RESEARCH STATEMENT

ELISA BELLAH

CONTENTS

1. Introduction 1
2. Norm Form Equations and Linear Divisibility Sequences 1
3. Index Form Equations over Biquadratic Fields 4
4. Bounding Lifts of Markoff Triples mod $p$ 5
References 7

1. Introduction

My research is in Diophantine Analysis, which is the 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. My thesis work involves three related Diophantine equations whose solutions can be studied through their associated recurrence sequences.

In [2], I show that certain families of quartic norm form equations lead to recurrence sequences that are also linear divisibility sequences. In an ongoing project, I am studying index form equations to find explicit information about monogenic quartic fields, which I expect can be used to strengthen the results in [2] and provide a family of sequences that satisfy a conjecture proposed by Silverman in [20]. In a forthcoming joint paper with Fuchs and Ye, we give bounds on lifts of Markoff triples modulo $p$. In the following sections, I briefly introduce each of these projects, and provide statements of main results and proposed future work.

2. Norm Form Equations and Linear Divisibility Sequences

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 the rational form defined by

$$(1) \quad F_W(X_1, \ldots, X_n) := N_K(X_1 w_1 + \cdots + X_n w_n).$$

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

$$(2) \quad F_W(X_1, \ldots, X_n) = c,$$

where $c$ is a fixed nonzero integer. For example, the Pell-type equations

$$x_1^2 - Dx_2^2 = c,$$
where \( c \) is a fixed nonzero integer and \( D \) a fixed nonsquare integer, are norm form equations over \( \mathbb{Q}(\sqrt{D}) \) with defining set \( W = \{1, \sqrt{D}\} \).

It is known that integer solutions to (2) can be generated by tuples of linear recurrence sequences (see Chapter 9 of [11], or Proposition 2.2 of [2]). In the main results of [2] (Results 2.1 and 2.2), I show that for norm forms defined over certain quartic fields, there exists integrally equivalent forms, which I construct explicitly, so that these recurrence sequences are linear divisibility sequences. Before stating these results, I briefly discuss the relevant background.

**Background.** Let \( K \) be a number field. Given a \( \mathbb{Q} \)-linearly independent subset \( W \) of \( K \), let \( M \) be the \( \mathbb{Z} \)-module in \( K \) generated by \( W \). Note that if we choose another basis \( T \) for \( M \), the norm forms \( F_W \) and \( F_T \) defined in (1) are integrally equivalent. So, the integer solutions to (2) can be found by instead studying the elements in \( M \) of fixed norm \( c \). It can be shown that all such elements are of the form

\[
\alpha(k) = \beta \varepsilon^k, \quad \text{for } k \in \mathbb{Z}_{\geq 0}
\]

where there are finitely many options for \( \beta \), and \( \varepsilon \) is a unit in the positive unit group \( U^+_M \) of \( M \), which is defined by

\[
U^+_M := \{ \alpha \in M \mid N_K(\alpha) = 1 \}
\]

(see Chapter 2 of [5], or Section 2 of [19], for example). So, if we write

\[
(3) \quad \alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n,
\]

then we obtain infinitely many solutions \((x_1(k), \ldots, x_n(k))\) to (2). Furthermore, all solutions to (2) are obtained in this way.

I am interested in studying the arithmetic of the sequences \( \{x_i(k) \colon k \in \mathbb{Z}_{\geq 0}\} \). In particular, I am interested in knowing when these sequences satisfy the property of being a divisibility sequence, which is a sequence \( b(k) \) with the following property: for all \( n, m \in \mathbb{Z}_{\geq 0} \),

\[
n \mid m \Rightarrow b(n) \mid b(m).
\]

Divisibility sequences have been widely studied. Oftentimes, this extra structure is helpful in understanding further arithmetic properties of a given sequence. For example, every Lucas sequence is a divisibility sequence. This property was used by Bilu, Hanrot, and Voutier in [4] to study the primitive divisors of Lucas sequences, and by Smyth in [22] to study their index divisibility sets, as well as in many other results throughout the literature. Elliptic Divisibility Sequences, introduced by Ward in [24], are examples of nonlinear divisibility sequences. Similar results for these sequences have also been found, such as by Silverman and Stange in [21] and Voutier and Yabuta in [23].

**Main Results.** The main results in [2] concern the sequences \( \{x_i(k) \colon k \in \mathbb{Z}_{\geq 0}\} \) defined in (3) where \( \varepsilon \) is a unit in a quartic field and \( \varepsilon^2 \) is a unit in a quadratic subfield. A Theorem of Kubota tells us that units of this type are one of three main cases needed to study norm forms defined over biquadratic fields (see Theorem 1 of [16], and the discussion in [2]), but our results hold for quartic fields containing elements of this type more generally. I show the following.

**Result 2.1** (Theorem 1.5 of [2]). Let \( K \) be a quartic field with a real quadratic subfield \( L \) containing a quartic unit \( \eta \) of positive norm, so that \( \eta^2 \) is a unit in \( L \). Fix an 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 I 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 linear divisibility sequence.

**Result 2.2** (Theorem 1.6 of [2]). 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 \( \eta^2 \) 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 I 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 linear divisibility sequence.

Note that Results 2.1 and 2.2 also hold for the sequences \( \{x_i(k) : k \in \mathbb{Z}_{\geq 0}\} \) for any fixed \( i \in \{1, 2, 3, 4\} \) just by changing the basis to reindex our coordinates. However, I show in [2] that [14] implies it is not possible to make all of these sequences divisibility sequences simultaneously.

**Powers of Algebraic Integers.** Given \( \alpha \in \bar{\mathbb{Z}} \), define the sequence

\[
d_k(\alpha) = \max\{d \in \mathbb{Z} \mid \alpha^k \equiv 1 \pmod{d}\},
\]

where the congruence \( \alpha^k \equiv 1 \pmod{d} \) means that there is an element \( \beta \in \bar{\mathbb{Z}} \) with \( \alpha^k = 1 + d\beta \).

In [20], Silverman proposed the following Conjecture.

**Conjecture 2.3** (Conjecture 9 of [20]). For \( \alpha \in \bar{\mathbb{Z}} \), the set

\[
\{k \in \mathbb{Z}_{\geq 1} \mid d_k(\alpha) = d_1(\alpha)\}
\]

is infinite, except for when \( \alpha \) is in one of two exceptional cases.

In Proposition 5.5 of [2] I use methods from the proofs of Results 2.1 and 2.2 to give a potential approach to studying this Conjecture. A consequence of this Proposition is stated below to motivate some further questions.

**Result 2.4** (Example 5.6 of [2]). Let \( \beta \) be an element of a quadratic number field, and \( \alpha \) any algebraic integer satisfying \( \alpha^2 = \beta \). Then Conjecture 2.3 holds whenever

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

Number fields \( K \) having an element \( \alpha \) with \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) are called monogenic.

**Future Work.** In Result 2.1, it was necessary to specify that our module \( M \) has positive unit group of the form \( \mathbb{Z}[\eta] \) in order for the result to hold. When the ring of integers of \( K \) is larger than \( \mathbb{Z}[\eta] \), for example when \( K \) is not monogenic, this restricts the possibilities for corresponding norm forms where such a result holds. It is then natural to ask the following question.

**Problem 2.5.** Are there infinitely many monogenic quartic fields \( K \) with

\[
\mathcal{O}_K = \mathbb{Z}[\alpha],
\]

where \( \alpha \) is a element of degree 4 in \( K \) with \( \alpha^2 \) an element in a quadratic subfield?

Note that if we could answer Problem 3.2, then this with Result 2.4 would also provide a family of examples where Conjecture 2.3 holds. In the following project, I study monogenic biquadratic fields through a related Diophantine equation.
3. INDEX FORM EQUATIONS OVER BIQUADRATIC FIELDS

Let $K$ be a number field, and $\{1, w_1, \ldots, w_n\}$ an integral basis for $K$. The index form $I_W(X_1, \ldots, X_n)$ is the rational form defined, up to sign, by

$$D_K(w_1 X_1 + \cdots + w_n X_n) = (I_W(X_1, \ldots, X_n))^2 D_K,$$

where $D_K$ denotes the field discriminant. Observe that $K$ is monogenic if and only if

$$I_W(X_1, \ldots, X_n) \equiv \pm 1.$$

Furthermore, solutions to (6) give all elements $\alpha \in K$ with $O_K = \mathbb{Z}[\alpha]$ up to the equivalence

$$\alpha \sim \beta \iff \alpha - \beta \in \mathbb{Q}.$$

In [13] Gaál, Pethő and Pohst used the following Proposition to study index form equations over certain biquadratic fields.

**Proposition 3.1** ([18]). Let $K$ be a biquadratic field containing a quadratic subfield $L = \mathbb{Q}(\sqrt{m})$ of class number 1. Let $\omega = \sqrt{m}$ or $(1 + \sqrt{m})/2$ so that $O_L = \mathbb{Z}[\omega]$. Then $\exists \psi \in K$ so that $K$ has integral basis

$$W = \{1, \omega, \psi, \omega \psi\}.$$

Furthermore, $\exists \mu \in L$ so that $K = \mathbb{Q}(\sqrt{\mu})$.

It is shown in [13] that solutions to the index form equation

$$(8) \quad I_W(X_1, X_2, X_3) = \pm 1$$

with respect to the basis $W$ defined in Proposition 3.1 imply solutions to simultaneous norm form equations, as well as terms in recurrence sequences of the form $y^2 + \delta$ for a fixed integer $\delta$. These results are stated below.

**Proposition 3.2** (Proposition 1 of [13]). If (8) has a solution, then there exists a solution to the simultaneous norm form equations

$$N_L(X + \omega Y) = \pm 1,$$

$$N_{L'}(\ell(X, Y, Z)) = \pm m,$$

where $L' = \mathbb{Q}(\sqrt{N_L(\mu)})$ and $\ell$ is a certain linear form depending on $\omega$ and $\psi$.

**Proposition 3.3** (Section 4 of [13]). Suppose that (8) has a solution $(x_1, x_2, x_3) \in \mathbb{Z}^3$. Let $G_n$ be the order two linear recurrence sequence defined by

$$G_{n+2} = AG_{n+1} - G_n,$$

where the initial values of $G_n$ and the constant $A$ depend on $m, x_1, x_2, x_3$. Then there exists integer $n$ and $y$ so that

$$G_n = y^2 + \delta$$

for a fixed $\delta \in \mathbb{Z}$. 

Preliminary Result and Future Work. The authors of [13] use Proposition 3.3 to computationally check for small solutions to (8). I expect that the results of this paper, in particular Proposition 3.2 and 3.3 above, can be used to obtain more theoretical results. For example, combining Proposition 3.2 and a result of Bennett from [3], I show the following.

Result 3.4. Suppose that $K$ is biquadratic, and contains a quadratic subfield $L = \mathbb{Q}(\sqrt{m})$ of class number 1. Then, up to the equivalence defined in (7), we have

$$\#\{\text{inequivalent } \alpha \in K \mid \mathcal{O}_K = \mathbb{Z}[\alpha]\} \leq C(4 \log(1 + \Delta_L)),$$

where $C$ is a constant and $\Delta_L$ is the discriminant of a polynomial depending on $m$.

I plan to study what other explicit information can be obtained from the results in [13], in particular whether these results can be used to study Problem 3.2.

4. Bounding Lifts of Markoff Triples mod $p$

The Markoff Equation is defined by

$$x_1^2 + x_2^2 + x_3^2 = 3x_1x_2x_3,$$

and the positive integer solutions to (9) are called Markoff triples. Markoff first studied these triples in the context of Diophantine approximation and the theory of quadratic forms (see [17] or Chapter 2 of [7]). Markoff triples have since found application in other areas. For example, Cohn used these triples to study free groups on two generators (see Theorem 2 of [9]), and in [15] Hirzebruch and Zagier used Markoff triples to study the signature of certain 4-dimensional manifolds.

More recently, work has been done to understand the structure of Markoff mod $p$ graphs (see Definition 4.2 below). It is conjectured that these graphs form an expander family, and so in light of [8] these graphs have been proposed as a means to produce cryptographic hash functions. In [12], it is noted that one avenue of attack depends on how difficult it is to find lifts of solutions to (9) modulo $p$. The main result in a forthcoming joint paper with Elena Fuchs and Lynnelle Ye gives an upper bound on the sizes of lifts of Markoff triples modulo $p$ (see Result 4.5).

4.1. Background. Define the Vieta group $\Gamma$ to be the group of affine morphisms on $\mathbb{A}^3$ generated by permutations of the coordinates and the Vieta involutions $R_i$, where

$$R_1(x_1, x_2, x_3) = (3x_2x_3 - x_1, x_2, x_3),$$

and $R_2, R_3$ are defined similarly. It is well-know that the orbit of $(1, 1, 1)$ under $\Gamma$ generates all Markoff triples (see Chapter 3 of [1], for example). It is expected that the same is true modulo $p$. More precisely, we have the following conjecture.

Conjecture 4.1 (Strong Approximation). The set of nonzero solutions modulo $p$ to equation (9) can be obtained by the orbit of $(1, 1, 1)$ under $\Gamma$.

In Theorem 1 of [6], Bourgain, Gamburd and Sarnak shown that Strong Approximation holds for primes $p$ where $p^2 - 1$ does not have too many divisors. The authors prove this theorem by showing algorithmically that the Markoff mod $p$ graphs, defined below, are connected.

For convenience, denote the nonzero solutions modulo $p$ to (9) by $X^*(p)$, and call the algorithm given by Bourgain, Gamburd and Sarnak in [6] the BGS algorithm.
Definition 4.2. Define the rotations to be the elements of $\Gamma$ given by

$$\text{rot}_1(x_1, x_2, x_3) = (x_1, x_3, 3x_1x_3 - x_2),$$
$$\text{rot}_2(x_1, x_2, x_3) = (x_3, x_2, 3x_2x_3 - x_1),$$
$$\text{rot}_3(x_1, x_2, x_3) = (x_2, 3x_2x_3 - x_1, x_3).$$

The Markoff mod $p$ graph is the graph with vertex set equal to $X^*(p)$ and with edges of the form $\{x, \text{rot}_i x\}$ for $x \in X^*(p)$ and $i = 1, 2, 3$.

Definition 4.3. The $i$th rotation order of a point $x \in X^*(p)$ is defined by

$$\text{ord}_{p,i}(x) := \min\{n \in \mathbb{Z}_{>0} : \text{rot}_i^n(x) \equiv x \pmod{p}\},$$

and the rotation order of $x$ is defined by

$$\text{ord}_p(x) := \max\{\text{ord}_{p,i}(x) : i = 1, 2, 3\}.$$

Main Results. The BGS algorithm constructs a path $\gamma$ between any point $x$ in the Markoff mod $p$ graph and $(1, 1, 1)$. Note that this gives a lift $\tilde{x} = \gamma \cdot (1, 1, 1)$ thinking now of $\Gamma$ acting on the integer solutions to (9). The following observation allows us to keep track of how the sizes change as we travel along the paths described in this algorithm.

Observation 4.4. For $i \in \{1, 2, 3\}$ we have

$$\text{rot}_i^n(x_1, x_2, x_3) = \sigma(x_i, a_n, a_{n+1}),$$

where $\sigma$ is a suitable permutation of the coordinates, and $a_n$ is the linear recurrence sequence with initial conditions $a_0 = x_2, a_1 = x_3$ and

$$a_{n+2} = 3x_ia_{n+1} - a_n.$$

Using Observation 4.4 and estimates on the growth of linear recurrence sequences, we show the following.

Result 4.5. Let $p$ be a prime where Strong Approximation holds, and suppose that $x \in X^*(p)$ has rotation order bounded away from zero by an absolute constant. For a lift $\tilde{x}$ of $x$ we have

$$\text{size}(\tilde{x}) \leq C\varepsilon p^{\tau_p/2},$$

where $\tau_p := \tau(p^2 - 1)$ is the number of positive divisors of $p^2 - 1$ and $C$ and $\varepsilon$ are constants depending on $x$ but not on $p$.

Future Work. We expect that for many points $x \in X^*(p)$ the bound from Result 4.5 can be improved. Certain steps of the BGS algorithm are nonconstructive, which requires our proof to assume long path lengths, thus increasing the bound. We consider instead the following problem.

Problem 4.6. What is the average size of a lift of a Markoff triple modulo $p$?

We expect to have heuristic results for Problem 4.6 by assuming that the Markoff mod $p$ graphs form an expander family, which is believed to be true (see [10], for example). Assuming this hypothesis, we have shown that the average path length from any point in the Markoff mod $p$ graph to $(1, 1, 1)$ is on the order of $\log(p^2 \pm 3p)$. We are now working to understand the distribution of sizes of Markoff triples along paths of a fixed length.
References


