On the factorization of lacunary polynomials

by

MICHAEL FILASETA (Columbia, SC)

Dedicated to the fond and inspirational memory of A. Schinzel

1. Introduction. The main goal of this paper is to explain how to obtain information about the factorization of polynomials of the form

\[ F(x) = \sum_{j=0}^{r} f_j(x)x^{nj}, \]

where \( r \) is an integer greater than or equal to 1, the polynomials \( f_0(x), \ldots, f_r(x) \) are in \( \mathbb{Z}[x] \) and \( n \) is a sufficiently large positive integer. Let \( R = \mathbb{Z} \) or \( R = \mathbb{Q} \). For a non-zero \( F(x, y) \in R[x, x^{-1}, y] \) (possibly in \( R[x, x^{-1}] \)), we define \( J_x F \) as \( \hat{F}(x, y) = x^k F(x, y) \) where \( k \in \mathbb{Z} \) is chosen so that \( \hat{F}(x, y) \in R[x, y] \) and \( \hat{F}(0, y) \neq 0 \). Note that \( x \) is a unit in \( R[x, x^{-1}, y] \). We will use the fact that, consequently, \( F \in R[x, x^{-1}, y] \) is irreducible in \( R[x, x^{-1}, y] \) if and only if \( J_x F \) is irreducible in \( R[x, y] \).

Our particular interest is in determining general conditions on the polynomials \( f_0(x), \ldots, f_r(x) \) for which the non-reciprocal part of \( F(x) \) is either 1 or irreducible provided only that \( n \) is sufficiently large. The non-reciprocal part of a polynomial \( F(x) \in \mathbb{Z}[x] \) is defined as follows. The reciprocal of a non-zero polynomial \( f(x) \in \mathbb{Q}[x] \) is \( \tilde{f}(x) = J_x f(1/x) = x^{\deg \tilde{f}} f(1/x) \). A non-zero polynomial \( f(x) \in \mathbb{Q}[x] \) is reciprocal if \( f(x) = \pm \tilde{f}(x) \). The non-reciprocal part of \( f(x) \in \mathbb{Z}[x] \) is \( f(x) \) removed of each irreducible reciprocal factor in \( \mathbb{Z}[x] \) with a positive leading coefficient. The latter is to be interpreted as removing these factors to the multiplicity to which they appear so that only irreducible non-reciprocal factors remain. In Schinzel’s work

2020 Mathematics Subject Classification: Primary 11R09; Secondary 11C08, 12E05, 57M50.

Key words and phrases: factorization, sparse polynomial, lacunary polynomial, reciprocal polynomial.

Received 23 July 2022; revised 28 April 2023.

Published online 5 July 2023.

DOI: 10.4064/aa220723-16-5

© Instytut Matematyczny PAN, 2023
of \([14, 16, 26]\), the non-reciprocal part of \(f(x)\) is denoted \(L_f(x)\), though we will not use this notation in the remainder of this paper.

This paper is motivated in part by the tremendous amount of work A. Schinzel produced on the factorization of lacunary (or sparse) polynomials (see \([12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 31]\)). In particular, his early papers on the subject gave a description of how the non-reciprocal part of a lacunary polynomial \(f(x)\) factors, and later he extended his results to the non-cyclotomic part of a lacunary polynomial \(f(x)\) (that is, \(f(x)\) removed of all of its cyclotomic polynomial factors) in the case that \(f(x)\) is not reciprocal. The latter was made possible by advancements by E. Bombieri and U. Zannier described in an appendix by Zannier in \([30]\) (also, see the work of E. Bombieri, D. W. Masser and U. Zannier \([1]\)).

The paper is also motivated by private communications of the author with S. Garoufalidis. S. Garoufalidis pointed out the significance of determining the factorization of polynomials of the form (1.1) to determine the trace field associated with \(\Gamma \subset \text{PSL}_2(\mathbb{C})\). In particular, he pointed out that the trace field of the Whitehead link \(W_{m/n}\) is \(\mathbb{Q}(x - 1/x)\) where \(x\) is some root of
\[
(x(x + 1))^m x^{4n} - (x - 1)^m
\]
(see W. D. Neumann and A. W. Reid \([10]\)); the trace field of the Whitehead link for the complement of the \((-2, 3, 3 + 2n)\) pretzel knot \(K_n\) is \(\mathbb{Q}(x + 1/x)\) where \(x\) is some root of
\[
x^{4n} + (-x^3 + 4x^2 - 8 + 4x^{-2} - x^{-3}) x^{2n} + 1
\]
(see M. L. Macasieb and T. W. Mattman \([9]\)); and the trace field under \(-a/b\) Dehn fillings of the complement of the \(4_1\) knot is \(\mathbb{Q}(x + 1/x)\) where \(x\) is some root of
\[
x^{4b} - x^{2b} - x^a - 2 - x^{-a} - x^{-2b} + x^{-4b}
\]
(S. Garoufalidis, private communication).

The first of these three Laurent polynomials is easier to approach given current information in the literature, and S. Garoufalidis and the author \([6]\) show that if \(m\) is a fixed odd positive integer, there is an \(N = N(m)\) such that if \(n \geq N\) is an integer relatively prime to \(m\), then the polynomial \((x(x + 1))^m x^{4n} - (x - 1)^m\) is \(x^2 + 1\) times an irreducible polynomial (over \(\mathbb{Q}\)).

The other two Laurent polynomials are more difficult to find literature to exploit. There are two reasons for this. First, if \(F(x)\) is one of these two Laurent polynomials, then \(J_x F(x)\) is reciprocal. Based on current knowledge, determining the complete factorization of reciprocal polynomials in a general form is more difficult than in the non-reciprocal case. For example, with regard to Schinzel’s work described above, he requires a condition that \(J_x F(x)\) is non-reciprocal when discussing the factorization of the non-cyclotomic part of \(F(x)\) (see \([26\, \text{Theorem 2}]\)). Second, the first of the three Laurent poly-
nomials is the special case of (1.1) with \( r = 1 \) which has been investigated more fully in the literature (e.g., \([5, 7, 11, 28]\)), whereas the second and third Laurent polynomials above are cases where \( r \geq 2 \) in (1.1) for which similar literature is lacking.

In general, what is reasonable to expect given the current literature on the subject is that except for exceptional cases, perhaps explicitly laid out, one can show that \( F(x) \) in (1.1) for large \( n \) has non-reciprocal part which is either identically 1 or irreducible. In the case that \( F(x) \) itself is reciprocal, this would necessarily mean that the non-reciprocal part is 1 and that each irreducible factor is reciprocal. The latter is of some significance. Given an arbitrary non-zero polynomial \( g(x) \in \mathbb{Q}[x] \), the polynomial \( g(x) \tilde{g}(x) \) is reciprocal. Thus, a priori, given only that \( F(x) \) is reciprocal, we cannot deduce that its irreducible factors are themselves reciprocal. Knowing the irreducible factors are reciprocal also provides information about the Galois group of a number field generated by the roots of an irreducible factor of the polynomial. More precisely, if \( f(x) \) is an irreducible reciprocal polynomial of degree \( n > 1 \), then \( n = 2m \) for some integer \( m \geq 1 \) and the associated Galois group is isomorphic to a subgroup of all signed permutations on \( m \) objects, and hence has order dividing \( 2^m m! \) (see \([2]\)).

With the above in mind, our main result is the following.

**Theorem 1.1.** Let \( r \geq 1 \) be an integer, and

\[
F(x, y) = f_0(x) + f_1(x)y + \cdots + f_r(x)y^r \in \mathbb{Z}[x, y]
\]

with

\[
gcd_{\mathbb{Z}[x]}(f_0(x), f_1(x), \ldots, f_r(x)) = 1, \quad f_0(0) \neq 0, \quad f_r(x) \neq 0.
\]

Let \( n \) be sufficiently large; more precisely, we may take

\[
\deg F(x, x^n) \geq \max \left\{ (r + 1)(2r + 3)^{2N+1}, \right. \]

\[
\left. \left( \max_{0 \leq j \leq r} \deg f_j \right) \left( 2(2r + 3)^N + \frac{1}{r + 1} \right) \right\}
\]

with

\[
N = 2\|F\|^2 + 2m + 2r - 8,
\]

where \( \|F\| \) represents the 2-norm defined as the square root of the sum of the squares of the coefficients of \( F(x, y) \) and \( m \) denotes the number of terms in \( F(x, y) \). Then the non-reciprocal part of \( F(x, x^n) \) is not reducible if, whenever we write \( n = k\ell + t \), where \( k, \ell \) and \( t \) are integers satisfying

\[
k \geq 2 \max_{0 \leq j \leq r} \deg f_j, \quad \ell \geq 1, \quad 0 \leq t < \frac{k}{r(r + 1)},
\]

the polynomial

\[
f_0(x) + f_1(x)x^ty^\ell + \cdots + f_{r-1}(x)x^{(r-1)t}y^{(r-1)\ell} + f_r(x)x^{rt}y^{r\ell}
\]
is irreducible in $\mathbb{Z}[x, y]$, and whenever we write $n = k\ell - t$, where $k$, $\ell$ and $t$ are integers satisfying (1.3), the polynomial

$$J_x \left( f_0(x)x^{rt} + f_1(x)x^{(r-1)t}y^\ell + \cdots + f_{r-1}(x)x^ty^{(r-1)\ell} + f_r(x)y^{r\ell} \right)$$

is irreducible in $\mathbb{Z}[x, y]$.

The subscript on the greatest common divisor in the above statement indicates that it is taken over the ring $\mathbb{Z}[x]$, so the polynomials $f_0(x), f_1(x), \ldots, f_r(x)$ are not all divisible by an element of $\mathbb{Z}[x]$ other than one of the units $\pm 1$. The terminology “not reducible” instead of “irreducible” is to allow for the possibility that the non-reciprocal part of $F(x, x^n)$ is $\pm 1$; alternatively, one can say that the non-reciprocal part of $F(x, x^n)$ has at most one non-reciprocal irreducible factor with a positive leading coefficient.

For clarification, the work of A. Schinzel beginning with [14] (see also [4]) already gives, in theory, an effective way of determining whether the non-reciprocal parts of $F(x, x^n)$ in Theorem 1.1 and even more general polynomials, are reducible. The goal in this paper is to provide a more practical approach, a method in particular of efficiently handling polynomials like the Laurent polynomials described earlier.

In Section 2 we elaborate on a method to show that polynomials in two variables of the form appearing throughout Theorem 1.1 are irreducible (or a power of $x$ times an irreducible polynomial). In Section 3 we establish a preliminary result for Theorem 1.1 along the lines given in [5]. A simpler variant of Theorem 1.1 and Theorem 1.1 itself, will be established in Section 4. In Section 5 we will look at consequences of Theorem 1.1. We provide one example there involving the non-reciprocal polynomial

$$x^{6n} + (x + 1)x^{5n+1} + 2x^{4n} + (x^4 - x^3 - x^2 - 2x - 2)x^{3n-2} + 2x^{2n} + (x + 1)x^{n-2} + 1,$$

showing that for $n$ sufficiently large, the polynomial is irreducible. We then give examples corresponding to the last two Laurent polynomials connected to trace fields indicated above, and we obtain results showing that, for large enough exponent variables, the associated polynomials have irreducible factors that are reciprocal.

Before leaving the introduction, we comment that under the assumption of Lehmer’s conjecture on the Mahler measure of a non-cyclotomic irreducible polynomial in $\mathbb{Z}[x]$, each irreducible non-cyclotomic factor of polynomials of the form (1.1) with $\gcd(f_0(x), f_1(x), \ldots, f_r(x)) = 1$ has degree $> cn$, where $c$ is a positive constant depending only on the polynomials $f_0(x), f_1(x), \ldots, f_r(x)$ and where $n$ is an arbitrary positive integer (see [8]). Furthermore, the recent proof of V. Dimitrov [3] of the Schinzel–Zassenhaus conjecture now implies the same result, but with a different constant, uncon-
ditionally under rather general conditions on the fixed $f_j(x)$. In particular, with $f_r(x)$ a power of $x$, as in all the examples in Section 5 such a result holds unconditionally.

2. Factorization of polynomials in two variables. In this section, we are interested in polynomials of the general form

$$(2.1) \quad F(x, y) = \sum_{j=0}^{r} f_j(x) y^j \in \mathbb{Z}[x, y], \quad \text{where } r \geq 1 \text{ and } f_r(x) \neq 0,$$

and determining an irreducibility result for $F(x, y^n)$ where $n$ is a positive integer. Suppose $F(x, y)$ is irreducible in $\mathbb{Z}[x, y]$ so that, in particular, there is no polynomial in $\mathbb{Z}[x]$ other than ±1 that divides every $f_j(x)$. Viewing $F(x, y)$ as a polynomial in $y$, we let $\alpha$ denote a root of $F(x, \alpha) = 0$ (so $F(x, \alpha) = 0$ and consider the field $K = \mathbb{Q}(x)[\alpha]$. An important theorem due to Alfredo Capelli (see [29]) implies that $F(x, y^n)$ is reducible in $\mathbb{Z}[x, y]$ if and only if the polynomial $y^n - \alpha$ is reducible in $K[y]$. Equally important, Capelli’s work also gives us precise knowledge on when $y^n - \alpha$ factors in $K[y]$. He shows that $y^n - \alpha$ factors in $K[y]$ if and only if at least one of the following holds:

(i) The number $n$ is divisible by a prime $p$ and $\alpha = \beta^p$ for some $\beta \in K$.

(ii) The number $n$ is divisible by 4 and $\alpha = -4\beta^4$ for some $\beta \in K$.

Observe that the first result of Capelli’s above implies that in the case of (i), the polynomial $F(x, y^p)$ is reducible in $\mathbb{Z}[x, y]$; and in the case of (ii), the polynomial $F(x, y^4)$ is reducible in $\mathbb{Z}[x, y]$. We will determine a small set $\mathcal{P}$ of odd primes with the property that if $\alpha = \beta^p$ for some odd prime $p$ and some $\beta \in K$, then $p \in \mathcal{P}$. Thus, determining the $n$ for which $F(x, y^n)$ is irreducible (or reducible) in $\mathbb{Z}[x, y]$ will be reduced to checking the factorization of $F(x, y^n)$ for $p \in \mathcal{P}$ and checking the factorization of $F(x, y^4)$.

A particularly easy consequence of $\alpha = \beta^p$ is that the norm of $\alpha$ in $K$ over $\mathbb{Q}(x)$ is the $p$th power of an element of $\mathbb{Q}(x)$. Thus, from (2.1), we see that if $\alpha = \beta^p$, then $(-1)^r f_0(x)/f_r(x)$ is a $p$th power in $\mathbb{Q}(x)$. Hence, an easy approach to determining a set $\mathcal{P}$ of odd primes $p$ for which $F(x, y^p)$ can factor non-trivially is simply to take $\mathcal{P}$ to be the odd primes $p$ for which the polynomial $(-1)^r f_0(x)/f_r(x)$ is a $p$th power. However, one case of interest to us is the case where $(-1)^r f_0(x)/f_r(x) = \pm 1$ which is a $p$th power for every odd prime $p$. With this in mind, an immediate goal is to determine something more, perhaps along similar lines, that one can use to narrow the search for primes $p$ for which $F(x, y^p)$ factors non-trivially.

We suppose as above that $F(x, y)$ is irreducible in $\mathbb{Z}[x, y]$. We also suppose that at least one of the $f_j(x)$ appearing in (2.1) has degree $> 0$ and that the coefficient of $y^r$ in $F(x, y)$ is a polynomial in $x$ (possibly of degree 0) having
a positive leading coefficient. Suppose further that \( \alpha = \beta^p \) as described in (i) above. Recall that \( \beta \in K = \mathbb{Q}(x)[\alpha] \). On the other hand, \( \alpha = \beta^p \) implies \( \alpha \in \mathbb{Q}(x)[\beta] \). Since the degree of the extension \( \mathbb{Q}(x)[\alpha] \) over \( \mathbb{Q}(x) \) is \( r \), we deduce that the degree of the extension \( \mathbb{Q}(x)[\beta] \) over \( \mathbb{Q}(x) \) is \( r \). Hence, there is an irreducible polynomial in \( \mathbb{Z}[x, y] \) of degree \( r \) in \( y \) having \( \beta \) as a root, say

\[
G(x, y) = \sum_{j=0}^{r} g_j(x)y^j \in \mathbb{Z}[x, y], \quad \text{where } g_r(x) \neq 0.
\]

As with \( F(x, y) \), we note that there is no polynomial in \( \mathbb{Z}[x] \) other than \( \pm 1 \) that divides every \( g_j(x) \), and we may suppose that the coefficient of \( y^r \) in \( G(x, y) \) is a polynomial in \( x \) (possibly of degree 0) having a positive leading coefficient.

Let \( \alpha_1, \ldots, \alpha_r \) be the conjugates of \( \alpha \) including \( \alpha \) so that \( F(x, \alpha_j) = 0 \) for \( 1 \leq j \leq r \). Since \( \beta \in K = \mathbb{Q}(x)[\alpha] \), we can write \( \beta \) as a polynomial in \( \alpha \) with coefficients in \( \mathbb{Q}(x) \), say \( \beta = w(\alpha) \in \mathbb{Q}(x)[\alpha] \). We denote by \( \beta_j \) the field conjugate \( w(\alpha_j) \). Observe that \( \alpha = \beta^p = w(\alpha)^p \). Thus, each \( \alpha_j \) is a root of \( y = w(y)^p \); in other words, \( \alpha_j = w(\alpha_j)^p \), and hence \( \alpha_j = \beta_j^p \), for \( 1 \leq j \leq r \).

We begin here with a description of the basic “idea” behind our approach connecting \( G(x, y) \) to \( F(x, y) \) and leading us to a set \( \mathcal{P} \) of odd primes as indicated above. If we view \( G(x, y) \) as a polynomial in \( \mathbb{F}_p(x)[y] \), and consider the \( r \) roots \( \beta_1', \ldots, \beta_r' \) of \( G(x, y) \) in an extension \( K' \) of \( \mathbb{F}_p(x) \), then

\[
G(x, y)^p = \sum_{j=0}^{r} g_j(x)^py^{pj} = g_r(x)^p \prod_{j=1}^{r} (y^p - (\beta_j')^p).
\]

Consequently, the polynomial \( H(x, y) = \sum_{j=0}^{r} g_j(x)^py^j \) will have roots \( (\beta_1')^p, \ldots, (\beta_r')^p \) in \( K' \). Thus, in \( \mathbb{F}_p[x, y] \), the polynomials \( F(x, y) \) and \( H(x, y) \) will differ at most by a factor in \( \mathbb{F}_p[x] \). With a little more work, one can see that \( F(x, y) = H(x, y) \) in \( \mathbb{F}_p[x, y] \). We give details for how one can establish such a result next. Of some importance to us, what follows works not just for odd primes \( p \) but for \( p = 2 \) as well.

Let

\[
\sigma_1 = \sum_{j=1}^{r} \alpha_j, \quad \sigma_2 = \sum_{1 \leq i < j \leq r} \alpha_i \alpha_j, \quad \ldots, \quad \sigma_r = \prod_{j=1}^{r} \alpha_j,
\]

denote the elementary symmetric functions of the roots of \( F(x, y) \) viewed as a polynomial in \( y \) over \( \mathbb{Q}(x) \). Thus,

\[
\sigma_1 = -\frac{f_{r-1}(x)}{f_r(x)}, \quad \sigma_2 = \frac{f_{r-2}(x)}{f_r(x)}, \quad \ldots, \quad \sigma_r = (-1)^r \frac{f_0(x)}{f_r(x)}.
\]

Let

\[
\sigma'_{1} = \sum_{j=1}^{r} \beta_j, \quad \sigma'_{2} = \sum_{1 \leq i < j \leq r} \beta_i \beta_j, \quad \ldots, \quad \sigma'_{r} = \prod_{j=1}^{r} \beta_j.
\]
For each \( j \in \{1, \ldots, r\} \), we have \( \sigma'_j = (-1)^j g_{r-j}(x)/g_r(x) \in \mathbb{Q}(x) \).

We show next that there exist \( w_{i,j}(x) \in \mathbb{Z}[x] \) satisfying

\[
(2.3) \quad \sigma_j = (\sigma'_j)^p + \frac{p}{g_r(x)^p} \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \quad \text{for } 1 \leq j \leq r.
\]

Before turning to the proof of (2.3), we explain our interest in it. Suppose then for the moment that we know (2.3) holds. We rewrite \( \sigma'_j = (-1)^j g_{r-j}(x)/g_r(x) \) to deduce that

\[
\sigma_j = \frac{1}{g_r(x)^p} \left( (-1)^{pj} g_{r-j}(x)^p + p \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \right) \quad \text{for } 1 \leq j \leq r,
\]

where we include the \( p \) in the exponent \( pj \) of \(-1\) so that the identity also holds for \( p = 2 \). Since the \( \sigma_j \) represent the elementary symmetric functions in \( \alpha_1, \ldots, \alpha_r \), the polynomial

\[
F_0(x, y) = \sum_{j=0}^{r} \left( (-1)^{(p+1)j} g_{r-j}(x)^p + (-1)^j p \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \right) y^{r-j}
\]

has roots \( \alpha_1, \ldots, \alpha_r \). Let \( u(x) \) denote an irreducible polynomial in \( \mathbb{Z}[x] \). We claim that \( u(x) \) cannot divide every coefficient of \( F_0(x, y) \) as a polynomial in \( y \). Assume otherwise. Then looking at the coefficients of \( y^r, y^{r-1}, \ldots, y^0 \) for \( F_0(x, y) \) in turn, we deduce that \( u(x) \) divides each of \( g_r(x), g_{r-1}(x), \ldots, g_0(x) \). This contradicts the assumption that no polynomial in \( \mathbb{Z}[x] \) other than \( \pm 1 \) divides every \( g_j(x) \). Hence, \( F_0(x, y) \) is a polynomial in \( y \) with coefficients having no common factors in \( \mathbb{Z}[x] \) other than \( \pm 1 \). Since \( F(x, y) \) also has this property and the coefficients of \( y^r \) in both \( F_0(x, y) \) and \( F(x, y) \) are polynomials in \( x \) having a positive leading coefficient, we obtain

\[
F(x, y) = F_0(x, y) \equiv \sum_{j=0}^{r} g_j(x)^p y^j \pmod{p},
\]

which as noted above, in our discussion of \( H(x, y) \), was our immediate goal.

We turn now to the proof of (2.3). For the proof, we recall that any symmetric polynomial in \( \beta_1, \ldots, \beta_r \) with coefficients in \( \mathbb{Z} \) can be expressed as a polynomial in \( \sigma'_1, \ldots, \sigma'_r \) with coefficients in \( \mathbb{Z} \). In fact, we make use of a particular argument for obtaining the polynomial in \( \sigma'_1, \ldots, \sigma'_r \). For a symmetric polynomial \( h(\beta_1, \ldots, \beta_r) \in \mathbb{Z}[\beta_1, \ldots, \beta_r] \), set \( T = T_h \) to be the set of \( r \)-tuples \( (\ell_1, \ldots, \ell_r) \) with the coefficient of \( \beta_1^{\ell_1} \cdots \beta_r^{\ell_r} \) in \( h(\beta_1, \ldots, \beta_r) \) non-zero. We define the size of \( h \) to be \( (k_1, \ldots, k_r) \) where \( (k_1, \ldots, k_r) \) is the element of \( T \) with \( k_1 \) as large as possible, \( k_2 \) as large as possible given \( k_1 \), etc. Since \( h(\beta_1, \ldots, \beta_r) \) is symmetric, it follows that \( (\ell_1, \ldots, \ell_r) \in T \) if and only if each permutation of \( (\ell_1, \ldots, \ell_r) \) is in \( T \). This implies that \( k_1 \geq \cdots \geq k_r \). Observe that we can use the notion of size to form an ordering on the symmetric polynomials in \( \mathbb{Z}[\beta_1, \ldots, \beta_r] \) in the sense that if \( h_1 \) has size \( (k_1, \ldots, k_r) \)
and $h_2$ has size $(k'_1, \ldots, k'_r)$, then $h_1 > h_2$ if there is an $i \in \{0, 1, \ldots, r-1\}$ such that $k_1 = k'_1, \ldots, k_i = k'_i$, and $k_{i+1} > k'_{i+1}$. Note that the elements of $\mathbb{Z}[\beta_1, \ldots, \beta_r]$ which have size $(0, \ldots, 0)$ are precisely the constants (the elements of $\mathbb{Z}$).

Since $\alpha_j = \beta_j^p$ for $1 \leq j \leq r$, we may view $\sigma_j$ as a symmetric polynomial in $\beta_1, \ldots, \beta_r$ of size $(p, \ldots, p, 0, \ldots, 0)$, where the number of leading $p$’s is $j$. In general, we can take a given symmetric polynomial in elements of $\mathbb{Z}$ for some symmetric polynomial $\sigma$ of $\mathbb{Z}$.

Suppose first that $i > 1$. Then we rewrite $s_2(\beta_1, \ldots, \beta_r)$ using (2.4) as

$$m_2(\sigma'_1)^{k_1-k_2}(\sigma'_2)^{k_2-k_3}\cdots(\sigma'_{r-1})^{k_{r-1}-k_r}(\sigma'_r)^{k_r} + s_3(\beta_1, \ldots, \beta_r),$$

where $m_2 \in \mathbb{Z}$ and where $s_3 = s_2(\beta_1, \ldots, \beta_r) \in \mathbb{Z}[\beta_1, \ldots, \beta_r]$. Since $k_1 = p$, we note that the first term above has total degree $k_1 \leq p$ in the variables $\sigma'_1, \ldots, \sigma'_r$. It will be of some significance that similarly the total degree in each polynomial in $\sigma'_1, \ldots, \sigma'_r$ below is $\leq p$ as we proceed. Observe further that $k_{i-1} = p$ and $k_i < p$ implies that $k_{i-1} - k_i$ is positive. Thus, in the first of the two terms above, $\sigma'_{i-1}$ appears as a factor. Note also that the size of $s_3$ is less than the size of $s_2$ and, in particular, still less than $(p, \ldots, p, 0, \ldots, 0)$. Thus, if the size still has a first component of $p$, then we can repeat this process, rewriting $s_3$ as a multiple of at least one of $\sigma'_t$ for $1 \leq t \leq i - 1$ plus a symmetric polynomial $s_4$ of smaller size, and then rewriting $s_4$ as well if the first component of the size remains $p$, and so
on. As the sizes are decreasing, at some point the summand involving a new symmetric polynomial will have size \((k'_1, \ldots, k'_r)\) with \(k'_1 < p\).

Combining terms arising from above, we see that

\[
\sigma_j = (\sigma'_j)^p + p \sum_{t=1}^{i-1} \sigma'_t s'_t(\sigma'_1, \ldots, \sigma'_r) + ps_0(\beta_1, \ldots, \beta_r),
\]

where each \(s'_t = s'_t(\sigma'_1, \ldots, \sigma'_r)\) is a polynomial in \(\mathbb{Z}[\sigma'_1, \ldots, \sigma'_r]\) and \(s_0 = s_0(\beta_1, \ldots, \beta_r)\) is a symmetric polynomial in \(\mathbb{Z}[\beta_1, \ldots, \beta_r]\) of size \((k'_1, \ldots, k'_r)\) with \(k'_1 < p\). The above display holds also in the case \(i = 1\) by taking \(s_0 = s_2\). Note that, for \(1 \leq t \leq i - 1\), the total degree of \(\sigma'_t s'_t\) in the variables \(\sigma'_1, \ldots, \sigma'_r\) is \(\leq p\), so consequently \(s'_t\) has total degree \(< p\). At this point, we simply repeat the process of using and reusing (2.4) to rewrite (2.6) holds. As noted earlier, this leads to

\[
\text{where each } s'_t = s'_t(\sigma'_1, \ldots, \sigma'_r) \text{ is a polynomial in } \mathbb{Z}[\sigma'_1, \ldots, \sigma'_r]. \text{ The significance of having } k_1 < p \text{ is that at each stage from this point on, the size of the symmetric polynomials introduced will have first component } < p. \text{ Observe that if } k_1 < p \text{ in the first term}
\]

\[
m(\sigma'_1)^{k_1} k_2 (\sigma'_2)^{k_2} k_3 \cdots (\sigma'_{r-1})^{k_{r-1}} k_r (\sigma'_r)^{k_r}
\]

of (2.4), then the total degree of this term as a polynomial in \(\sigma'_1, \ldots, \sigma'_r\) is \(k_1 < p\). In other words, we can repeatedly use (2.4) to rewrite \(s_0\) as a polynomial \(s'_0 = s'_0(\sigma'_1, \ldots, \sigma'_r)\) in the variables \(\sigma'_1, \ldots, \sigma'_r\) with total degree \(< p\).

Now, we have

\[
(2.5) \quad \sigma_j = (\sigma'_j)^p + p \sum_{t=1}^{i-1} \sigma'_t s'_t(\sigma'_1, \ldots, \sigma'_r) + ps'_0(\sigma'_1, \ldots, \sigma'_r),
\]

where each \(s'_t\) for \(0 \leq t \leq i - 1\) is a polynomial in \(\mathbb{Z}[\sigma'_1, \ldots, \sigma'_r]\) with total degree \(< p\) in the variables \(\sigma'_1, \ldots, \sigma'_r\). We make the substitution \(\sigma'_t = (-1)^t g_{r-t}(x)/g_r(x)\) in (2.5) to obtain

\[
\sigma_j = (\sigma'_j)^p + p \sum_{t=1}^{i-1} \frac{g_{r-t}(x)w_{t,j}(x)}{g_r(x)^p} + \frac{pw_{0,j}(x)}{g_r(x)^p - 1},
\]

where each \(w_{t,j}(x)\) for \(0 \leq t \leq i - 1\) is in \(\mathbb{Z}[x]\). Since \(i \leq j\), we deduce that (2.3) holds. As noted earlier, this leads to

\[
(2.6) \quad F(x, y) \equiv \sum_{j=0}^{r} g_j(x)^p y^j \pmod{p}.
\]

The above follows from the condition \(\alpha = \beta^p\) in (i) and holds for any prime \(p\) satisfying this condition.

Recall that we have required that at least one of the \(f_j(x)\) appearing in (2.1) has degree \(> 0\). We also took the coefficient of \(y^r\) in \(F(x, y)\) to be a polynomial in \(x\) (possibly of degree 0) having a positive leading coefficient.
This latter condition can be removed at this point since what we are interested in is the information from (2.6) that each coefficient of \(F(x, y)\) is a \(p\)th power modulo \(p\), and if necessary we can multiply both sides of (2.6) by \((-1)^p\) to obtain a result in the case that the latter condition does not hold. We define the height of \(f_j(x)\) to be the maximum of the absolute values of the coefficients of \(f_j(x)\). Suppose \(p\) is an odd prime that is greater than the height \(H(f_j)\) for each \(f_j(x)\). This is more than we will need and only really require here that \(f_j(x)\) is not constant modulo \(p\) for some \(j\). Thus, for some \(j\), the coefficient \(f_j(x)\) of \(y^j\) on the left-hand side of (2.6) viewed modulo \(p\) is of degree \(> 0\). It follows that the corresponding \(g_j(x)\) is a non-constant polynomial modulo \(p\) on the right-hand side of (2.6). In this case, the polynomial \(g_j(x)^p\) modulo \(p\) must be of degree at least \(p\), which in turn implies that \(\deg f_j \geq p\). Thus, we may take \(\mathcal{P}\) to be the set of odd primes \(p\) of the form given in (2.6), and when verifying which \(p\) are of this form, we may restrict to

\[
(2.7) \quad p \leq \max \{\deg f_0, \ldots, \deg f_r, H(f_0), \ldots, H(f_r)\}.
\]

In other words, (2.6) implies (2.7). In particular, with \(\mathcal{P}\) so chosen, if \(F(x, y^p)\) for \(p \in \mathcal{P}\) and \(F(x, y^4)\) are all irreducible, then \(F(x, y^4)\) is irreducible for every positive integer \(n\). Recalling the opening paragraph of this section, we summarize the above as follows.

**Theorem 2.1.** Let \(F(x, y)\) be given as in (2.1), with \(F(x, y)\) irreducible in \(\mathbb{Z}[x, y]\) and with at least one \(f_j(x)\) non-constant. Let \(\mathcal{P}\) be the set of odd primes \(p\) satisfying both (2.7) and (2.6) for some \(g_j(x) \in \mathbb{Z}[x]\) depending on \(p\). Then \(F(x, y^n)\) is reducible in \(\mathbb{Z}[x, y]\) if and only if either \(p | n\) and \(F(x, y^p)\) is reducible for some \(p \in \mathcal{P}\), or \(2 | n\) and \(F(x, y^2)\) is reducible, or \(4 | n\) and \(F(x, y^4)\) is reducible. In particular, if \(F(x, y^p)\) for \(p \in \mathcal{P}\) and \(F(x, y^4)\) are all irreducible, then \(F(x, y^n)\) is irreducible in \(\mathbb{Z}[x, y]\) for every positive integer \(n\). Furthermore, if \(p \in \mathcal{P} \cup \{2\}\) and \(F(x, y^p)\) is reducible, then \(F(x, y)\) is necessarily of the form (2.6).

There is some value in looking closer at the case \(\alpha = -4\beta^4\) as in (ii), which we briefly sketch here. We suppose now that \(\alpha = -4\beta^4\) and \(G(x, y)\) in (2.2) has \(\beta\) as a root, where again \(G(x, y)\) is an irreducible polynomial in \(\mathbb{Z}[x, y]\) and \(g_r(x)\) has a positive leading coefficient. For \(1 \leq j \leq r\), we define \(\sigma_j\) and \(\sigma'_j\) as before. Instead of (2.3), we have in this case

\[
(2.8) \quad \sigma_j = (-4)^j (\sigma'_j)^4 + \frac{2^{2j+1}}{g_r(x)^4} \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \quad \text{for } 1 \leq j \leq r,
\]

for some polynomials \(w_{i,j}(x) \in \mathbb{Z}[x]\). The proof of (2.8) is analogous to the proof of (2.3). The implications are a bit different, and we discuss that next.

We will want to take advantage of a little more information on the \(w_{i,j}(x)\).
Observe that
\[ \sigma_r = \alpha_1 \cdots \alpha_r = (-4)^r (\beta_1^4 \cdots \beta_r^4) = (-4)^r (\sigma'_r)^4. \]
Thus, in regard to (2.8), we can take \( w_{i,r}(x) = 0 \) for \( 0 \leq i < r \).
Recalling \( \sigma'_r = (-1)^j g_{r-j}(x)/g_r(x) \), we deduce
\[ F_1(x, y) = \sum_{j=0}^{r} \left( 2^{2j} g_{r-j}(x)^4 + (-1)^j 2^{2j+1} \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \right) y^{r-j} \]
has roots \( \alpha_1, \ldots, \alpha_r \). As with \( F_0(x, y) \), we would like to determine whether the coefficients of \( F_1(x, y) \) viewed as a polynomial in \( y \) have any common factors. Analogous to \( F_0(x, y) \), if \( u(x) \in \mathbb{Z}[x] \) is a non-constant irreducible polynomial or if \( u(x) \) is an odd prime, then there must be a coefficient of \( F_1(x, y) \) which is not divisible by \( u(x) \). In other words, the only irreducible polynomials in \( \mathbb{Z}[x] \) that might divide every coefficient of \( F_1(x, y) \) are \( \pm 2 \). Suppose \( 2^s \) divides every coefficient of \( F_1(x, y) \) for some positive integer \( s \) with \( s \) maximal. It follows that \( F_1(x, y)/2^s \) is an irreducible polynomial in \( \mathbb{Z}[x, y] \) having roots \( \alpha_1, \ldots, \alpha_r \). Since \( g_r(x) \) and \( f_r(x) \) have a positive leading coefficient, we necessarily have
\[ F(x, y) = \frac{F_1(x, y)}{2^s} = \frac{1}{2^s} \sum_{j=0}^{r} \left( 2^{2j} g_{r-j}(x)^4 + (-1)^j 2^{2j+1} \sum_{0 \leq i < j} g_{r-i}(x) w_{i,j}(x) \right) y^{r-j}. \]
Let \( e_j \) be the non-negative integer for which \( 2^{e_j} \) is the largest power of \( 2 \) dividing the coefficient of \( y^j \) in \( F_1(x, y) \) in \( \mathbb{Z}[x] \). Let \( e'_j \) be the non-negative integer for which \( 2^{e'_j} \) is the largest power of \( 2 \) dividing \( g_j(x) \) in \( \mathbb{Z}[x] \). In particular, \( e_r = 4e'_r \). From the formulation of \( F_1(x, y) \) above, we see that \( e_j \geq 2r - 2j \) for each \( j \in \{0, 1, \ldots, r\} \) and if \( e'_j = 0 \), then \( e_j = 2r - 2j \). Also, the irreducibility of \( G(x, y) \) guarantees that some \( e'_i \) is zero. Given such an \( i \), we deduce \( s \leq 2r - 2i \), and \( 2^{2(i-j)} \) divides the coefficient of \( y^j \) in \( F(x, y) \) for \( 0 \leq j < i \). In particular, if the maximal such \( i \) is \( \geq 1 \), then \( f_0(x) \) is divisible by \( 4 \). Suppose the only such \( i \) is \( i = 0 \). Then either \( s < 2r \) and \( f_0(x) \) is divisible by \( 2 \), or \( s = 2r \). We consider the case that \( s = 2r \). From \( s = 2r \), \( e'_0 = 0 \) and \( w_{i,r}(x) = 0 \) for \( 0 \leq i < r \), we have \( f_0(x) = g_0(x)^4 \). If \( r \) is odd, then \( s \equiv 2 \pmod{4} \). As \( e_r = 4e'_r \equiv 0 \pmod{4} \), we see that \( f_r(x) \) is divisible by \( 4 \) in this case.
Thus far we have seen that either \( f_0(x) \) is divisible by \( 2 \) or \( f_r(x) \) is divisible by \( 4 \) unless \( r \) is even, \( s = 2r \), \( e'_0 = 0 \), and \( e'_j \geq 1 \) for \( 1 \leq j \leq r \). Furthermore, in this case, \( s = 2r \) implies that \( 2^{2r} \) divides each coefficient of \( y^j \) in \( F_1(x, y) \), and in particular \( 2^{2r} \) divides \( g_r(x)^4 \). Thus, \( e'_j \geq r/2 \). We will be interested in the particular case that \( r = 4 \), so suppose \( f_0(x) \) is not divisible by \( 2 \) and \( f_r(x) \) is not divisible by \( 4 \), giving the above conclusions
with \( r = 4 \). We make use of the explicit formula in this case that
\[
\sigma_1 = \sum_{j=1}^{4} (-4\beta_j^4) = -4((\sigma_1')^4 - 4(\sigma_1')^2(\sigma_2') + 4(\sigma_1')(\sigma_3') + 2(\sigma_2')^2 - 4(\sigma_4')),
\]
which leads to the more precise formulation of the polynomial
\[
4g_3(x)^4 - 16g_3(x)^2g_2(x)g_4(x) + 16g_3(x)g_1(x)g_4(x)^2 + 8g_2(x)^2g_4(x)^2 - 16g_0(x)g_4(x)^3
\]
for the coefficient of \( y^{r-1} = y^3 \) in \( F_1(x, y) \). This polynomial is required to be divisible by \( 2^{2r} = 2^8 \) in \( \mathbb{Z}[x] \). As \( e_4' \geq 4/2 = 2 \) and \( e_j' \geq 1 \) for \( 1 \leq j \leq 3 \), we see that each term beyond the first term is divisible by \( 2^9 \) in \( \mathbb{Z}[x] \), so the first term \( 4g_3(x)^4 \) must be divisible by \( 2^8 \). It follows that \( e_3' \geq 2 \). We deduce that the coefficient of \( y^3 \) in \( F_1(x, y) \) is divisible by \( 2^9 \) so that the coefficient of \( y^3 \) in \( F(x, y) \) is divisible by \( 2 \). Hence, in the case that \( \alpha = -4\beta^4 \) as in (ii) and \( r = 4 \), either \( f_0(x) \) or \( f_3(x) \) is divisible by \( 2 \), or \( f_4(x) \) is divisible by \( 4 \).

To summarize, in the case \( r = 4 \), we have shown that if \( F(x, y^4) \) is reducible, then either \( F(x, y^2) \) is reducible and (2.6) holds, or one of \( f_0(x) \) or \( f_3(x) \) is divisible by \( 2 \), or \( f_4(x) \) is divisible by \( 4 \). For general odd \( r \), we have also seen that if \( F(x, y^4) \) is reducible, then either \( F(x, y^2) \) is reducible and (2.6) holds with \( p = 2 \), or \( f_0(x) \) is divisible by \( 2 \), or \( f_4(x) \) is divisible by \( 4 \).

We end this section with an example that will play a role later in our paper.

**Example.** Let
\[
F(x, y) = 1 - x(x + 1)y - 2x^2y^2 - x^2(x + 1)y^3 + x^4y^4
\]
so that \( F(x, y) \) is of the form (2.1) with
\[
\begin{align*}
f_0(x) &= 1, & f_1(x) &= -x(x+1), & f_2(x) &= -2x^2, & f_3(x) &= -x^2(x+1), & f_4(x) &= x^4.
\end{align*}
\]
One checks directly that \( F(x, y) \) and \( F(x, y^4) \) are irreducible. Since \( f_1(x) = -x(x+1) \), we see that for every odd prime \( p \), the congruence in (2.6) does not hold. Theorem 2.1 now implies that \( F(x, y^n) \) is irreducible for every positive integer \( n \).

### 3. A theorem connecting single and multivariate polynomials.

To help with the statements of the results below and the proofs to follow, we discuss notation here. The expression \( a \pmod{k} \) will denote the unique integer \( b \) in \( [0, k) \) for which \( a \equiv b \pmod{k} \). If \( u \) is a real number, \( \lfloor u \rfloor \) will denote the greatest integer \( \leq u \), \( \lceil u \rceil \) the least integer \( \geq u \), and \( \|u\| \) the minimal distance from \( u \) to an integer. We will use \( \{u\} \) to denote \( u - \lfloor u \rfloor \) unless it is clear from the context that \( \{u\} \) refers to a set consisting of the single element \( u \). In the case that \( f(x) \) is a polynomial, \( \|f\| \) represents the 2-norm defined
as earlier as the square root of the sum of the squares of the coefficients of \( f(x) \), which should not be confused with the use of \( \|u\| \) mentioned above. As before, the reciprocal of the polynomial \( f(x) \) is \( \hat{f}(x) = x^{\text{deg} f} f(1/x) \), and the non-reciprocal part of \( f(x) \in \mathbb{Z}[x] \) is \( f(x) \) removed of each irreducible reciprocal factor in \( \mathbb{Z}[x] \) with a positive leading coefficient.

**Theorem 3.1.** Let \( F(x) = \sum_{j=0}^{r} a_j x^{d_j} \in \mathbb{Z}[x] \), where \( 0 = d_0 < d_1 < \cdots < d_r \) and \( a_r a_0 \neq 0 \). Let \( \varepsilon \in (0, 1/4] \), and let \( k_0 \) be a real number \( \geq 2 \). Set \( \kappa = \lfloor 1/\varepsilon \rfloor + 1 \). Suppose that

\[
\deg F \geq \max \left\{ \frac{\kappa^{2N}}{2} \left( \varepsilon - \frac{1}{\kappa} \right)^{-1}, k_0 (\kappa^N + \varepsilon) \right\}, \quad \text{where } N = 2 \|F\|^2 + 2r - 6.
\]

If the non-reciprocal part of \( F(x) \) is reducible in \( \mathbb{Z}[x] \), then there exists an integer \( k \) in the interval \([k_0, (\deg F)/(1 - \varepsilon)]\) satisfying:

(i) For \( j \in \{0, 1, \ldots, r\} \), \( d_j \mod k \) is in \([0, \varepsilon k) \cup ((1 - \varepsilon)k, k)\).

(ii) Let \( \ell_j \) and \( \overline{d}_j \) be the quotient and remainder upon dividing \( d_j + [\varepsilon k] \) by \( k \).

In other words, define \( \ell_j \) and \( \overline{d}_j \) by

\[
d_j = (d_j + [\varepsilon k]) \mod k \quad \text{and} \quad d_j + [\varepsilon k] = k \ell_j + \overline{d}_j.
\]

If \( G(x, y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j} \), then \( J_x G(x, y) \) is reducible in \( \mathbb{Z}[x, y] \).

The above result is very similar to Theorem 2 in [5] and follows along very similar lines. As the result nevertheless is different, we present the details below.

Before beginning the proof, we observe that \( k < d_r/(1 - \varepsilon) \) implies

\[
k - 1 - [\varepsilon k] < k(1 - \varepsilon) < d_r.
\]

Hence, \( d_r + [\varepsilon k] \geq k \) so that \( \ell_r \geq 1 \). Thus, \( G(x, y) \) depends on \( y \).

To establish Theorem 3.1, we make use of a seemingly unconnected combinatorial result of interest in itself. Fix \( \varepsilon > 0 \). Suppose that \( v_1, \ldots, v_\rho \) are distinct non-negative integers written in increasing order and that we wish to determine an integer \( k \geq 2 \) with the property that for each \( j \in \{1, \ldots, \rho\} \), we have \( v_j \equiv v'_j \mod k \) for some \( v'_j \in (-\varepsilon k, \varepsilon k) \). In [5], the case \( \varepsilon = 1/4 \) was of particular importance and focused on there. Observe that the value \( k = \lfloor v_\rho/\varepsilon \rfloor + 1 \) has the property stated above for \( k \), but we will want a smaller value of \( k \). We show that for each \( \rho \), there exists a \( V(\rho) = V(\rho, \varepsilon) \) such that if \( v_\rho \geq V(\rho) \), then there is a \( k \in [2, v_\rho/(1 - \varepsilon)] \) such that for each \( j \in \{1, \ldots, \rho\} \), we have \( v_j \equiv v'_j \mod k \) for some \( v'_j \in (-\varepsilon k, \varepsilon k) \).

**Lemma 3.2.** Let \( \varepsilon \in (0, 1/2] \), let \( \rho \) be a positive integer, and let \( k_0 \) be a real number \( \geq 2 \). Set \( \kappa = \lfloor 1/\varepsilon \rfloor + 1 \) and

\[
V(\rho) = \max \left\{ \frac{\kappa^{2\rho - 2}}{2} \left( \varepsilon - \frac{1}{\kappa} \right)^{-1}, k_0 (\kappa^{\rho - 1} + \varepsilon) \right\}.
\]
Let \( v_1, \ldots, v_\rho \) be non-negative integers satisfying \( v_1 < \cdots < v_\rho \) and \( v_\rho \geq V(\rho) \). Then there exists an integer \( k \in [k_0, v_\rho/(1-\varepsilon)) \) such that \( v_j \mod k \) is in \([0, \varepsilon k) \cup ((1-\varepsilon)k, k)\) for each \( j \in \{1, \ldots, \rho\} \).

**Proof.** For \( \rho = 1 \), the conditions imply \( v_\rho \geq k_0 \) and we can take \( k = v_\rho \).

We consider now the case that \( \rho > 1 \). The condition \( v_\rho \geq V(\rho) \) implies that

\[
(3.1) \quad \frac{v_\rho}{k^{\rho-1} + \varepsilon} \geq k_0 \quad \text{and} \quad \sqrt{2v_\rho(\varepsilon - 1/k)}^{1/2} \geq k^{\rho-1}.
\]

We will show that one may take

\[
(3.2) \quad k \in \left( \frac{v_\rho}{k^{\rho-1} + \varepsilon}, \frac{v_\rho}{1 - \varepsilon} \right).
\]

Note that the conditions in the lemma and \( \rho > 1 \) imply that such a \( k \) exists since the interval in (3.2) has length

\[
\frac{v_\rho(k^{\rho-1} + 2\varepsilon - 1)}{(k^{\rho-1} + \varepsilon)(1 - \varepsilon)} \geq k_0 \cdot \frac{\kappa + 2\varepsilon - 1}{1 - \varepsilon} \geq 2k_0 \cdot \frac{1 + \varepsilon}{1 - \varepsilon} > 1.
\]

Also, for \( k \) as in (3.2), we see from (3.1) that \( k > k_0 \). Observe that, to establish the lemma, it suffices to show that there is an integer \( k \) satisfying (3.2) and integers \( w_1, \ldots, w_\rho \) such that

\[
(3.3) \quad |v_j - w_jk| < \varepsilon k \quad \text{for } 1 \leq j \leq \rho.
\]

Let \( x_j = v_j/v_\rho \) for \( j \in \{1, \ldots, \rho\} \). We explain next how the Dirichlet box principle implies that there is a positive integer \( d \) satisfying \( d \leq k^{\rho-1} \) for which

\[
(3.4) \quad ||dx_j|| \leq 1/k \quad \text{for } 1 \leq j \leq \rho - 1.
\]

For each \( d' \in \{1, \ldots, k^{\rho-1} + 1\} \), we define the point

\[
P(d') = \{(d'x_1), \ldots, (d'x_{\rho-1})\}.
\]

Each \( P(d') \) has its coordinates in the interval \([0,1)\). For each of the \( k^{\rho-1} \) choices of \( u_j \in \{0, 1, \ldots, \kappa - 1\} \), where \( 1 \leq j \leq \rho - 1 \), we consider the cube

\[
C(u_1, \ldots, u_{\rho-1}) = \{(t_1, \ldots, t_{\rho-1}) : u_j/k \leq t_j < (u_j + 1)/k \}
\]

for \( 1 \leq j \leq \rho - 1 \).

By the Dirichlet box principle, there are \( d'_1 \) and \( d'_2 \) in \( \{1, \ldots, k^{\rho-1} + 1\} \) with \( d'_1 > d'_2 \) such that the points \( P(d'_1) \) and \( P(d'_2) \) are both in the same cube \( C(u_1, \ldots, u_{\rho-1}) \). Set \( d = d'_1 - d'_2 \in \{1, \ldots, k^{\rho-1}\} \). For every \( j \in \{1, \ldots, \rho - 1\} \), we obtain

\[
dx_j = d'_1x_j - d'_2x_j = |d'_1x_j| - |d'_2x_j| + \{d'_1x_j\} - \{d'_2x_j\}.
\]

It follows that each such \( dx_j \) is within \( |\{d'_1x_j\} - \{d'_2x_j\}| \leq 1/k \) of the integer \( |d'_1x_j| - |d'_2x_j| \). This establishes (3.4). Clearly, (3.4) holds with \( j = \rho \) as well. Observe that (3.1) implies that
For $1 \leq j \leq \rho$, take $w_j$ to be the nearest integer to $dx_j$. For the moment, suppose $w_j \neq 0$ (so that $w_j \geq 1$) for each $j \in \{1, \ldots, \rho\}$. Then (3.3) follows provided

$$\frac{k}{v_\rho} \in \left( \frac{x_j}{w_j + \varepsilon}, \frac{x_j}{w_j - \varepsilon} \right).$$

For each $j \in \{1, \ldots, \rho\}$, since $w_j \leq d$, we deduce from (3.4) that

$$\frac{d + (1/\kappa)}{d + \varepsilon} \geq \frac{w_j + (1/\kappa)}{w_j + \varepsilon} \geq \frac{dx_j}{w_j + \varepsilon}$$

and

$$\frac{d - (1/\kappa)}{d - \varepsilon} \leq \frac{w_j - (1/\kappa)}{w_j - \varepsilon} \leq \frac{dx_j}{w_j - \varepsilon}.$$  

Hence, (3.3) holds provided

$$\frac{k}{v_\rho} \in \left( \frac{d + (1/\kappa)}{d + \varepsilon}, \frac{d - (1/\kappa)}{d - \varepsilon} \right).$$

Using (3.5), we see that the length of the interval on the right is

$$\frac{2}{d^2 - \varepsilon^2} \left( \varepsilon - \frac{1}{\kappa} \right) > \frac{2}{d^2} \left( \varepsilon - \frac{1}{\kappa} \right) \geq \frac{1}{v_\rho},$$

so that there exists $k$ satisfying (3.6). Observe that (3.6) and the definition of $d$ imply (3.2) holds.

Now, suppose some $w_j$ with $j \in \{1, \ldots, \rho\}$ are zero. We again choose $k$ so that (3.6) holds. For each $w_j \neq 0$, the above argument gives $|v_j - w_jk| < \varepsilon k$ as in (3.3). On the other hand, if $w_j = 0$, then (3.4) and the definitions of $w_j, x_j, and k$ imply

$$\kappa dv_j \leq v_\rho < k \frac{d(d + \varepsilon)}{d + (1/\kappa)} \leq \kappa \varepsilon dk.$$  

Hence, (3.3) holds for such $w_j$ as well, completing the proof.

**Proof of Theorem 3.1.** Suppose that the non-reciprocal part of $F(x)$ is reducible. As described in detail in the proof of [5, Theorem 2], there exist non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$. Let $W(x) = u(x)\tilde{v}(x)$. The polynomials $F(x), \tilde{F}(x), W(x),$ and $\tilde{W}(x)$ are distinct polynomials of degree $d_r$ with any two having greatest common divisor of degree $< d_r$. Note that

$$(3.7) \quad F(x)\tilde{F}(x) = u(x)v(x)\tilde{u}(x)\tilde{v}(x) = W(x)\tilde{W}(x).$$

By comparing the coefficient of $x^{d_r}$ on the left and right sides of (3.7), we deduce that $\|F\|^2 = \|W\|^2$. 

$$(3.5) \quad d \leq \sqrt{2v_\rho \left( \frac{\varepsilon - 1}{\kappa} \right)^{1/2}}.$$
We write $W(x)$ in the form $W(x) = \sum_{j=0}^{s} b_j x^{e_j}$ where the $b_j$ are non-zero and $0 = e_0 < e_1 < \cdots < e_s = d_r$. Then $\|W\|^2 = \|F\|^2$ implies $s \leq \|F\|^2 - 1$. Consider the set

$$T = \{d_1, \ldots, d_r\} \cup \{d_r - d_1, d_r - d_2, \ldots, d_r - d_{r-1}\}$$

$$\cup \{e_1, \ldots, e_{s-1}\} \cup \{e_s - e_1, e_s - e_2, \ldots, e_s - e_{s-1}\}.$$  

Observe that $|T| \leq 2 \|F\|^2 + 2r - 5$. We use the lower bound on $d_r = \deg F$ in the statement of the theorem together with Lemma 3.2 to deduce that there exists an integer $k \in [k_0, d_r/(1 - \varepsilon))$ such that $t$ mod $k$ is in $[0, \varepsilon k) \cup ((1 - \varepsilon) k, k)$ for every $t \in T$. Fix such an integer $k$.

Define $\overline{d}_j$ and $\ell_j$ as in the theorem, and define $\overline{e}_j$ and $m_j$, for $0 \leq j \leq s$, similarly by

$$\overline{e}_j = (e_j + \lfloor \varepsilon k \rfloor) \mod k \quad \text{and} \quad e_j + \lfloor \varepsilon k \rfloor = km_j + \overline{e}_j.$$ 

For $0 \leq j \leq r$, we also define $\overline{d}_j'$ and $\ell_j'$ by

$$\overline{d}_j' = (d_r - d_j + \lfloor \varepsilon k \rfloor) \mod k, \quad \text{and} \quad d_r - d_j + \lfloor \varepsilon k \rfloor = k\ell_j' + \overline{d}_j';$$

and, for $0 \leq j \leq s$, we also define $\overline{e}_j'$ and $m_j'$ by

$$\overline{e}_j' = (e_s - e_j + \lfloor \varepsilon k \rfloor) \mod k \quad \text{and} \quad e_s - e_j + \lfloor \varepsilon k \rfloor = km_j' + \overline{e}_j'.$$

Since $t$ mod $k$ is in $[0, \varepsilon k) \cup ((1 - \varepsilon) k, k)$ for every $t \in T$, we see that the numbers $\overline{d}_j$ and $\overline{d}_j'$, for $0 \leq j \leq r$, and the numbers $\overline{e}_j$ and $\overline{e}_j'$, for $0 \leq j \leq s$, all lie in the interval $[0, 2\varepsilon k)$. Define $G_1(x, y) = G(x, y)$ (as in the statement of the theorem),

$$G_2(x, y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j'} y^{\ell_j'}, \quad H_1(x, y) = \sum_{j=0}^{s} b_j x^{\overline{e}_j} y^{m_j},$$

$$H_2(x, y) = \sum_{j=0}^{s} b_j x^{\overline{e}_j} y^{m_j}.$$ 

Hence,

$$G_1(x, x^k) = x^{\lfloor \varepsilon k \rfloor} F(x), \quad G_2(x, x^k) = x^{\lfloor \varepsilon k \rfloor} \tilde{F}(x),$$

$$H_1(x, x^k) = x^{\lfloor \varepsilon k \rfloor} W(x), \quad H_2(x, x^k) = x^{\lfloor \varepsilon k \rfloor} \tilde{W}(x).$$

Corresponding to (3.7), we establish next that

$$G_1(x, y)G_2(x, y) = H_1(x, y)H_2(x, y).$$

Recall that we are working with the condition that $\varepsilon \leq 1/4$ so that $2\varepsilon k \leq k/2$. Expanding the left-hand side of (3.9), we obtain an expression of the form $\sum_{j=0}^{J} g_j(x) y^j$ where possibly some $g_j(x)$ are 0 but otherwise $\deg g_j < k$. 

for each $j$. Since

$$x^{2[\varepsilon k]} F(x) \tilde{F}(x) = G_1(x, x^k) G_2(x, x^k) = \sum_{j=0}^J g_j(x)x^{kj},$$

we see that the terms in each $g_j(x)x^{kj}$ correspond precisely to the terms in the expansion of $x^{2[\varepsilon k]} F(x) \tilde{F}(x)$ having degrees in the interval $[kj, k(j+1))$. Similarly, writing the right-hand side of (3.9) in the form $\sum_{j'=0}^{J'} h_j(x)y^j$, we find that each $h_j(x)$ is either 0 or has degree $< k$ and the terms in $h_j(x)x^{kj}$ correspond to the terms in the expansion of $x^{2[\varepsilon k]} W(x) \tilde{W}(x)$ having degrees in the interval $[kj, k(j+1))$. We see now that (3.9) is a consequence of (3.7).

From (3.7) and (3.8), given any two of $G_1(x, y)$, $G_2(x, y)$, $H_1(x, y)$ and $H_2(x, y)$, each one will have a factor different from $x$ that does not divide the other. The theorem now follows from (3.9).

4. Reduction to polynomials in one variable. In this section, we will be interested in obtaining information about the factorization of $F(x, x^n)$ in $\mathbb{Z}[x]$ given $F(x, y)$ as in (2.1). As suggested by the previous section, the methods we employ here give us results about the factorization of the non-reciprocal part of $F(x, x^n)$.

We restrict ourselves to the case that

$$\gcd_{\mathbb{Z}[x]}(f_0(x), f_1(x), \ldots, f_r(x)) = 1, \quad f_0(0) \neq 0, \quad f_r(x) \neq 0.$$  

The above restrictions are minor; in particular, we can simply factor out an element of $\mathbb{Z}[x]$ from $F(x, y)$ if either of the first two conditions do not hold and proceed from there. To clarify, we allow for the possibility that $f_j(0) = 0$ for some or all $j \in \{1, \ldots, r\}$ and $f_j(x) = 0$ for some or all $j \in \{1, \ldots, r-1\}$.

Let

(4.1) $$F_0(x) = F(x, x^n) = \sum_{j=0}^r f_j(x)x^{nj},$$

where we consider

(4.2) $$n > \max_{0 \leq j \leq r-1} \deg f_j.$$  

For the purposes of using Theorem 3.1, we write

$$F_0(x) = \sum_{j=0}^m a_j x^{d_j},$$

where $0 = d_0 < d_1 < \cdots < d_m$, the numbers $n, 2n, \ldots, rn$ are included in the set $\{d_0, d_1, \ldots, d_m\}$, and possibly the coefficients $a_j$ corresponding to $x^n, x^{2n}, \ldots, x^{rn}$ are 0 but otherwise $a_j \neq 0$. With this understanding, there
exist non-negative integers \( \rho_0, \ldots, \rho_r \) such that
\[
    f_0(x) = \sum_{j=0}^{\rho_0} a_j x^{d_j}, \quad f_1(x) = \sum_{j=\rho_0+1}^{\rho_1} a_j x^{d_j-n}, \quad \ldots, \quad f_r(x) = \sum_{j=\rho_{r-1}+1}^{\rho_r} a_j x^{d_j-rn},
\]
where
\[
    d_0 = 0, \quad d_{\rho_0+1} = n, \quad d_{\rho_1+1} = 2n, \quad \ldots, \quad d_{\rho_{r-1}+1} = rn.
\]
As noted, some or all of the coefficients \( a_{\rho_0+1}, a_{\rho_1+1}, \ldots, a_{\rho_{r-1}+1} \) may be 0.

Set
\[
    k_0 = 2 \max_{0 \leq j \leq r} \deg f_j \quad \text{and} \quad \varepsilon = \frac{1}{2r+2} \leq \frac{1}{4}.
\]
Choose \( n \) sufficiently large so that the inequality on \( \deg F_0 \) holds in Theorem 3.1. One checks that this is equivalent to the degree bound (1.2) on \( F(x, y) \). Suppose further that the non-reciprocal part of \( F_0(x) \) is reducible. Fix \( k \) as in Theorem 3.1. For \( j \in \{0, \ldots, r\} \), define \( \overline{d}_j \) and \( \ell_j \) as in Theorem 3.1. Since \( k \geq 2 \deg f_0 \), we see that \( d_j + \lceil \varepsilon k \rceil < k \) for \( j \in \{0, 1, \ldots, \rho_0\} \).

Hence, each of \( \ell_0, \ell_1, \ldots, \ell_{\rho_0} \) is 0. We show next, for each \( i \in \{1, \ldots, r\} \), the numbers \( \ell_{\rho_{i-1}+1}, \ell_{\rho_{i-1}+2}, \ldots, \ell_{\rho_i} \) are all equal. Assume that \( \ell_s \neq \ell_{\rho_i} \) for some \( s \in \{\rho_{i-1}+1, \rho_{i-1}+2, \ldots, \rho_i - 1\} \). The ordering on the \( d_j \) and the definition of the \( \ell_j \) imply that \( \ell_s < \ell_{\rho_i} \). From the way \( \overline{d}_j \) is defined, we know that each \( \overline{d}_j \) is in \( [0, 2\varepsilon k) \subseteq [0, k/2) \). Hence, by the definition of \( \ell_j \), we obtain
\[
    d_{\rho_i} - d_s = k(\ell_{\rho_i} - \ell_s) + (\overline{d}_{\rho_i} - \overline{d}_s) > k - \frac{k}{2} = \frac{k}{2} \geq \deg f_i.
\]
On the other hand, from the definition of the \( \rho_j \), we see that
\[
    d_{\rho_i} - d_s \leq d_{\rho_i} - d_{\rho_{i-1}+1} \leq \deg f_i.
\]
This apparent contradiction implies that \( \ell_{\rho_{i-1}+1}, \ldots, \ell_{\rho_i} \) are all equal.

Since the \( d_j \) are increasing, the equality of the numbers \( \ell_{\rho_{i-1}+1}, \ldots, \ell_{\rho_i} \) implies that
\[
    \overline{d}_{\rho_{i-1}+1} = \min \{\overline{d}_{\rho_{i-1}+1}, \overline{d}_{\rho_{i-1}+2}, \ldots, \overline{d}_{\rho_i}\} \quad \text{for} \quad 1 \leq i \leq r.
\]
Similarly,
\[
    \overline{d}_0 = \min \{\overline{d}_0, \overline{d}_1, \ldots, \overline{d}_{\rho_0}\} = [\varepsilon k].
\]
Set
\[
    M_0 = \min_{0 \leq j \leq m} \overline{d}_j = \min \{\overline{d}_0, \overline{d}_{\rho_0+1}, \ldots, \overline{d}_{\rho_{r-1}+1}\}.
\]
Define
\[
    t_i = \overline{d}_{\rho_{i-1}+1} - M_0 \quad \text{for} \quad 1 \leq i \leq r, \quad t_0 = \overline{d}_0 - M_0 = [\varepsilon k] - M_0.
\]
Thus, \( t_0, t_1, \ldots, t_r \) are non-negative integers \( < 2\varepsilon k \) with at least one equal to 0.
Let $G(x, y)$ be defined as in Theorem 3.1. Thus,

$$G(x, y) = \sum_{j=0}^{\rho_0} a_j x^{\overline{d}_j} y^{\ell_j} = \sum_{j=0}^{\rho_0} a_j x^{\overline{d}_j} + \sum_{j=\rho_0+1}^{\rho_1} a_j x^{\overline{d}_j} y^{\ell_{\rho_1}} + \cdots + \sum_{j=\rho_{r-1}+1}^{\rho_r} a_j x^{\overline{d}_j} y^{\ell_{\ rho_r}}.$$  

For $0 \leq j \leq \rho_0$, we have

$$\overline{d}_j = d_j + \lfloor |\varepsilon k| \rfloor = d_j + t_0 + M_0.$$  

For $1 \leq i \leq r$ and $\rho_{i-1} + 1 \leq j \leq \rho_i$, we have

$$\overline{d}_j = d_j + \lfloor |\varepsilon k| \rfloor - k\ell_{\rho_i} = d_j + \overline{d}_{\rho_{i-1}+1} - d_{\rho_{i-1}+1} + \ell_{\rho_i}.$$  

Observe that, for $1 \leq i \leq r$, we deduce from (4.4) and the definition of $t_i$ that

$$in + \lfloor |\varepsilon k| \rfloor = k\ell_{\rho_i} + t_i + M_0 \quad \text{with } t_i + M_0 \in [0, 2|\varepsilon k|].$$  

As $\ell_{\rho_0} = 0$ and $t_0 + M_0 = \lfloor |\varepsilon k| \rfloor$, we see that (4.5) also holds for $i = 0$. Substituting (4.4) and then (4.5) into (4.3), we deduce

$$G(x, x^k) = f_0(x)x^{t_0+M_0} + f_1(x)x^{t_1+M_0}x^{k\ell_{\rho_1}} + \cdots + f_r(x)x^{t_r+M_0}x^{k\ell_{\rho_r}} = x^{\lfloor |\varepsilon k| \rfloor} F_0(x).$$  

Fix $i \in \{1, \ldots, r\}$. From (4.5), we obtain

$$(i - 1)n + \lfloor |\varepsilon k| \rfloor = k\ell_{\rho_{i-1}} + t_{i-1} + M_0 \quad \text{with } t_{i-1} + M_0 \in [0, 2|\varepsilon k|].$$  

By multiplying (4.6) by $i$ and (4.5) by $i - 1$ and taking a difference, we deduce

$$|\varepsilon k| = ki\ell_{\rho_{i-1}} - (i - 1)\ell_{\rho_i} + d'_i$$  

where

$$d'_i = i(t_{i-1} + M_0) - (i - 1)(t_i + M_0) \in (-2(r + 1)|\varepsilon k|, 2r|\varepsilon k|).$$  

As $\varepsilon = 1/(2r + 2)$, we deduce that $k(i\ell_{\rho_{i-1}} - (i - 1)\ell_{\rho_i})$ is a multiple of $k$ in the interval $(-k, k)$, and therefore $0$. Thus, $i\ell_{\rho_{i-1}} = (i - 1)\ell_{\rho_i}$ for each $i \in \{1, \ldots, r\}$. Considering $i = 1, \ldots, r$ in turn, we deduce

$$\ell_{\rho_0} = 0 \quad \text{and } \ell_{\rho_i} = i\ell_{\rho_1} \quad \text{for } 1 \leq i \leq r.$$  

Define $\ell = \ell_{\rho_1}$. Recall that after the statement of Theorem 3.1, we showed that $\ell_j \geq 1$ for some $j$. Hence, $\ell \geq 1$.

From $i\ell_{\rho_{i-1}} = (i - 1)\ell_{\rho_i}$, (4.7) and the definition of $d'_i$, we deduce

$$it_{i-1} - (i - 1)t_i + M_0 = \lfloor |\varepsilon k| \rfloor \quad \text{for } 1 \leq i \leq r.$$
Taking $i = j + 1$ and $i = j$ in this equation, subtracting the first from the second, and dividing by $j$, we obtain
\[2t_j = t_{j+1} + t_{j-1} \quad \text{for } 1 \leq j \leq r - 1.\]

In other words, $t_j$ is the average of $t_{j-1}$ and $t_{j+1}$ for $1 \leq j \leq r - 1$. Hence, the minimum value of $t_i$ occurs for $i = 0$ or $i = r$. Recall that the $t_i$ are non-negative with at least one equal to 0. Therefore, either $t_0 = 0$ or $t_r = 0$. Define
\[t = \begin{cases} t_1 & \text{if } t_0 = 0, \\ t_{r-1} & \text{if } t_r = 0. \end{cases}\]

Since $t_j$ is the average of $t_{j-1}$ and $t_{j+1}$ for $1 \leq j \leq r - 1$, we deduce that either $t_i = it$ for $0 \leq i \leq r$, or $t_i = (r - i)t$ for $0 \leq i \leq r$.

Combining the above, we find that one of
\[(4.9) \quad x^{M_0}(f_0(x) + f_1(x)x^tx^{kt} + \cdots + f_{r-1}(x)x^{(r-1)t}x^{(r-1)kt} + f_r(x)x^{rt}x^{rk \ell})
\]
and
\[(4.10) \quad x^{M_0}(f_0(x)x^{rt} + f_1(x)x^{(r-1)t}x^{kt} + \cdots + f_{r-1}(x)x^{t}x^{(r-1)kt} + f_r(x)x^{rk \ell})
\]
is equal to $x^{[\varepsilon k]}F_0(x)$. In the first case above, (4.8) with $i = 1$ implies $M_0 = [\varepsilon k]$. In the second case, (1.8) with $i = r$ implies $M_0 = [\varepsilon k] - rt$.

We focus now on $G(x, y)$. We know that $G(x, y)$ is either
\[x^{M_0}(f_0(x) + f_1(x)x^ty^\ell + \cdots + f_{r-1}(x)x^{t}x^{(r-1)\ell} + f_r(x)x^{rt}y^{\ell})
\]
or
\[x^{M_0}(f_0(x)x^{rt} + f_1(x)x^{(r-1)t}y^\ell + \cdots + f_{r-1}(x)x^{t}y^{(r-1)\ell} + f_r(x)y^{r\ell}).
\]

We deduce that $M$ in Theorem 3.1 is $M_0$ in the first case, but the value of $M$ depends on whether $f_r(0) = 0$ in the second case. If $f_r(0) \neq 0$, then $M = M_0$ in this case as well.

In any case, to deduce the irreducibility of the non-reciprocal part of $F(x, x^n)$ for $n$ satisfying (1.2), Theorem 3.1 implies that it suffices to show that both
\[(4.11) \quad f_0(x) + f_1(x)x^ty^\ell + \cdots + f_{r-1}(x)x^{(r-1)t}y^{(r-1)\ell} + f_r(x)x^{t}y^{r\ell}
\]
and
\[(4.12) \quad f_0(x)x^{rt} + f_1(x)x^{(r-1)t}y^\ell + \cdots + f_{r-1}(x)x^{t}y^{(r-1)\ell} + f_r(x)y^{r\ell},
\]
apart from possibly having a factor of a power of $x$, are irreducible as polynomials in two variables for every non-negative integer $t$.

We summarize this as follows.

**Theorem 4.1.** Let $F(x, y)$ be as in (2.1) with
\[\gcd_{\mathbb{Z}[x]}(f_0(x), f_1(x), \ldots, f_r(x)) = 1, \quad f_0(0) \neq 0, \quad f_r(x) \neq 0.
\]
Let $n$ be large enough so that (1.2) holds. Then the non-reciprocal part of $F(x, x^n)$ is not reducible if, for every non-negative integer $t$ and every positive integer $\ell$, the polynomials (4.11) and (4.12) are irreducible in $\mathbb{Z}[x, x^{-1}, y]$.

Theorem 4.1 is close to what we stated as Theorem 1.1 in the introduction. However, if we are not interested in establishing that $F(x, x^n)$ is irreducible for all $n$ sufficiently large but rather for $n$ sufficiently large of a certain form, then Theorem 1.1 is valuable and needs a little more justification. We begin by showing $n = k\ell \pm t$.

First, consider (4.11). We recall the discussion after (4.9) and (4.10). In the case of (4.11), we have $M_0 = \lfloor \varepsilon k \rfloor$ in (4.9). The values of $t$ and $\ell$ were determined by

$$t = t_1 = \overline{d}_{\rho_0+1} - M_0 = \overline{d}_{\rho_0+1} - \lfloor \varepsilon k \rfloor \quad \text{and} \quad \ell = \ell_{\rho_1} = \ell_{\rho_0+1}.$$

Further, $d_{\rho_0+1} = n$. From Theorem 3.1, we deduce

$$n + \lfloor \varepsilon k \rfloor = d_{\rho_0+1} + \lfloor \varepsilon k \rfloor = k\ell_{\rho_0+1} + \overline{d}_{\rho_0+1} = k\ell + t + \lfloor \varepsilon k \rfloor.$$ 

Thus, $n = k\ell + t$. In the notation of Theorem 3.1 and (4.1), $F_0(x) = F(x, x^n)$ and the value of $n$ comes from the expression $f_1(x)x^n$ that one obtains by replacing $y$ with $x^{\varepsilon k}$ in (4.11). In the case of (4.12), we have

$$0 = t_r = \overline{d}_{\rho_{r-1}+1} - M_0 = \overline{d}_{\rho_{r-1}+1} - \lfloor \varepsilon k \rfloor + rt \quad \text{and} \quad \ell_r = r\ell.$$

Thus,

$$rn + \lfloor \varepsilon k \rfloor = d_{\rho_{r-1}+1} + \lfloor \varepsilon k \rfloor = k\ell_{\rho_{r-1}+1} + \overline{d}_{\rho_{r-1}+1} = k\ell_r + \lfloor \varepsilon k \rfloor - rt = r(k\ell - t) + \lfloor \varepsilon k \rfloor.$$ 

Hence, in this case, $n = k\ell - t$, and the value of $n$ can be viewed as coming from the expression $f_1(x)x^n$ that one obtains by dividing the polynomial in (4.12) by $x^{rt}$ and replacing $y$ with $x^{\varepsilon k}$.

The condition on $k$ in Theorem 1.1 follows from our choice of $k \geq k_0$. Recall that the $t_j$ are non-negative integers $< 2\varepsilon k$ and that $\varepsilon = 1/(2r + 2)$. As $t_0, t_1, \ldots, t_r$ are the same as $0, t, 2t, \ldots, rt$ in some order, we deduce $t < k/(r(r + 1))$.

This completes the justification of Theorem 1.1.

5. Applications. In this section, we give three examples using a couple different approaches to show how one can apply Theorem 1.1. The first example is meant just to demonstrate the power of the approach for non-reciprocal polynomials. The last two examples come from the Laurent polynomials discussed in the introduction. Recalling the first one listed there was handled in [6], the last two examples here address the two other Laurent polynomials beginning with the last one.

We begin with a preliminary result.
LEMMA 5.1. Let \( r \in \mathbb{Z}^+ \) and \( f_0(x), f_1(x), \ldots, f_r(x) \in \mathbb{Z}[x] \) with \( \gcd_{\mathbb{Z}[x]}(f_0(x), f_1(x), \ldots, f_r(x)) = 1 \), \( f_0(0) \neq 0 \), \( f_r(x) \neq 0 \).

For \( t \in \mathbb{Z}^+ \cup \{0\} \), set

\[
F_{1,t}(x,y) = \sum_{j=0}^{r} f_j(x)x^j y^t \quad \text{and} \quad F_{2,t}(x,y) = \sum_{j=0}^{r} f_j(x)x^{(r-j)t} y^j.
\]

Let \( m \in \mathbb{Z}^+ \). For each \( j \in \{1, 2\} \), if \( J_x F_{j,s}(x,y^m) \) is irreducible in \( \mathbb{Z}[x,y] \) for all \( s \in \{0, 1, \ldots, m-1\} \), then \( J_x F_{j,t}(x,y^m) \) is irreducible in \( \mathbb{Z}[x,y] \) for all \( t \in \mathbb{Z}^+ \cup \{0\} \).

**Proof.** Fix \( t \in \mathbb{Z}^+ \cup \{0\} \), and let \( q \) and \( s \) be non-negative integers with \( 0 \leq s < m \) such that \( t = mq + s \). Observe that

\[
F_{1,t}(x,(y/x^t)^m) = F_{1,s}(x,y^m) \quad \text{and} \quad F_{2,t}(x,(x^q y)^m) = x^{mrq} F_{2,s}(x,y^m).
\]

Fix \( j \in \{1, 2\} \). The greatest common divisor condition on the \( f_j(x) \) implies that there are no irreducible polynomials in \( \mathbb{Z}[x] \) dividing all the coefficients of \( J_x F_{j,t}(x,y) \) viewed as a polynomial in \( y \). A factorization of \( F_{j,t}(x,y^m) \) in \( \mathbb{Q}(x)[y] \) into polynomials of degree > 0 in \( y \) will correspond to a factorization of \( F_{j,s}(x,y^m) \) in \( \mathbb{Q}(x)[y] \) into polynomials of degree > 0 in \( y \), and vice versa. We deduce from Gauss’s lemma that \( J_x F_{j,t}(x,y^m) \) is an irreducible polynomial in \( \mathbb{Z}[x,y] \) if and only if \( J_x F_{j,s}(x,y^m) \) is an irreducible polynomial in \( \mathbb{Z}[x,y] \), implying the lemma. ■

Lemma 5.1 allows us to take a polynomial \( F_{j,t}(x,y) \) as above and determine whether \( J_x F_{j,t}(x,y^m) \) is irreducible in \( \mathbb{Z}[x,y] \) for some \( m \in \mathbb{Z}^+ \) and all \( t \in \mathbb{Z}^+ \cup \{0\} \) by directly checking the irreducibility of \( J_x F_{j,t}(x,y^m) \) for \( t \) in the restricted range \( \{0, 1, \ldots, m-1\} \). This will be particularly useful in our examples when \( m = 1 \) and \( m = 4 \) for \( F_{j,t}(x,y) \) associated with (4.11) and (4.12), allowing us to easily apply Theorem 4.1. The basic steps to applying Theorem 1.1 or Theorem 4.1 in our examples below can be summarized as follows.

**STEP 1:** Given \( F(x,y) \) as in Theorem 1.1 or Theorem 4.1 set \( F_{\ell}(x,y) \) to be one of the polynomials in (4.11) and (4.12) with \( \ell = 1 \). Apply Lemma 5.1 with \( m = 1 \) to show that \( J_x F_{\ell}(x,y) \) is irreducible in \( \mathbb{Z}[x,y] \) for all non-negative integers \( t \).

**STEP 2:** With \( F(x,y) = J_x F_{\ell}(x,y) \), determine the finite set \( \mathcal{P} \) of odd primes \( p \) satisfying (2.6) for some \( g_j(x) \in \mathbb{Z}[x] \) depending on \( p \). In our applications, the set \( \mathcal{P} \) will be independent of \( t \).

**STEP 3:** Apply Lemma 5.1 with \( F(x,y) = J_x F_{\ell}(x,y) \) and with \( m = 4 \) and \( m = p \in \mathcal{P} \).

**STEP 4:** Deduce from Theorem 2.1 that \( J_x F_{\ell}(x,y^\ell) \) is irreducible for all non-negative integers \( t \) and all positive integers \( \ell \).
Factorization of lacunary polynomials

STEP 5: Deduce from Theorem 1.1 or Theorem 4.1 that the non-reciprocal part of \( F(x, x^n) \) is not reducible.

Our second example will be more elaborate with two unknowns in the exponents of our polynomial, and hence will require some additional work.

EXAMPLE 1. Let \( n \geq 2 \) be an integer, and set
\[
G(x) = x^{6n} + (x + 1)x^{5n+1} + 2x^{4n} + (x^4 - x^3 - x^2 - 2x - 2)x^{3n-2} \\
+ 2x^{2n} + (x + 1)x^{n-2} + 1.
\]
One can check that if \( n = 4 \), the polynomial factors as a product of two irreducible non-reciprocal polynomials. For \( n \) sufficiently large, we show that \( G(x) \) has no reciprocal irreducible factors and the non-reciprocal part of \( G(x) \) is irreducible. Then it will follow that \( G(x) \) is irreducible for all \( n \) sufficiently large.

Assume \( u(x) \) is an irreducible reciprocal factor of \( G(x) \), and let \( \alpha \) be a root of \( u(x) \). Since \( G(0) \neq 0 \), we see that \( \alpha \neq 0 \), and \( u(x) \) being reciprocal implies that \( 1/\alpha \) is a root of \( u(x) \). We deduce that \( \alpha \) is a root of \( G(x) \) and of \( \tilde{G}(x) = x^{\deg G} G(1/x) \). Since
\[
\tilde{G}(x) = x^{6n} + (x + 1)x^{5n+1} + 2x^{4n} + (-2x^4 - 2x^3 - x^2 - x + 1)x^{3n-2} \\
+ 2x^{2n} + (x + 1)x^{n-2} + 1,
\]
we deduce that \( \alpha \) is a root of
\[
G(x) - \tilde{G}(x) = (3x^4 + x^3 - x - 3)x^{3n-2}.
\]
Therefore, \( u(x) \) is an irreducible factor of
\[
3x^4 + x^3 - x - 3 = (x - 1)(x + 1)(3x^2 + x + 3).
\]
One checks that \( \pm 1 \) are not roots of \( G(x) \). Furthermore, since \( G(x) \in \mathbb{Z}[x] \) is monic, the irreducible polynomial \( 3x^2 + x + 3 \) cannot be a factor of \( G(x) \). We obtain a contradiction. Thus, \( G(x) \) has no reciprocal irreducible factors.

Let \( n \) be sufficiently large. Let
\[
F(x, y) = \sum_{j=0}^{6} f_j(x) y^j,
\]
where
\[
f_0(x) = 1, \quad f_1(x) = x + 1, \quad f_2(x) = 2x^4, \\
f_3(x) = x^4(x^4 - x^3 - x^2 - 2x - 2), \\
f_4(x) = 2x^8, \quad f_5(x) = x^{11}(x + 1), \quad f_6(x) = x^{12}.
\]
Then \( F(x, x^{n-2}) = G(x) \).
Our goal now is to apply Theorem 4.1 or, for this example, Theorem 4.1. Let
\[
F_{1,t}(x, y) = \sum_{j=0}^{6} f_j(x)x^jy^j \quad \text{and} \quad F_{2,t}(x, y) = \sum_{j=0}^{6} f_j(x)x^{(6-j)t}y^j.
\]
To show \(J_x F_{1,t}(x, y^\ell)\) and \(J_x F_{2,t}(x, y^\ell)\) are irreducible polynomials in \(\mathbb{Z}[x, y]\) for all non-negative integers \(t\) and positive integers \(\ell\), we apply Theorem 2.1. To ensure the condition in Theorem 2.1 that \(F(x, y)\) is irreducible in \(\mathbb{Z}[x, y]\) holds, one can justify that \(J_x F_{1,t}(x, y)\) and \(J_x F_{2,t}(x, y)\) are irreducible polynomials for all non-negative integers \(t\) by a direct application of Lemma 5.1 with \(m = 1\).

Now, since \(f_1(x) = x + 1\), we see that for each prime \(p\), (2.6) holds neither with \(F\) replaced by \(F_{1,t}\) nor with \(F\) replaced by \(F_{2,t}\). To finish applying Theorem 2.1 it remains to show \(J_x F_{1,t}(x, y^4)\) and \(J_x F_{2,t}(x, y^4)\) are irreducible polynomials for all non-negative integers \(t\). One can establish this by simply once again appealing to Lemma 5.1 in this case with \(m = 4\).

Given \(G(x)\) has no irreducible reciprocal factors, Theorem 4.1 now implies that \(G(x)\) is irreducible for all \(n\) sufficiently large.

**Example 2.** In the introduction, we mentioned the Laurent polynomial
\[
x^{4b} - x^{2b} - x^a - 2 - x^{-a} - x^{-2b} + x^{-4b}
\]
associated with the trace field under \(-a/b\) Dehn fillings of the complement of the 4_1 knot. Here, \(a\) and \(b\) are coprime positive integers. For fixed \(a\) and sufficiently large \(b\) or for fixed \(b\) and sufficiently large \(a\), one can apply the prior material to obtain information on the factorization of the non-reciprocal part of the polynomial \(J_x(x^{4b} - x^{2b} - x^a - 2 - x^{-a} - x^{-2b} + x^{-4b})\).

We illustrate this here by considering the case that \(a\) is fixed and \(b\) is sufficiently large. Then we are interested in the factorization of
\[
F_0(x) = x^{8b} - x^{6b} - x^{4b+a} - 2x^{4b} - x^{4b-a} - x^{2b} + 1
\]
\[
= x^{4a}x^{2b-a} - x^{3a}x^{3b-a} - (x^a + 1)^2x^ax^{2(2b-a)} - x^{4a}x^{2b-a} + 1.
\]
We define
\[
F(x, y) = f_0(x) + f_1(x)y + f_2(x)y^2 + f_3(x)y^3 + f_4(x)y^4,
\]
where
\[
f_0(x) = 1, \quad f_1(x) = -x^a, \quad f_2(x) = -(x^a + 1)^2x^a, \quad f_3(x) = -x^{3a}, \quad f_4(x) = x^{4a}.
\]

Thus, with \(n = 2b - a\), we have \(F(x, x^n) = F_0(x)\). Further, define
\[
F_1(x, y) = f_0(x) + f_1(x)x^ty + f_2(x)x^{2t}y^2 + f_3(x)x^{3t}y^3 + f_4(x)x^{4t}y^4,
\]
\[
F_2(x, y) = f_0(x)x^{4t} + f_1(x)x^{3t}y + f_2(x)x^{2t}y^2 + f_3(x)x^{t}y^3 + f_4(x)y^4.
\]
For Theorem 1.1 we want to determine whether the polynomials \( J_x F_1(x, y^t) \) and \( J_x F_2(x, y^t) \) are irreducible polynomials in \( \mathbb{Z}[x, y] \).

Fix \( j \in \{1, 2\} \). We want to apply Theorem 2.1 to \( J_x F_j(x, y) \), so we show first that \( J_x F_j(x, y) \) is irreducible. In the example at the end of Section 2 we saw that the polynomial

\[
1 - x(x+1)^n - 2x^2y^{2n} - x^2(x+1)^n + x^4y^{4n}
\]

is irreducible for every positive integer \( n \). By a change of variables, we see then that

\[
1 - y(y+1)x^a - 2y^2x^{2a} - y^2(x+1)x^{3a} + y^4x^{4a}
\]

is irreducible for every positive integer \( a \). Observe that this is the same as \( F_1(x, y) \) and \( F_2(x, y) \) with \( t = 0 \). Applying Lemma 5.1 with \( m = 1 \), we deduce that \( J_x F_j(x, y) \) is irreducible independently of the value of \( t \in \mathbb{Z}^+ \cup \{0\} \).

In the case of \( F_1(x, y) \), in Theorem 1.1 we have \( n = k\ell + t \). Also, \( F_0(x) = F(x, x^n) = F_1(x, x^{k\ell}) \) so that \( n = 2b - a \).

Assume that \( F_1(x, y^t) \) is irreducible but \( F_1(x, y^\ell) \) is reducible for some positive integer \( \ell \). By Theorem 2.1 there must then be an odd prime \( p \) dividing \( \ell \) for which \( F_1(x, y^p) \) is irreducible. Further, as stated in Theorem 2.1 we obtain (2.6) with \( F \) there replaced by \( F_1 \). We want to obtain a contradiction, but if \( p \mid a \) and \( p \mid t \), then in fact (2.6) holds with \( F \) replaced by \( F_1 \). However, then we have \( p \mid a \), \( p \mid t \) and \( p \mid \ell \) so that \( p \mid (k\ell + t) \), which is equivalent to \( p \mid n \). As \( n = 2b - a \) and \( p \) is an odd prime dividing \( a \), we would have \( p \mid b \), contrary to the assumption that \( a \) and \( b \) are coprime positive integers. Thus, either \( p \nmid a \) or \( p \nmid t \). Using (2.6) with \( F \) replaced by \( F_1 \), we see that \( f_1(x)x^t \) is a \( p \)th power modulo \( p \), and consequently \( p \mid (a + t) \). Also, \( f_2(x)x^{2t} \) is a \( p \)th power modulo \( p \), so its degree as a polynomial modulo \( p \), which is \( 3a + 2t \), must be divisible by \( p \). On the other hand, \( p \) divides both \( a + t \) and \( 3a + 2t \) implies \( p \mid a \) and \( p \mid t \), giving a contradiction.

Observe that if \( F_1(x, y^t) \) is reducible, the remarks after Theorem 2.1 immediately give us that \( F_1(x, y^2) \) is reducible and (2.6) holds with \( F \) there replaced by \( F_1 \) and \( p = 2 \). From (2.6), we deduce that \( f_1(x)x^t \) and \( f_2(x)x^{2t} \) are squares modulo 2 so that \( a + t \) and \( a + 2t \) are even. Hence, both \( a \) and \( t \) are even. We make particular use of the latter.

We write \( t \) in the form \( 2q \), where \( q \) is a non-negative integer. Since \( f_0(x) = 1 \), we see that if \( F_1(x, y^2) \) is reducible, then so is \( F_1(x, (y/x^q)^2) \). As \( F_1(x, (y/x^q)^2) \) takes the form of \( F_1(x, y^2) \) with \( t = 0 \), we can restrict our attention to determining whether \( F_1(x, y^2) \) is reducible with \( t = 0 \).

Set \( t = 0 \). Let \( W(x, y) = F_1(x, y^2) \). We provide here an alternative approach from prior material in this paper for establishing that \( W(x, y) \) is
irreducible. The degree of $F_1(x, y^2)$ in $y$ is 8. We consider explicit values of $y \in \mathbb{Z}$ for which $W(x, y)$ can be checked to be irreducible in $\mathbb{Z}[x]$. For example, consider

$$W(x, 2) = 2^8x^{4a} - 2^6x^{3a} - 2^4(x^a + 1)^2x^a - 2^2x^a + 1.$$ 

We write $W(x, 2) = w(x^a)$ where in this case

$$w(x) = 256x^4 - 80x^3 - 32x^2 - 20x + 1.$$ 

One checks that the quartic $w(x)$ is irreducible in $\mathbb{Z}[x]$ (using Maple, for example). By Capelli’s theorem, $w(x^a)$ can be reducible only if $p | a$ for some prime $p$ and $w(x^p)$ is reducible, or $4 | a$ and $w(x^4)$ is reducible. A computation shows that $w(x^4)$ is irreducible, so this second case does not happen. In the first case, Capelli’s theorem implies we can furthermore assume that if $\gamma$ is a root of $w(x)$, then $\gamma$ is a $p$th power in $\mathbb{Q}(\gamma)$ so that the norm of $\gamma$ is a $p$th power in $\mathbb{Q}$. The norm of a root of $w(x)$ is $1/256 = (1/2)^8$. Hence, in this case $p = 2$. As we have already verified that $w(x^4)$ is irreducible, we know $w(x^2)$ is irreducible. Thus, $W(x, 2)$ is irreducible for all integers $a \geq 1$.

The idea now is to repeat the above process to obtain the irreducibility of $W(x, k)$ for 17 different $k \in \mathbb{Z}$ and for all positive integers $a$. We used $k \in \{2, 3, \ldots, 18\}$. Let $w_k(x)$ be the analog to $w(x)$ above so that $w_k(x^a) = W(x, k)$. For each $k$, we verified computationally the irreducibility of $w_k(x^a)$ for $a \in \{1, 3, 4\}$. As the norm of a root of $w_k(x)$ is $1/k^8$ and this can be a $p$th power for $k \in \{2, 3, \ldots, 18\}$ only for $p \in \{2, 3\}$, we deduce as above that $W(x, k)$ is irreducible for each $k \in \{2, 3, \ldots, 18\}$ and for all positive integers $a$.

Assume that there is a positive integer $a$ for which $W(x, y)$ is reducible in $\mathbb{Z}[x, y]$. As the constant term of $W(x, y)$ is 1, we deduce that $W(x, y) = F_1(x, y^2) = U(x, y)V(x, y)$ where $U(x, y)$ and $V(x, y)$ are in $\mathbb{Z}[x, y]$ and each of degree $\geq 1$ in $y$. Denote these degrees by $d_U$ and $d_V$, respectively. For each $k \in \{2, 3, \ldots, 18\}$, the irreducibility of $W(x, k) = U(x, k)V(x, k)$ in $\mathbb{Z}[x]$ implies that one of $U(x, k)$ or $V(x, k)$ is $\pm 1$. Since $W(x, y) = U(x, y)V(x, y)$, we have $d_U + d_V = 8$. The pigeon-hole principle guarantees that there is a subset $S$ of $\{2, 3, \ldots, 18\}$ such that one of the following holds:

- The size of $S$ is $d_U + 1$ and $U(x, k) = 1$ for all $k \in S$.
- The size of $S$ is $d_U + 1$ and $U(x, k) = -1$ for all $k \in S$.
- The size of $S$ is $d_V + 1$ and $V(x, k) = 1$ for all $k \in S$.
- The size of $S$ is $d_V + 1$ and $V(x, k) = -1$ for all $k \in S$.

We consider the first possibility above, noting the argument in each case is similar. Writing $S = \{k_0, k_1, \ldots, k_s\}$ and $U(x, y) = u_0(x) + u_1(x)y + \cdots + u_s(x)y^s$ where $s = d_U$, we obtain

$$u_0(x) + u_1(x)k_j + \cdots + u_s(x)k_j^s = 1 \quad \text{for} \quad 0 \leq j \leq s.$$
Thus,
\[
\begin{pmatrix}
1 & k_0 & \cdots & k_s^0 \\
1 & k_1 & \cdots & k_s^1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & k_s & \cdots & k_s^s
\end{pmatrix}
\begin{pmatrix}
u_0(x) \\
u_1(x) \\
\vdots \\
u_s(x)
\end{pmatrix}
= \begin{pmatrix}
1 \\
1 \\
\vdots \\
1
\end{pmatrix}.
\]

The matrix above is a Vandermonde matrix, and its determinant is non-zero. Hence, there are unique \(u_0(x), u_1(x), \ldots, u_s(x)\) satisfying the matrix equation above. Since the values \(u_0(x) = 1\) and \(u_j(x) = 0\) for \(1 \leq j \leq s\) satisfy the equation, we deduce that \(U(x, y) = 1\), contradicting \(d_U \geq 1\). Therefore, \(W(x, y)\) is irreducible in \(\mathbb{Z}[x, y]\) for all positive integers \(a\).

So far we have shown that \(F_1(x, y^t)\) is irreducible in \(\mathbb{Z}[x, y]\) for all integers \(t \geq 0\) and \(\ell \geq 0\) for which \(n = 2b - a = k\ell + t\). We now turn to \(F_2(x, y^\ell)\) where the integers \(t \geq 0\) and \(\ell \geq 0\) that we are interested in satisfy \(n = 2b - a = k\ell - t\). We give a similar argument to that just given for \(F_1(x, y)\). In the case of \(F_2(x, y)\), write \(F_2(x, y) = x^{k_2}G_2(x, y)\), where \(G_2 = J_x F_2\) and \(k_2\) may be positive (and will be unless \(t = 0\)). We want to show \(G_2(x, y^\ell)\) is irreducible. We note that the explicit values of \(f_j(x)\) give

\[
k_2 = \begin{cases}
4t & \text{if } 0 \leq t \leq a/2, \\
a + 2t & \text{if } a/2 < t \leq 3a/2, \\
4a & \text{if } t > 3a/2.
\end{cases}
\]

Fix an odd prime \(p\) satisfying \([2.7]\). To simplify notation, we set \(u = k_2\).

Observe that \(u\) is independent of \(p\) and \(u \leq 4t\). Assume that \(F_2(x, y^p)/x^{u} = G_2(x, y^p)\) is a reducible polynomial. By Theorem 2.1 we know that \([2.6]\) holds. Looking at the constant term and the coefficients of \(y\) and \(y^2\) in \(F_2(x, y^p)/x^{u}\), we see that \(p \mid (4t - u), p \mid (a + 3t - u)\) and \(p \mid (3a + 2t - u)\). These imply \(p \mid a, p \mid t\) and \(p \mid u\). As in the case of \(F_1(x, y^p)\), this leads to \(p\) dividing both \(a\) and \(b\), contradicting the fact that \(a\) and \(b\) are relatively prime.

Defining \(u\) as above, we assume now that \(F_2(x, y^4)/x^{u} = G_2(x, y^4)\) is reducible. As with \(F_1(x, y)\), we can deduce from the comments after Theorem 2.1 that \(F_2(x, y^2)/x^{u}\) is reducible. Taking \(p = 2\) in our discussion above about \(F_2(x, y^p)/x^{u}\), we deduce \(2 \mid t, 2 \mid u\) and \(2 \mid a\) (but not necessarily \(2 \mid b\)). Writing \(t = 2q\), we see that \(F_2(x, (x^q y)^2)/x^{8q}\) is of the form \(F_2(x, y^2)\) with \(t = 0\). Furthermore, as the coefficients of \(F_2(x, y^2)/x^{u}\) as a polynomial in \(y\) have no common irreducible factor in \(\mathbb{Z}[x]\), we can conclude that if \(F_2(x, y^2)/x^{u}\) is reducible, then \(F_2(x, y^2)\) with \(t = 0\) is reducible.

With \(t = 0\), we have

\[F_2(x, y) = F_1(x, y) = F(x, y)\]
As we have already established in this case that $F_1(x, y^2)$ is irreducible for all positive integers $a$, we deduce that $F_2(x, y^2)$ is irreducible for all positive integers $a$.

We therefore see that any polynomial $F_1(x, y)$ or $F_2(x, y)$ arising from $J_x F_0(x)$ is an irreducible polynomial in $\mathbb{Z}[x, y]$. Theorem 1.1 now implies that for each fixed positive integer $a$ and every sufficiently large positive integer $b$ relatively prime to $a$, the non-reciprocal part of $F_0(x)$ is not reducible. The phrase “not reducible” is deliberate here, as $F_0(x)$ is a reciprocal polynomial and cannot have exactly one irreducible non-reciprocal factor. The fact that the non-reciprocal part of $F_0(x)$ is not reducible implies then that the non-reciprocal part of $F_0(x)$ is identically 1. In other words, we deduce that $F_0(x)$ is a product of irreducible reciprocal polynomials (for fixed $a$ and sufficiently large $b$ relatively prime to $a$).

**Example 3.** We consider

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

associated with the trace field of the Whitehead link for the complement of the $(-2, 3, 3 + 2n)$ pretzel knot $K_n$. This polynomial $F(x)$ is in $\mathbb{Z}[x]$ for all $n \geq 2$, and one easily checks that $(x-1)^2$ is a factor. A computation suggests that the other factor is always irreducible. Observe that the polynomial $x^{2n} + (-x^3 + 4x^2 - 8 + 4x^{-2} - x^{-3})x^n + 1$ with more general exponents does not have this property. For example, for $n = 7$, this polynomial factors as

$$(x^4 + x^3 + 3x^2 + x + 1)(x^6 - x^5 + 2x^3 - x + 1)(x-1)^2(x+1)^2.$$ 

It is reasonable to obtain a similar result below for this more general polynomial; however, some adjustments to the arguments below would be needed.

We show here that, for $n$ sufficiently large, $F(x)$ is a product of reciprocal irreducible polynomials. We rewrite

$$F(x) = f_0(x) + f_1(x)x^{n-2} + f_2(x)x^{2(n-2)} + f_3(x)x^{3(n-2)} + f_4(x)x^{4(n-2)},$$

where

$$f_0(x) = 1, \quad f_1(x) = 0, \quad f_2(x) = -x^7 + 4x^6 - 8x^4 + 4x^2 - x,$$

$$f_3(x) = 0, \quad f_4(x) = x^8.$$ 

To apply Theorem 1.1, we want to determine whether the polynomials $J_x F_1(x, y^t)$ and $J_x F_2(x, y^t)$ are irreducible polynomials in $\mathbb{Z}[x, y]$, where

$$F_1(x, y) = f_0(x) + f_2(x)x^{2t}y^2 + f_4(x)x^{4t}y^4,$$

$$F_2(x, y) = f_0(x)x^{4t} + f_2(x)x^{2t}y^2 + f_4(x)y^4.$$ 

We make use of Theorem 2.1.
Fix $j \in \{1, 2\}$. A direct application of Lemma 5.1 with $m = 1$ implies each $J_x F_j(x, y)$ is irreducible independent of $t \in \mathbb{Z}^+ \cup \{0\}$. We are now ready to apply Theorem 2.1 to $J_x F_j(x, y)$. We let $g(x) = -x^6 + 4x^5 - 8x^3 + 4x - 1$, so $f_2(x) = xg(x)$. For each odd prime $p$, observe that $g(0) \equiv -1 \pmod{p}$ and the degree of $g(x)$ is 6 modulo $p$. Hence, $f_2(x)$ times a power of $x$ cannot be a $p$th power modulo $p$ if $p \geq 7$. A direct check shows that $g(x)$ is furthermore not a $p$th power modulo $p$ for $p \in \{3, 5\}$, and hence the same holds for $f_2(x)$ times a power of $x$. It follows that for any odd prime $p$, $J_x F_j(x, y)$ does not satisfy (2.6). To finish applying Theorem 2.1, we are left with considering the factorization of $J_x F_j(x, y^4)$. Applying Lemma 5.1 with $m = 4$ establishes that $J_x F_j(x, y^4)$ is irreducible in $\mathbb{Z}[x, y]$.

Hence, Theorem 2.1 implies $J_x F_1(x, y^\ell)$ and $J_x F_2(x, y^\ell)$ are irreducible polynomials in $\mathbb{Z}[x, y]$ for every positive integer $\ell$. Then Theorem 4.1 implies that the non-reciprocal part of $F(x)$ is not reducible for $n$ sufficiently large. Since $F(x)$ is a reciprocal polynomial, we conclude that $F(x)$ is a product of irreducible reciprocal polynomials.

Acknowledgements. The author thanks Stavros Garoufalidis for discussions which helped motivate this study and an anonymous referee for a number of helpful suggestions. He is also grateful for the encouragement and interest Andrzej Schinzel expressed to him on this research when they last met during a conference in Poznań, Poland, in 2017.

References


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