LINEAR RECURRENCE SEQUENCES IN DIOPHANTINE ANALYSIS

by

ELISA BELLAH

A DISSERTATION

Presented to the Department of Mathematics
and the Division of Graduate Studies of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

June 2022

DISSERTATION APPROVAL PAGE

Student: Elisa Bellah

Title: Linear Recurrence Sequences in Diophantine Analysis

This dissertation has been accepted and approved in partial fulfillment of the requirements for the Doctor of Philosophy degree in the Department of Mathematics by:

Shabnam Akhtari	Chair
Daniel Dugger	Core Member
Christopher Sinclair	Core Member
Benjamin Young	Core Member
Brittany Erickson	Institutional Representative

and

Krista Chronister	Vice Provost for Graduate Studies

Original approval signatures are on file with the University of Oregon Division of Graduate Studies.

Degree awarded June 2022

© 2022 Elisa Bellah

DISSERTATION ABSTRACT

Elisa Bellah

Doctor of Philosophy

Department of Mathematics

June 2022

Title: Linear Recurrence Sequences in Diophantine Analysis

Diophantine analysis is an area of number theory concerned with finding integral solutions to polynomial equations defined over the rationals, or more generally over a number field. In some cases, it is possible to associate a well-behaved recurrence sequence to the solution set of a Diophantine equation, which can be useful in generating explicit results. It is known that the solution set to any norm form equation is naturally associated to a family of linear recurrence sequences. As these sequences have been widely studied, Diophantine problems involving norm forms are well-suited to be studied through their associated sequences. In this dissertation, we use this method to study two such problems.

CURRICULUM VITAE

NAME OF AUTHOR: Elisa Bellah

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, OR
Portland State University, Portland, OR

DEGREES AWARDED:

Doctor of Philosophy, Mathematics, 2022, University of Oregon
Master of Science, Mathematics, 2017, University of Oregon
Bachelor of Science, Mathematics, 2015, Portland State University

AREAS OF SPECIAL INTEREST:

Number Theory
Diophantine Analysis

PROFESSIONAL EXPERIENCE:

Graduate Employee, University of Oregon, 2015-2022

GRANTS, AWARDS AND HONORS:

Anderson Distinguished Graduate Teaching Award, Department of Mathematics, University of Oregon, 2020

PUBLICATIONS:

Bellah, E. (2021). Norm Form Equations and Linear Divisibility Sequences. *International Journal of Number Theory.*

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Shabnam Akhtari, for all of her support and guidance over the years. I would also like to thank my WiN group leaders, Elena Fuchs and Damaris Schindler, for their advice and support, and for coming up with a fun project to keep me motivated through the last stages of my program.

Many thanks as well to my friends and fellow graduate students who supported me throughout the program, and to the community at AYE for keeping me sane through this process and reminding me what's important. Finally a special thank you to my sister, to whom I owe everything.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION AND BACKGROUND

1.1. Motivation

Diophantine analysis is an area of number theory concerned with finding integral solutions to Diophantine equations; that is, equations of the form

$$F(x_1, \ldots, x_n) = 0,$$

where F is a polynomial defined over the rationals, or more generally over a number field. Given such a Diophantine equation, typical problems include (1) determining the existence of solutions, (2) studying their distribution, and (3) giving explicit descriptions of the solution set and its arithmetic properties. Possibly the most famous Diophantine problem is on the existence of solutions to the Fermat equation

$$x^n + y^n = z^n \tag{1.1.1}$$

where n is some fixed positive integer. Conjectured by Fermat in the 17th century, and then only recently proven in the 1990s, it is now known that there are no positive integer solutions to (1.1.1) when $n \geq 3$. The solution set in the remaining nontrivial case, when $n = 2$, make up the Pythagorean triples. It is classically known that there are infinitely many Pythagorean triples, opening up further Diophantine problems. Explicit problems on the distribution of Pythagorean triples (as in [3] and [21]) and their arithmetic properties (as in [25] and [31]) have been widely studied. It is often the case that explicit Diophantine results such as

these lead to applications in cryptography and information security (see [18] for applications of Pythagorean triples in cryptography, for example).

In some cases, it is possible to associate a well behaved recurrence sequence to the solution set of a Diophantine equation. This strategy can be useful in generating explicit Diophantine results. One example of this is the use of Elliptic Divisibility Sequences, defined below, to study integer points on elliptic curves defined over $\mathbb{Q}$; for example, integer solutions to the cubic equation

$$y^2 = x^3 + ax + b. \tag{1.1.2}$$

By Siegel's theorem, we know that there are only finitely many integer solutions to (1.1.2) (see Chapter 9 of [27], for example). However little is known about the structure of the solution set. In [34], Ward showed that rational points on elliptic curves are associated to the terms of the nonlinear recurrence sequence $\{h_n\}$ satisfying

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_n^2. \tag{1.1.3}$$

More precisely, Ward showed that for any rational point P on an elliptic curve (1.1.2), we have

$$x(nP) = \frac{a_n}{h_n^2},$$

for some integer sequence $\{a_n\}$ and $x(nP)$ denoting the x-coordinate of the point obtained from adding P to itself n times using the usual group law on elliptic curves. The sequence $\{h_n\}$ is called an Elliptic Divisibility Sequence (EDS) and has several nice arithmetic properties as outlined in [34]. In particular, $\{h_n\}$ satisfies the divisibility property given in Definition 1.3.3 of Section 1.3. This association has led to several Diophantine results. For example, Hindry and Silverman studied

bounds on the number of integral multiples of points on elliptic curves in [16]. More recently, work has been done to bound the size of the largest n so that nP is integral. In [17] Ingram found a uniform bound on n by studying the sequence of valuations of an EDS, which was later improved by Stange in [30].

In this dissertation, we focus on Diophantine problems coming from norm form equations, which we discuss in detail in the next section. It is known that all rational reducible forms are integrally equivalent to a constant multiple of a product of norm forms (see Theorem 2 in Section 2.1 of [7], for example). Furthermore, as we'll see in Chapter II, the solution set to any norm form equation is naturally associated to a family of linear recurrence sequences. As these sequences have been widely studied, Diophantine problems involving norm forms are well-suited to be studied through their associated linear recurrence sequences. In this dissertation, we use this method to study two such problems. In the following sections, we provide the background on norm form equations and linear recurrence sequences used throughout this manuscript, and conclude the chapter with an outline of this dissertation.

1.2. Background on Norm Form Equations

Let K be a number field, and $W = \{w_1, \ldots, w_n\}$ a $\mathbb{Q}$-linearly independent subset of K. The *norm form* associated to the set W is given by

$$F_W(X_1, \ldots, X_n) := N_K(X_1 w_1 + \cdots + X_n w_n). \tag{1.2.4}$$

Note that F_W is in fact a rational form. To see this, let $\sigma_1, \ldots, \sigma_n$ denote the embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. By definition,

$$F_W(X_1, \ldots, X_n) = \prod_{i=1}^{n} (X_1\sigma_i(w_1) + \cdots + X_n\sigma_i(w_n)).$$

So F_W is homogeneous of degree n. Now, let $\tilde{\sigma}_j$ be an element in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ extending σ_j, where $\tilde{K}$ denotes the Galois closure of K. If we act on F_W by any $\tilde{\sigma}_j$, we have

$$\tilde{\sigma}_j F_W(X_1, \ldots, X_n) = \prod_{i=1}^{n} (X_1\tilde{\sigma}_j\sigma_i(w_1) + \cdots + X_n\tilde{\sigma}_j\sigma_i(w_n)),$$

which only reindexes our product. So, $\tilde{\sigma_j} F_W = F_W$ for each j, implying our coefficients must be rational.

Given a norm form F_W, it then is a classical Diophantine problem to ask for integer solutions to equations of the form

$$F_W(X_1, \ldots, X_n) = c, \tag{1.2.5}$$

where c is a fixed nonzero integer. We consider two simple examples.

Example. Let D be a nonsquare integer. If we let $W = \{1, \sqrt{D}\}$, then the corresponding norm form defined over $\mathbb{Q}(\sqrt{D})$ is $F_W(X, Y) = X^2 - DY^2$. In this case, we see that (1.2.5) is a Pell-type equation.

Example. If W is an integral basis for a number field K, the set of solutions to (1.2.5) with $c = \pm 1$ gives a complete list of units in K. So, the problem of finding units in a number field can be interpreted as such a Diophantine problem.

Given a $\mathbb{Q}$-linearly independent set W, let M be the $\mathbb{Z}$-module in K generated by W. Observe that if T is another basis for M, the norm forms F_W and F_T, which are defined in (1.2.4), are integrally equivalent. That is, there exist $(a_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$ so that if

$$Y_i = \sum_{j=1}^{n} a_{ij} X_j,$$

then we have $F_W(X_1, \ldots, X_n) = F_T(Y_1, \ldots, Y_n)$. So, integer solutions to (1.2.5) can be found by instead studying the elements in the associated module M of fixed norm c. The characterization of solutions to (1.2.5) depends on whether or not the associated module M is full in K (that is, whether $\operatorname{rank} M = [K : \mathbb{Q}]$).

Characterization in the case that M is full. Let

$$\mathcal{O}_M := \{\alpha \in K \mid \alpha M \subseteq M\}$$

denote the *coefficient ring* of the module M. It is known that when M is full in K, the coefficient ring $\mathcal{O}_M$ is an order in K (see Theorem 3 in Section 2.2 of [7], for example), and furthermore that M contains only a finite number of nonassociate elements of fixed norm c (see the Corollary to Theorem 5 in Section 2.2 of [7], for example). So, the set of elements in M of fixed norm c can be written as a disjoint union of finitely many families

$$\alpha_1 \mathcal{U}_M^+, \ldots, \alpha_\ell \mathcal{U}_M^+,$$

where

$$\mathcal{U}_M^+ := \{\varepsilon \in \mathcal{O}_M \mid N_K(\varepsilon) = 1\} \tag{1.2.6}$$

denotes the *positive unit group* of M.

Characterization in the case that M is not full. While the characterization in the full case is well-known, the characterization in the nonfull case was more recently provided by Schmidt in [23] and [24]. We give an overview of these results below. For each subfield L of K, let

$$M^L := \{\alpha \in M \mid \forall \lambda \in L, \exists z \in \mathbb{Z}_{\neq 0} \text{ so that } z\lambda\alpha \in M\},$$

and observe that M^L is a submodule of M. As above, we let $\mathcal{O}_{M^L}$ denote the coefficient ring of M^L, and $\mathcal{U}^+_{M^L}$ the units in $\mathcal{O}_{M^L}$ of positive norm. In [23], Schmidt showed that $\mathcal{O}_{M^L}$ is an order in L, and furthermore that the solutions to (1.2.5) are contained in finitely many families of the form

$$\mu\mathcal{U}^+_{M^L},$$

for some $\mu \in K$ and subfields $L \subset K$. The methods in [23] do not give an explicit method to construct all such families, but the following Lemma tells us when these families are finite.

Lemma 1.2.1 (Section 5 of [23])**.** M^L is nonzero if and only if M^L contains a submodule of the form αN, where N is full in L and $\alpha \in K$.

We call M *nondegenerate* when $M^L = \{0\}$ for every subfield L of K that is not rational or imaginary quadratic. By Lemma 1.2.1 and Dirichlet's unit theorem, there are only finitely many solutions to (1.2.5) in the nondegenerate case. In [24], Schmidt provided explicit upper bounds on the number of these solutions. We state this result below.

Theorem 1.2.2 (Theorem 1 of [24])**.** Suppose that F_W is a norm form with associated module M that is nondegenerate. Then, the number of solutions to (1.2.5) is upper bounded by

$$\min(r^{2^{30n}}, r^{c_2(n)}),$$

where $c_2(n) = (2n)^{n2^{n+4}}$ and $r = [K : \mathbb{Q}]$.

The results of Chapter II will focus on studying the arithmetic of the solutions to (1.2.5) obtained from families of the form

$$\alpha\,\mathcal{U}_M^+$$

where $\mathcal{U}_M^+$ is the positive unit group of an order in a number field not equal to the rationals or an imaginary quadratic, as in the full and degenerate cases. By Dirichlet's unit theorem, $\mathcal{U}_M^+$ is a finitely generated abelian group with positive rank. So, for any nontorsion element ε of $\mathcal{U}_M^+$, we can generate an infinite sequence of elements in M of fixed norm c given by

$$\alpha(k) = \beta\varepsilon^k, \text{ where } k \in \mathbb{Z}_{\geq 0}.$$

So, if we write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n, \tag{1.2.7}$$

then we obtain infinitely many solutions $(x_1(k), \ldots, x_n(k))$ to (1.2.5). Furthermore, the characterization above implies that all infinite families of solutions to (1.2.5) are obtained in this way. In Chapter II we study the arithmetic of the sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$, which are known to satisfy a linear recurrence relation.

1.3. Background on Linear Recurrence Sequences

An integer sequence $\{b(k) : k \in \mathbb{Z}_{\geq 0}\}$ is said to be a *linear recurrence sequence* (LRS) if it satisfies a homogeneous linear recurrence

$$b(k+d) = s_1 b(k+d-1) + \cdots + s_d b(k), \tag{1.3.8}$$

for $s_i \in \mathbb{Z}$ and $d \in \mathbb{Z}_{\geq 0}$. We say that $b(k)$ has order d if (1.3.8) is minimal. The *characteristic polynomial* of $b(k)$ is given by

$$f(X) = X^d - s_1 X^{d-1} - \cdots - s_d,$$

and the roots of f are the *characteristic roots* of $b(k)$. When $b(k)$ has order d, $f(X)$ is called the *minimal polynomial* of $b(k)$. For a linear recurrence sequence $b(k)$ of order d, we call $b(0), \ldots, b(d-1)$ its *initial conditions*. The following result tells us how to construct explicit formulas for linear recurrence sequences.

Proposition 1.3.1 (Chapter 1 of [9], for example)**.** Let $b(k)$ be a LRS of order d with characteristic roots $\alpha_1, \ldots, \alpha_m$ and write the minimal polynomial of $b(k)$ as

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i)^{n_i}.$$

Then, there exists polynomials $A_i(X) \in \mathbb{Q}[X]$ of degree $n_i - 1$ so that

$$b(k) = \sum_{i=1}^{m} A_i(k) \alpha_i^k.$$

As suggested in Proposition 1.3.1, linear recurrence sequences are known to grow exponentially. Since we will only consider sequences that are nondegenerate

with distinct characteristic roots we state the result on growth of these special families below. Note that similar results hold for more general families of linear recurrence sequences.

Proposition 1.3.2 (Theorem 2.3 of [9])**.** Let $b(k)$ be a LRS with distinct characteristic roots α_i so that α_i/α_j is not a root of unity for any $i \neq j$. Suppose that α_1 has maximal absolute value. Then, there is a constant $A \in \mathbb{R}$ and for all $\varepsilon > 0$ there is a constant $k_0 = k_0(\varepsilon)$ so that

$$|\alpha|^{(1-\varepsilon)k} \leq |b(k)| \leq A|\alpha|^k,$$

for all $k \geq k_0$.

While it is challenging to obtain arithmetic results on linear recurrence sequences in general (see Section 6.1 of [9] for a survey of such results), it has been found to be more tractable to study the arithmetic of sequences with the following divisibility property.

Definition 1.3.3. A linear recurrence sequence $b(k)$ is a *linear divisibility sequence* (LDS) if $b(k)$ has the following property: for all $n, m \in \mathbb{Z}_{>0}$,

$$n \mid m \Rightarrow b(n) \mid b(m).$$

For example, the fact that Lucas sequences, which we discuss below, are divisibility sequences was used in [6] to study their primitive divisors, and in [29] to study their index divisibility sets, as well as in many other results throughout the literature. Elliptic Divisibility Sequences, discussed in Section 1.1, are examples of

nonlinear divisibility sequences. Similar results for these sequences have also been found, such as in [28] and [32].

The characterization in Proposition 1.3.7 below shows that Lucas sequences are fundamental in studying linear divisibility sequence. We first give some background on these sequences.

Let P, Q be nonzero coprime integers. The Lucas sequence with integer parameters (P, Q) is defined to be the order 2 linear recurrence sequence $u_k = u_k(P, Q)$ with initial values $u_0 = 0$, $u_1 = 1$, and recurrence

$$u_{k+2} = Pu_{k+1} - Qu_k.$$

For example, the Fibonacci sequence is the Lucas sequence with integer parameters $(1, -1)$. Let $\theta, \bar{\theta}$ be roots of the polynomial $X^2 - PX + Q$. Using Proposition 1.3.1 and the initial conditions of u_n we can write

$$u_k = \frac{\theta^k - \bar{\theta}^k}{\theta - \bar{\theta}}.$$

Note that Lucas sequences are sometimes defined by the parameters $(\theta, \bar{\theta})$, rather than the integer parameters (P, Q).

Lemma 1.3.4. Every Lucas sequence is a LDS.

Proof. Let P, Q be nonzero coprime integers, and consider the matrix

$$A = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

Observe that for any positive integer k, we have

$$A^k = \begin{pmatrix} u_{k+1} & -Qu_k \\ u_k & -Qu_{k-1} \end{pmatrix},$$

where u_k is the Lucas sequence with integer parameters (P, Q). Now, take any positive integers m, n. Then we have

$$A^{mn} = \begin{pmatrix} u_{m+1} & -Qu_m \\ u_m & -Qu_{m-1} \end{pmatrix}^n \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod}\, u_m).$$

On the other hand, we have

$$A^{mn} = \begin{pmatrix} u_{mn+1} & -Qu_{mn} \\ u_{mn} & -Qu_{mn-1} \end{pmatrix}.$$

Comparing the lower left hand entries, we see that $u_m \mid u_{mn}$ for every $m, n \in \mathbb{Z}_{>0}$. So, u_k is a LDS. □

Characterization of Linear Divisibility Sequences. Determining precisely which linear recurrence sequences are linear divisibility sequences is an open problem. We give a survey of some of the current characterizations below.

Note that an order one linear recurrence sequence $b(k)$ with initial condition $b(0) = c$ takes the form $b(k) = ca^k$. So, every nonzero order one linear recurrence sequence is a linear divisibility sequence. In order two, we have the following.

Proposition 1.3.5 (Theorem 1 of [15])**.** Let $b(k)$ be an order two linear recurrence sequence. Then $b(k)$ is a linear divisibility sequence if and only if $b(0) = 0$.

Using Proposition 1.3.1, we obtain that the only linear divisibility sequences in order two are of the form

$$c \cdot u_k \text{ or } c \cdot k\alpha^{k-1},$$

where u_k is a Lucas sequence, and $\alpha, c \in \mathbb{Z}_{\neq 0}$.

The order three case was studied by Hall in [14]. The main result of this paper is as follows.

Proposition 1.3.6 (Theorem 4 of [14])**.** Let $b(k)$ be a linear recurrence sequence of order three with $b(0) = 0$ and characteristic polynomial

$$f(X) = X^3 - s_1X^2 - s_2X - s_3.$$

If $f(X)$ is an irreducible cubic with $\gcd(s_2, s_3) = 1$, then $b(k)$ is not a linear divisibility sequence.

It is conjectured that the only order three linear recurrence sequences $b(k)$ with $b(0) = 0$ that are linear divisibility sequences are of the form

$$c \cdot k^2\alpha^{k-1}, \ c \cdot ku_k, \ \text{ or } c \cdot u_k^2,$$

where u_k is a Lucas sequence, and $c, \alpha \in \mathbb{Z}_{\neq 0}$ (see Section 3.4 of [5], for example). For higher order sequences, little explicit information is known. The best known result in this direction tells us that the terms of a linear divisibility sequence must at least divide a product which generalizes the the conjectured order three characterization.

Proposition 1.3.7 (Section 1.3 of [5])**.** Let $b(k)$ be a linear divisibility sequence with $b(0) = 0$. Then, there exists $\alpha_i, \beta_i \in \mathbb{C}$ and nonzero integers c, ℓ so that if we

write

$$a(k) := c \cdot k^{\ell} \prod_i \left(\frac{\alpha_i^k - \beta_i^k}{\alpha_i - \beta_i} \right)$$

then we have $b(k) \mid a(k)$ for all $k \in \mathbb{Z}_{\geq 0}$.

1.4. Organization

This dissertation is organized as follows. In Chapter II we show that for certain families of quartic norm form equations, there exists integrally equivalent forms making any one of coordinate sequences defined in (1.2.7) a linear divisibility sequence. The results in this chapter provide new families of order 4 linear divisibility sequences, as well as some further arithmetic structure to the solution set of certain quartic norm form equations.

In Chapter III we discuss how to translate the question of monogeniety of a number field to a Diophantine problem through the use of index forms. We then discuss ongoing work to use the methods from a paper of Gaál, Pethö and Pohst to obtain explicit information about monogenizers in certain families of biquadratic fields by studying near squares in an associated order two linear recurrence sequence.

CHAPTER II

NORM FORM EQUATIONS AND LINEAR DIVISIBILITY SEQUENCES

In this chapter, we show that for certain families of norm form equations defined over quartic fields, we can find an integrally equivalent forms so that one of the sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ defined in (1.2.7) is a linear divisibility sequence. The families we consider are motivated by the following theorem of Kubota.

Proposition 2.0.1 (Theorem 1 of [19])**.** Let K be a real biquadratic field with quadratic subfields L_i, and let ε_i be a fundamental unit of L_i. Then, K has a system of fundamental units of one of the following forms, up to relabeling:

(i) $\varepsilon_1, \varepsilon_2, \varepsilon_3$

(ii) $\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3$

(iii) $\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3$

(iv) $\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_3, \varepsilon_3$

(v) $\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}, \varepsilon_2$

(vi) $\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{\varepsilon_3\varepsilon_1}$

(vii) $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3$

(viii) $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3$, with $N_{K_i}(\varepsilon_i) = -1$ for $i = 1, 2, 3$,

where $\sqrt{\varepsilon}$ denotes any element $\eta \in K$ with $\eta^2 = \varepsilon$, and the ε_i in cases (i) to (vii) appearing under a radical have $N_{L_i}(\varepsilon_i) = 1$. Furthermore, there are infinitely many K of each type.

Proposition 2.0.1 tells us that to study solutions to a norm form equation

$$F_W(X_1, X_2, X_3, X_4) = c$$

defined over a real biquadratic field, it suffices to understand the coordinates of the sequences $\alpha(k) = \beta\eta^k$ where η is of one of the following three types:

(a) η is a unit in quadratic subfield of K,

(b) η^2 is a unit in a quadratic subfield of K, or

(c) η is a product of units of types (a) and (b)

Our main results concern the sequences $\alpha(k) = \beta\eta^k$ where η is type (b). In fact, our results hold for quartic fields containing a unit of type (b) more generally. We will show the following.

Theorem 2.0.2. Let K be a quartic field with a real quadratic subfield L containing a quartic unit η of positive norm, so that η^2 is a unit in L. Fix a nonzero element $\beta \in K$, and write $\alpha(k) = \beta\eta^k$. Then, there is a choice of basis $W = \{w_1, w_2, w_3, w_4\}$ for the module $M' = \beta\,\mathbb{Z}[\eta]$, which we construct explicitly, so that if we write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_4(k)w_4$$

then $\{x_1(k) : k \in \mathbb{Z}_{\geq 0}\}$ is a LDS.

Theorem 2.0.3. Let $M = \mathbb{Z}[\sqrt{m}, \sqrt{m+1}]$, where m and $m+1$ are non-square integers. Then, $\eta = \sqrt{m} + \sqrt{m+1}$ is a unit in the positive unit group $\mathcal{U}_M^+$ with η^2 a unit in a quadratic subfield of $K = \mathbb{Q}(\eta)$, and there is a choice of basis $W =$

$\{w_1, w_2, w_3, w_4\}$ for the module M, which we construct explicitly, so that if we write

$$\eta^k = x_1(k)w_1 + \cdots + x_4(k)w_4,$$

then $\{x_1(k) : k \in \mathbb{Z}_{\geq 0}\}$ is a LDS.

Remark 2.0.4. Note that Theorems 2.0.2 and 2.0.3 hold for the sequence

$$\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$$

for any fixed $i \in \{1, 2, 3, 4\}$, just by changing the basis to reindex our coordinates. However, we show in Sections 2.2 and 2.3 that there does not exist a choice of basis for the modules M' and M in Theorems 2.0.2 and 2.0.3 so that the coordinate sequences $x_1(k), x_2(k), x_3(k), x_4(k)$ defined in (1.2.7) are LDS simultaneously.

This chapter is organized as follows. In Section 2.1, we show that the sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ defined in (1.2.7) are linear recurrence sequences, each with characteristic polynomial equal to the minimal polynomial of our unit ε. In Section 2.2, we discuss how to use Lucas sequences to study norm forms defined over real quadratic fields. In Section 2.3, we prove Theorems 2.0.2 and 2.0.3. In Section 2.4, we discuss a related sequence proposed by Silverman in [26], and provide examples where Conjecture 9 of this paper holds.

2.1. Coordinate Sequences

Let M be a full module in a number field K, and ε a nontorsion element in the positive unit group $\mathcal{U}_M^+$ defined in (1.2.6). For $\beta \in M$ with $N_K(\beta) = c$, set

$\alpha(k) = \beta\varepsilon^k$. If we choose a basis $W = \{w_1, \ldots, w_n\}$ for M, and write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n, \tag{2.1.1}$$

then we obtain tuples of solutions $(x_1(k), \ldots, x_n(k))$ to the corresponding norm form equation $F_W(X_1, \ldots, X_n) = c$.

Definition 2.1.1. We call the integer sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$, where $x_i(k)$ is defined in (2.1.1), the *coordinate sequences* of $\alpha(k)$ with respect to our choice of basis W.

In this section, we show that the coordinate sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ have characteristic polynomial equal to the minimal polynomial of ε. We also provide sufficient conditions so that the minimal polynomial of the coordinate sequence $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ is equal to the minimal polynomial of ε.

Proposition 2.1.2. Let K be a number field, and take $\gamma \in K$ and $\theta \in \mathcal{O}_K$. Consider the sequence $x(k) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma\theta^k)$.

(a) The sequence $x(k)$ satisfies a linear recurrence with characteristic polynomial equal to the minimal polynomial of θ.

(b) Let $L = \mathbb{Q}(\theta)$. If $\mathrm{Tr}_{K/L}(\gamma) \neq 0$, then the minimal polynomial of the sequence $x(k)$ is equal to the minimal polynomial of θ.

Remark 2.1.3. Suppose that θ has minimal polynomial

$$f(X) = X^d - s_1X^{d-1} - \cdots - s_d,$$

for $s_i \in \mathbb{Z}$. Then, Proposition 2.1.2(a) implies that the sequence $x(k) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma\theta^k)$ satisfies the recurrence

$$x(k+d) = s_1 x(k+d-1) + \cdots + s_d x(k).$$

However, it is possible that this recurrence is not minimal. For example, take

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}),$$

$\theta = \sqrt{2} + \sqrt{3}$ and $\gamma = \sqrt{5}$. Then, Proposition 2.1.2 (a) implies that $x(k)$ satisfies an order 4 recurrence, but we can check that $x(k) = 0$ for $k = 0, 1, 2, 3$. So, $x(k)$ is a constant sequence, while $\deg \theta = 4$.

There does not appear to be a complete characterization for when the sequence $x(k)$ is exactly of order $\deg \theta$ in the current literature, so Proposition 2.1.2 (b) gives a new result in this direction. We note that Proposition 2.1.2 (a) follows from known results on generalized power sums (see Chapter 1 of [9], for example), but we provide a more elementary proof below.

Proof of Proposition 2.1.2. Let $n = [K : \mathbb{Q}]$ and $\sigma_i : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings fixing $\mathbb{Q}$. Set $\gamma_i := \sigma_i(\gamma)$ and $\theta_i := \sigma_i(\theta)$, for $i \in \{1, \ldots, n\}$. Then, we can write

$$x(k) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma\theta^k) = \sum_{i=1}^{n} \gamma_i \theta_i^k. \tag{2.1.2}$$

Let

$$f(X) = X^d - s_1 X^{d-1} - \cdots - s_d$$

be the minimal polynomial of θ over $\mathbb{Q}$. Since $\theta \in \mathcal{O}_K$ we have $s_i \in \mathbb{Z}$. Then,

$$\begin{aligned}\sum_{j=1}^{d} s_j x(k+d-j) &= \sum_{j=1}^{d}\sum_{i=1}^{n} s_j \gamma_i \theta_i^{k+d-j} \quad \text{by (2.1.2)} \\ &= \sum_{i=1}^{n} \gamma_i \theta_i^k \sum_{j=1}^{d} s_j \theta_i^{d-j} \\ &= \sum_{i=1}^{n} \gamma_i \theta_i^k \theta_i^d,\end{aligned}$$

where the final equality follows because each θ_i is a root of $f(X)$. So, our sequence satisfies the recurrence $x(k+d) = \sum_{j=1}^{d} s_j x(k+d-j)$, which has characteristic polynomial equal to $f(X)$, which proves part (a).

Next, suppose that $x(k)$ satisfies an order m recurrence for $0 < m \leq d$, say

$$x(k+m) = \sum_{j=1}^{m} r_j x(k+m-j),$$

where $r_j \in \mathbb{Z}$. Then, we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\gamma\theta^{k+m}) = \sum_{j=1}^{m} r_j \,\mathrm{Tr}_{K/\mathbb{Q}}(\gamma\theta^{k+m-j}),$$

and by linearity of the trace, we get $\mathrm{Tr}_{K/\mathbb{Q}}(C\theta^k \cdot \gamma) = 0$, where

$$C = \theta^m - \sum_{i=1}^{m} r_i \theta^{m-i}.$$

Order the embeddings so that $\sigma_1(\theta) = \theta_1, \ldots, \sigma_d(\theta) = \theta_d$ are distinct, and

$$\sigma_i(\theta) = \sigma_{dm+i}(\theta)$$

for $m = 1, 2, \ldots, \ell$. Then,

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(C\theta^k \cdot \gamma) = \sigma_1(C\theta^k)\left(\sigma_1(\gamma) + \sigma_{d+1}(\gamma) + \cdots + \sigma_{\ell d+1}(\gamma)\right) \\ + \sigma_2(C\theta^k)\left(\sigma_2(\gamma) + \sigma_{d+2}(\gamma) + \cdots + \sigma_{\ell d+2}(\gamma)\right) \\ \vdots \\ + \sigma_d(C\theta^k)\left(\sigma_d(\gamma) + \sigma_{2d}(\gamma) + \cdots + \sigma_{(\ell+1)d}(\gamma)\right)\end{aligned}$$

where $n = (\ell + 1)d$. For $i = 1, \ldots, d$. Set

$$S_i = \sigma_i(\gamma) + \sigma_{d+i}(\gamma) + \cdots + \sigma_{\ell d+i}(\gamma).$$

Then, we can write

$$\begin{pmatrix} \sigma_1(C\theta^0) & \cdots & \sigma_d(C\theta^0) \\ \vdots & \ddots & \vdots \\ \sigma_1(C\theta^{d-1}) & \cdots & \sigma_d(C\theta^{d-1}) \end{pmatrix} \begin{pmatrix} S_1 \\ \vdots \\ S_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{2.1.3}$$

Without loss of generality, suppose that $\sigma_1(\theta) = \theta$. Then,

$$S_1 = \mathrm{Tr}_{K/L}(\gamma),$$

where $L = \mathbb{Q}(\theta)$. If $C \neq 0$ then the set $\{C, C\theta, \ldots, C\theta^{d-1}\}$ would be $\mathbb{Q}$-linearly independent, and we would have

$$\det \begin{pmatrix} \sigma_1(C\theta^0) & \cdots & \sigma_n(C\theta^0) \\ \vdots & \ddots & \vdots \\ \sigma_1(C\theta^{d-1}) & \cdots & \sigma_d(C\theta^{d-1}) \end{pmatrix} = \mathrm{disc}(C, C\theta, \ldots, C\theta^{d-1})^{1/2} \neq 0.$$

But this contradicts (2.1.3), since $S_1 \neq 0$ by assumption. So, we must have $C = 0$, and so θ is a root of

$$X^m - \sum_{i=1}^{m} r_i X^{m-i} \in \mathbb{Z}[X]$$

But since θ is degree d, and $m \leq d$ we get $m = d$. Hence, the recurrence

$$x(k+d) = \sum_{j=1}^{d} s_j x(k+d-j)$$

is minimal, and so $f(X)$ is the minimal polynomial of the sequence $x(k)$. □

We have the following Corollary to Proposition 2.1.2.

Corollary 2.1.4. Let K be a number field and M a full module in K. Suppose that ε is a nontorsion element in $\mathcal{U}_M^+$. For a fixed nonzero $\beta \in M$, let

$$\alpha(k) = \beta\varepsilon^k$$

and $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ be a coordinate sequence of $\alpha(k)$ with respect to some basis, as defined in (2.1.1). Then, $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ is a linear recurrence sequence with characteristic polynomial equal to the minimal polynomial of ε. Furthermore, if $\deg \varepsilon = [K : \mathbb{Q}]$ then the minimal polynomial of this sequence is equal to the minimal polynomial of ε.

Proof. Let $W = \{w_1, \ldots, w_n\}$ be any basis for M, and write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n.$$

Since M is a full module, W is a $\mathbb{Q}$-basis for K. So, there exists a dual basis $W^* = \{w_1^*, \ldots, w_n^*\}$ to W with respect to the trace pairing. That is, W^* is a basis for K,

and we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(w_i^* w_j) = \delta_{ij}$$

for all i, j, where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Let $\gamma = w_i^* \beta$. Then we have

$$x_i(k) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma \varepsilon^k).$$

Note that if $\deg \varepsilon = [K : \mathbb{Q}]$ then $\mathbb{Q}(\varepsilon) = K$. So

$$\mathrm{Tr}^K_{\mathbb{Q}(\varepsilon)}(\gamma) = \gamma \neq 0.$$

Hence, the result follows from Proposition 2.1.2 (b). □

2.2. Norm Form Equations over Real Quadratic Fields

Suppose that K is a real quadratic field, and let M be a full module in K. For any $\beta \in M$ and ε a nontorsion element in $\mathcal{U}_M^+$, let $\alpha(k) = \beta\varepsilon^k$ as before. Since ε is degree 2 over $\mathbb{Q}$, Corollary 2.1.4 implies that the coordinate sequences of $\alpha(k)$ are order 2 linear recurrence sequences. Such sequences have been well-studied, and so Corollary 2.1.4 implies some immediate consequences.

Proposition 2.2.1. Let K be a real quadratic field and M a full module in K. Fix a nonzero element $\beta \in M$ and write $\alpha(k) = \beta\varepsilon^k$. Then, there is a choice of basis

$W = \{w_1, w_2\}$ for M, which we construct explicitly, so that if we write

$$\alpha(k) = x_1(k)w_1 + x_2(k)w_2$$

then the sequence $x_1(k)$ is a LDS.

Recall from Proposition 1.3.5 of Chapter I that order two linear divisibility sequences must initialize at zero. So, given $\alpha(k)$ as in Proposition 2.2.1, it is not possible to find a basis for M so that $x_1(k)$ and $x_2(k)$ are LDS simultaneously.

Proof of Proposition 2.2.1. By Proposition 1.3.5, it suffices to find a basis $\{w_1, w_2\}$ for M so that $x_1(0) = 0$. Let $\{t_1, t_2\}$ be any basis for M, and B be the matrix given by

$$\begin{pmatrix} \beta \\ \beta\varepsilon \end{pmatrix} = B \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}.$$

Note that $\exists C \in \mathrm{GL}_2(\mathbb{Z})$ so that BC is lower triangular. So, we can define a new basis $\{v_1, v_2\}$ from $\{t_1, t_2\}$ by change of basis matrix C^{-1}. Then,

$$\begin{pmatrix} \beta \\ \beta\varepsilon \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \tag{2.2.4}$$

for some $a_{ij} \in \mathbb{Z}$. Now, let $W = \{w_1, w_2\}$ be the basis defined by

$$\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

We claim that we can take W as our desired basis. To see this, observe that

$$\begin{pmatrix} 0 & a_{11} \\ a_{22} & a_{21} - a_{22} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

So, if we write $\alpha(k) = x_1(k)w_1 + x_2(k)w_2$ then by (2.2.4) $x_1(k)$ has initial conditions $x_1(0) = 0$ and $x_1(1) = a_{22}$. So, $x_1(k) = a_{22}u_k$, where u_k is the Lucas sequence with parameters $(\varepsilon, \bar{\varepsilon})$. By Corollay 2.1.4 we know that $x_1(k)$ is an order 2 recurrence sequence, and so we must have $a_{22} \neq 0$. Hence, $x_1(k)$ is a LDS. □

2.3. Norm Form Equations over Quartic Fields

Let K be a quartic field, and M a full module in K. Choose an element β in M, and suppose there exists a unit $\eta \in \mathcal{U}_M^+$ of degree 4 over $\mathbb{Q}$. By Corollary 2.1.4, the coordinate sequences of $\alpha(k) = \beta\eta^k$ are order 4 linear recurrence sequences. Unlike in the order 2 case, much less is known about higher-order linear recurrence sequences, and so it is generally quite challenging to determine when an arbitrary order 4 linear recurrence sequence is a LDS.

Suppose that η is a quartic unit with $\eta^2 =: \varepsilon$ a unit in a quadratic subfield of $\mathbb{Q}(\eta)$. Recall, by Proposition 2.0.1, this is one of the three cases needed to understand solutions to norm forms over real biquadratic fields. Let $\tilde{K}$ be the Galois closure of K. Observe that for $\sigma \in \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ we have $\sigma(\varepsilon) = \sigma(\eta)^2$. So, the conjugates of η are of the form

$$\pm\sqrt{\varepsilon}, \pm\sqrt{\bar{\varepsilon}}, \tag{2.3.5}$$

where $\bar{\varepsilon}$ denotes the conjugate of ε. Since η is of degree 4 over $\mathbb{Q}$, it has minimal polynomial

$$f(X) = X^4 - (\varepsilon + \bar{\varepsilon})X^2 + 1. \tag{2.3.6}$$

So, Corollary 2.1.4 implies that the coordinate sequences $x(k)$ of $\alpha(k)$ are order 4 linear recurrence sequences satisfying

$$x(k+4) = Tx(k+2) - x(k), \tag{2.3.7}$$

where $T = \varepsilon + \bar{\varepsilon}$. The following Proposition gives sufficient initial conditions for $x(k)$ to be a LDS, and will be used to prove our main results.

Proposition 2.3.1. Let $x(k)$ be an order 4 linear recurrence sequence with initial conditions $x(0) = 0$, $x(1) = x(2) = a$, $x(3) = a(T+1)$, and recurrence

$$x(k+4) = Tx(k+2) - x(k),$$

where a and T are nonzero integers. Then, $x(k)$ is a LDS.

Proof. Note that it suffices prove our claim for $a = 1$. Let u_k denote the Lucas sequence with integer parameters $(T, 1)$. Since we assumed that $x(0) = 0$ and $x(2) = 1$, we have $x(2n) = u_n$ for every $n \in \mathbb{Z}_{\geq 0}$. Consider the matrix

$$A = \begin{pmatrix} T & -1 \\ 1 & 0 \end{pmatrix}.$$

Recall from the proof of Lemma 1.3.4 that we have the identity

$$A^n = \begin{pmatrix} u_{n+1} & -u_n \\ u_n & -u_{n-1} \end{pmatrix}, \tag{2.3.8}$$

and so we have

$$A^n = \begin{pmatrix} x(2n+2) & -x(2n) \\ x(2n) & -x(2n-2) \end{pmatrix}, \tag{2.3.9}$$

for every $n \in \mathbb{Z}_{>0}$. Using the recurrence for $x(k)$, we observe that

$$A^n \begin{pmatrix} x(3) \\ x(1) \end{pmatrix} = \begin{pmatrix} x(2n+3) \\ x(2n+1) \end{pmatrix}. \tag{2.3.10}$$

Combining (2.3.9) and (2.3.10) yields

$$\begin{pmatrix} x(2n+3) \\ x(2n+1) \end{pmatrix} = \begin{pmatrix} x(3)x(2n+2) - x(1)x(2n) \\ x(3)x(2n) - x(1)x(2n-2) \end{pmatrix}.$$

That is, we have $x(2n+1) = x(3)x(2n) - x(1)x(2(n-1))$ for any positive integer n. Recalling that $x(1) = 1$, $x(3) = T + 1$ and $x(2n) = u_n$, we obtain

$$\begin{aligned} x(2n+1) &= (T+1)u_n - u_{n-1} \\ &= u_{n+1} + u_n, \end{aligned}$$

where the final equality follows by using the recurrence for u_k. So, we have

$$x(k) = \begin{cases} u_n, & \text{if } k = 2n \\ u_{n+1} + u_n, & \text{if } k = 2n+1, \end{cases} \tag{2.3.11}$$

for any $k \in \mathbb{Z}_{\geq 0}$. Note that we need to show $x(k) \mid x(k\ell)$ for every $k, \ell \in \mathbb{Z}_{\geq 0}$. Suppose that $k = 2n$. Then, $x(k) = u_n$ and $x(k\ell) = u_{n\ell}$. So, by Lemma 1.3.4 we have $x(k) \mid x(k\ell)$. Next, suppose that $k = 2n + 1$ and $\ell = 2m$. Noting that $A^{2n} = (A^n)^2$, and using identity (2.3.8) we have

$$\begin{pmatrix} u_{2n+1} & -u_{2n} \\ u_{2n} & -u_{2n-1} \end{pmatrix} = \begin{pmatrix} u_{n+1} & -u_n \\ u_n & -u_{n-1} \end{pmatrix}^2.$$

After squaring the matrix on the right, we compare the upper left-hand entries to get the identity $u_{2n+1} = u_{n+1}^2 - u_n^2$. So, we have

$$\begin{aligned} \frac{x(2k)}{x(k)} &= \frac{x(2(2n+1))}{x(2n+1)} \\ &= \frac{u_{2n+1}}{u_{n+1} + u_n} \\ &= u_{n+1} - u_n \in \mathbb{Z}. \end{aligned}$$

Hence, $x(k) \mid x(2k)$, and by the previous case we have

$$x(2k) \mid x(2km) \Rightarrow x(k) \mid x(k\ell).$$

Now, suppose that $k = 2n + 1$ and $\ell = 2m + 1$. Let $\varepsilon, \bar{\varepsilon}$ denote the roots of $X^2 - TX + 1$. Recall from Section 1.3 we can write

$$u_k = \frac{\varepsilon^k - \bar{\varepsilon}^k}{\varepsilon - \bar{\varepsilon}},$$

for every $k \in \mathbb{Z}_{\geq 0}$. So, we have

$$\begin{aligned} x(2n+1) &= u_{n+1} + u_n \\ &= \frac{\varepsilon^{n+1} - \bar{\varepsilon}^{n+1}}{\varepsilon - \bar{\varepsilon}} + \frac{\varepsilon^n - \bar{\varepsilon}^n}{\varepsilon - \bar{\varepsilon}} \\ &= \frac{\varepsilon^n(\varepsilon+1) - \bar{\varepsilon}^n(\bar{\varepsilon}+1)}{\varepsilon - \bar{\varepsilon}} \\ &= \frac{\varepsilon^n(\varepsilon+1) - \dfrac{1}{\varepsilon^{n+1}}(1+\varepsilon)}{\varepsilon - \bar{\varepsilon}} \\ &= \frac{\varepsilon+1}{\varepsilon - \bar{\varepsilon}} \cdot \frac{\varepsilon^{2n+1} - 1}{\varepsilon^{n+1}}. \end{aligned}$$

This gives

$$\begin{aligned} \frac{x((2n+1)(2m+1))}{x(2n+1)} &= \frac{x(2(2nm+n+m)+1)}{x(2n+1)} \\ &= \frac{\varepsilon^{2(2nm+n+m)+1} - 1}{\varepsilon^{2nm+n+m+1}} \cdot \frac{\varepsilon^{n+1}}{\varepsilon^{2n+1} - 1} \\ &= \frac{\varepsilon^{(2n+1)(2m+1)} - 1}{\varepsilon^{2n+1} - 1} \cdot \frac{1}{\varepsilon^{m(2n+1)}}. \end{aligned}$$

To see this value is in $\mathbb{Z}$, let $\alpha = \varepsilon^{2n+1}$. Then, from above we obtain

$$\begin{aligned} \frac{x((2n+1)(2m+1))}{x(2n+1)} &= \frac{\alpha^{2m+1} - 1}{\alpha - 1} \cdot \frac{1}{\alpha^m} \\ &= \frac{\alpha^{2m} + \alpha^{2m-1} + \cdots + \alpha + 1}{\alpha^m} \\ &= (\alpha^m + \alpha^{-m}) + \cdots + (\alpha + \alpha^{-1}) + 1. \end{aligned}$$

Since $\alpha = \varepsilon^{2n+1}$ and $N_K(\varepsilon) = 1$, then α and α^{-1} are quadratic conjugates. So, we have $\alpha^t + \alpha^{-t} \in \mathbb{Z}$ for every $t = 1, \ldots, m$. Hence,

$$x(2n+1) \mid x((2n+1)(2m+1)),$$

and so $x(k)$ is a LDS. $\square$

Theorem 2.0.2 will now follow from Proposition 2.1.2. Recall that K is a quartic number field containing a quartic unit η of positive norm so that η^2 is a unit in a quadratic subfield of K.

Proof of Theorem 2.0.2. Note that the module $M' = \beta\mathbb{Z}[\eta]$ has basis $\{\beta, \beta\eta, \beta\eta^2, \beta\eta^3\}$. Define the set $W = \{w_1, w_2, w_3, w_4\}$ by

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ T+1 & 1 & 0 & 0 \end{pmatrix}}_{A} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} \beta \\ \beta\eta \\ \beta\eta^2 \\ \beta\eta^3 \end{pmatrix},$$

where $T = \varepsilon + \bar{\varepsilon}$. Note that $A \in \mathrm{GL}_4(\mathbb{Z})$, and so W is a basis for M. Since η has minimal polynomial

$$f(X) = X^4 - TX^2 + 1,$$

then by Corollary 2.1.4 we know that the sequence $x_1(k)$ is an order 4 linear recurrence sequence satisfying (2.3.7). Moreover, if we write $\alpha(k) = \beta\varepsilon^k$ in terms of the basis W, then

$$x_1(0) = 0,\ x_1(1) = x_1(2) = 1,\ \text{and}\ x_1(3) = T + 1.$$

So, by Proposition 2.3.1, $x_1(k)$ is a LDS. $\square$

In the following Corollary, we provide explicit formulas for the coordinate sequences of $\alpha(k)$, with respect to the basis constructed in Theorem 2.0.2, in terms of Lucas sequences.

Corollary 2.3.2. Let $W = \{w_1, w_2, w_3, w_4\}$ be the basis for the module $\beta\mathbb{Z}[\eta]$ constructed in Theorem 2.0.2, and $\alpha(k) = \beta\eta^k$ be as above. If we write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_4(k)w_4,$$

then for any integer $k \geq 3$ we have

$$x_1(k) = \begin{cases} u_n & \text{if } k = 2n \\ u_{n+1} + u_n & \text{if } k = 2n+1, \end{cases} \qquad x_2(k) = \begin{cases} 0 & \text{if } k = 2n \\ u_n & \text{if } k = 2n+1, \end{cases}$$

$$x_3(k) = \begin{cases} -u_{n-1} & \text{if } k = 2n \\ 0 & \text{if } k = 2n+1, \end{cases} \qquad x_4(k) = \begin{cases} 0 & \text{if } k = 2n \\ -u_{n-1} & \text{if } k = 2n+1, \end{cases}$$

where u_n is the Lucas sequence with parameters $(\varepsilon, \bar{\varepsilon})$, defined in Section 2.1.

Proof. Recall, by Corollary 2.1.4 we know that all of the coordinate sequences $x_i(k)$ of $\alpha(k)$ satisfy the order 4 recurrence

$$x_i(k+4) = Tx_i(k+2) - x_i(k), \tag{2.3.12}$$

where $T = \varepsilon + \bar{\varepsilon}$, and by construction of our basis W these sequences have initial conditions

k	$x_1(k)$	$x_2(k)$	$x_3(k)$	$x_4(k)$
0	0	0	1	0
1	1	0	0	1
2	1	0	0	0
3	$T+1$	1	0	0

From (2.3.11) in the proof of Proposition 2.3.1 we see that $x_1(k)$ satisfies the desired formula. Next, let $y_i(n) = x_i(2n+1)$ for $i = 2, 4$ and $y_3(n) = x_3(2n)$. By (2.3.12) we have that $y_i(n)$ satisfies the order 2 recurrence

$$y_i(n+2) = Ty_i(n+1) - y_i(n).$$

Since $y_2(0) = 0$ and $y_2(1) = 1$ we get

$$x_2(2n+1) = y_2(n) = u_n \text{ for all } n \geq 0,$$

where u_n is the Lucas sequence with integer parameters $(T, 1)$. Since $y_3(1) = 0$ and $y_3(2) = -1$ we have

$$x_3(2n) = y_3(n) = -u_{n-1} \text{ for all } n \geq 1.$$

Similarly, since $y_4(1) = 0$ and $y_4(2) = -1$ we have

$$x_4(2n+1) = y_4(n) = -u_{n-1} \text{ for all } n \geq 1.$$

□

Remark 2.3.3. Let M be an arbitrary full module in our quartic field K and let $\alpha(k) = \beta\eta^k$ as above. Note that $M' = \beta\mathbb{Z}[\eta]$ is a finite index submodule of M containing $\alpha(k)$ for every $k \in \mathbb{Z}_{\geq 0}$. So, we can always write the coordinate sequences for $\alpha(k)$ in terms of the basis constructed in Theorem 2.0.2. It turns out to be more challenging to apply Proposition 2.3.1 to find a basis for the entire module M. The following Proposition provides sufficient conditions for when this can be done.

First, we set some notation. For a basis $\{t_1, t_2, t_3, t_4\}$ of M, write

$$\begin{pmatrix} \beta \\ \beta\eta \\ \beta\eta^2 \\ \beta\eta^3 \end{pmatrix} = B \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix}. \tag{2.3.13}$$

Writing B in Smith normal form, we know that there exists $X, Y \in \mathrm{GL}_4(\mathbb{Z})$ so that

$$XBY = \mathrm{diag}(\delta_1, \ldots, \delta_4) \tag{2.3.14}$$

with $\delta_1 \mid \cdots \mid \delta_4$. Let $X = (x_{ij})$. Then, we have the following.

Proposition 2.3.4. If there exists a matrix $X \in \mathrm{GL}_4(\mathbb{Z})$ satisfying (2.3.14) and

$$\gcd\left(\chi_4, \frac{\delta_4}{\delta_1}\right) = 1,$$

where $\chi_i = x_{i2} + x_{i3} + (T+1)x_{i4}$, and $T = \varepsilon + \bar{\varepsilon}$, then there is a choice of basis W for the module M so that the coordinate sequence $x_1(k)$ of $\alpha(k)$ with respect to the basis W satisfies the initial conditions of Proposition 2.3.1.

Proof. Suppose that we have a basis $W = \{w_1, w_2, w_3, w_4\}$ for M as above. Set

$$\vec{w} = \begin{pmatrix} w_1 & \cdots & w_4 \end{pmatrix}^\top \text{ and } \vec{t} = \begin{pmatrix} t_1 & \cdots & t_4 \end{pmatrix}^\top.$$

Then, $A\vec{w} = B\vec{t}$, where B is defined in (2.3.13) and A is a matrix with first column

$$\begin{pmatrix} 0 & a & a & a(T+1) \end{pmatrix}^\top.$$

Let X be any matrix satisfying (2.3.14), which we know exists by writing B is Smith normal form. Write $D = \operatorname{diag}(\delta_1, \ldots, \delta_4)$. Observe that $\gcd(\chi_1, \ldots, \chi_4) = 1$, since if there were a prime p dividing every χ_i, then we would have

$$p \cdot \begin{pmatrix} q_1 \\ \vdots \\ q_4 \end{pmatrix} = 0 \cdot \begin{pmatrix} x_{11} \\ \vdots \\ x_{41} \end{pmatrix} + \begin{pmatrix} x_{12} \\ \vdots \\ x_{42} \end{pmatrix} + \begin{pmatrix} x_{13} \\ \vdots \\ x_{43} \end{pmatrix} + (T+1) \begin{pmatrix} x_{14} \\ \vdots \\ x_{44} \end{pmatrix},$$

where $q_i \in \mathbb{Z}$. But then the columns of X would be $(\mathbb{Z}/p)$-linearly dependent, which contradicts the fact that $X \in \mathrm{GL}_4(\mathbb{Z})$. Now, let

$$\vec{c}_1 = \begin{pmatrix} \frac{\delta_4}{\delta_1}\chi_1 & \frac{\delta_4}{\delta_2}\chi_2 & \frac{\delta_4}{\delta_3}\chi_3 & \chi_4 \end{pmatrix}^\top.$$

It is known that any lattice element can be extended to a basis precisely when it is primitive (see Chapter 1 of [8], for example). Since $\delta_1 \mid \cdots \mid \delta_4$, and we've assumed that $\gcd(\chi_4, \delta_4/\delta_1) = 1$, then we have

$$\gcd\left(\frac{\delta_4}{\delta_1}\chi_1, \frac{\delta_4}{\delta_2}\chi_2, \frac{\delta_3}{\delta_2}\chi_3, \chi_4\right) = 1.$$

So, there is a matrix $C \in \mathrm{GL}_4(\mathbb{Z})$ with first column equal to $\vec{c}_1$. Next, let $A = X^{-1}DC$. Then, A has first column

$$\vec{a}_1 = \begin{pmatrix} 0 & \delta_4 & \delta_4 & \delta_4(T+1) \end{pmatrix}^\top.$$

Furthermore, $D^{-1}XA = C \in \mathrm{GL}_4(\mathbb{Z})$. Let $Z = YD^{-1}XA \in \mathrm{GL}_4(\mathbb{Z})$, and define a new basis $W = \{w_1, w_2, w_3, w_4\}$ from $\{t_1, t_2, t_3, t_4\}$ by change of basis matrix Z^{-1}. Since $Z = B^{-1}A$, we have

$$A \begin{pmatrix} w_1 \\ \vdots \\ w_4 \end{pmatrix} = \begin{pmatrix} \beta \\ \vdots \\ \beta\eta^3 \end{pmatrix}.$$

So, if we write $\alpha(k) = x_1(k)w_1 + \cdots + x_4(k)w_4$, then $x_1(k)$ satisfies the initial conditions $x_1(0) = 0$, $x_1(1) = x_1(2) = \delta_4$, $x_1(3) = \delta_4(T+1)$. □

Theorem 2.0.3 provides a family of modules satisfying the conditions of Proposition 2.3.4. An interesting future direction could be to provide a characterization of all such modules.

Proof of Theorem 2.0.3. Recall that $M = \mathbb{Z}[\sqrt{m}, \sqrt{m+1}]$, and $\eta = \sqrt{m} + \sqrt{m+1}$. Observe that $\eta = \sqrt{\varepsilon}$, where $\varepsilon = 2m + 1 + 2\sqrt{m(m+1)}$. Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{m+1})$, and $L = \mathbb{Q}(\sqrt{m(m+1)})$. A short computation shows that $N_L(\varepsilon) = 1$ and $\eta \in \mathcal{U}_M^+$. Next, observe that

$$\begin{pmatrix} 1 \\ \eta \\ \eta^2 \\ \eta^3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 2m+1 & 0 & 0 & 2 \\ 0 & 4m+3 & 4m+1 & 0 \end{pmatrix}}_{B} \begin{pmatrix} 1 \\ \sqrt{m} \\ \sqrt{m+1} \\ \sqrt{m(m+1)} \end{pmatrix}.$$

We can compute $XBY = \mathrm{diag}(1, 1, -2, 2)$ where

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -4m-3 & 0 & 1 \\ -2m-1 & 0 & 1 & 0 \end{pmatrix}, \text{ and } Y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hence, $\chi_4 = 1$ and so Proposition 2.3.4 applies. That is, there is a basis W so that the coordinate sequence $x_1(k)$ of $\alpha(k)$ with respect to the basis W satisfies the initial conditions of Proposition 2.3.1. So, $x_1(k)$ is a LDS. □

Remark 2.3.5. Note that the proof of Proposition 2.3.4 provides an algorithm for computing our desired basis in Theorem 2.0.3 explicitly. We demonstrate this computation. Note that

$$\mathrm{Tr}_{L/\mathbb{Q}}(\varepsilon) = 4m + 2.$$

Recall that we need to find a matrix $C = D^{-1}XA$ in $\mathrm{GL}_4(\mathbb{Z})$ with first column being a primitive vector and $A \in \mathbf{Mat}_4(\mathbb{Z})$ with first column

$$\vec{a} = \begin{pmatrix} 0 & a & a & a(4m+3) \end{pmatrix}^\top$$

. We compute the first column of C to be

$$\vec{c_1} = \begin{pmatrix} 0 & a & 0 & a/2 \end{pmatrix}^\top.$$

So, we choose $a = 2$ and the rest of the entries of C so that $C \in \mathrm{GL}_4(\mathbb{Z})$. For example, we can take

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then, we compute $A = X^{-1}DC$, where $D = \mathrm{diag}(1, 1, -2, 2)$, to get

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 2m+1 & 0 & 0 \\ 8m+6 & 0 & 4m+3 & -2 \end{pmatrix}.$$

So, setting $Z = B^{-1}A$, and using Z^{-1} as our change of basis matrix from $\{1, \sqrt{m}, \sqrt{m+1}, \sqrt{m(m+1)}\}$ we obtain basis $W = \{w_1, w_2, w_3, w_4\}$ for M given by

$$w_1 = \sqrt{m},\ w_2 = 2 + \sqrt{m+1} - \sqrt{m(m+1)},$$

$$w_3 = \sqrt{m(m+1)},\ w_4 = 1.$$

So, if we write $\eta^k = x_1(k)w_1 + \cdots + x_4(k)w_4$, we can check that $x_1(k)$ satisfies the initial conditions $x_1(0) = 0,\ x_1(1) = x_1(2) = 2,\ x_1(3) = 2(4m+3)$, and so by Proposition 2.3.1 we have that $x_1(k)$ is a LDS.

Remark 2.3.6. If $\alpha(k)$ is as in Theorems 2.0.2 and 2.0.3, the coordinate sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ contain order two subsequences $\{x_i(2k) : k \in \mathbb{Z}_{\geq 0}\}$. By Proposition 1.3.5 in Chapter I, an order two linear recurrence sequence must

initialize at zero. So, it is not possible to find a basis for the corresponding module that makes $x_1(k), x_2(k), x_3(k), x_4(k)$ LDS simultaneously.

2.4. Powers of Algebraic Integers

We conclude this chapter by discussing a related sequence studied by Silverman in [26], and show how methods from the previous sections might be used in its analysis.

Given $\alpha \in \bar{\mathbb{Z}}$, define the sequence

$$d_k(\alpha) = \max\{d \in \mathbb{Z} \mid \alpha^k \equiv 1 (\mathrm{mod}\, d)\}. \tag{2.4.15}$$

where the congruence $\alpha^k \equiv 1 (\mathrm{mod}\, d)$ means that there is an element $\beta \in \bar{\mathbb{Z}}$ with

$$\alpha^k = 1 + d\beta.$$

In [26], Silverman proved that $d_k(\alpha)$ is a divisibility sequence, and showed that, except for some exceptional cases, this sequence grows slower than exponentially. We record this Theorem below.

Theorem 2.4.1 (Theorem 1 of [26])**.** Let $\alpha \in \bar{\mathbb{Z}}$. Then,

$$\lim_{n\to\infty} \frac{\log d_n(\alpha)}{n} = 0$$

unless $\alpha^\ell \in \mathbb{Z}$ for some $\ell \in \mathbb{Z}$, or α^ℓ is a unit in a quadratic extension of $\mathbb{Q}$.

In the exceptional case where α is an element of $\mathbb{Z}[\sqrt{D}]$ for a nonsquare integer $D \geq 2$, and $N_K(\alpha) = 1$, it is shown in Theorem 7 of [26] that $d_k := d_k(\alpha)$

satisfies the order 4 linear recurrence

$$d_{k+4} = Td_{k+2} - d_k, \tag{2.4.16}$$

where $T = \alpha + \bar{\alpha}$.

Let η be an algebraic number of degree 4 with η^2 quadratic. Choose an integral basis $\{w_1, w_2, w_3, w_4\}$ for $L = \mathbb{Q}(\eta)$, and write

$$\eta^k = x_1(k)w_1 + \cdots + x_4(k)w_4. \tag{2.4.17}$$

Then, by Corollary 2.1.4 we have that the $x_i(k)$ also satisfy the order 4 linear recurrence

$$x_i(k+4) = Tx_i(k+2) - x_i(k). \tag{2.4.18}$$

We have the following observation.

Proposition 2.4.2. Let α be a nontorsion unit of positive norm in $\mathbb{Z}[\sqrt{D}]$ for a nonsquare integer $D \geq 2$, and let η be any algebraic integer satisfying $\eta^2 = \alpha$. Let $L = \mathbb{Q}(\eta)$. If $\mathcal{O}_L = \mathbb{Z}[\eta]$, then there exists a choice of basis for $\mathcal{O}_L$ so that

$$x_1(k) = \begin{cases} d_k(\alpha) & \text{if } d_1(\alpha) = 1 \\ d_k(\alpha)/d_1(\alpha) & \text{if } d_1(\alpha) \neq 1, \end{cases}$$

where $d_k(\alpha)$ and $x_1(k)$ are defined as in (2.4.15) and (2.4.17), respectively.

Proof. By (2.4.16) and (2.4.18), we know that $x_1(k)$ and $d_k(\alpha)$ both satisfy the same recurrence. So, it suffices to find a basis for $\mathcal{O}_L$ so that the initial conditions

of $x_1(k)$ match those of $d_k(\alpha)$. Let

$$\vec{a} = \begin{pmatrix} d_0 & d_1 & d_2 & d_3 \end{pmatrix}^\top.$$

If $d_1(\alpha) = 1$, then $\vec{a}$ is a primitive lattice element in $\mathbb{Z}^4$ and so there exists $A \in \mathrm{GL}_4(\mathbb{Z})$ with first column $\vec{a}$. Let $\{w_1, w_2, w_3, w_4\}$ be the basis obtained from $\{1, \sqrt{\alpha}, \sqrt{\alpha}^2, \sqrt{\alpha}^3\}$ by change of basis matrix A^{-1}. Then $x_1(k)$ has the desired initial conditions. If $d_1(\alpha) \neq 1$, then we replace the sequence $d_k(\alpha)$ by $d_k(\alpha)/d_1(\alpha)$ in the argument above. □

Remark 2.4.3. Since the coordinate sequence $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ of β^k for any $\beta \in \bar{\mathbb{Z}}$ defined in (2.4.17) are linear recurrence sequences with distinct characteristic roots, then by Proposition 1.3.2 they grow exponentially. So Theorem 2.4.1 implies that if $x_i(k) = d_k(\alpha)$ for some $\alpha \in \bar{\mathbb{Z}}$ and fixed index i, then α must be in one of the exceptional cases. That is, we must have a power of α either in $\mathbb{Z}$ or a quadratic unit. It would be interesting to know when a result like Proposition 2.4.2 holds in the other exceptional cases.

We finish this section by discussing how the recurrence for the coordinate sequences $\{x_i(k) : k \in \mathbb{Z}_{\geq 0}\}$ of α^k, for some $\alpha \in \bar{\mathbb{Z}}$, could be used to study the sequence $d_k(\alpha)$ defined in (2.4.15).

By definition, we have that $d_k(\alpha)$ is the largest positive integer satisfying

$$\alpha^k - 1 \in d_k(\alpha)\mathcal{O}_K. \tag{2.4.19}$$

Let $\{1, w_2, \ldots, w_n\}$ be an integral basis for K. If we write

$$\alpha^k = x_1(k) + x_2(k)w_2 + \cdots + x_n(k)w_n.$$

Then we have

$$d_k(\alpha) = \gcd(x_1(k) - 1, x_2(k), \ldots, x_n(k)). \tag{2.4.20}$$

Furthermore, by Corollary 2.1.4 each of the sequences $x_i(k)$ has characteristic polynomial equal to the minimal polynomial of α. As in the previous sections, we can change the initial conditions of $x_i(k)$ by changing the basis of $\mathcal{O}_K$. We use these observations to study the following conjecture.

Conjecture 2.4.4 (Conjecture 9 of [26])**.** For $\alpha \in \bar{\mathbb{Z}}$, suppose one of the following holds:

(a) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 3$ for all $r \geq 1$, or

(b) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 2$ for all $r \geq 1$ and $N_K(\alpha) \neq \pm 1$.

Then, the set $\{k \geq 1 \mid d_k(\alpha) = d_1(\alpha)\}$ is infinite.

The following proposition can be used to construct examples where Conjecture 2.4.4 holds.

Proposition 2.4.5. Let $\alpha \in \bar{\mathbb{Z}}$ have minimal polynomial

$$f(X) = X^n - s_1 X^{n-1} - \cdots - s_n,$$

and set $K = \mathbb{Q}(\alpha)$. If there exists a positive divisor $t > 1$ of n so that $s_i = 0$ $\forall i \notin t\mathbb{Z}$, then we have $d_k(\alpha) \leq |\mathcal{O}_K/\mathbb{Z}[\alpha]|$ for all $k \in 1 + t\mathbb{Z}$. In particular, if $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $d_k(\alpha) = d_1(\alpha) = 1$ for all $k \in 1 + t\mathbb{Z}$.

Proof. Let $\Delta = |\mathcal{O}_K/\mathbb{Z}[\alpha]|$, and $\tilde{d}_k$ denote the largest integer with

$$\alpha^k - 1 \in \frac{\tilde{d}_k}{\Delta}\mathbb{Z}[\alpha].$$

Since $\mathcal{O}_K \subset \frac{1}{\Delta}\mathbb{Z}[\alpha]$, then by (2.4.19) we have

$$\alpha^k - 1 \in d_k \mathcal{O}_K \subset \frac{d_k}{\Delta}\mathbb{Z}[\alpha].$$

So, $d_k \leq \tilde{d}_k$. Next, write

$$\alpha^k = y_1(k) + y_2(k)\alpha + \cdots + y_n(k)\alpha^{n-1}.$$

Then, similar to (2.4.20) we observe that

$$\tilde{d}_k = \Delta \gcd(y_1(k) - 1, y_2(k), \ldots, y_n(k)).$$

If $s_i = 0 \ \forall i \notin t\mathbb{Z}$, then by Corollary 2.1.4 we have

$$y_1(k+n) = s_t y_1(k+n-t) + \cdots + s_{\ell t} y_i(k+n-\ell t).$$

Since $y_1(k)$ has initial conditions $y_1(0) = 1, y_1(1) = \cdots = y_1(n-1) = 0$, we see that $y_1(1+\ell t) = 0$ for any $\ell \in \mathbb{Z}_{\geq 0}$. So, $d_k \leq \tilde{d}_k = \Delta$. □

We give an example to demonstrate how to use Proposition 2.4.5 to generate examples where Conjecture 2.4.4 holds.

Example 2.4.6. Let α be an algebraic number of degree 4 so that $\beta := \alpha^2$ is quadratic. Observe that the minimal polynomial of α is of the form

$$f(X) = X^4 - \mathrm{Tr}_{L/\mathbb{Q}}(\beta)X^2 + N_{L/\mathbb{Q}}(\beta),$$

where $L = \mathbb{Q}(\beta)$, and so by Proposition 2.4.5 we have that

$$d_k(\alpha) \leq |\mathcal{O}_K/\mathbb{Z}[\alpha]|$$

whenever k is odd. So, Conjecture 2.4.4 holds whenever

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \text{ where } K = \mathbb{Q}(\alpha). \tag{2.4.21}$$

Number fields K satisfying (2.4.21) are called *monogenic*, and elements α satisfying (2.4.21) are called *monogenizers* of K.

We searched for elements α as in Example 2.4.6 that are monogenizers of $K = \mathbb{Q}(\alpha)$. Using Sage to check whether $\mathcal{O}_K = \mathbb{Z}[\alpha]$, we searched the first five real quadratic fields (ordered by discriminant), and found the following list of examples:

$$\sqrt{2+\sqrt{2}}, \sqrt{1+\sqrt{3}}, \sqrt{\tfrac{1}{2}(5+\sqrt{5})}, \sqrt{1+\sqrt{6}}, \sqrt{1+\sqrt{7}}.$$

It would be interesting to provide a characterization of all monogenic quartic fields with generator of the form α where α^2 is contained in a quadratic subfield, as this would provide a family of examples where Conjecture 2.4.4 holds for the sequence $d_k(\alpha)$ and could improve the results of Section 2.3. In the following chapter, we study the monogenizers of certain biquadratic fields through their associated index forms.

CHAPTER III

INDEX FORM EQUATIONS OVER BIQUADRATIC FIELDS

Let K be a number field and $\mathcal{O}$ an order in K. That is, $\mathcal{O}$ is a $\mathbb{Z}$-module in K of rank $[K : \mathbb{Q}]$ that is also a ring with unity. We call $\mathcal{O}$ *monogenic* if there exists an element $\alpha \in \mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$. In this case we call α a *monogenizer* of $\mathcal{O}$. Note that if α is a monogenizer of $\mathcal{O}$, so is $\alpha \pm c$ for any integer c. We define the equivalence

$$\alpha \sim \beta \Leftrightarrow \alpha \pm \beta \in \mathbb{Z} \tag{3.0.1}$$

and call each equivalence class a *monogenization* of $\mathcal{O}$. It is well-known that every order is contained in the ring of integers $\mathcal{O}_K$ of K, and so we will say that K is monogenic whenever $\mathcal{O}_K$ is, and that α is a monogenizer of K when α is a monogenizer of $\mathcal{O}_K$. In Remark 2.3.3 and Example 2.4.6, we saw that the results of Chapter II could be improved when our quartic field K has monogenizer α with α^2 contained in a quadratic subfield of K.

A *biquadratic field* is a quartic field of the form $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ where m and n are distinct nonsquare integers. In [11], Gaál, Pethö and Pohst give a method to algorithmically search for monogenizers of certain biquadratic fields, which we expect will lead to further theoretical results. In this chapter, we give an exposition of the methods outlined in [11]. Our main contribution is a rewriting of this algorithmic paper in order to motivate further theoretical results.

This chapter is organized as follows. In Section 3.1 we give some background on index form equations, which translate the question of monogeneity of a number field K to a Diophantine problem. In Section 3.2 we use the results of [11] to

reduce this Diophantine problem to solving a system of norm form equations. In Section 3.3 we outline how the authors of [11] associate the monogenizers of a biquadratic field to near squares of an associated linear recurrence sequence. We then discuss ongoing work to use this result to obtain bounds on the height of monogenizers in biquadratic fields.

3.1. Background on Index Form Equations

Let K be a number field and α an element of $\mathcal{O}_K$. Note that $\mathbb{Z}[\alpha]$ is finite index in $\mathcal{O}_K$ when $\deg \alpha = [K : \mathbb{Q}]$, and that α is a monogenizer precisely when the index is equal to 1. We use this observation to translate the problem of finding monogenizers of K to a Diophantine problem.

Let σ_i be the distinct embeddings of $K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. For any m-tuple of elements $\alpha_1, \ldots, \alpha_m$ in K, the *discriminant* of $\alpha_1, \ldots, \alpha_m$ is defined to be the quantity

$$D_K(\alpha_1, \ldots, \alpha_m) := \det(\sigma_i(\alpha_j))^2.$$

For an element $\alpha \in K$ of degree m, the discriminant of α is given by

$$D_K(\alpha) := D_K(1, \alpha, \ldots, \alpha^{m-1}).$$

Let $\{1, w_1, \ldots, w_n\}$ be an integral basis for K so that $[K : \mathbb{Q}] = n + 1$. For an element $\alpha \in \mathcal{O}_K$ of degree $[K : \mathbb{Q}]$ write

$$\alpha = x_0 + x_1 w_1 + \cdots + x_n w_n, \tag{3.1.2}$$

with $x_i \in \mathbb{Z}$. Let $\sigma_0, \ldots, \sigma_n$ be the distinct embeddings $K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$, and suppose that σ_0 is the identity embedding. We have

$$D_K(\alpha) = \det \begin{pmatrix} 1 & \alpha & \cdots & \alpha^n \\ 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^n \end{pmatrix}^2.$$

This is a Vandermonde determinant, and so we get

$$D_K(\alpha) = \prod_{0 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

For convenience, we denote $\underline{X} := (X_1, \ldots, X_n)$. If we write α as in (3.1.2) we see that $D_K(\alpha)$ does not depend on x_0. For the linear form

$$\ell(\underline{X}) := w_1 X_1 + \cdots + w_n X_n \tag{3.1.3}$$

in $K[\underline{X}]$ we define the discriminant of $\ell(\underline{X})$ in K to be

$$D_K(\ell(\underline{X})) := \prod_{0 \le i < j \le n} (\sigma_i(\ell(\underline{X})) - \sigma_j(\ell(\underline{X})))^2, \tag{3.1.4}$$

where the embeddings σ_i act on $\ell(\underline{X})$ in the usual way. That is,

$$\sigma_i(\ell(\underline{X})) = \sigma_i(\omega_1) X_1 + \cdots + \sigma_i(\omega_n) X_n.$$

For any $\alpha \in \mathcal{O}_K$ we have the following well-known identity

$$D_K(\alpha) = |\mathcal{O}_K/\mathbb{Z}[\alpha]|^2 D_K, \tag{3.1.5}$$

where D_K denotes the discriminant of K; that is,

$$D_K := D_K(1, w_1, \ldots, w_n) \tag{3.1.6}$$

(see of Remark 2.25 of [20], for example). We define the *index form* $I_W(\underline{X})$ with respect to basis W by the equation

$$D_K(\ell(\underline{X})) = I_W^2(\underline{X}) D_K. \tag{3.1.7}$$

By identity (3.1.5) we have that $\alpha = x_0 + x_1 w_1 + \cdots + x_n w_n$ is a monogenizer of K precisely when the integer tuple $(x_1, \ldots, x_n)$ is a solution to the following equation

$$I_W(\underline{X}) = \pm 1. \tag{3.1.8}$$

The following Lemma tells us that finding integral solutions to (3.1.8) is in fact a Diophantine problem.

Lemma 3.1.1. The form $I_W(\underline{X})$ defined in (3.1.7) is an integral form (that is, a homogeneous polynomial with integer coefficients) of degree $n(n+1)/2$, where $[K : \mathbb{Q}] = n + 1$.

Proof. Define $F_{ij}(\underline{X})$ to be the polynomials in $K[\underline{X}]$ given by

$$\ell^j(\underline{X}) = F_{0j}(\underline{X}) + F_{1j}(\underline{X}) w_1 + \cdots + F_{nj}(\underline{X}) w_n,$$

where $\ell^j(\underline{X})$ denotes the product of $\ell(\underline{X}) = X_1w_1 + \cdots + X_nw_n$ with itself j times. Observe that each $F_{ij}(\underline{X})$ is of homogeneous degree j, and since $\{1, w_1, \ldots, w_n\}$ is an integral basis, each $F_{ij}(\underline{X})$ is in $\mathbb{Z}[\underline{X}]$. So, for any σ_k we have

$$\sigma_k(F_{ij}(\underline{X})) = F_{ij}(\underline{X}).$$

From the definition of the discriminant form given in (3.1.4), we have

$$D_K(\ell(\underline{X})) = \det \begin{pmatrix} 1 & \ell(\underline{X}) & \cdots & \ell^n(\underline{X}) \\ 1 & \sigma_1(\ell(\underline{X})) & \cdots & \sigma_1(\ell^n(\underline{X})) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\ell(\underline{X})) & \cdots & \sigma_n(\ell^n(\underline{X})) \end{pmatrix}^2.$$

Setting $w_0 = 0$ we use the notation above to write

$$D_K(\ell(\underline{X})) = \det \begin{pmatrix} 1 & \sum_{i=0}^n F_{i1}(\underline{X})w_i & \cdots & \sum_{i=0}^n F_{in}(\underline{X})w_i \\ 1 & \sum_{i=0}^n F_{i1}(\underline{X})\sigma_1(w_i) & \cdots & \sum_{i=0}^n F_{in}(\underline{X})\sigma_1(w_i) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sum_{i=0}^n F_{i1}(\underline{X})\sigma_n(w_i) & \cdots & \sum_{i=0}^n F_{in}(\underline{X})\sigma_n(w_i) \end{pmatrix}^2$$

$$= \det \begin{pmatrix} 1 & w_1 & \cdots & w_n \\ 1 & \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix}^2 \det \begin{pmatrix} 1 & F_{01}(\underline{X}) & \cdots & F_{0n}(\underline{X}) \\ 0 & F_{11}(\underline{X}) & \cdots & F_{1n}(\underline{X}) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & F_{n1}(\underline{X}) & \cdots & F_{nn}(\underline{X}) \end{pmatrix}^2$$

By definition of the field discriminant D_K given in (3.1.6) we have

$$D_K(\ell(\underline{X})) = D_K \cdot \det \begin{pmatrix} 1 & F_{01}(\underline{X}) & \cdots & F_{0n}(\underline{X}) \\ 0 & F_{11}(\underline{X}) & \cdots & F_{1n}(\underline{X}) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & F_{n1}(\underline{X}) & \cdots & F_{nn}(\underline{X}) \end{pmatrix}^2.$$

Using definition (3.1.7) this gives

$$I_W(\underline{X}) = \pm \det \begin{pmatrix} 1 & F_{01}(\underline{X}) & \cdots & F_{0n}(\underline{X}) \\ 0 & F_{11}(\underline{X}) & \cdots & F_{1n}(\underline{X}) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & F_{n1}(\underline{X}) & \cdots & F_{nn}(\underline{X}) \end{pmatrix}.$$

Since each $F_{ij}(\underline{X})$ is in $\mathbb{Z}[\underline{X}]$ with homogeneous degree j, we conclude that $I_W(\underline{X})$ is an integral form with

$$\deg I_W(\underline{X}) = \sum_{j=0}^{n} j = n(n+1)/2. \qquad \square$$

It is known that every index form equation (3.1.8) has only finitely many integral solutions, which implies that there are only finitely many monogenizations of $\mathcal{O}_K$ for a given number field K. An effective upper bound on the number of integral solutions to (3.1.8) was given by Győry in [12]. While this bound has since been improved (see [13] for a survey of these results), it is generally too large to be computationally feasible. Current research aims to improve these bounds in special cases. For example, in [10], the authors use a number of reductions to show that integral solutions to index form equations over quartic fields imply solutions to a

cubic Thue equation and a system of quadratic equations (see Proposition 3.1 of [1] for details of this result). In [1], Akhtari uses this result to provide a new proof for the best known upper bound on the number of monogenizers in quartic fields up to the equivalence given in (3.0.1). In particular, Akhtari shows the following.

Proposition 3.1.2 (Theorem 1.1 of [1])**.** Let K be a quartic number field. Then, the number of elements $\alpha \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbb{Z}[\alpha]$ up to the equivalence defined in (3.0.1) is at most 2760.

In fact, Akthari proves this bound for the number of monogenizations of any quartic order $\mathcal{O}$, which we recall is always finite index in $\mathcal{O}_K$. Improvements on this bound are also given based on the size of the discriminant of $\mathcal{O}$.

In [11], Gaál, Pethö and Pohst study index forms defined over biquadratic fields with class number one by using the special integral basis due to Pohst below.

Lemma 3.1.3 (see [22])**.** Let K be a biquadratic field with quadratic subfield $L = \mathbb{Q}(\sqrt{m})$ having class number 1. Then, there is a non-square element μ in L so that we can write $K = \mathbb{Q}(\sqrt{\mu})$. Furthermore, let

$$\omega = \begin{cases} \sqrt{m} & \text{if } m \equiv 2, 3 (\mathrm{mod}\, 4) \\ \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

so that $\mathcal{O}_L = \mathbb{Z}[\omega]$. Then there exists $\alpha, \beta \in \mathcal{O}_L$ so that if $\psi = (\alpha + \beta\sqrt{\mu})/4$ then

$$\{1, \omega, \psi, \omega\psi\} \tag{3.1.9}$$

forms an integral basis for K.

Using this basis, the authors of [11] give a number of reductions in order to algorithmically find small solutions to (3.1.8) over fields of this type. The following sections outline these reductions, which we plan to use to obtain further explicit results such as those in Theorem 3.1.2.

3.2. Reduction to Simultaneous Norm Form Equations

Let K be a biquadratic field containing a quadratic subfield L with class number 1 as in Lemma 3.1.3. We let $\underline{X} = (X_1, X_2, X_3)$ and $\ell(\underline{X})$ be the linear form given in (3.1.3) with respect to the basis $W = \{1, \omega, \psi, \omega\psi\}$ from Lemma 3.1.3. That is,

$$\ell(\underline{X}) = X_1\omega + X_2\psi + X_3\omega\psi.$$

From Lemma 3.1.1, we know that $I_W(\underline{X})$ is a degree 6 integral form. In this section, we show how to reduce the index form equation

$$I_W(\underline{X}) = \pm 1$$

to a system of norm form equations. We combine Proposition 1 and Theorem 1 of [11] to obtain the following result, and provide an alternate proof to that given in [11] using the language of algebraic number theory.

Proposition 3.2.1. Let K, L, μ and ω be as in Lemma 3.1.3. The index form equation $I_W(\underline{X}) = \pm 1$ has an integer solution $\underline{x} = (x_1, x_2, x_3)$ if and only if

$$N_L(x_2 + x_3\omega) = \pm 1, \text{ and}$$

$$N_{L'}(\mathscr{L}(\underline{x})) = \pm(\omega - \bar{\omega})^2$$

where $L' = \mathbb{Q}(\sqrt{N_L(\mu)})$ and $\mathscr{L}(\underline{X}) \in \mathcal{O}_{L'}[\underline{X}]$ is the fixed quadratic form defined in (3.2.11).

Proof. Write $L = \mathbb{Q}(\sqrt{m})$, and label the embeddings σ_i so that $\sigma_0 = \mathrm{id}$ and

$$\sigma_1 : \sqrt{m} \mapsto -\sqrt{m},\ \sqrt{\mu} \mapsto \sqrt{\bar{\mu}}$$

$$\sigma_2 : \sqrt{m} \mapsto \sqrt{m},\ \sqrt{\mu} \mapsto -\sqrt{\mu}$$

$$\sigma_3 : \sqrt{m} \mapsto -\sqrt{m},\ \sqrt{\mu} \mapsto -\sqrt{\bar{\mu}}$$

where $\bar{\alpha}$ denotes the quadratic conjugate of an element $\alpha \in L$. For convenience, set

$$\ell_{ij}(\underline{X}) := \sigma_i(\ell(\underline{X})) - \sigma_j(\ell(\underline{X})). \tag{3.2.10}$$

By the definitions given in (3.1.4) and (3.1.7) we get

$$I_W^2(\underline{X}) D_K = \prod_{0 \le i < j \le 3} \ell_{ij}^2(\underline{X}).$$

Using the integral basis W, we compute the discriminant of K to be

$$D_K = ((\omega - \bar{\omega})^2 (\psi - \psi_2)(\psi_1 - \psi_3))^2,$$

and we observe that

$$\ell_{02}(\underline{X}) = (\psi - \psi_2)(X_2 + \omega X_3)$$

$$\ell_{13}(\underline{X}) = (\psi_1 - \psi_3)(X_2 + \bar{\omega} X_3)$$

where $\psi_i = \sigma_i(\psi)$. So, we have

$$I_W(\underline{X}) = \pm\frac{1}{(\omega-\bar{\omega})^2}(X_2+\omega X_3)(X_2+\bar{\omega}X_3)\prod_{\substack{0\le i<j\le 3\\(i,j)\notin\{(0,2),(1,3)\}}}\ell_{ij}(\underline{X}).$$

Since $(X_2+\omega X_3)(X_2+\bar{\omega}X_3) \in \mathbb{Z}[X_2, X_3]$ is monic in X_2, and $(\omega-\bar{\omega})^2$ is divisible by m, then by above we must have that $(\omega-\bar{\omega})^2$ divides

$$\prod_{\substack{0\le i<j\le 3\\(i,j)\notin\{(0,2),(1,3)\}}}\ell_{ij}(\underline{X}).$$

So, $\underline{x} = (x_1, x_2, x_3)$ is a solution to $I_W(\underline{X}) = \pm 1$ precisely when

$$(x_2+\omega x_3)(x_2+\bar{\omega}x_3) = \pm 1, \text{ and}$$

$$\ell_{01}(\underline{x})\ell_{12}(\underline{x})\ell_{23}(\underline{x})\ell_{03}(\underline{x}) = \pm(\omega-\bar{\omega})^2.$$

Define

$$\mathscr{L}(X) := \ell_{01}(\underline{X})\ell_{23}(\underline{X}). \tag{3.2.11}$$

Note that the coefficients of $\mathscr{L}(\underline{X})$ are algebraic, since we assumed ω, ψ are elements of an integral basis of K. So, to complete our proof, we need to show that

$$\mathscr{L}(\underline{X}) \in L'[\underline{X}]$$

and that $\mathscr{L}(\underline{x})$ has conjugate $\ell_{12}(\underline{x})\ell_{03}(\underline{x})$ in $L' = \mathbb{Q}(\sqrt{N_L(\mu)})$. For the first claim, note that the nontrivial embedding fixing L' is σ_1. To see this, note that $\mathrm{Gal}(K/\mathbb{Q})$

is $\mathbb{Z}/2 \times \mathbb{Z}/2$ so every embedding has order 2. This gives us

$$\sigma_1(\sqrt{\overline{\mu}}) = \sigma_1(\sigma_1(\sqrt{\mu})) = \sqrt{\mu}$$

and so $\sigma_1(\sqrt{N_L(\mu)}) = \sigma_1(\sqrt{\mu})\sigma_1(\sqrt{\overline{\mu}}) = \sqrt{N_L(\mu)}$. By Galois correspondence we know that L' is fixed by two elements, and so to see whether $\mathscr{L}(\underline{X})$ has coefficients in L', it suffices to show it is fixed under the action by σ_1. Recalling that ψ is of the form $\psi = (\alpha + \beta\sqrt{\mu})/4$ for $\alpha, \beta \in L$ we can check that

$$\sigma_1(\psi_1) = \psi, \sigma_1(\psi_2) = \psi_3 \text{ and } \sigma_1(\psi_3) = \psi_2,$$

which gives

$$\sigma_1(\ell_{01}(\underline{X})) = -\ell_{01}(\underline{X}), \sigma_1(\ell_{23}(\underline{X})) = -\ell_{23}(\underline{X})$$

$$\sigma_1(\ell_{12}(\underline{X})) = \ell_{03}(\underline{X}) \text{ and } \sigma_1(\ell_{03}(\underline{X})) = \ell_{12}(\underline{X}).$$

So, we have $\mathscr{L}(\underline{X}) := \ell_{01}(\underline{X})\ell_{23}(\underline{X}) \in L'[\underline{X}]$ and $\ell_{12}(\underline{X})\ell_{03}(\underline{X}) \in \text{Ł}'[\underline{X}]$. To see these two quadratic forms are conjugates, it suffice to show that

$$\sigma_2(\mathscr{L}(\underline{X})) = \ell_{12}(\underline{X})\ell_{03}(\underline{X}).$$

As before we can check that

$$\sigma_2(\psi_1) = \psi_3, \sigma_2(\psi_2) = \psi, \text{ and } \sigma_2(\psi_3) = \psi_1,$$

to get $\sigma_2(\ell_{01}(\underline{X})) = \ell_{23}(\underline{X})$ and $\sigma_2(\ell_{23}(\underline{X})) = \ell_{01}(\underline{X})$, as desired. □

Remark 3.2.2. Note that Proposition 3.2.1 implies solutions to the simultaneous norm form equations

$$N_L(x_2 + x_2\omega) = \pm 1 \text{ and}$$

$$N_{L'}(\gamma_i y_i + \gamma_j y_j) = \pm(\omega - \bar{\omega})^2,$$

for $\gamma_i, \gamma_j \in \mathcal{O}_{L'}$, and where $y_i = x_i + ax_j$ and $y_2 = x_k + bx_j$ for $i, j, k \in \{1, 2, 3\}$ and some fixed $a, b \in \mathbb{Q}$. To see this, write the quadratic form $\mathscr{L}(\underline{X})$ as

$$\mathscr{L}(\underline{X}) = (\alpha_1 X_1 + \alpha_{13} X_3)X_1 + (\alpha_2 X_2 + \alpha_{12} X_1)X_2 + (\alpha_3 X_3 + \alpha_{23} X_2)X_3,$$

for some $\alpha_i \in \mathcal{O}_{L'}$. So, if $\underline{x} = (x_1, x_2, x_3)$ is a solution to the system of equations in Proposition 3.2.1 then we have $\mathscr{L}(\underline{x}) = \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3$, for $\gamma_i \in \mathcal{O}_{L'}$. But since L' is quadratic, $\{\gamma_1, \gamma_2, \gamma_3\}$ are linearly dependent. So we can write

$$\mathscr{L}(\underline{x}) = \gamma_i y_i + \gamma_j y_j,$$

where $y_i = x_i + ax_j$ and $y_2 = x_k + bx_j$ for $i, j, k \in \{1, 2, 3\}$ and fixed rational constants a, b. So solutions to the system in Proposition 3.2.1 imply solutions to the system of norm form equations above. It would be interesting to study whether any explicit information can be gathered from this observation. For example, in [4] Bennett gives explicit upper bounds on the integral solutions to simultaneous Pell-type equations. We plan to study whether such a method extends to simultaneous quadratic norm form equations more generally.

3.3. Near Squares in Linear Recurrence Sequences

The authors of [11] show that integral solutions to $I_W(\underline{X}) = \pm 1$, with W as in Lemma 3.1.3, can be found by studying terms in an associated order 2 linear recurrence sequence that are a constant away from a perfect square. We state this result below and give an alternate proof using language of algebraic number theory.

Proposition 3.3.1 (Section 4 of [11])**.** Let K, L and W be as above. Suppose that $I_W(\underline{X}) = \pm 1$ has a solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$, and let ε be a fundamental unit in $\mathcal{O}_L$. Let $G(k)$ be the order two linear recurrence sequence defined by

$$G(k+2) = \mathrm{Tr}(\varepsilon^2)G(k+1) - G(k)$$

Then, for a fixed constant δ there exists $k \in \mathbb{Z}_{\geq 0}$ and $y \in \mathbb{Z}$ so that

$$G(k) = y^2 + \delta.$$

Furthermore, the constant δ and the initial conditions of $G(k)$ are explicitly computable and depend on L, x_2, x_3.

Proof. Let $\mathscr{L}(\underline{X})$ be the quadratic form defined by

$$\mathscr{L}(\underline{X}) = \ell_{01}(\underline{X})\ell_{23}(\underline{X})$$

where $\ell_{ij}(\underline{X}) = \sigma_i(\ell(\underline{X})) - \sigma_j(\ell(\underline{X}))$ as in the proof of Proposition 3.2.1. Recall in this proof that we showed $\mathscr{L}(\underline{X})$ has coefficients in $\mathcal{O}_{L'}$ where $L' = \mathbb{Q}(\sqrt{N_K(\mu)})$. This gives

$$\mathrm{Tr}_{L'}(\mathscr{L}(\underline{X})) \in \mathbb{Z}[\underline{X}]$$

where here we use the definition of trace given by $\mathrm{Tr}_{L'}(\gamma) = \gamma + \bar{\gamma}$ for an element $\gamma \in L'$ and let the conjugate embedding act on our polynomial in the usual way. Furthermore, since $\ell_{ij}(\underline{X})$ is a linear form, then $\mathscr{L}(\underline{X})$ is a quadratic form, and so we can write

$$\mathrm{Tr}_K(\mathscr{L}(\underline{X})) = a_1X^2 + a_2X_2^2 + a_3X_3^2 + a_{12}X_1X_2 + a_{13}X_1X_3 + a_{23}X_2X_3,$$

for $a_i, a_{ij} \in \mathbb{Z}$. Since $\mathrm{Tr}_K(\mathscr{L}(\underline{x})) \in \mathbb{Z}$ then the quadratic

$$f(X_1) := \mathrm{Tr}_K(\mathscr{L}(X, x_2, x_3)) - \mathrm{Tr}_K(\mathscr{L}(x_1, x_2, x_3)) \in \mathbb{Z}[X]$$

must have discriminant

$$\Delta_f(x_2, x_3) := b_2x_2^2 + b_3x_3^2 + b_{23}x_2x_3 + b_0 \tag{3.3.12}$$

equal to an integer square, where $b_i \in \mathbb{Z}$. Next, by Proposition 3.2.1, since $\underline{x}$ is a solution to our index form equation $I_W(\underline{X}) = \pm 1$ we must have

$$N_L(x_2 + \omega x_3) = \pm 1.$$

From our characterization of solutions to norm form equations from Chapter I, for a fundamental unit ε in $\mathcal{O}_K$ we can write $(x_2, x_3) = (x(k), y(k))$ for some integer k, where

$$\varepsilon^k = x(k) + \omega y(k).$$

So, $x(k)$ and $y(k)$ are order 2 linear recurrence sequences with characteristic roots $\varepsilon, \bar{\varepsilon}$. We use Proposition 1.3.1 from Chapter I to find an explicit formula for these

sequences. Note that $y(0) = 0$ and so we have

$$y(k) = y(1)\,\frac{\varepsilon^k - \bar{\varepsilon}^k}{\varepsilon - \bar{\varepsilon}}.$$

But since $\varepsilon - \bar{\varepsilon} = y(1)(\omega - \bar{\omega})$ we get

$$y(k) = \frac{\varepsilon^k - \bar{\varepsilon}^k}{\omega - \bar{\omega}}. \tag{3.3.13}$$

Next, we write $x(k) = A\varepsilon^k + B\bar{\varepsilon}^k$, and use the initial conditions of $x(k)$ to solve for $A, B \in L$. We have $A + B = 1$ and $x(1) = A\varepsilon + B\bar{\varepsilon}$, but also

$$x(1) = \varepsilon - \omega y(1) = \frac{\bar{\varepsilon}\omega - \varepsilon\bar{\omega}}{\omega - \bar{\omega}},$$

which gives

$$x(k) = \frac{\bar{\omega}\varepsilon^k - \omega\bar{\varepsilon}^k}{\bar{\omega} - \omega}. \tag{3.3.14}$$

So, plugging (3.3.14) and (3.3.13) in for (x_2, x_3) in our discriminant formula (3.3.12), we get

$$\begin{aligned}\Delta_f(x_2, x_3) =& b_2\left(\frac{\bar{\omega}^2\varepsilon^{2k} + \omega^2\bar{\varepsilon}^{2k}}{(\bar{\omega} - \omega)^2} \mp \frac{2\omega\bar{\omega}}{(\bar{\omega} - \omega)^2}\right) + b_3\left(\frac{\varepsilon^{2k} + \bar{\varepsilon}^{2k}}{(\omega - \bar{\omega})^2} \mp \frac{2}{(\omega - \bar{\omega})^2}\right) \\ & - b_{23}\left(\frac{\bar{\omega}\varepsilon^{2k} + \omega\bar{\varepsilon}^{2k}}{(\bar{\omega} - \omega)^2} \mp \frac{\bar{\omega} + \omega}{(\omega - \bar{\omega})^2}\right) + b_0,\end{aligned}$$

where the option in signs depends on whether ε has positive or negative norm. It can be checked that all summands above are in $\frac{1}{2}\mathbb{Z}$. Let

$$G(k) := b_2 a_1(k) + b_3 a_2(k) + b_{23} a_3(k) \in \mathbb{Z}$$

where

$$a_1(k) := 4\,\frac{\bar{\omega}^2\varepsilon^{2k} + \omega^2\bar{\varepsilon}^{2k}}{(\bar{\omega}-\omega)^2}$$

$$a_2(k) := 4\,\frac{\varepsilon^{2k} + \bar{\varepsilon}^{2k}}{(\omega-\bar{\omega})^2}$$

$$a_3(k) := 4\,\frac{\bar{\omega}\varepsilon^{2k} + \omega\bar{\varepsilon}^{2k}}{(\bar{\omega}-\omega)^2},$$

and each $a_i(k) \in \mathbb{Z}$. Then we have

$$G(k) = 4\Delta_f + 4b_0,$$

where $\Delta_f = \Delta_f(k)$ depends on k. Since Δ_f must be an integer square, there must exist $k \in \mathbb{Z}_{\geq 0}$ and $y \in \mathbb{Z}$ so that $G(k) = y^2 + \delta$, where

$$\delta = 4b_0 \mp \frac{8b_2\omega\bar{\omega}}{(\bar{\omega}-\omega)^2} \mp \frac{8b_3}{(\omega-\bar{\omega})^2} \pm \frac{4b_{23}(\bar{\omega}+\omega)}{(\omega-\bar{\omega}^2)}.$$

Now, since $a_i(k)$ has characteristic roots $\varepsilon^2, \bar{\varepsilon}^2$, each of these sequences satisfy the order 2 recurrence $a_i(k+2) = \mathrm{Tr}_L(\varepsilon^2)a_i(k+1) - a_i(k)$. It is then straightforward to check that $G(k)$ also satisfies the order 2 recurrence

$$G(k+2) = \mathrm{Tr}_L(\varepsilon^2)G(k+1) - G(k). \qquad \square$$

Given an order 2 linear recurrence $L(k)$ and polynomial $P(X)$ over $\mathbb{Z}$, finding solutions $k \in \mathbb{Z}_{\geq 0}$ and $x \in \mathbb{Z}$ to equations of the form

$$L(k) = P(x) \tag{3.3.15}$$

have been widely studied, especially when P is quadratic. For example, in [33] Walsh explicitly provides solutions to (3.3.15) for a family of order 2 sequences $L(k)$ and polynomials $P(X)$ of the form $P(X) = cX^2 \pm 1$. As outlined in [33], the method of Baker from [2] can be used to bound the size of solutions to $G(k) = y^2 + \delta$ from Proposition 3.3.1, which we expect would lead to a bound on the height of monogenizers over biquadratic fields.

REFERENCES CITED

[1] S. Akhtari. Quartic index form equations and monogenizations of quartic orders. *arXiv preprint arXiv:2203.10235*, 2022.

[2] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65:439–444, 1969.

[3] M. Benito and J. L. Varona. Pythagorean triangles with legs less than n. *J. Comput. Appl. Math.*, 143(1):117–126, 2002.

[4] M. A. Bennett. On the number of solutions of simultaneous Pell equations. *J. Reine Angew. Math.*, 498:173–199, 1998.

[5] J.-P. Bézivin, A. Pethö, and A. J. van der Poorten. A full characterisation of divisibility sequences. *Amer. J. Math.*, 112(6):985–1001, 1990.

[6] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[7] Z. I. Borevich and I. R. Shafarevich. *Number Theory*. "Nauka", Moscow, third edition, 1985.

[8] J. W. S. Cassels. *An introduction to the geometry of numbers*. Springer Science & Business Media, 2012.

[9] G. Everest, A. J. Van Der Poorten, I. Shparlinski, T. Ward, et al. *Recurrence sequences*, volume 104. American Mathematical Society Providence, RI, 2003.

[10] I. Gaál, A. Pethő, and M. Pohst. Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields. *J. Number Theory*, 57(1):90–104, 1996.

[11] I. Gaál, A. Pethö, and M. Pohst. On the resolution of index form equations in biquadratic number fields, i. *Journal of Number Theory*, 38(1):18–34, 1991.

[12] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. III. *Publ. Math. Debrecen*, 23(1-2):141–165, 1976.

[13] K. Győry. Discriminant form and index form equations. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 191–214. de Gruyter, Berlin, 2000.

[14] M. Hall. Divisibility Sequences of Third Order. *Amer. J. Math.*, 58(3):577–584, 1936.

[15] T.-X. He and P. J.-S. Shiue. An approach to the construction of linear divisibility sequences of higher orders. *J. Integer Seq.*, 20(9):17–9, 2017.

[16] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

[17] P. Ingram. Multiples of integral points on elliptic curves. *J. Number Theory*, 129(1):182–208, 2009.

[18] S. Kak and M. Prabhu. Cryptographic applications of primitive pythagorean triples. *Cryptologia*, 38(3):215–222, 2014.

[19] T. Kubota. Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10:65–85, 1956.

[20] J. S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[21] W. G. Nowak and W. Recknagel. The distribution of Pythagorean triples and a three-dimensional divisor problem. *Math. J. Okayama Univ.*, 31:213–220, 1989.

[22] M. Pohst. Berechnung unabhängiger einheiten und klassenzahlen in total reellen biquadratischen zahlkörpern. *Computing*, 14(1-2):67–78, 1975.

[23] W. M. Schmidt. Norm form equations. *Ann. of Math. (2)*, 96:526–551, 1972.

[24] W. M. Schmidt. The number of solutions of norm form equations. *Trans. Amer. Math. Soc.*, 317(1):197–227, 1990.

[25] A. G. Shannon and A. F. Horadam. Generalized Fibonacci number triples. *Amer. Math. Monthly*, 80:187–190, 1973.

[26] J. H. Silverman. Divisibility sequences and powers of algebraic integers. *Documenta Mathematica*, pages 711–727, 2007.

[27] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[28] J. H. Silverman and K. E. Stange. Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.*, 146(4):355–378, 2011.

[29] C. Smyth. The terms in Lucas sequences divisible by their indices. *J. Integer Seq.*, 13(2):Article 10.2.4, 18, 2010.

[30] K. E. Stange. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.*, 68(5):1120–1158, 2016.

[31] A. Tripathi. On Pythagorean triples containing a fixed integer. *Fibonacci Quart.*, 46/47(4):331–340, 2008/09.

[32] P. Voutier and M. Yabuta. Primitive divisors of certain elliptic divisibility sequences. *Acta Arith.*, 151(2):165–190, 2012.

[33] P. G. Walsh. Near squares in linear recurrence sequences. *Glas. Mat. Ser. III*, 38(58)(1):11–18, 2003.

[34] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.