ ,  
if  $i \neq 2j$ ,  $i = 2k$ ,  $j \neq 2k$ ,  $i+k \neq 2j$ ,  $i \neq j+k$ ;
- 4)  $4x^{2i} + x^{2i-k} + x^{2i-j} + 5x^{i+j-k} + 4x^{i+j} + 19x^i + 4x^{i-j} + 5x^{i-j+k} + x^j + x^k + 4$ ,  
if  $i \neq 2j$ ,  $i \neq 2k$ ,  $j = 2k$ ,  $i+k \neq 2j$ ,  $i \neq j+k$ ;
- 5)  $4x^{2i} + x^{2i-k} + 2x^{2i-j} + 4x^{i+j} + 4x^{i+k} + 19x^i + 4x^{i-k} + 4x^{i-j} + 2x^j + x^k + 4$ ,  
if  $i \neq 2j$ ,  $i \neq 2k$ ,  $j \neq 2k$ ,  $i+k = 2j$ ,  $i \neq j+k$ ;
- 6)  $4x^{2i} + 5x^{2i-k} + 5x^{2i-j} + x^{i+j-k} + 19x^i + x^{i-j+k} + 5x^j + 5x^k + 4$ ,  
if  $i \neq 2j$ ,  $i \neq 2k$ ,  $j \neq 2k$ ,  $i+k \neq 2j$ ,  $i = j+k$ ;
- 7)  $4x^{2i} + x^{2i-k} + 5x^{2i-j} + 5x^{i+j-k} + 19x^i + 5x^{i-j+k} + 5x^j + x^k + 4$ ,  
if  $i = 2j$ ,  $i \neq 2k$ ,  $j = 2k$ ,  $i+k \neq 2j$ ,  $i \neq j+k$ ;
- 8)  $4x^{2i} + 5x^{2i-k} + 2x^{2i-j} + 4x^{i+j} + 19x^i + 4x^{i-j} + 2x^j + 5x^k + 4$ ,  
if  $i \neq 2j$ ,  $i = 2k$ ,  $j \neq 2k$ ,  $i+k = 2j$ ,  $i \neq j+k$ ;
- 9)  $4x^{2i} + 5x^{2i-k} + 6x^{2i-j} + 19x^i + 6x^j + 5x^k + 4$ ,  
if  $i \neq 2j$ ,  $i \neq 2k$ ,  $j = 2k$ ,  $i+k = 2j$ ,  $i = j+k$ .

## 3. COMPUTATIONS

In order to answer the second part of the problem 007 : 14, we have used the computer to search for the examples of reducible polynomials of the form  $P(x) = x^i + x^j + x^k + n$ . Since the polynomial  $P(x)$  has no roots of modulus less or equal to 1 if  $n \geq 4$ , the polynomial  $P(x)$  is irreducible provided the coefficient  $n$  is equal to the prime integer  $p \geq 5$ . With MAPLE computer algebra package we factored all primitive quadrinomials  $P(x)$  with composite constant coefficient  $n$  and exponents  $i, j, k$  in the range  $5 < n \leq 120, i-j \leq 20, j-k \leq 20, k \leq 20$ . In addition, we factored all primitive quadrinomials  $P(x)$  of this form satisfying inequalities  $120 < n \leq 1000, i-j \leq 15, j-k \leq 15, k \leq 15$ . We also searched for the irreducible polynomials  $P(x)$ , such that  $P(x^l)$  is reducible for some integer  $l$  in the range  $5 < n \leq 120, (i-j)l \leq 12, (j-k)l \leq 12, kl \leq 12$ . In all the cases reducible polynomials  $P(x)$  had a factor of the form  $Q(x^l)$ , where  $Q(x)$  was a linear polynomial or a quadratic polynomial. The example  $x^7 + x^5 + x^3 + 8$  of Walsh was the only notable exception. However, it does not seem easy to prove this.

All found examples of reducible quadrinomials  $P(x)$  had two or three irreducible factors. During the preparation of this paper, A. Schinzel sent a short remark that any irreducible polynomial dividing the quadrinomial  $P(x)$  has constant coefficient greater than 1, hence the number of irreducible factors cannot exceed  $\Omega(n)$ , the total number of prime factors of  $n$ . The sharpness of this estimate may be shown by the example

$$x^{12} + x^8 + x^4 + 52 = (x^2 - 2x + 2)(x^2 + 2x + 2)(x^8 - 3x^4 + 13).$$

Since  $\Omega(n) \leq \log n / \log 2$ , the number  $\log n / \log 2$  is the best known bound for the total number of prime factors of the quadrinomials  $P(x)$  in question.

Finally, we note that there exist the examples of reducible quadrinomials  $P(x)$  with no linear or quadratic factors and negative coefficient  $n < -5$ , namely, the polynomials

$$\begin{aligned} x^6 + x^4 + x^2 - 16 &= (x^3 - 3x^2 + 5x - 4)(x^3 + 3x^2 + 5x + 4), \\ x^{12} + x^8 + x^4 - 16 &= (x^3 - x^2 - x + 2)(x^3 + x^2 - x - 2)(x^6 + 3x^4 + 5x^2 + 4), \\ x^7 + x^3 + x^2 - 98 &= (x^3 - x^2 + 2x - 7)(x^4 + x^3 - x^2 + 4x + 14), \end{aligned}$$

and

$$\begin{aligned} x^{17} + x^{14} + x^8 - 16 &= (x^5 + x^3 - x^2 - 2) \\ &\quad (x^{12} - x^{10} + 2x^9 + x^8 - x^7 + x^6 + 2x^4 + 4x^3 - 4x^2 + 8). \end{aligned}$$

## 4. PROOFS

PROOF OF LEMMA 2.2. Let  $P(x^l) = Q(x)R(x)$  for some integer  $l > 0$  and polynomials  $Q, R \in \mathbb{Z}[x]$ . The inequality  $|a_0| > |a_1| + |a_2| + \dots + |a_{d_1}| + 1$  implies that  $P, Q$  and  $R$  have no roots of modulus  $|z| \leq 1$ . Thus the constant

terms of  $Q$  and  $R$  are equal to  $\pm p$  and they are irreducible in  $\mathbb{Z}[x]$ . Otherwise one of the polynomials  $Q$  or  $R$  would be divisible by the monic non-constant polynomial  $S \in \mathbb{Z}[x]$  with the constant term  $S(0) = \pm 1$ . This is impossible, since such a polynomial  $S$  has at least one root of modulus less or equal to 1. The same argument also implies the irreducibility of polynomials  $Q(x^r)$  and  $R(x^r)$  which divide  $P(x^{rl})$ .

Now, assume that the exponent  $l$  has the property that for any positive integer  $m < l$  which divides  $l$ , the polynomial  $P(x^m)$  is irreducible. If  $m = 1$ , this means that  $P(x)$  is irreducible. Let  $\alpha$  be the root of the irreducible factor  $Q(x)$ . Since  $P(x^l) = Q(x)R(x)$ , the power of this root  $\beta = \alpha^l$  is the root of the irreducible polynomial  $P$ . Let  $K = \mathbb{Q}(\beta)$ ,  $L = \mathbb{Q}(\alpha)$ ,  $K \subset L$ . Let  $g$  be the degree  $[L : K]$ . The absolute norm of an algebraic integer  $\beta$  over  $\mathbb{Q}$   $N_{L/\mathbb{Q}}(\beta) = N_{L/\mathbb{Q}}(\alpha^l) = N_{L/\mathbb{Q}}(\alpha)^l = \pm p^l$ . In the other hand, by the relative norm property,  $N_{L/\mathbb{Q}}(\beta) = N_{K/\mathbb{Q}}(\beta)^{[L:K]} = \pm p^{2g}$ . Thus  $l = 2g$ .

Since  $l$  is even, the number  $-\alpha$  is the root of  $P(x^l)$ . The irreducible polynomial  $Q(-x)$  divides  $P(x^l)$ . Then  $R(x) = \pm Q(-x)$ . Indeed, otherwise  $Q(-x) = -Q(x)$  or  $Q(-x) = Q(x)$ . The first case is impossible: the identity  $Q(-x) = -Q(x)$  with  $x = 0$  implies  $Q(0) = P(0) = 0$ , contradicting the inequality  $|a_0| > 1$ . The second identity  $Q(-x) = Q(x)$  implies  $Q(x) = T(x^2)$  for the polynomial  $T \in \mathbb{Z}[x]$ , thus  $R(x) = P(x^l)/Q(x) = P(x^{2g})/T(x^2) = S(x^2)$ ,  $S \in \mathbb{Z}[x]$ . This leads to the expression  $P(x^{2g}) = T(x^2)S(x^2)$ , hence  $P(x^g) = T(x)S(x)$ . This implies that  $P(x^g)$  is reducible for the integer  $g$  which is a proper divisor of  $l$ , contradicting the condition of Lemma 2.2.  $\square$

PROOF OF LEMMA 2.3. Assume that integers  $i, j, k$  satisfy the inequality  $i > j > k > 0$ . The reciprocal of the polynomial  $P(x) = x^i + x^j + x^k + 4$  is  $P^*(x) = 4x^i + x^{i-k} + x^{i-j} + 1$ . The product  $F = PP^*$  takes the form

$$F(x) = 4x^{2i} + x^{2i-k} + x^{2i-j} + 4x^{i+j} + x^{i+j-k} + 4x^{i+k} \\ + 19x^i + 4x^{i-k} + x^{i-j+k} + 4x^{i-j} + x^j + x^k + 4.$$

Let

$$v_1 = 2i, \quad v_2 = 2i - k, \quad v_3 = 2i - j, \quad v_4 = i + j, \quad v_5 = i + j - k, \\ v_6 = i + k, \quad v_7 = i, \quad v_8 = i - k, \quad v_9 = i - j + k, \quad v_{10} = i - j, \\ v_{11} = j, \quad v_{12} = k, \quad v_{13} = 0.$$

The multi-set  $V = \{v_r, r = 0, \dots, 13\}$  contains all possible exponents which appear in the polynomial  $F$ . If none of them are equal,  $F$  takes the form in Case 1). We shall classify all other cases where some exponents  $v_r$  and  $v_s, r \neq s$  are equal, and the terms of  $F$  with equal exponents add together. Set

$$e_1 = \{i = 2j\}, \quad e_2 = \{i = 2k\}, \quad e_3 = \{j = 2k\}, \\ e_4 = \{i + k = 2j\}, \quad e_5 = \{i = j + k\}.$$

The elements of the set  $E = \{e_r, r = 1, \dots, 5\}$  denote the linear relations among the integers  $i, j, k$ . Note that  $v_1$  and  $v_{13}$  are the largest and smallest integers in  $V$ . Since  $i > j > k > 0$ , all the exponents  $v_1, v_2, v_3, v_4, v_5, v_6$  are strictly greater than the exponent of the middle term  $v_7 = i$ , exponents  $v_8, v_9, v_{10}, v_{11}, v_{12}, v_{13}$  are strictly less than  $v_7 = i$ .  $F$  is self-reciprocal, since  $F = PP^* = F^*$ . Hence  $v_s = 2i - v_{13-s+1}$ ,  $s = 8, \dots, 13$ . Thus it suffices to check all possible cases when some of the integers  $v_2, v_3, v_4, v_5, v_6$  are equal. Observe that

$$v_2 > v_3, \quad v_2 > v_5, \quad v_4 > v_5, \quad v_4 > v_6.$$

Hence, all possible pairs of equal exponents  $v_s, s = 2, \dots, 6$  are:  $v_2 = v_4$  (this is equivalent to the linear relation  $e_5$ ),  $v_2 = v_6$  (equivalent to  $e_2$ ),  $v_3 = v_4$  ( $e_1$ ),  $v_3 = v_5$  ( $e_4$ ),  $v_3 = v_6$  ( $e_5$ ),  $v_5 = v_6$  ( $e_3$ ). The remaining pairs of equal exponents  $v_s, s = 8, \dots, 13$  are determined uniquely by the symmetry  $v_s = 2i - v_{13-s+1}$ .

The forms of the polynomial  $F$  where the integer exponents  $i, j, k$  satisfy precisely one linear relation in the set  $E$  are listed in Cases 2)-6). In order to check Cases 2)-6), use the expression in Case 1) and add terms with equal powers  $x^{v_r}$  and  $x^{v_s}$  together if  $v_r = v_s$ . The next step is to determine all possible forms of  $F$  where the integers  $i, j, k$  satisfy two linear relations  $\{e_s, e_t\} \subset E$ . Observe that no one pair of the linear relations  $\{e_1, e_2\}, \{e_1, e_4\}, \{e_1, e_5\}, \{e_2, e_3\}, \{e_2, e_5\}$  is possible if  $i > j > k > 0$ . The possible pairs are  $\{e_1, e_3\}, \{e_2, e_4\}, \{e_3, e_4\}, \{e_3, e_5\}, \{e_4, e_5\}$ . Consider the pair  $\{e_1, e_3\}$  as a system of two linear equations in three integer variables  $i, j, k$ . All positive integer solutions of this system are vectors  $(i, j, k) = (4u, 2u, u), u \in \mathbb{Z}, u > 0$ . In this case, the form of the polynomial  $F$  with equal exponents  $v_3 = v_4, v_5 = v_6, v_8 = v_9, v_{10} = v_{11}$  is described in Case 7) of Lemma 2.3. Similarly, the integer solutions to the equations  $\{e_2, e_4\}$  are  $(i, j, k) = (4u, 3u, 2u), u \in \mathbb{Z}, u > 0$  and  $F$  takes the form given in Case 8). Observe that all the pairs of equations from the system  $\{e_3, e_4, e_5\}$  are equivalent and have the solution  $(i, j, k) = (3u, 2u, u), u \in \mathbb{Z}, u > 0$ . Hence, any two of the three relations  $\{e_3, e_4, e_5\}$  imply the third one. This situation is depicted in Case 9). It remains to show that there are no other cases where three or more linear relations  $e_s \in E$  hold. Indeed, in such case three different pairs of linear relations, other than all 3 possible pairs from the set  $\{e_3, e_4, e_5\}$  must be satisfied. There would be at least one of pairs  $\{e_1, e_3\}, \{e_2, e_4\}$  and one pair from the set  $\{e_3, e_4, e_5\}$ . This is impossible, since all the intersections of the sets of integer triples  $(i, j, k)$  which satisfy such linear relations

$$\{(4u, 2u, u), u \in \mathbb{Z}, u > 0\}, \quad \{(4u, 3u, 2u), u \in \mathbb{Z}, u > 0\},$$

$$\{(3u, 2u, u), u \in \mathbb{Z}, u > 0\}$$

are empty. □

SKETCH OF THE PROOF OF THEOREM 2.1 Before proceed to prove Theorem 2.1, we give the sketch of the proof. First, we show that any primitive quadrinomial  $P(x) = x^i + x^j + x^k + 4$  in question whose exponents  $(i, j, k)$  satisfy a certain linear relation is precisely the quadrinomial  $x^4 + x^3 + x^2 + 4$ . Secondly, we consider the polynomial  $G(x) = Q(-x)Q^*(x)$ , where  $Q$  is the polynomial from the factorization  $P(x^l) = \pm Q(x)Q(-x)$ . This factorization is a consequence of Lemma 2.2. We determine the form of the polynomial  $G$  using reduction modulo 2 and the identity  $\|P\| = \|G\|$  for the Euclidean norms of  $P$  and  $G$ . Recall that the Euclidean norm  $\|f\|$  of the polynomial  $f(x) = \sum_{j=1}^{\deg f} a_j x^j \in \mathbb{Z}[x]$  is defined as  $\|f\| = (\sum_{j=1}^{\deg f} a_j^2)^{1/2}$ . Following [7], we refer to the equality  $\|P\| = \|G\|$  as the *identity of Ljunggren*. Thirdly, we use the expression  $GG^*(x) = PP^*(x^l)$  and compare  $PP^*(x^l)$  from Lemma 2.3 to  $GG^*(x)$ . We establish that the case  $x^4 + x^3 + x^2 + 4$  is the only one possible.

PROOF OF THEOREM 2.1. First suppose that the exponents  $i, j, k$  of  $P(x) = x^i + x^j + x^k + 4$  satisfy linear relations  $i = 2k$  and  $i + k = 2j$ . Then  $(i, j, k) = (4u, 3u, 2u)$  for some positive integer  $u$  so  $P(x) = x^{4u} + x^{3u} + x^{2u} + 4$ , which is primitive for  $u = 1$ . A simple computation shows that the polynomial  $P_1(x) = x^4 + x^3 + x^2 + 4$  is irreducible, and  $P_1(x^2) = (x^4 - x^3 + x^2 - 2x + 2)(x^4 + x^3 + x^2 + 2x + 2)$ . For even integers  $l = 2g > 0$  the polynomial  $P_1(x^l)$  splits in  $\mathbb{Z}[x]$  into  $P_1(x^l) = (x^{4g} - x^{3g} + x^{2g} - 2x^g + 2)(x^{4g} + x^{3g} + x^{2g} + 2x^g + 2)$ . By Lemma 2.2, both factors are irreducible. By Lemma 2.2,  $P_1(x^l)$  is irreducible for odd exponents  $l$ . Below we shall show that this case is the only possible. Note that the linear relations  $i = 2k, i + k = 2j$  appear in the Case 8) of Lemma 2.3. Hence we have to prove that every quadrinomial  $P(x)$  in the question of Walsh satisfies  $P(x^l)P^*(x^l) = F(x^l)$ , where  $F$  is a polynomial in Case 8) of Lemma (2.3).

Let  $P(x) = x^i + x^j + x^k + 4$  be an irreducible polynomial and  $l > 0$  be an integer such that  $P(x^l)$  splits in  $\mathbb{Z}[x]$ , while  $P(x^m)$  is irreducible for any integer  $m, 1 \leq m < l$  dividing the exponent  $l$ . By Lemma 2.2,  $l = 2g, g \in \mathbb{Z}$ , and  $P(x^l) = \pm Q(x)Q(-x)$ . Without loss of generality, we may assume that  $Q(x)$  is monic. Then  $P(x^l) = (-1)^{ig}Q(x)Q(-x)$ . The polynomials  $Q(x)$  and  $Q(-x)$  have equal constant terms  $\pm 2$ , hence  $P(x) = Q(x)Q(-x)$ . This implies that the degree  $ig$  is even. Also,  $Q(0) = 2$ . Otherwise  $Q(x)$  has a positive real root which is impossible, since  $P(x) > 0$  if  $x > 0$ . Consider the reduction of  $P(x^{2g})$  modulo 2:

$$P(x^g)^2 \equiv P(x^{2g}) = Q(x)Q(-x) \equiv Q(x)^2 \pmod{2}.$$

Hence  $Q(x) \equiv P(x^g) \equiv x^{ig} + x^{jg} + x^{kg} \pmod{2}$ . Let  $G$  be the product  $G(x) = Q(-x)Q^*(x)$  of degree  $2ig$ . Note that the polynomial  $G$  satisfies the identity  $x^{2ig}G(1/x) = (-1)^{ig}G(-x)$ . Since  $ig$  is even,  $G^*(x) = G(-x)$ . Hence the integer coefficients of  $G(x) = \sum_{s=0}^{2ig} b_s x^s$  which are symmetric with the

respect of middle term are equal in modulus, more precisely,

$$(4.1) \quad b_s = (-1)^s b_{2ig-s}, 0 \leq s \leq 2ig.$$

Reduce  $G(x)$  modulo 2:

$$(4.2) \quad \begin{aligned} G(x) &= Q^*(x)Q(-x) \equiv Q^*(x)Q(x) \equiv (x^{(i-k)g} + x^{(i-j)g} + 1)(x^{ig} + x^{jg} + x^{kg}) \\ &\equiv x^{(2i-k)g} + x^{(2i-j)g} + x^{(i+j-k)g} + x^{ig} + x^{(i-j+k)g} + x^{jg} + x^{kg} \pmod{2}. \end{aligned}$$

Note that in (4.2) the commuting of the operation  $*$  and reduction  $\pmod{2}$  is essentially used, which make sense since  $f^*(x) \pmod{2} = (f(x) \pmod{2})^*$  if and only if the leading coefficient of  $f \in \mathbb{Z}[x]$  is odd.

Since  $Q$  is monic,  $Q(0) = 2$ , the leading and constant coefficients of  $G$  are equal to 2. Since  $i > j > k > 0$ , the exponents in  $G$  modulo 2 satisfy the inequalities

$$(2i-k)g > (2i-j)g \geq (i+j-k)g > ig > (i-j+k)g \geq jg > kg,$$

provided  $i+k \geq 2j$  or

$$(2i-k)g > (i+j-k)g \geq (2i-j)g > ig > jg \geq (i-j+k)g > kg,$$

provided  $i+k \leq 2j$ . Hence the polynomial  $G(x)$  in (4.2) has 7 odd coefficients if  $i+k \neq 2j$ . If  $i+k = 2j$ ,  $G(x)$  modulo 2 takes the form

$$(4.3) \quad G(x) \equiv x^{(2i-k)g} + x^{ig} + x^{kg} \pmod{2},$$

with 3 odd coefficients. Observe that  $P(x^l)P^*(x^l) = G(x)G^*(x)$ . The equality holds since  $(Q^*)^* = Q$  which is true since  $Q(0) \neq 0$ . By the identity of Ljunggren,  $\|G\|^2 = \|P\|^2 = 1^2 + 1^2 + 1^2 + 4^2 = 19$ . The leading and constant coefficients of  $G$  are equal to 2, thus the sum of squares of coefficients  $b_s, 1 \leq s \leq 2ig-1$  is equal to 11. In addition, there must be precisely 3 or 7 odd coefficients by (4.2) and (4.3). All such possible sums of squares are

$$(4.4) \quad 11 = 3^2 + 1^2 + 1^2 = 2^2 + 2^2 + 1^2 + 1^2 + 1^2 = 2^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2$$

The absolute values of the coefficients of  $G$  are symmetric with respect to the middle term  $b_{ig} \equiv 1 \pmod{2}$ . Thus an integer which appears in the sum of squares above the odd number of times must be the absolute value of the middle coefficient  $b_{ig}$ . Hence the summands in the third sum in (4.4) cannot be the squares of coefficients of the polynomial  $G$ . This implies that  $G$  has 3 odd coefficients and the exponents  $i, j, k$  satisfy the relation  $i+k = 2j$ . Using the identities (4.1), (4.3), and (4.4) we deduce that  $G$  takes one of the forms:

$$(4.5) \quad G(x) = 2x^{2ig} + \varepsilon x^{(2i-k)g} + 3\delta x^{ig} + (-1)^{kg} \varepsilon x^{kg} + 2,$$

$$(4.6) \quad \begin{aligned} G(x) &= 2x^{2ig} + \varepsilon_1 x^{(2i-k)g} + 2\varepsilon_2 x^{t+ig} + \delta x^{ig} \\ &\quad + (-1)^t 2\varepsilon_2 x^{ig-t} + (-1)^{kg} \varepsilon_1 x^{kg} + 2, \end{aligned}$$

the coefficients  $\varepsilon, \varepsilon_1, \varepsilon_2, \delta$  are all equal to  $-1$  or  $1$  and  $t$  is an integer  $0 < t < ig$ . Also, note that the terms  $x^{t+ig}, x^{ig-t}$  do not coincide with any other term



of the polynomial  $G$  in (4.6) by (4.4). We shall determine the coefficients  $\varepsilon, \varepsilon_1, \varepsilon_2, \delta$ . Observe that  $G(1) = Q(1)Q(-1) = P(1) = 7$ . In (4.5), this is possible if and only if  $\delta = 1$  and  $\varepsilon + (-1)^{kg}\varepsilon = 0$ , hence the exponent  $kg$  is odd in (4.5). Moreover, we may assume that  $\varepsilon = 1$ . Otherwise, replace  $x$  by  $-x$ . Thus  $G$  in (4.5) takes the form

$$(i) \quad 2x^{2ig} + x^{(2i-k)g} + 3x^{ig} - x^{kg} + 2, \quad 2 \nmid kg.$$

Consider  $G$  in (4.6). There are three cases where  $G(x)$  takes the value  $G(1) = 7$ :

- (a)  $2 \mid kg, 2 \nmid t, \varepsilon_1 = 1, \delta = 1$ . Assume  $\varepsilon_2 = 1$ , otherwise change  $x$  to  $-x$ ;
- (b)  $2 \mid t, 2 \nmid kg, \varepsilon_2 = 1, \delta = -1$ . Assume  $\varepsilon_1 = 1$ , otherwise change  $x$  to  $-x$ ;
- (c)  $2 \mid kg, 2 \mid t, \varepsilon_1 = -1, \varepsilon_2 = 1, \delta = 1$ .

The polynomial  $G$  in Cases (a),(b),(c) takes the forms (ii), (iii), (iv) below, respectively.

- (ii)  $2x^{2ig} + x^{(2i-k)g} + 2x^{t+ig} + x^{ig} - 2x^{ig-t} + x^{kg} + 2,$
- (iii)  $2x^{2ig} + x^{(2i-k)g} + 2x^{t+ig} - x^{ig} + 2x^{ig-t} - x^{kg} + 2,$
- (iv)  $2x^{2ig} - x^{(2i-k)g} + 2x^{t+ig} + x^{ig} + 2x^{ig-t} - x^{kg} + 2.$

In each case (i), (ii), (iii), (iv) we check if  $G(x)G^*(x) = P(x^{2g})P^*(x^{2g}) = F(x^{2g})$ , where  $F(x)$  is one of the polynomials in Lemma 2.3. Since  $i+k = 2j$ , it suffices to check Cases 5), 8), 9) in Lemma 2.3. First, assume that  $G$  takes the form (i). Then

$$G(x)G^*(x) = 4x^{4ig} + 12x^{3ig} - x^{(4i-2k)g} + 19x^{2ig} - x^{2kg} + 12x^{ig} + 4$$

has 7 non-zero coefficients, hence it must coincide with  $F(x^{2g})$  in Case 9) of Lemma 2.3. This is impossible, since the coefficients of  $F$  are different from the coefficients of  $GG^*$ . Next, assume that  $G$  takes the form (iii). Compute the product  $GG^*$  modulo 4:

$$G(x)G^*(x) \equiv -x^{(4i-2k)g} - x^{2ig} - x^{2kg} \pmod{4}.$$

None of the polynomials  $F$  in Lemma 2.3 satisfy  $F(x^{2g}) \equiv G(x)G^*(x) \pmod{4}$ . Thus the form (iii) is impossible.

Assume that  $G$  takes the form (iv). The integer  $2ig$  is largest exponent in  $G$ . Let  $v$  be the second largest exponent in  $G$ . Clearly,  $v = (2i-k)g$  or  $v = t+ig$ . Observe that  $2ig+v > s+r$  if at least one inequality  $r \leq 2ig, s \leq v$  is strict. Hence the second largest exponent in  $GG^*$  is  $2ig+v$ . Thus the first two terms of  $GG^*$  are  $x^{4ig} - 4x^{(4i-k)g}$  if  $(2i-k)g > t+ig$  or  $x^{4ig} + 8x^{3ig+t}$  if  $(2i-k)g < t+ig$ . Such terms do not occur in any polynomial in Lemma 2.3. Hence we reject the form (iv).

This implies that  $G$  takes the form (ii). The product  $GG^*$  is

$$\begin{aligned} G(x)G^*(x) &= 4x^{4ig} + 4x^{(4i-k)g} - 4x^{2t+2ig} + x^{(4i-2k)g} + 4x^{3ig} + 2x^{(3i-k)g} \\ &\quad + 4x^{(2i+k)g} + 19x^{2ig} + 4x^{(2i-k)g} + 2x^{(i+k)g} + 4x^{ig} + x^{2kg} \\ &\quad - 4x^{2ig-2t} + 4x^{kg} + 4. \end{aligned}$$

Thus  $GG^*$  coincides with the polynomial  $F(x^{2g})$  in Case 5), 8) or 9) of Lemma 2.3, since  $i+k=2j$  in (ii). Since  $i > k > 0$ , the integer  $4i-k$  is strictly greater than  $3i, 4i-2k, 3i-k, 2i+k$ . If  $(4i-k)g > 2ig+2t$ , then the second leading term of  $GG^*$  is  $4x^{(4i-k)g}$ . This leads directly to the Case 8) of the Lemma 2.3. Indeed, only polynomials  $F(x)$  in Case 5) or Case 8) have terms with coefficients equal to 4 which are not leading nor constant terms. The term with the second highest exponent  $4x^{(4i-k)g}$  in  $GG^*$  must coincide with the term  $4x^{2(i+j)g}$  or  $4x^{2(i+k)g}$  in  $F(x^{2g})$  in Case 5). Since  $j > k$ , the exponent  $2(i+j)g$  is greater than  $2(i+k)g$ . Thus  $(4i-k)g = 2(i+j)g$ , so  $4i-k = 2i+2j$ . Together with the identity  $i+k=2j$  in Case 5) the linear relation  $4i-k = 2i+2j$  implies  $i = 2k$ , which implies Case 8) of Lemma 2.3.

Hence we may assume that  $(4i-k)g \leq 2ig+2t$ . If the inequality is strict, then the second leading term of  $GG^*$  is  $-4x^{2ig+2t}$ . However, the polynomials in Lemma 2.3 have no negative terms. Hence  $(4i-k)g = 2ig+2t$ . Thus

$$\begin{aligned} GG^* &= 4x^{4ig} + x^{(4i-2k)g} + 4x^{3ig} + 2x^{(3i-k)g} + 4x^{(2i+k)g} \\ &\quad + 19x^{2ig} + 4x^{(2i-k)g} + 2x^{(i+k)g} + 4x^{ig} + x^{2kg} + 4. \end{aligned}$$

Let  $F(x)$  be the polynomial in Case 5) of Lemma 2.3. Replace  $x$  by  $x^{2g}$  and use the identity  $2j = i+k$ . The resulting polynomial is

$$\begin{aligned} F(x^{2g}) &= 4x^{4ig} + x^{(4i-2k)g} + 2x^{(4i-2j)g} + 4x^{(2i+2j)g} + 4x^{(2i+2k)g} \\ &\quad + 19x^{2ig} + 4x^{(2i-2k)g} + 4x^{(2i-2j)g} + 2x^{2jg} + x^{2kg} + 4 \\ &= 4x^{4ig} + x^{(4i-2k)g} + 2x^{(3i-k)g} + 4x^{(3i+k)g} + 4x^{(2i+2k)g} \\ &\quad + 19x^{2ig} + 4x^{(2i-2k)g} + 4x^{(i-k)g} + 2x^{(i+k)g} + x^{2kg} + 4. \end{aligned}$$

The difference  $F(x^{2g}) - GG^* = 4x^{(3i+k)g} + 4x^{(2i+2k)g} + 4x^{(2i-2k)g} + 4x^{(i-k)g} - 4x^{3ig} - 4x^{(2i+k)g} - 4x^{(2i-k)g} - 4x^{ig} \neq 0$ , since the exponent  $(3i+k)g$  is the larger than other exponents in  $F(x^{2g}) - GG^*$ . Thus  $GG^*$  does not coincide with a polynomial given in Case 5) of Lemma 2.3.

Let  $F(x)$  be the polynomial in Case 9) of Lemma 2.3. The equations  $j = 2k, 2j = i+k, i = j+k$  imply  $(i, j, k) = (3u, 2u, u), u \in \mathbb{Z}, u > 0$ . Hence

$$\begin{aligned} GG^* &= 4x^{12ug} + x^{10ug} + 4x^{9ug} + 2x^{8ug} + 4x^{7g} + 19x^{6ug} + 4x^{5ug} \\ &\quad + 2x^{4ug} + 4x^{3ug} + x^{2ug} + 4. \end{aligned}$$

Also,  $F(x^{2g}) = 4x^{12ug} + 5x^{10ug} + 6x^{8ug} + 19x^{6ug} + 6x^{4ug} + 5x^{2ug} + 4$  and  $F(x^{2g}) \neq GG^*$ , so Case 9) is impossible. Hence we conclude that Case 8) is the only one possible. This completes the proof.  $\square$

## ACKNOWLEDGEMENTS.

We thank A. Schinzel for the remarks concerning the paper [5] and his note on the total number of irreducible factors of quadrinomials  $x^i + x^j + x^k + n$ . We are grateful to the referees for useful comments and corrections.

## REFERENCES

- [1] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*, In: Number theory in progress (Zakopane-Koscielisko, 1997), de Gruyter, Berlin, **1** (1999), 143–163.
- [2] M. Filaseta, A. Granville and A. Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials*, In: Number Theory and Polynomials (ed. James McKee and Chris Smyth), LMS Lecture Note Series **352**, Cambridge Univ. Press, 2008, 155–176.
- [3] M. Filaseta, F. Luca, P. Stănică and R. G. Underwood, *Two Diophantine approaches to the irreducibility of certain trinomials*, Acta Arith. **128** (2007), 149–156.
- [4] M. Filaseta and I. Solan, *An extension of a theorem of Ljunggren*, Math. Scand. **84** (1999), 5–10.
- [5] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. **21** (1972), 153–171.
- [6] A. T. Jonassen, *On the irreducibility of the trinomials  $x^m \pm x^n \pm 4$* , Math. Scand. **21** (1967), 177–189.
- [7] W. Ljunggren, *On the reducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.
- [8] W. H. Mills, *The factorization of certain quadrinomials*, Math. Scand. **57** (1985), 44–50.
- [9] G. Myerson, *Western Number Theory Problems, 17–19 Dec 2007*, 6. Available online at <http://www.math.colostate.edu/~achter/wntc/problems/problems2007.pdf>
- [10] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.
- [11] A. Schinzel, *Reducibility of lacunary polynomials. I*, Acta Arith. **16** (1969/1970), 123–159.
- [12] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its applications **77**, Cambridge Univ. Press, 2000.
- [13] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.

J. Jankauskas  
 Department of Mathematics and Informatics  
 Vilnius University  
 Naugarduko 24, Vilnius LT-03225  
 Lithuania  
 E-mail: [jonas.jankauskas@gmail.com](mailto:jonas.jankauskas@gmail.com)

Received: 10.6.2009.

Revised: 19.6.2009.