NUMBER THEORY WEEK 2017
BANACH CENTER PUBLICATIONS, VOLUME 118
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2019

COMPUTATIONALLY CLASSIFYING POLYNOMIALS WITH SMALL EUCLIDEAN NORM HAVING REDUCIBLE NON-RECIPROCAL PARTS

MICHAEL FILASETA

Mathematics Department, University of South Carolina
Columbia, SC 29208, USA
E-mail: filaseta@math.sc.edu

ROBERT MURPHY

Mathematics Department, University of Illinois
1409 W. Green Street, Urbana, IL 61801, USA
E-mail: murphyrf@illinois.edu

ANDREW VINCENT

Forest City Gear, 11715 Main Street, Roscoe, IL 61073, USA
E-mail: avincent@forestcitygear.com

Dedicated to Jerzy Kaczorowski
on the occasion of his 60th birthday

Abstract. Let $f(x)$ be a polynomial with integer coefficients. If either $f(x) = x^{\deg f} f(1/x)$ or $f(x) = -x^{\deg f} f(1/x)$, then $f(x)$ is called reciprocal. We refer to the non-reciprocal part of $f(x)$ as the polynomial $f(x)$ removed of each of its irreducible reciprocal factors in $\mathbb{Z}[x]$ with a positive leading coefficient. In 1970, Schinzel proved that for a given collection of $r+1$ integers $a_0, \dots, a_r$ it is possible to classify the positive integers $d_1, \dots, d_r$ for which the non-reciprocal part of $a_0 + a_1 x^{d_1} + \dots + a_r x^{d_r}$ is reducible. Specific classification results have been given by Selmer, Tverberg, Ljunggren, Mills, Schinzel, Solan, and the first author. We extend an approach of the first author to complete a similar classification for all polynomials with norm $\le 5^{1/2}$ and some additional sparse polynomials.

2010 *Mathematics Subject Classification*: Primary 11Y05; Secondary 11C08.
Key words and phrases: polynomial factorization, non-reciprocal.
The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc118-15

1. Introduction. The *Euclidean norm* of a polynomial $g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{R}[x]$ is

$$\|g\| = \sqrt{b_0^2 + b_1^2 + \ldots + b_r^2}\,.$$

The *reciprocal*, denoted $\tilde{f}(x)$, of a polynomial $f(x) \in \mathbb{C}[x]$ with $f(x) \not\equiv 0$ is defined to be $\tilde{f}(x) = x^{\deg f} f(1/x)$. If $f = \pm\tilde{f}$, then f is called *reciprocal*. For $f(x) \in \mathbb{Z}[x]$, we refer to the *non-reciprocal part of* $f(x)$ as the polynomial $f(x)$ removed of its irreducible reciprocal factors in $\mathbb{Z}[x]$ where each such factor is chosen with a positive leading coefficient. For example, the non-reciprocal part of $3(-x+1)x(x^2+2)$ is $-x(x^2+2)$. Analogously, we refer to the *non-cyclotomic part of a non-zero* $f(x) \in \mathbb{Z}[x]$ as $f(x)$ removed of its cyclotomic factors.

In 1960, generalizing a 1956 result of Selmer [10], Ljunggren [4] and Tverberg [11] established independently that if a and b are integers with $a > b > 0$ and $\varepsilon_j \in \{1, -1\}$ for $j \in \{1, 2\}$, then the non-cyclotomic part of $x^a + \varepsilon_1 x^b + \varepsilon_2$ is irreducible or identically 1. Ljunggren [4] considered the analogous arguments for quadrinomials. He overlooked certain cases in his argument, and later, in 1985, Mills [5] revised Ljunggren's arguments to take these cases into consideration. Thus, Mills classified those quadrinomials $x^a + \varepsilon_1 x^b + \varepsilon_2 x^c + \varepsilon_3$, $a > b > c > 0$ and $\varepsilon_j \in \{-1, 1\}$ for $j \in \{1, 2, 3\}$, for which the non-cyclotomic part is reducible. As we have an interest in giving classifications of the polynomials in $\mathbb{Z}[x]$ with small Euclidean norm that have reducible non-cyclotomic or non-reciprocal parts, we will elaborate on his result later in this paper, after some terminology on variations of factorizations has been defined.

In 1999, Solan and the first author [2] showed that if a, b, c, and d are positive integers satisfying $a > b > c > d$, then the non-reciprocal part of $f(x) = x^a + x^b + x^c + x^d + 1$ is irreducible or identically 1. The same year, the first author [1] classified those polynomials $x^a + x^b + x^c + x^d + x^e + 1$, $a > b > c > d > e > 0$, for which the non-reciprocal part is reducible. We elaborate on this result momentarily.

In 1970, Schinzel [7] gave more general results which showed that any theorem similar to those referenced above can be effectively established. The following can be viewed as a consequence of this work.

THEOREM 1.1. *Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let $F(x_1, \ldots, x_r) = a_r x_r + \ldots + a_1 x_1 + a_0$. Then there exist two finite computable sets R and S of matrices satisfying*:

(i) *Each matrix in R or S is an $r \times \rho$ matrix with integer entries and of rank ρ, depending on the matrix, with $\rho \le r$.*

(ii) *For every set of positive integers $d_1, \ldots, d_r$ with $d_1 < d_2 < \ldots < d_r$, the non-reciprocal part of $F(x^{d_1}, \ldots, x^{d_r})$ is reducible if and only if there is an $r \times \rho$ matrix $N = (v_{ij})$ in R and integers $v_1, \ldots, v_\rho$ satisfying*

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $r \times \rho'$ matrix M in S with $\rho' < \rho$ and no integers $v'_1, \ldots, v'_{\rho'}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

Schinzel's work in [7] does not specifically state Theorem 1.1. We will elaborate on the argument for Theorem 1.1 based on [7] in the last section of this paper; the authors thank Andrzej Schinzel for providing us with the details of this argument. The argument is similar to one given in [8] (also, see [9]), where the non-cyclotomic parts of polynomials were considered but with the added condition that the polynomials considered are non-reciprocal. Theorem 1.1 should also be compared to Theorem 74 of [9]. Here, one finds a similar result, in a more general context, to Theorem 1.1. However, we were not able to deduce from Theorem 74 of [9] the existence of the set S described in Theorem 1.1.

Schinzel's results are quite general. They imply that for a given collection of $r+1$ non-zero integers $a_0, a_1, \ldots, a_r$, it is possible to classify the positive integers $d_1, d_2, \ldots, d_r$ with $d_1 < d_2 < \ldots < d_r$ for which the non-reciprocal part of the polynomial

$$a_0 + a_1 x^{d_1} + a_2 x^{d_2} + \ldots + a_r x^{d_r}$$

is reducible (or irreducible).

The work of the first author in [1] can be viewed as another demonstration of this result. He describes a general approach for establishing whether the non-reciprocal part of a given $f(x) \in \mathbb{Z}[x]$ is irreducible. He also describes how to extend the approach to an algorithm for classifying polynomials with variable exponents having reducible non-reciprocal part. The purpose of the current work is to provide some computational results obtained through an implementation of the algorithm. In particular, noting that for $a \in \mathbb{Z}^+$ the polynomial $x^a \pm 2$ is irreducible, the results in this paper combined with the prior work stated give a complete characterization of the polynomials in $\mathbb{Z}[x]$ with norm $\leq \sqrt{5}$ having reducible non-reciprocal part. In addition, our methods show that for a and b in $\mathbb{Z}^+$ with $a > b$ the non-reciprocal part of $x^a \pm x^b \pm 2$ is irreducible. Combining the results in this paper, the prior results stated here and the computations given in [12], there is consequently a similar classification for polynomials in $\mathbb{Z}[x]$ with norm $\leq \sqrt{6}$ having reducible non-reciprocal part.

The following definition can be found in [1]. Suppose that we have $f(x) = u(x)v(x)$, where $u(x)$ and $v(x)$ are polynomials in $\mathbb{Z}[x]$. Then $\pm u(x)\tilde{v}(x)$ is called a variation of $f(x)$ (or a polynomial obtained from a variation of $f(x)$). Observe that we allow the possibility that $u(x) = 1$ or $v(x) = 1$; in particular, $f(x)$ itself is a variation of $f(x)$, albeit not much of a variation.

With the above notion, we can easily state the results of Mills [5] and the first author [1] alluded to earlier. Let a, b and c be integers with $a > b > c > 0$, and let $\varepsilon_j \in \{1, -1\}$ for $j \in \{1, 2, 3\}$. Mills [5] established that the non-cyclotomic part of $f(x) = x^a + \varepsilon_1 x^b + \varepsilon_2 x^c + \varepsilon_3$ is irreducible or identically 1 unless $f(x)$ is a variation of

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

where $k \in \mathbb{Z}^+$. Now, let a, b, c, d and e be integers with $a > b > c > d > e > 0$. The first author [1] showed that the non-reciprocal part of $f(x) = x^a + x^b + x^c + x^d + x^e + 1$ is irreducible or identically 1 unless $f(x)$ is a variation of

$$x^{5s+3t} + x^{4s+2t} + x^{2s+2t} + x^t + x^s + 1 = (x^{3s+2t} - x^{s+t} + x^t + 1)(x^{2s+t} + x^s + 1),$$

where s and t denote arbitrary distinct positive integers.

Of related interest is the following result of Schinzel [6]. Let a and b be integers with $a > b > 0$. Then the non-cyclotomic part of $f(x) = x^a - 2x^b + 1$ is irreducible or identically 1 unless $f(x)$ is a variation of

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

where $k \in \mathbb{Z}^+$. Our methods here allow us to further show that with $f(x) = x^a \pm 2x^b \pm 1$, the only other cases where the non-cyclotomic part of $f(x)$ is reducible is for $f(x)$ a variation of one of

$$x^{7k} + 2x^{2k} - 1 = (x^k + 1)(x^{3k} - x^{2k} + 1)(x^{3k} + x^k - 1)$$
$$x^{7k} + 2x^{3k} + 1 = (x^{3k} - x^{2k} + 1)(x^{4k} + x^{3k} + x^{2k} + 1)$$

and

$$x^{7k} + 2x^{3k} - 1 = (x^{3k} + x^{2k} - 1)(x^{4k} - x^{3k} + x^{2k} + 1),$$

where $k \in \mathbb{Z}^+$. The first of these is related to Schinzel's result by replacing x^k with $-x^k$, and the third is related to the second by the same replacement. In a moment we will refer to this (in more generality) as a second type of variation.

In order to present the main results of this paper, we now describe some related terminology. Suppose $F(X,Y) = U(X,Y)V(X,Y)$, where $U(X,Y)$ and $V(X,Y)$ are polynomials in $\mathbb{Z}[X,Y]$. Suppose also that a and b are nonnegative integers such that the coefficient of X^aY^b in $V(X,Y)$ is non-zero and $X^aY^bV(1/X,1/Y) \in \mathbb{Z}[X,Y]$. Then

$$U(X,Y)X^aY^bV(1/X,1/Y)$$

is called a type I variation of $F(X,Y)$, and we will say the polynomials

$$U(X,Y)X^aY^bV(1/X,1/Y) \quad \text{and} \quad -U(X,Y)X^aY^bV(1/X,1/Y)$$

are polynomials obtained from a type I variation of $F(X,Y)$. Observe that in the case $F(X,Y) \in \mathbb{Z}[X]$, polynomials obtained from type I variations coincide precisely with polynomials obtained from variations as described above. Now, for any polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$, $F(X,-Y)$ (or $F(-X,Y)$) is called a type II variation of $F(X,Y)$, and we will say the polynomials $F(X,-Y)$ and $-F(X,-Y)$ (as well as $F(-X,Y)$ and $-F(-X,Y)$) are polynomials obtained from a type II variation of $F(X,Y)$. We then say that $G(X,Y) \in \mathbb{Z}[X,Y]$ is a modification of $F(X,Y) \in \mathbb{Z}[X,Y]$ if there exists a nonnegative integer k and polynomials $H_0(X,Y), H_1(X,Y), \dots, H_k(X,Y)$ in $\mathbb{Z}[X,Y]$ such that $G(X,Y) = H_k(X,Y)$, $F(X,Y) = H_0(X,Y)$, and we have that for all $i \in \{1,2,\dots,k\}$, either it is the case that $H_i(X,Y)$ is obtained from a type I variation of $H_{i-1}(X,Y)$ or it is the case that $H_i(X,Y)$ is obtained from a type II variation of $H_{i-1}(X,Y)$. Observe that if the polynomials in question have non-zero constant terms, the property that $G(X,Y)$ is a modification of $F(X,Y)$ is symmetric.

As an example, consider

$$F(X,Y) = (X^3Y + X^2Y + 1)(X^2Y - XY - 1) = X^5Y^2 - X^3Y^2 - X^3Y - XY - 1.$$

We obtain the polynomial

$$-(X^3Y + X^2Y + 1)(-X^2Y - X + 1) = X^5Y^2 + X^4Y^2 + X^4Y + X - 1$$

from a type I variation of $F(X,Y)$. We may then obtain the polynomial

$$-(-X^3Y - X^2Y + 1)(X^2Y - X + 1) = X^5Y^2 + X^4Y^2 - X^4Y + X - 1$$

from a type II variation of the previous polynomial. All three of these polynomials are modifications of $F(X,Y)$.

We can now state our computational results.

THEOREM 1.2. *Let $f(x) \in \mathbb{Z}[x]$, with $f(0) \neq 0$, have Euclidean norm $\|f\| = \sqrt{5}$. Then the non-reciprocal part of $f(x)$ is reducible if and only if there exist positive integers t and u such that $f(x)$ can be obtained by making the substitutions $X = x^t$ and $Y = x^u$ in a modification of one of the following*:

- $X^5Y^2 - X^3Y^2 - X^3Y - XY - 1 = (X^3Y + X^2Y + 1)(X^2Y - XY - 1)$
- $X^5Y^3 - X^3Y^2 - X^3Y - X - 1 = (X^3Y^2 + X^2Y + 1)(X^2Y - X - 1)$
- $X^{10} - X^7 - X^6 - X^4 - 1 = (X^3 - X - 1)(X^7 + X^5 + X^2 - X + 1)$
- $X^{11} - X^8 - X^6 - X^5 - 1 = (X^4 - X + 1)(X^7 - X^3 - X^2 - X - 1)$
- $X^9 - X^7 - X^6 - X + 1 = (X^3 + X^2 - 1)(X^6 - X^5 - X^2 + X - 1)$
- $X^8 - X^7 - X^4 + X^2 - 1 = (X^3 - X - 1)(X^5 - X^4 + X^3 - X + 1)$
- $X^{13} - X^{11} - X^9 - X^4 - 1 = (X^3 - X - 1)(X^{10} + X^7 - X^6 + X^5 + X^2 - X + 1)$
- $X^{11} - X^8 - X^6 - X + 1 = (X^3 + X^2 - 1)(X^8 - X^7 + X^6 - X^5 - X^2 + X - 1)$
- $X^{12} - X^7 - X^4 - X^2 + 1 = (X^3 + X^2 - 1)(X^9 - X^8 + X^7 - X^5 + X^4 - X^3 - 1)$
- $X^{10} - X^9 - X^6 + X^3 - 1 = (X^3 - X - 1)(X^7 - X^6 + X^5 - X^3 + X^2 - X + 1)$
- $X^{13} - X^8 - X^4 - X^3 + 1 = (X^5 + X^4 - X^2 - X - 1)(X^8 - X^7 + X^6 + X - 1)$
- $X^{10} - X^6 - X^5 + X^4 - 1 = (X^5 + X^4 - X^2 - X - 1)(X^5 - X^4 + X^3 - X + 1)$
- $X^{14} - X^9 - X^8 + X^7 - 1 = (X^7 - X^6 + X^5 - X^3 + X^2 - X + 1)(X^7 + X^6 - X^4 - X - 1)$.

We have obtained an analogous result for polynomials of Euclidean norm $\sqrt{6}$, but the list, consisting of 128 cases, is not presented here. We direct the reader to the third author's dissertation [12] for the statement of this result.

We remark that for the previous result and for the result that follows it is in fact possible to enumerate a finite parametrized list containing precisely those polynomials satisfying the hypotheses with reducible non-reciprocal part. Specifically, such a complete list of polynomials, without reference to "modifications", can be obtained by recursively adding every type I and type II variation of a polynomial appearing on the list to the list until a list has been generated such that any type I or type II variation of a polynomial on the list is already on the list. We state the theorems in terms of "substitutions", "variations", and "modifications" purely for the sake of brevity.

The computations used to establish the above result provide the following simply stated corollary.

COROLLARY 1.3. *Let a, b, c, and d be integers satisfying $a > b > c > d > 0$. Then the non-reciprocal part of $f(x) = x^a - x^b + x^c - x^d + 1$ is irreducible or identically 1.*

As expected, it appears to be the case that acquiring classification results for polynomials of Euclidean norm $\sqrt{7}$ requires a great deal more time and space than for those of norm less than or equal to $\sqrt{6}$. We were, however, able to establish the following.

THEOREM 1.4. *Let a, b, c, d, e, and f be integers with $a > b > c > d > e > f > 0$. Then the non-reciprocal part of $g(x) = x^a + x^b + x^c + x^d + x^e + x^f + 1$ is reducible if and only if one of the following holds*:

(i) *There exist positive integers t and u such that $g(x)$ can be obtained by making the substitutions $X = x^t$ and $Y = x^u$ in a modification of one of the following*:

- $X^{12}+X^{11}+X^7+X^5+X^4+X^2+1 = (X^7+X^6+X^5+X^4+X^3+X^2+1)(X^5-X^3+1)$
- $X^{17} + X^{12} + X^9 + X^7 + X^6 + X^2 + 1 =$
  $(X^6 - X^4 + 1)(X^{11} + X^9 + X^7 + X^6 + X^4 + X^2 + 1)$
- $X^{19} + X^{12} + X^{11} + X^9 + X^6 + X^2 + 1 =$
  $(X^6 - X^4 + 1)(X^{13} + X^{11} + X^9 + X^6 + X^4 + X^2 + 1)$
- $X^7Y^6 + X^5Y^5 + X^4Y^3 + X^2Y + XY + X + 1 =$
  $(X^3Y^3 - X^2Y^2 + 1)(X^4Y^3 + X^3Y^2 + X^2Y^2 + X^2Y + XY + X + 1)$
- $X^8Y^7 + X^5Y^5 + X^5Y^4 + X^3Y^2 + X^2Y + XY + 1 =$
  $(X^5Y^4 + X^4Y^3 + X^3Y^2 + X^2Y^2 + X^2Y + XY + 1)(X^3Y^3 - X^2Y^2 + 1)$
- $X^{11}Y + X^7Y + X^6Y + X^6 + X^3 + X + 1 =$
  $(X^8Y + X^7Y + X^6Y + X^3 + X^2 + X + 1)(X^3 - X^2 + 1)$
- $X^{11}Y^{10} + X^7Y^6 + X^6Y^6 + X^6Y^5 + X^3Y^3 + XY + 1 =$
  $(X^8Y^7 + X^7Y^6 + X^6Y^5 + X^3Y^3 + X^2Y^2 + XY + 1)(X^3Y^3 - X^2Y^2 + 1)$
- $X^{15} + X^{11} + X^9 + X^4 + X^3 + X + 1 =$
  $(X^{12} + X^{11} + X^{10} - X^7 + X^4 + X^3 + X^2 + 1)(X^3 - X^2 + 1)$
- $X^{15} + X^{13} + X^8 + X^7 + X^6 + X^3 + 1 =$
  $(X^7 - X^6 + X^5 - X^4 + X^2 - X + 1)(X^8 + X^7 + X^6 + X^5 + X^4 + X + 1)$
- $X^{16} + X^{13} + X^{11} + X^5 + X^4 + X + 1 =$
  $(X^9 - X^7 + X^4 - X^2 + 1)(X^7 + X^5 + X^4 + X^3 + X^2 + X + 1)$
- $X^{16} + X^{13} + X^{11} + X^{10} + X^5 + X + 1 =$
  $(X^7 - X^3 + 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)(X^3 - X^2 + 1)$
- $X^{17} + X^{12} + X^{11} + X^7 + X^4 + X^2 + 1 = (X^8 + X^7 + X^4 + X^3 + X^2 + X + 1)$
  $(X^9 - X^8 + X^7 - X^6 + X^4 - X^3 + X^2 - X + 1)$.

(ii) *The polynomial $g(x)$ is a variation of one of the following*:

- $x^{6t+6u} + x^{6t+5u} + x^{5t+5u} + x^{5t+4u} + x^{3t+3u} + x^t + 1 =$
  $(x^{3t+3u} - x^{t+u} + 1)(x^{3t+3u} + x^{3t+2u} + x^{2t+2u} + x^{2t+u} + x^{t+u} + x^t + 1),\ u \neq t$
- $x^{6t} + x^{5t+u} + x^{3t} + x^{t+u} + x^u + x^t + 1 =$
  $(x^{3t} - x^{2t} + 1)(x^{3t} + x^{2t+u} + x^{2t} + x^{t+u} + x^u + x^t + 1),\ u \notin \{t/2, 4t\}$
- $x^{6t+u} + x^{3t+u} + x^{5t} + x^{t+u} + x^u + x^t + 1 =$
  $(x^{3t} - x^{2t} + 1)(x^{3t+u} + x^{2t+u} + x^{2t} + x^{t+u} + x^u + x^t + 1),\ u \neq 3t$

for some positive integers t and u satisfying the conditions given for the applicable entry.

We remark that the restrictions on u and t appearing in (ii) above correspond to the second set of matrices S given in Theorem 1.1. As is easily checked, for the u and t that are omitted from consideration, the second factor in the given factorization is a polynomial that only has cyclotomic and, hence, reciprocal factors. Thus, the non-reciprocal part of $g(x)$ is the non-reciprocal part of the first factor shown, which by the result of Ljunggren [4] and Tverberg [11] mentioned earlier, is irreducible. One can check that in fact the factors $x^{6t} - x^{2t} + 1$ and $x^{3t} - x^{2t} + 1$ arising here have no irreducible reciprocal factors, and hence are irreducible.

We further remark that our approach does not give us information about the non-cyclotomic part of a polynomial, at least when the number of terms exceeds 4. Indeed, we do not even know, for example, if the result of Solan and the first author discussed above remains true if "non-reciprocal" is replaced by "non-cyclotomic".

Our theorems were obtained by implementing the algorithm described in the next section using the computer algebra system Maple. The worksheet is currently available at `http://maple.math.sc.edu/maplenet/research/` under the heading "NONRECIPROCAL_REDUCIBLE_PROCEDURES" (where the differences in the two linked worksheets is insignificant). Included in this worksheet are routines capable of enumerating (in finite time and space) all parametrized polynomials corresponding to substitutions, variations, and modifications referenced above. We further note that the factorizations included in the statements of the above theorems were provided by the computer algebra system Sage.

2. The algorithm. We suppose that we are given a polynomial $f(x)$ with variable exponents. More precisely, we consider

$$f(x) = a_r x^{d_r} + \ldots + a_1 x^{d_1} + a_0,$$

where we view the a_j's as given integers and the d_j's as unknown integers with

$$0 < d_1 < \ldots < d_{r-1} < d_r. \tag{2.1}$$

We also suppose that each a_j is non-zero. We seek a description of the r-tuples $(d_1, \ldots, d_r)$ for which the non-reciprocal part of $f(x)$ is reducible. The strategy we proceed with is a slight modification of the one in [1].

We write

$$w(x) = b_s x^{k_s} + \ldots + b_1 x^{k_1} + b_0, \tag{2.2}$$

where we view the b_j's and k_j's as unknown integers with

$$0 < k_1 < \ldots < k_{s-1} < k_s = d_r. \tag{2.3}$$

We also suppose that each b_j is non-zero.

We make use of the following theorem, which is proven in [1] and based on the prior work of Ljunggren [4].

THEOREM 2.1. *Let $f(x) \in \mathbb{Z}[x]$ with $f(0) \neq 0$. The non-reciprocal part of $f(x)$ is reducible if and only if there exists $w(x)$ different from $f(x)$, $-f(x)$, $\tilde{f}(x)$, and $-\tilde{f}(x)$ such that*

$$f(x)\tilde{f}(x) = w(x)\tilde{w}(x). \tag{2.4}$$

We want to determine when a polynomial $w(x)$ exists satisfying (2.2), (2.3), and (2.4) that is different from $f(x)$, $-f(x)$, $\tilde{f}(x)$, and $-\tilde{f}(x)$. The idea is to solve the various systems of equations for $d_1, \dots, d_r, k_1, \dots, k_s$ obtained by comparing exponents on both sides of (2.4).

As noted in [1], we may restrict our attention to $(b_0, \dots, b_s)$ that satisfy $\|w\| = \|f\|$. For each such $(b_0, \dots, b_s)$, we explicitly compute both sides of equation (2.4). We then rearrange the terms so that each side of the equation has only positive coefficients and like terms from each side have been cancelled. This will be referred to as the simplified equation. Of significance here is that we are only interested in solution sets for $d_1, \dots, d_r, k_1, \dots, k_s$ for which every exponent appearing on one side of the simplified equation also appears on the other.

We go through each possibility for the coefficients $(b_0, \dots, b_s)$ appearing in $w(x)$. For each choice of coefficients for $w(x)$, we solve for the unknowns $d_1, \dots, d_r, k_1, \dots, k_s$ appearing in $f(x)$ and $w(x)$ using ideas from [1]. The approach is as follows.

(A) Use the ordering on the d_j and k_j to determine possibilities for the least exponent on the left and right sides of the simplified equation (this is done using Lemma 4 of [1]). Let L denote a set of possible least exponents on the left-hand side of the simplified equation, and let R denote a set of possible least exponents on the right-hand side. Thus, L and R are sets of linear combinations of the d_j and k_j.

(B) For each exponent e_L from L and e_R from R, consider $e_L = e_R$ and solve for a variable in this equation. We solve for the variable in this equation which appears first in the ordering $k_s, \dots, k_1, d_{r-1}, \dots, d_1$. If no solution exists, then we continue with a different choice of e_L from L and e_R from R until all possibilities have been considered.

(C) For a fixed equation $e_L = e_R$ from (B) having a solution, we substitute the solution from (B) into (2.4). If this substitution makes both sides of (2.4) the same, then we record this solution to (2.4) and backtrack to continue with considering another equation of the form $e_L = e_R$ in (B) until every possibility has been considered. If after the substitution both sides of (2.4) are not identical, then we form a new simplified equation and repeat part (A).

We note that there are different levels of (B) that arise, and backtracking to an earlier level is done until all cases of $e_L = e_R$ in (B) have been considered. In the computations used to establish Theorems 1.2 and 1.4, a solution set to this system corresponded to one or two of the d_j's being free variables that can be chosen arbitrarily (but in such a way that the full set of d_j's and k_j's are integers) and the remaining d_j's and k_j's being linear combinations of these free variables.

There is one more matter that we must address, namely whether a value of $w(x)$ obtained in the above procedure resulting in a solution to (2.4) satisfies $w(x) \in \{f(x), -f(x), \tilde{f}(x), -\tilde{f}(x)\}$. If so, then according to Theorem 2.1, we do not want to view this solution to (2.4) as producing an $f(x)$ with reducible non-reciprocal part. Suppose then that we have a choice of $f(x)$ and $w(x)$ satisfying (2.4) as above and want to check whether $w(x) \in \{f(x), -f(x), \tilde{f}(x), -\tilde{f}(x)\}$. At this point each of $f(x)$ and $w(x)$ has fixed coefficients and also exponents that depend on some fixed free variables.

Let $\mathcal{V}$ denote the set of free variables. For each $h(x) \in \{f(x), -f(x), \tilde{f}(x), -\tilde{f}(x)\}$, we proceed as follows to determine whether $w(x) = h(x)$ (or, more accurately, when). Recalling (2.1) and (2.3), we need only consider the case that $s = r$, that is that the number of terms in $w(x)$ equals the number of terms in $h(x)$. We form another system of equations by equating exponents in $w(x)$ with exponents in $h(x)$. If the corresponding coefficients of $w(x)$ and $h(x)$ do not agree, then $w(x) \neq h(x)$, and we proceed to a different $h(x) \in \{f(x), -f(x), \tilde{f}(x), -\tilde{f}(x)\}$. If the corresponding coefficients of $w(x)$ and $h(x)$ do agree, we solve the new system of equations in the free variables in $\mathcal{V}$ to obtain a new solution set in which a subset of $\mathcal{V}$ forms new free variables and the remaining elements of $\mathcal{V}$ are expressed in terms of them. Such a solution set gives a description of when the original solution set leads to a case where $w(x) = h(x)$. Note that the restrictions on t and u appearing in the second possibility in Theorem 1.4 arise from such cases.

We remark that in order to enumerate all possible cases above the authors utilized built-in functions available in Maple's combinatorics package along with algorithms described in [1] and [3].

3. Proof of Theorem 1.1. The statement of Theorem 1.1 first appears in [1] where it is indicated that it follows from [7]; though no details are given. Theorem 4 in [8] is a generalization of Theorem 1.1 where the role of non-reciprocal parts of polynomials is replaced by non-cyclotomic parts of polynomials, except that Theorem 4 in [8] has the added condition that the polynomial $F(x^{d_1}, \ldots, x^{d_r})$ is non-reciprocal (see the definition of "reciprocal" below). In this section, we provide a proof of Theorem 1.1 by imitating the proof of Theorem 4 in [8].

We begin with some notation, which follows the work of Schinzel [7, 8, 9]. We will use bold face capital Roman letters to denote integral matrices. Vectors will be denoted by bold face small Roman or Greek letters and are treated as matrices with one row. If $\boldsymbol{u}$ and $\boldsymbol{v}$ are vectors in $\mathbb{Z}^k$, then $\boldsymbol{uv}$ is the dot product of $\boldsymbol{u}$ and $\boldsymbol{v}$. The set of all integral matrices with l rows and k columns is denoted by $\mathfrak{M}_{l,k}(\mathbb{Z})$. For $\boldsymbol{A} = (a_{ij}) \in \mathfrak{M}_{l,k}(\mathbb{Z})$, we define

$$h(\boldsymbol{A}) = \max_{\substack{1 \le i \le l \\ 1 \le j \le k}} \{|a_{ij}|\}.$$

For $\boldsymbol{x} = [x_1, x_2, \ldots, x_k]$, $\boldsymbol{y} = [y_1, y_2, \ldots, y_l]$ and a polynomial $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$, we define

$$|F| = \max_{1 \le i \le k} \{\deg_{x_i} F\} \quad \text{and} \quad F(\boldsymbol{y}^{\boldsymbol{A}}) = F\Big(\prod_{i=1}^{l} y_i^{a_{i1}}, \ldots, \prod_{i=1}^{l} y_i^{a_{ik}}\Big).$$

If $\boldsymbol{n} = [n_1, \ldots, n_k] \in \mathbb{Z}^k$, then we write $F(x^{\boldsymbol{n}}) = F([x]^{\boldsymbol{n}}) = F(x^{n_1}, \ldots, x^{n_k})$. There is a unique term $ax_1^{e_1} \ldots x_k^{e_k}$ of F such that for every term $bx_1^{n_1} \ldots x_k^{n_k}$ of F, with $[n_1, \ldots, n_k] \neq [e_1, \ldots, e_k]$, the left-most non-zero component of the vector $[e_1, \ldots, e_k] - [n_1, \ldots, n_k]$ is positive. We refer to the term $ax_1^{e_1} \cdots x_k^{e_k}$ with this property as the leading term of F and to a as the leading coefficient of F. If $a = 1$, then we call F monic. We can write a Laurent polynomial $F \in \mathbb{Q}[x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_k, x_k^{-1}] \setminus \{0\}$ in the form

$$F = \sum_{i=0}^{m} a_i \, x_1^{\alpha_{i1}} \cdots x_k^{\alpha_{ik}},$$

where each a_i is non-zero and the $\boldsymbol{\alpha}_i = [\alpha_{i1}, \dots, \alpha_{ik}] \in \mathbb{Z}^k$ are distinct. We define

$$JF = \left(\prod_{j=1}^{k} x_j^{-\min_{0 \le i \le m} \{\alpha_{ij}\}} \right) F,$$

so $JF \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$ and JF is not divisible by x_i for every $i \in \{1, 2, \dots, k\}$. The *reciprocal of a polynomial* $F \in \mathbb{Q}[\boldsymbol{x}]$ is the polynomial

$$\widetilde{F} = JF(x_1^{-1}, x_2^{-1}, \dots, x_k^{-1}) \in \mathbb{Q}[\boldsymbol{x}].$$

If $F \in \mathbb{Q}[\boldsymbol{x}]$ and $F = UV$ where U and V are in $\mathbb{Q}[\boldsymbol{x}]$, then one sees that $\widetilde{F} = \widetilde{U}\widetilde{V}$. A polynomial $F \in \mathbb{Q}[\boldsymbol{x}]$ is called *reciprocal* if

$$F = \pm \widetilde{F},$$

and otherwise F is said to be *non-reciprocal*. We define LF to be JF deprived of all its monic irreducible reciprocal factors, where from here onward all factors refer to factors over $\mathbb{Q}$. The leading coefficient of LF is then equal to the leading coefficient of F. For a Laurent polynomial $F \in \mathbb{Q}[x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_k, x_k^{-1}]$, we have the relationship

$$LF = LJF.$$

The first lemma has been established in the case of a single variable in [2, the first paragraph in Section 2]. We give a detailed proof for the multi-variable case following the argument there.

LEMMA 3.1. *Let $k \in \mathbb{Z}^+$, and let $F \in \mathbb{Z}[\boldsymbol{x}]$ where $\boldsymbol{x} = [x_1, \dots, x_k]$. If LF is reducible, then there exist non-reciprocal F_1 and F_2 in $\mathbb{Q}[\boldsymbol{x}]$ such that $LF = F_1F_2$.*

Proof. Since LF is reducible, there are not necessarily distinct non-reciprocal irreducible polynomials U and V in $\mathbb{Z}[\boldsymbol{x}]$ dividing LF. Then the polynomials $\widetilde{U}$ and $\widetilde{V}$ are irreducible factors of the reciprocal of LF. If the reciprocal of U, that is $\widetilde{U}$, also divides LF, we split the irreducible factors of LF to form F_1 and F_2 with $LF = F_1F_2$ in such a way that $\widetilde{U}$ does not divide F_1 and U does not divide F_2. Then U divides F_1 and $\widetilde{U}$ does not divide F_1. The former implies $\widetilde{U}$ divides $\widetilde{F}_1$ so that, by unique factorization in $\mathbb{Q}[\boldsymbol{x}]$, we see that F_1 is non-reciprocal. Similarly, F_2 is non-reciprocal since U divides $\widetilde{F}_2$ but U does not divide F_2. A similar argument applies in the case that $\widetilde{V}$ divides LF. We consider now the case that both $\widetilde{U}$ and $\widetilde{V}$ are not divisors of LF in $\mathbb{Q}[\boldsymbol{x}]$. In this case, we split the irreducible factors of LF to form F_1 and F_2 with $LF = F_1F_2$ in such a way that U divides F_1 and V divides F_2. In this case, $\widetilde{U}$ is not a factor of F_1 since $\widetilde{U}$ is not a factor of F. Since $\widetilde{U}$ is a factor of $\widetilde{F}_1$, we deduce by unique factorization in $\mathbb{Q}[\boldsymbol{x}]$ that F_1 is non-reciprocal. Similarly, F_2 is non-reciprocal, completing the proof. ∎

We make use of Lemma 6, Lemma 10 and Lemma 12 in [7]. We state these as Lemma 3.2, Lemma 3.3 and Lemma 3.4, respectively, below, noting here that Lemma 3.4 is a much weakened form of Lemma 12 in [7] which suffices for our purposes.

LEMMA 3.2. *If an m-dimensional sublattice of the n-dimensional integral lattice $\mathbb{Z}^n$ contains m linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$, then it has a basis of the form*

$$\sum_{j=1}^{m} c_{1j}\boldsymbol{v}_j, \ldots, \sum_{j=1}^{m} c_{mj}\boldsymbol{v}_j,$$

where

$$0 \le c_{ij} < c_{jj} \le 1 \quad \text{for } i \ne j, \qquad \text{and} \qquad c_{ij} = 0 \quad \text{for } i < j.$$

LEMMA 3.3. *Let $\boldsymbol{v} = [v_1, v_2, \ldots, v_k] \in \mathbb{Z}^k$. Let $Q \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$, where $\boldsymbol{x} = [x_1, x_2, \ldots, x_k]$. If JQ is non-reciprocal and $LQ(x^{\boldsymbol{v}})$ is a constant, then there is a non-zero $\boldsymbol{\beta} \in \mathbb{Z}^k$ satisfying*

$$\boldsymbol{\beta}\boldsymbol{v} = 0 \qquad \text{and} \qquad h(\boldsymbol{\beta}) \le 2|Q|.$$

LEMMA 3.4. *For any polynomial $F(x_1, \ldots, x_k)$ and any integral vector $\boldsymbol{n} = [n_1, \ldots, n_k]$ such that $F(x^{\boldsymbol{n}}) \ne 0$, there exist computable constants $c_1 = c_1(F)$ and $c_2 = c_2(F)$ depending only on F, a matrix $\boldsymbol{M} = [\mu_{ij}] \in \mathfrak{M}_{k,k}(\mathbb{Z})$ of rank k and an integral vector $\boldsymbol{v} = [v_1, v_2, \ldots, v_k]$ such that*

$$0 \le \mu_{ij} < \mu_{jj} \le c_1 \quad \text{for } i \ne j, \qquad \mu_{ij} = 0 \quad \text{for } i < j, \qquad \boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}$$

and one of the following holds:

(i) $LF\big([y_1, \ldots, y_k]^{\boldsymbol{M}}\big)$ *and* $LF\big(x^{\boldsymbol{n}}\big)$ *are both reducible,*
(ii) $LF\big([y_1, \ldots, y_k]^{\boldsymbol{M}}\big)$ *and* $LF\big(x^{\boldsymbol{n}}\big)$ *are both irreducible,*
(iii) $LF\big([y_1, \ldots, y_k]^{\boldsymbol{M}}\big)$ *and* $LF\big(x^{\boldsymbol{n}}\big)$ *are both constant,*
(iv) *there is a non-zero $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma}\boldsymbol{n} = 0$ and $h(\boldsymbol{\gamma}) < c_2$.*

Of some interest to us is the following corollary to Lemma 3.2 which is a strengthening of Corollary 6 of Appendix E in [9] (though this strengthening is not required for establishing Theorem 3.6 below).

COROLLARY 3.5. *Let r be an integer > 1, and let $\boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z})$ having rank r. Let $\boldsymbol{\gamma} \ne \boldsymbol{0}$ be a vector in $\mathbb{Z}^r$. Then the vectors $\boldsymbol{v} \in \mathbb{Z}^r$ orthogonal to $\boldsymbol{\gamma}$ form a lattice $\boldsymbol{\Lambda}$ in $\mathbb{Z}^r$ which has a basis that, written in the form of rows of a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$, satisfies*

$$\operatorname{rank} \boldsymbol{B} = r - 1,$$

and

$$h(\boldsymbol{B}) \le h(\boldsymbol{\gamma}). \tag{3.1}$$

Proof. What requires some justification here is the inequality in (3.1). We write $\boldsymbol{\gamma} = [c_1, \ldots, c_r]$. Let $1 \le i_1 < i_2 < \ldots < i_u \le r$ be the complete list of i for which $c_i \ne 0$. To prove (3.1) using Lemma 3.2, we set

$$\mathcal{I} = \{1, 2, \ldots, r\} - \{i_u\}$$

and describe a set of vectors

$$\mathcal{V} = \{\boldsymbol{v}_i : i \in \mathcal{I}\} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i_u-1}, \boldsymbol{v}_{i_u+1}, \ldots, \boldsymbol{v}_r\}$$

that span the lattice $\boldsymbol{\Lambda}$. Write

$$\boldsymbol{v}_i = [v_1^{(i)}, \ldots, v_r^{(i)}] \quad \text{for } i \in \mathcal{I}.$$

For $i \in \mathcal{I} - \{i_1, i_2, \dots, i_{u-1}\}$, set

$$v_j^{(i)} = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i. \end{cases}$$

For $\kappa \in \{1, 2, \dots, u-1\}$, set

$$v_j^{(i_\kappa)} = \begin{cases} -(|c_{i_\kappa}|/c_{i_\kappa})\,|c_{i_{\kappa+1}}| & \text{if } j = i_\kappa \\ (|c_{i_{\kappa+1}}|/c_{i_{\kappa+1}})\,|c_{i_\kappa}| & \text{if } j = i_{\kappa+1} \\ 0 & \text{if } j \notin \{i_\kappa, i_{\kappa+1}\}. \end{cases}$$

To clarify, $v_{i_\kappa}^{(i_\kappa)}$ has the opposite sign as c_{i_κ} and has absolute value $|c_{i_{\kappa+1}}|$. Similarly, $v_{i_{\kappa+1}}^{(i_\kappa)}$ has the same sign as $c_{i_{\kappa+1}}$ and has absolute value $|c_{i_\kappa}|$. For $\kappa \in \{2, \dots, u-1\}$, the i_κth component of a $\boldsymbol{v} \in \mathcal{V}$ is non-zero precisely for $\boldsymbol{v}_{i_{\kappa-1}}$ and $\boldsymbol{v}_{i_\kappa}$ and these two components have opposite signs. For the remaining $i \notin \{i_2, i_3, \dots, i_{u-1}\}$, the ith component is non-zero in only one $\boldsymbol{v} \in \mathcal{V}$. In every case, the values of $|v_j^{(i)}|$ are bounded above by $h(\boldsymbol{\gamma})$. One checks that the $r-1$ vectors $\boldsymbol{v} \in \mathcal{V}$ are orthogonal to $\boldsymbol{\gamma}$ and that they are linearly independent. By Lemma 3.2, we can find a basis for $\boldsymbol{\Lambda}$ where each basis element is a linear combination of the $\boldsymbol{v} \in \mathcal{V}$ with coefficients between 0 and 1. Our construction of the v_j's ensures that each component of any such linear combination has absolute value at most the maximum of the absolute values of the components of the $\boldsymbol{v} \in \mathcal{V}$. Hence, the inequality in (3.1) follows. ∎

We prove now the following generalization of Theorem 1.1 to arbitrary F from $\mathbb{Z}[x_1, \dots, x_k] \setminus \{0\}$.

THEOREM 3.6. *Let $F \in \mathbb{Z}[x_1, \dots, x_k] \setminus \{0\}$. There exist two finite, effectively computable subsets R and S of $\bigcup_{r=1}^{k} \mathfrak{M}_{r,k}(\mathbb{Z})$ with the following property. If $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, then $LF(x^{\boldsymbol{n}})$ is reducible if and only if there is a positive integer $r \leq k$ such that $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$ is soluble in $\boldsymbol{v} \in \mathbb{Z}^r$ and $\boldsymbol{N} \in R \cap \mathfrak{M}_{r,k}(\mathbb{Z})$ of rank r, but insoluble in $\boldsymbol{v} \in \mathbb{Z}^s$ and $\boldsymbol{N} \in S \cap \mathfrak{M}_{s,k}(\mathbb{Z})$ of rank $s < r$.*

Proof. We begin by defining subsets S_i and R_i of $\mathfrak{M}_{k-i,k}(\mathbb{Z})$, for $0 \leq i \leq k-1$, inductively. Let

$$S_0 = \{\boldsymbol{I}_k\}, \tag{3.2}$$

and supposing that S_i is already defined and $\boldsymbol{y} = [y_1, \dots, y_{k-i}]$, define

$$R_i = \big\{\boldsymbol{M}\boldsymbol{N} : \boldsymbol{N} \in S_i,\ \boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z}),\ \operatorname{rank} \boldsymbol{M} = k-i, \\ h(\boldsymbol{M}) \leq c_1(JF(\boldsymbol{y}^{\boldsymbol{N}})),\ LF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}}) \text{ reducible}\big\} \tag{3.3}$$

and, for $i < k-1$,

$$S_{i+1} = \Big\{\boldsymbol{N} \in \mathfrak{M}_{k-i-1,k}(\mathbb{Z}) : \operatorname{rank} \boldsymbol{N} = k-i-1, \\ h(\boldsymbol{N}) \leq (k-i) \max_{\boldsymbol{N}_1 \in S_i} \big\{h(\boldsymbol{N}_1) \max\{c_2(JF(\boldsymbol{y}^{\boldsymbol{N}_1})), \\ 2(k-i) \max{}^{*}\{h(\boldsymbol{M}) | JF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1})|\}\}\big\}\Big\}, \tag{3.4}$$

where $\max^*$ is taken over all $\boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z})$ with $\det \boldsymbol{M} \neq 0$ and $h(\boldsymbol{M}) \leq c_1(JF(\boldsymbol{y}^{\boldsymbol{N}_1}))$. In this way R_i and S_i are defined for all $i < k$ and we put

$$R = \bigcup_{i=0}^{k-1} R_i \quad \text{and} \quad S = \bigcup_{i=1}^{k-1} S_i.$$

We first prove that the condition given in the theorem is necessary. By (3.2), there is at least one index i, namely $i = k$, such that there exist $\boldsymbol{u} \in \mathbb{Z}^i$ and $\boldsymbol{U} \in S_{k-i}$ with $\boldsymbol{n} = \boldsymbol{u}\boldsymbol{U}$. Let r be the least such index satisfying

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \quad \text{for some } \ \boldsymbol{v} \in \mathbb{Z}^r \ \text{ and } \ \boldsymbol{N} \in S_{k-r}. \tag{3.5}$$

By Lemma 3.4, if $LF(x^{\boldsymbol{n}}) = LF(x^{\boldsymbol{v}\boldsymbol{N}})$ is reducible, then there is a matrix $\boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z})$ of rank r such that

$$h(\boldsymbol{M}) \leq c_1(JF(\boldsymbol{y}^{\boldsymbol{N}})), \quad \text{where } \ \boldsymbol{y} = [y_1, \ldots, y_r],$$

and

$$\boldsymbol{v} = \boldsymbol{v}_1\boldsymbol{M}, \quad \text{for some } \ \boldsymbol{v}_1 \in \mathbb{Z}^r \tag{3.6}$$

and either $L(F(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}}))$ is reducible, or there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^r$ such that

$$\boldsymbol{\gamma}\boldsymbol{v} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \leq c_2(JF(\boldsymbol{y}^{\boldsymbol{N}})).$$

The second possibility can only hold for $r > 1$, since for $r = 1$ it gives $\boldsymbol{v} = \boldsymbol{0}$ and, by (3.5), $\boldsymbol{n} = \boldsymbol{0}$. For $r > 1$, the vectors $\boldsymbol{v}$ orthogonal to $\boldsymbol{\gamma}$ form a lattice $\boldsymbol{\Lambda}$ in $\mathbb{Z}^r$. As a consequence of Corollary 3.5, this lattice has a basis that written in the form of rows of a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ satisfies

$$\operatorname{rank} \boldsymbol{B} = r - 1, \tag{3.7}$$

and

$$h(\boldsymbol{B}) \leq h(\boldsymbol{\gamma}) \leq c_2(JF(\boldsymbol{y}^{\boldsymbol{N}})). \tag{3.8}$$

We see that in the case that $\boldsymbol{\gamma}$ exists, since $\boldsymbol{v} \in \boldsymbol{\Lambda}$, we have

$$\boldsymbol{v} = \boldsymbol{w}\boldsymbol{B}, \quad \text{for some } \ \boldsymbol{w} \in \mathbb{Z}^{r-1}.$$

Hence, by (3.5), we obtain

$$\boldsymbol{n} = \boldsymbol{w}\boldsymbol{B}\boldsymbol{N}, \quad \text{where } \ \boldsymbol{B}\boldsymbol{N} \in \mathfrak{M}_{r-1,k}. \tag{3.9}$$

Since, by (3.4) and (3.5), we have $\operatorname{rank} \boldsymbol{N} = r$, it follows from (3.7) that

$$\operatorname{rank} \boldsymbol{B}\boldsymbol{N} = r - 1.$$

Moreover, by (3.8),

$$h(\boldsymbol{B}\boldsymbol{N}) \leq r\, h(\boldsymbol{B})\, h(\boldsymbol{N}) \leq r\, h(\boldsymbol{N})\, c_2(JF(\boldsymbol{y}^{\boldsymbol{N}}))$$

and, by (3.4), $\boldsymbol{B}\boldsymbol{N} \in S_{k-r+1}$, contrary, in view of (3.9), to the definition of r. The contradiction obtained proves that $LF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}})$ is reducible. Since $\boldsymbol{M}$ and $\boldsymbol{N}$ have rank r, so does $\boldsymbol{M}\boldsymbol{N}$. Hence, $\boldsymbol{M}\boldsymbol{N} \in R_{k-r}$ by (3.3). By (3.5) and (3.6) we have

$$\boldsymbol{n} = \boldsymbol{v}_1\boldsymbol{M}\boldsymbol{N},$$

while by the definition of r the equation $\boldsymbol{n} = \boldsymbol{u}\,\boldsymbol{U}$ is insoluble in $\boldsymbol{u} \in \mathbb{Z}^i$ and $\boldsymbol{U} \in S_{k-i}$ for $i < r$. Thus, the condition given in the theorem is necessary.

Now we shall prove that it is sufficient. Suppose that for a certain matrix $\boldsymbol{N} \in R_{k-r}$, with $1 \le r \le k$, we have

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \quad \text{for some } \boldsymbol{v} \in \mathbb{Z}^r,$$

but

$$\boldsymbol{n} \ne \boldsymbol{u}\boldsymbol{U} \quad \text{for all } s < r,\ \boldsymbol{u} \in \mathbb{Z}^s \text{ and } \boldsymbol{U} \in S_{k-s}. \tag{3.10}$$

Then, by (3.3), we see that there are $\boldsymbol{N}_1 \in S_{k-r}$ and $\boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z})$ of rank r with $\boldsymbol{N} = \boldsymbol{M}\boldsymbol{N}_1$ satisfying

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}\boldsymbol{N}_1, \quad h(\boldsymbol{M}) \le c_1(JF(\boldsymbol{y}^{\boldsymbol{N}_1})), \quad \text{where } \boldsymbol{y} = [y_1, \dots, y_r] \tag{3.11}$$

and

$$LF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1}) \quad \text{is reducible.}$$

From Lemma 3.1, we obtain

$$LF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1}) = F_1F_2, \tag{3.12}$$

for some non-reciprocal F_1 and F_2 in $\mathbb{Q}[\boldsymbol{y}] \setminus \mathbb{Q}$.

It follows from (3.11) and (3.12) that

$$LF(x^{\boldsymbol{n}}) = LF_1(x^{\boldsymbol{v}})LF_2(x^{\boldsymbol{v}}). \tag{3.13}$$

Assume that for some $i \in \{1, 2\}$, we have $LF_i(x^{\boldsymbol{v}}) \in \mathbb{Q}$. By Lemma 3.3, there is a vector $\boldsymbol{\beta} \in \mathbb{Z}^r$ for which

$$\boldsymbol{\beta}\boldsymbol{v} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\beta}) \le 2|F_i| \le 2\big|JF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1})\big|.$$

Again, this case occurs only for $r > 1$, and from Corollary 3.5 we find a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ and a vector $\boldsymbol{w} \in \mathbb{Z}^{r-1}$ such that

$$\operatorname{rank} \boldsymbol{B} = r - 1, \quad h(\boldsymbol{B}) \le h(\boldsymbol{\beta}) \le 2\big|JF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1})\big|, \quad \boldsymbol{v} = \boldsymbol{w}\boldsymbol{B},$$

and

$$h(\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1) \le r^2h(\boldsymbol{B})h(\boldsymbol{M})h(\boldsymbol{N}_1) \le 2r^2h(\boldsymbol{M})h(\boldsymbol{N}_1)\big|JF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1})\big|.$$

Hence, by (3.4) and (3.11), we have

$$\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1 \in S_{k-r+1}, \quad \text{where } \boldsymbol{n} = \boldsymbol{w}\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1,$$

which contradicts (3.10). The contradiction implies that $LF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q}$ for both $i \in \{1, 2\}$. Hence by (3.13), we deduce that $LF(x^{\boldsymbol{n}})$ is reducible. ∎

Acknowledgments. The authors are grateful to Andrzej Schinzel for allowing them to include his argument that Theorem 1.1 follows from his work [7]. They also express their appreciation to Maciej Radziejewski and an anonymous referee for a number of helpful comments in the presentation of the results and arguments.

References

[1] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*, in: Number Theory in Progress, vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 143–163.

[2] M. Filaseta, I. Solan, *An extension of a theorem of Ljunggren*, Math. Scand. 84 (1999), 5–10.

[3] D. E. Knuth, *The Art of Computer Programming. Combinatorial Algorithms. Part I*, vol. 4A, Addison-Wesley, Upper Saddle River, NJ, 2011.

[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), 65–70.

[5] W. H. Mills, *The factorization of certain quadrinomials*, Math. Scand. 57 (1985), 44–50.

[6] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*, Colloq. Math. 9 (1962), 291–296; Selecta, 295–300.

[7] A. Schinzel, *Reducibility of lacunary polynomials*, I, Acta Arith. 16 (1969), 123–159; corrigenda: Acta Arith. 19 (1971), 201, ibid. 24 (1978), 265; Selecta, 344–380.

[8] A. Schinzel, *Reducibility of lacunary polynomials*, XII, Acta Arith. 90 (1999), 273–289; Selecta, 563–579.

[9] A. Schinzel, *Polynomials with special regard to reducibility* (with an appendix by U. Zannier), Encyclopedia Math. Appl. 77, Cambridge Univ. Press, Cambridge, 2000.

[10] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.

[11] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$, Math. Scand. 8 (1960), 121–126.

[12] A. F. Vincent, *Classifying polynomials with reducible nonreciprocal parts and the factorization of values of polynomials*, Doctoral Dissertation, Univ. of South Carolina, ProQuest, UMI Dissertations Publishing, Ann Arbor, 2012.