REDUCED IDEALS AND PERIODIC SEQUENCES
IN PURE CUBIC FIELDS
G. Tony Jacobs

Dissertation Prepared for the Degree of
DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS
August 2015

APPROVED:
Lior Fishman, Major Professor
Mariusz Urbanski, Committee Member
Olav Richter, Committee Member
Su Gao, Chair
of the Department of Mathematics
Mark Wardell, Dean
of the Toulouse Graduate School

Doctor of Philosophy (Mathematics), August 2015, 44 pp., 18 numbered references.

The “infrastructure” of quadratic fields is a body of theory developed by Dan Shanks, Richard Mollin and others, in which they relate “reduced ideals” in the rings and sub-rings of integers in quadratic fields with periodicity in continued fraction expansions of quadratic numbers. In this thesis, we develop cubic analogs for several infrastructure theorems. We work in the field $K=\mathbb{Q}(\alpha)$, where $\alpha^3=m$ for some square-free integer $m$, not congruent to $\pm1$, modulo 9. First, we generalize the definition of a reduced ideal so that it applies to $K$, or to any number field. Then we show that $K$ has only finitely many reduced ideals, and provide an algorithm for listing them. Next, we define a sequence based on the number alpha that is periodic and corresponds to the finite set of reduced principal ideals in $K$. Using this rudimentary infrastructure, we are able to establish results about fundamental units and reduced ideals for some classes of pure cubic fields. We also introduce an application to Diophantine approximation, in which we present a 2-dimensional analog of the Lagrange value of a badly approximable number, and calculate some examples.
ACKNOWLEDGMENTS

I would like to thank all of the teachers of mathematics who have guided me in my journey so far. From my sister Iris who first taught me to add and multiply numbers, to my advisor Lior Fishman who has been my mentor in the assembly of this paper, you have all inspired me.

I would like to thank David Simmons for his invaluable proof-reading, suggestions, and willingness to sit down with me and talk through the details of it all. Thanks also to Olav Richter for his extremely helpful notes and suggestions on my penultimate drafts.

For helping take care of the non-dissertation-writing details of life so that I could finish this paper, I would like to thank Aurora Wynne and KJ Jones. For the environment in which the ideas in this paper were gestated and developed, I would like to thank the owners and staff of the (now defunct) Treehouse Bar and Grill in Denton, Texas.
TABLE OF CONTENTS

ACKNOWLEDGMENTS iii

CHAPTER 1 Introduction 1
  1.1. Background 1
  1.2. Structure of this thesis 3

CHAPTER 2 Reduced Ideals in Certain Cubic Fields 8
  2.1. Comments on scope 8
  2.2. Basic results on ideals 8
  2.3. Reduced ideals 11

CHAPTER 3 Periodic Norm Sequences 17

CHAPTER 4 Sequences Associated with Cube Roots 21

CHAPTER 5 Application to Diophantine Approximation 24

APPENDIX A Sequence Interleaving Algorithm 28

APPENDIX B Proof of lemma on $\mathbb{Z}$-modules 32

APPENDIX C Python code for reduced ideals 35

APPENDIX D Python code for minimal sequences 40

BIBLIOGRAPHY 43
CHAPTER 1

INTRODUCTION

1.1. Background

It has long been known that continued fractions and quadratic irrationals have a special relationship. Real numbers with continued fraction expansions that are eventually periodic are precisely irrational numbers of algebraic degree 2, known as quadratic numbers. In the 1980s and '90s, this relationship was explored in depth by Mollin, Shanks, Williams and others. Much of this work is compiled and summarized in [10].

Their work, which Dan Shanks described as “infrastructure” in quadratic fields, relates the continued fraction algorithm to sub-rings of algebraic integers, called “orders”, and the presence in these sub-rings of certain “reduced ideals”. Understanding this infrastructure is beneficial in two ways: our understanding of continued fractions is put into an algebraic context, and as a result, continued fractions become a computational tool for addressing questions about the structure of rings in quadratic fields.

The question of whether there exists some analog to continued fractions, but for cubic numbers, algebraic numbers of degree 3, is known as “Hermite’s Problem”. Charles Hermite posed a version of it in 1839 in a letter to Carl Gustav Jacob Jacobi, in the context of discussing integer quadratic forms [9]. In particular, he asked whether there exists some algorithm for associating a sequence of natural numbers to a real number $\alpha$ in such a way that the sequence will be eventually periodic if and only if $\alpha$ is algebraic of degree 3, a cubic number.

Constructions that begin to address Hermite’s Problem generally fall under the heading of “multi-dimensional continued fractions”, and a variety of them exist. For example, Dasaratha et. al. described in 2014 a multidimensional continued fraction algorithm which, given a real number, produces a countable family of sequences, with the property that if the input belongs to a wide class of cubic numbers, then at least one sequence in the output family is guaranteed to be periodic [5].
The authors conjecture that the best solution possible to Hermite’s problem might be to produce such a family of algorithms, taking a real input, with the property that at least one of them yields an eventually periodic sequence, if and only if the real number input is a cubic irrational. We note that, if this is achieved, then it could be adapted into an algorithm that produces a single sequence with the desired property.

In our first appendix to this thesis, we define a “sequence interleaving algorithm” that takes a countable family of sequences as input, and produces from them a single sequence. We prove the following:

**Theorem A.3.** Given a countable family of sequences of natural numbers as input, the output of the sequence interleaving algorithm is an eventually periodic sequence if and only if some sequence in the input family is eventually periodic.

Thus, if a family of algorithms with the property described by Dasaratha et al. exists, then the sequence interleaving algorithm could be composed with that family to yield an algorithm producing a single sequence that does what Hermite requested. This would seem to satisfy the letter of Hermite’s problem, but not the spirit of it. We want some kind of machinery that “does” for cubic fields what continued fractions “do” for quadratic fields - they reveal their infrastructure, and periodicity is a consequence of that.

With this in mind, we step away from addressing Hermite’s problem directly, and look for periodic sequences that relate to cubic infrastructure, i.e., to reduced ideals in cubic fields. Thus, we take a different approach from Dasaratha et al., who examined a 2-dimensional generalization of the Gauss map on the unit interval. (The Gauss map is \( h(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor \), and it is associated with continued fractions). Instead, to keep our focus on infrastructure, we build sequences that relate directly to rings and ideals in cubic fields, in analogy to infrastructure in quadratic fields. We do not attempt to produce sequences from arbitrary real inputs, but only relating to known cubic inputs.

We use geometric techniques, which have much in common with previous work on cubic fields. The most well-known early example is Voronoi’s algorithm (1896), with which
he calculated systems of fundamental units in cubic fields. His construction was based on quadratic forms; in 1964 Delone and Faddeev expressed Voronoi’s algorithm in terms of the theory of “multiplicative lattices”, now known as fractional ideals [6]. Their version examines chains of minimal elements in fractional ideals.

In a more modern context, Williams and others have adapted Voronoi’s algorithm in calculating regulators in pure cubic fields, as well as for other calculations [2, 3, 7, 8, 12, 13, 14, 15, 16, 17, 18]. Their work, insofar as it addresses reduced ideals, discusses reduced principal ideals in the context of algebraic fields with rank 1 unit groups.

Our work here differs in that we mirror the approach of Mollin in Quadratics, and begin with the geometry of reduced ideals. We do not restrict our attention to principal ideals, either, although there is more we can say about them. Certain results here overlap with [3]. We also present an application in Diophantine approximation, which generalizes the Lagrange value of a badly approximable number.

1.2. Structure of this thesis

We begin in chapter 2, proving cubic versions of results from the first chapter of Mollin’s book. He begins by writing the ring of integers of a quadratic field as a rank 2 \( \mathbb{Z} \)-module \( [1, \omega] (= \mathbb{Z} \oplus \omega \mathbb{Z}) \) for some generator \( \omega \). He then notes that any full-rank submodule can be written uniquely in the canonical form \( [a, b + c\omega] \) with \( a > 0, c > 0, \) and \( 0 \leq b < a \). He then shows that, for such a submodule to be an ideal, these coefficients from its canonical form must satisfy certain requirements: \( c|a, c|b, \) and \( ac|N(b + c\omega) \).

Next, Mollin defines reduced ideals in quadratic fields in the following way: \( I = [a, b + c\omega] \), an ideal in \( K \) a quadratic field, is reduced if it is a primitive ideal (no integral divisors, so \( c = 1 \)) and if there is no non-zero \( \beta \in I \) satisfying \( |\beta| < a \) and \( |\beta'| < a \). We mean by \( \beta' \) the algebraic conjugate of \( \beta \).

Finally, Mollin writes down conditions on \( a \) and \( b \) for the primitive ideal \( I = [a, b + \omega] \) to be reduced ideal. As corollaries to this result, he is able to show two bounds. First, if \( a \) is smaller than a lower bound depending on the field, then \( I \) is reduced, and secondly, if \( a \) exceeds an upper bound depending on the field, then \( I \) is not reduced. These lead to the
conclusion that the ring of integers of \( K \) (or one of its sub-rings) can only have finitely many reduced ideals.

We consider pure cubic fields of the form \( \mathbb{Q}(\alpha) \), where \( \alpha^3 = m \) for some square-free rational integer \( m \not\equiv \pm 1 \) (mod 9). In such fields, we have a particularly simple structure for the ring of integers: we can write it as the \( \mathbb{Z} \)-module \([1, \alpha, \alpha^2]\). We begin, mirroring Mollin, by noting that any full-rank submodule can be written in the canonical form \( I = [a, b + ca, d + ea + f\alpha^2] \) with \( a > 0, c > 0, f > 0, 0 \leq b < a \), \( 0 \leq d < a \) and \( 0 \leq e < c \).

After establishing divisibility conditions on \((a, b, c, d, e, f)\) for \( I \) to be an ideal, we generalize Mollin’s definition of a reduced ideal to ideals in a field of degree \( n \). Taking the “shadow”, \( \text{Sh}(\alpha) \) of an algebraic number \( \alpha \) in the field to be the product of all of \( \alpha \)’s algebraic conjugates for that field, excluding itself, and taking the “length” \( \text{Len}(I) \) of an ideal \( I \) to be the smallest positive rational integer in \( I \), we define a reduced ideal to be a primitive ideal with no non-zero element \( \beta \) satisfying \(|\beta| < \text{Len}(I)\) and \(|\text{Sh}(\beta)| < \text{Len}(I)^{n-1}\).

Next, we go on to our main theorems in the section. First, we have criteria on \((a, b, c, d, e)\) for a primitive ideal \( I = [a, b + ca, d + ea + \alpha^2] \) to be reduced:

**Theorem 2.8** (Identification of reduced ideals). Let \( I = [L, b + ca, d + ea + \alpha^2] \) be the canonical form of a primitive ideal in \( K = \mathbb{Q}(\alpha) \), with \( \alpha^3 = m \) for some square-free integer \( m \not\equiv \pm 1 \) (mod 9). Then \( I \) is reduced if and only if for every integer pair \((y, z) \neq (0,0)\) satisfying:

\[
\begin{align*}
(1) \quad &0 \leq z < \frac{L}{\alpha^2} \\
(2) \quad &\alpha z - \frac{2L}{\sqrt{3}a} \leq y \leq \frac{L - \alpha^2 z + \sqrt{L^2 + 2L \alpha^2 z - 3 \alpha^4 z^2}}{2a} \\
(3) \quad &c|y - ez,
\end{align*}
\]

we have the inequality:

\[
\left\lfloor \frac{q - (yb + zd)}{L} \right\rfloor < \frac{p - (yb + zd)}{L},
\]

where
\[ p = p(y, z) = \max \left\{ -L - \alpha (y + \alpha z), \frac{1}{2} \left( \alpha (y + \alpha z) - \sqrt{4L^2 - 3\alpha^2 (y - \alpha z)^2} \right) \right\}, \]

and

\[ q = q(y, z) = \min \left\{ L - \alpha (y + \alpha z), \frac{1}{2} \left( \alpha (y + \alpha z) + \sqrt{4L^2 - 3\alpha^2 (y - \alpha z)^2} \right) \right\}. \]

Next, we give lower and upper bounds on the length of a reduced ideal:

**Theorem 2.9 (Lower bound).** If \( L < \alpha \), then \( I \) is reduced.

**Theorem 2.10 (Upper bound).** If \( L > \frac{6\sqrt{3m}}{\pi} \), then \( I \) is not reduced.

Using these results, it is fairly convenient to list all reduced ideals in one of the fields under consideration. In an appendix, we provide computer code that does precisely this. We are also now able to establish our finiteness result:

**Theorem 2.11.** Let \( K = \mathbb{Q}(\alpha) \) where \( \alpha^3 = m \), for a square-free integer \( m \not\equiv \pm 1 \pmod{9} \).

Then the ring \( \mathcal{O}_K \) contains at least one, and only finitely many, reduced ideals.

As we said, these results mimic part of Mollin’s first chapter, but for cubic fields, and give us a concrete geometric way of talking about reduced ideals.

The next step in Mollin’s exposition of infrastructure is to connect reduced ideals with the periodic parts of quadratic numbers’ continued fraction expansions. In the quadratic case, we note that, if \( \frac{p}{q} \) is a convergent of a quadratic number \( \sqrt{m} \) (with \( m \) square-free and not congruent to 1 modulo 4), then \( p + q\sqrt{m} \) is a “minimal element” in the ring of integers of \( K = \mathbb{Q}(\sqrt{m}) \). By “minimal”, we mean that it has the property that no other non-zero element in the ring is smaller than it, both in absolute value and in shadow size. We define minimal elements in our cubic rings in the same way at the end of chapter 2.

Given \( \alpha^3 = m \) as above, we begin chapter 3 by defining the minimal sequence associated with \( \alpha \) as the sequence of minimal elements in the ring \( \mathcal{O}_K \), starting with 1 and
proceeding in order of increasing absolute value. Taking norms of elements in the minimal sequence, we define the norm sequence associated with \( \alpha \). We include in an appendix computer code which, given a value for \( m \), calculates terms of the minimal sequence and norm sequence of \( \alpha \).

These sequences play a role similar to continued fractions for quadratic numbers, in a way that we make precise with the following results:

**Theorem 3.4.** The norm sequence of \( \alpha \) is periodic, and the minimal sequence, \( (\beta_k)_{k \geq 0} \), has the property that \( \beta_{h+l} = \varepsilon_0 \beta_h \), where \( l \) is the period of the norm sequence, and \( \varepsilon_0 \) is the fundamental unit of the field \( K = \mathbb{Q}(\alpha) \).

Now, let \( \mathcal{M} \) be the set of elements in the minimal sequence of \( \alpha \) on the interval \([1, \varepsilon_0)\), and let \( \mathcal{R} \) be the set of reduced principal ideals in \( K \). We construct functions \( F : \mathcal{M} \to \mathcal{R} \) and \( G : \mathcal{R} \to \mathcal{M} \), and prove the following:

**Theorem 3.5.** The functions \( F \) and \( G \) are inverses, providing a bijection between the sets \( \mathcal{M} \) and \( \mathcal{R} \).

Thus, we can use minimal sequences to obtain information about reduced ideals, and vice-versa. In chapter 4, we give an example of this. In particular, we use our minimal sequence construction to establish the following two theorems, which would seem to be the tip of an iceberg of similar theorems, accessible via similar techniques:

**Theorem 4.1.** Let \( k \geq 1 \) be an natural number so that \( m = k^3 + 1 \) is square-free and not congruent to \( \pm 1 \) modulo 9, let \( a^3 = m \) and let \( K = \mathbb{Q}(\alpha) \). Then:

- The fundamental unit of \( K \) is \( \varepsilon_0 = k^2 + k\alpha + \alpha^2 \)
- The norm sequence associated with \( \alpha \) is \( (1) \).
- The only reduced principal ideal in the ring of integers of \( K \) is the entire ring, \( (1) \).

**Theorem 4.2.** Let \( k \geq 2 \) be an natural number so that \( m = k^3 - 1 \) is square-free and not congruent to \( \pm 1 \) modulo 9. Let \( a^3 = m \) and let \( K = \mathbb{Q}(\alpha) \). Then:
• The fundamental unit of $K$ is $\varepsilon_0 = k^2 + k\alpha + \alpha^2$.

• The norm sequence associated with $\alpha = \sqrt[3]{m}$ is \((1, 3k(k-1))\).

• The ring of integers of $K$ has two reduced principal ideals, namely \([1, \alpha, \alpha^2]\), which is principally generated by 1, and \([3k(k-1), 3k(k-1)\alpha, (k-1)^2 + (k-1)\alpha + \alpha^2]\), which is principally generated by \((k-1)^2 + (k-1)\alpha + \alpha^2\).

Both of these theorems have precise analogs relating to continued fraction expansions of square roots.

In chapter 5, we move on from pure algebraic number theory, and consider an application to Diophantine approximation of the same geometric ideas developed here. In particular, we examine a 2-dimensional analog of the Lagrange value of a badly approximable number. We calculate some of these for vectors based on pure cube roots, and compare again with the quadratic case, in particular with Lagrange values of square roots.

The analog of Lagrange value that we define is the following: Let $\langle \alpha, \beta \rangle \in \mathbb{R}^2$ be a badly approximable vector, then we define the coefficient of approximation of $\langle \alpha, \beta \rangle$ to be:

$$c_0(\alpha, \beta) = \liminf_{z \to \infty} \sqrt{z} \max \{\|\beta z\|, \|\alpha z\|\},$$

where $\|x\|$ represents the distance between $x$ and the nearest rational integer. We then use geometric techniques to show the following:

**Theorem 5.3.** Let $\alpha$ be as above. Then we have,

$$c_0(\alpha, \alpha^2) = \frac{1}{\alpha \sqrt{3(1+\alpha+\alpha^2)}},$$

and we compare this with the corresponding result for Lagrange values of square roots.

We have four appendices: the interleaving algorithm mentioned above, a proof of one technical lemma, computer code that executes the algorithms from chapter 2 for identifying reduced ideals, and computer code that calculates the minimal sequence and norm sequence defined in chapter 3.
2.1. Comments on scope

In this thesis, we work in cubic fields of a certain form, namely \( \mathbb{Q}(\alpha) \) where \( \alpha^3 = m \) for some square-free integer \( m \) not congruent to \( \pm 1 \) modulo 9. Before proceeding at this level of specificity, we remark briefly on why this is our chosen purview.

We know from Dirichlet’s unit theorem (see e.g. [1, p. 346]) that a cubic field with three real embeddings (equivalently, positive discriminant) has a unit group of rank 2, whereas a field with one real embedding and two complex embeddings (equivalently, negative discriminant) has a unit group of rank 1. This makes the fields with complex embeddings easier to study, especially when generalizing notions from real quadratic fields, which also have rank 1 unit groups.

Besides the structure of the unit group, we are working with the integral basis of each field under consideration. Among the cubic fields of negative discriminant, those of the form we study here have a particularly simple integral basis. A clear next step in generalization would be to address fields generated by cube roots of arbitrary cube-free integers, and then arbitrary cubic fields of negative discriminant, and possibly arbitrary fields with rank one unit groups, as in [3].

There are some notions present in this work that would seem to generalize to algebraic numbers and fields of arbitrary degree, with arbitrary unit group structure.

2.2. Basic results on ideals

We begin with some notation.

**Remark 2.1.** Throughout this work, we adopt the following convention: The free \( \mathbb{Z} \)-module \( \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z} \) will be denoted \([\alpha_1, \ldots, \alpha_n] \).

Let \( m \) be a square-free integer such that \( m^2 \not\equiv 1 \pmod{9} \), and let \( \alpha \) be the unique real root of the \( \mathbb{Q} \)-irreducible polynomial \( x^3 - m \). Then the field \( K = \mathbb{Q}(\alpha) \) is a degree three
extension with integral basis \{1, \alpha, \alpha^2\} [1, p.176].

We consider the ring of integers of this field, \( \mathcal{O}_K \), as the free \( \mathbb{Z} \)-module \([1, \alpha, \alpha^2]\). A proper, non-zero ideal in this ring is necessarily a proper \( \mathbb{Z} \)-submodule of full rank, but not every proper, rank-3 submodule is an ideal. Our first results concern the understanding of ideals in terms of their structure as \( \mathbb{Z} \)-submodules. We begin with an elementary fact about free \( \mathbb{Z} \)-modules, which is certainly true in greater generality than stated here.

**Lemma 2.2.** Let \( M = [u_1, u_2, u_3] \) be a free \( \mathbb{Z} \)-module of rank 3. Let \( M' \subseteq M \) be a submodule of full rank. Then we can write \( M' = [au_1, bu_1 + cu_2, du_1 + eu_2 + fu_3] \), with all coefficients integral. Furthermore, we can suppose without loss of generality that \( a, c, f \) are strictly positive, that \( 0 \leq e < c \) and that \( 0 \leq b, d < a \). Subject to these conditions, all six coefficients are uniquely determined.

**Proof.** See appendix.

**Definition 2.3.** Let \( I \) be a submodule of the ring of integers in \( K = \mathbb{Q}(\alpha) \), \( \alpha^3 = m \), \( m \not\equiv \pm 1 \pmod{9} \) squarefree in \( \mathbb{Z} \), and let \( I \) be written in the form \( I = [a, b + c\alpha, d + e\alpha + f\alpha^2] \) with \( a, c, f > 0 \), \( 0 \leq b < a \), \( 0 \leq d < a \), and \( 0 \leq e < c \). We refer to this expression as the **canonical form** for the submodule. The product \( N(I) = acf \) is uniquely determined by canonical form, and we define the **norm of the submodule**, to be this number. The smallest rational integer in the ideal, given by the number \( a \) in canonical form, is defined as the **length of the submodule**, sometimes denoted \( \text{Len}(I) \), and we will sometimes denote it as \( L \) instead of \( a \).

We note that the norm we have defined is precisely the index of the submodule in the ring. Thus, in cases where the submodule is an ideal, the norm is the same as the ideal norm, defined in the usual way [1, p.221]. In this case, we may refer to the submodule's norm, length, and canonical form as the norm, length, and canonical form of the ideal. We recall that an ideal is called “primitive” if it has no rational integer factor, and the following result gives us a way to determine when a submodule is a primitive ideal.

**Proposition 2.4 (Identification of ideals).** Let \( \alpha^3 = m \), for \( m \not\equiv \pm 1 \pmod{9} \) a square-
free integer, let \( K = \mathbb{Q}(\alpha) \), so \( \mathcal{O}_K = [1, \alpha, \alpha^2] \) is the ring of integers of \( K \). Let \( M = [a, b + c\alpha, d + e\alpha + f\alpha^2] \) be a submodule of \( \mathcal{O}_K \) in canonical form. Then \( M \) is a primitive ideal if and only if:

- \( f = 1 \)
- \( c|a \)
- \( c|b \)
- \( c|d - e^2 \)
- \( c|m - de \)
- \( ac|bce - c^2d - b^2 \)
- \( ac|mc^2 + b^2e - bcd \)
- \( ac|mc - bd + be^2 - cde \)
- \( ac|mc - mb + bde - cd^2 \)

**Proof.** Consider the augmented matrix:

\[
\begin{bmatrix}
a & b & d & mc & mf & me \\
c & e & a & b & d & mf \\
f & a & c & b & e & d
\end{bmatrix}
\]

In order for \( M \) to be an ideal, all of the columns on the right must be integer combinations of the columns on the left. As a first observation, we note that the coefficient \( f \) must divide every other coefficient. If \( f > 1 \), then it is a rational integer divisor of the submodule. Thus, if \( M \) is primitive, we must have that \( f = 1 \).

We rewrite our matrix accordingly:

\[
\begin{bmatrix}
a & b & d & mc & m & me \\
c & e & a & b & d & m \\
1 & a & c & b & e & d
\end{bmatrix}
\]

Reducing this augmented matrix, we obtain:
and it is thus clear that our list of divisibility conditions is both necessary and sufficient for the augmented matrix to have all integer solutions, i.e., for \( M \) to be an ideal. This completes the proof. \( \square \)

Using this result, we can fix \( m \), thus choosing a field, and write down all primitive ideals of a given norm \( N \). A computationally efficient way to do this is as follows: First, list pairs of positive integers \((a, c)\) satisfying the conditions \( ac = N \) and \( c | a \). For each choice of \((a, c)\), there are only finitely many triples \((b, d, e)\) satisfying the canonical form inequalities \((0 \leq b < a, 0 \leq d < a, 0 \leq e < c)\) and the condition \( c | b \). In this way, it is convenient to run through a sufficient set of quintuples \((a, b, c, d, e)\) for which we check divisibility conditions 3-8. This may be done by hand in simple cases, and with computer assistance as the numbers get larger.

In a similar fashion, we can list all primitive ideals of a given length \( L \). We set \( a = L \), and our list of possible \( c \)-values are simply positive factors of \( a \). It is then straightforward to run through possible values of \( b, d, e \) for each pair \((a, c)\) and check the remaining divisibility conditions. See the appendix to this thesis for an example of code in the Python language that executes this algorithm in addition to an algorithm for determining which ideals are “reduced”.

2.3. Reduced ideals

Next, we generalize the definition of a reduced ideal in a quadratic field ([10, p.19]) to fields of arbitrary degree. First, we introduce a term.

**Definition 2.5.** Let \( \beta \) be an algebraic number in a field \( K \), a finite extension of \( \mathbb{Q} \). Then we define the shadow of \( \beta \), \( \text{Sh}(\beta) = \text{Sh}_K(\beta) \), as the product of all of its algebraic conjugates for that field, excluding itself.
If $K$ is a quadratic extension of $\mathbb{Q}$ and $\beta$ is irrational, then $\text{Sh}(\beta)$ is simply the algebraic conjugate of $\beta$. If $K$ is a degree $n$ extension, and $\beta$ is rational, then $\text{Sh}(\beta) = \beta^{n-1}$. In any case, we have that $\text{Sh}(\beta) \cdot \beta = N(\beta)$, where $N(\beta)$ represents the usual norm of an algebraic number in a number field. This gives us that $\text{Sh}(\beta) \in K$, and if $\beta$ is an algebraic integer, then $\text{Sh}(\beta)$ is as well.

We give two formulas for the shadow of a number, when that number is given in terms of our known integral basis for certain pure cubic fields:

**Proposition 2.6.** Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = m$, for some square-free integer $m \not\equiv \pm 1 \pmod{9}$. Let $\beta = x + \alpha y + \alpha^2 z$ for rational $x, y, z$. Then:

\[
\text{Sh}(\beta) = (x^2 - m y z) + (m z^2 - x y)\alpha + (y^2 - x z)\alpha^2 \\
= (x - \alpha^2 z)^2 - \alpha(x - \alpha^2 z)(y - \alpha z) + \alpha^2(y - \alpha z)^2.
\]

Also, $\text{Sh}(\beta) \geq 0$ for all $\beta \in K$.

**Proof.** To obtain the first formula, first let $\omega$ equal a primitive cube root of unity. Then we have that the algebraic conjugates of $\alpha$ are $\omega \alpha$ and $\omega^2 \alpha$. Thus the algebraic conjugates of $\beta$ are $x + \omega \alpha y + \omega^2 \alpha^2 z$ and $x + \omega^2 \alpha y + \omega \alpha^2 z$. Mutiplying these expressions together and grouping terms according to their degree in $\alpha$, we obtain our first formula.

Observing the form of each term, we note that, considered as an equation in $\mathbb{R}^3$, our first formula vanishes along the line $x = \alpha y = \alpha^2 z$. We therefore rewrite it in terms of the displacements $x - \alpha^2 z$ and $y - \alpha z$, and we have the second formula. The equivalence is most easily checked by expanding both.

Finally, it is clear from the second formula that the function $\text{Sh}$ is a positive definite quadratic form in the variables $(x - \alpha^2 z)$ and $(y - \alpha z)$.

We are now ready to give a general definition of a reduced ideal.

**Definition 2.7.** Let $K$ be a degree $n$ extension of the rationals, let $I$ be a primitive ideal in its ring of integers, and let $L = \text{Len}(I)$. We define $I$ to be a reduced ideal if for all $\beta \in I$, 

\[
\text{Sh}(\beta) \geq 0
\]
the pair of inequalities $|\beta| < L$ and $\text{Sh}(\beta) < L^{n-1}$ together imply that $\beta = 0$.

In our case, with $K = \mathbb{Q}(\alpha), \alpha = \sqrt[3]{m}$, we have an explicit description of ideals, and we can say something about the canonical form of a reduced ideal. Let $I = [a, b + c\alpha, d + e\alpha + f\alpha^2]$ be in canonical form. Our first observation is that, since reduced ideals are primitive, we have the above results on primitive ideals.

To say more, we establish the following three results, inspired by Mollin’s Theorem 1.4.1 and corollaries from *Quadratics*.

**Theorem 2.8 (Identification of reduced ideals).** Let $I = [L, b + c\alpha, d + e\alpha + \alpha^2]$ be the canonical form of a primitive ideal in $K = \mathbb{Q}(\alpha)$, with $\alpha^3 = m$ for some square-free integer $m \not\equiv \pm 1 \pmod{9}$. Then $I$ is reduced if and only if for every integer pair $(y, z) \neq (0, 0)$ satisfying:

1. $0 \leq z < \frac{L}{\alpha^2}$
2. $\alpha z - \frac{2L}{\sqrt{3}\alpha} \leq y \leq \frac{L - \alpha^2 z + \sqrt{L^2 - 3L^2 z^2 - 3\alpha^4 z^2}}{2\alpha}$
3. $c | y - ez$,

we have the inequality:

$$\left| \frac{q - (yb + zd)}{L} \right| < \frac{p - (yb + zd)}{L},$$

where

$$p = p(y, z) = \max \left\{ -L - \alpha (y + \alpha z), \frac{1}{2} \left( \alpha (y + \alpha z) - \sqrt{4L^2 - 3\alpha^2 (y - \alpha z)^2} \right) \right\},$$

and

$$q = q(y, z) = \min \left\{ L - \alpha (y + \alpha z), \frac{1}{2} \left( \alpha (y + \alpha z) + \sqrt{4L^2 - 3\alpha^2 (y - \alpha z)^2} \right) \right\}.$$
PROOF. Let $\phi : O_K \to \mathbb{R}^3$ be the additive homomorphism defined by $1 \mapsto (1,0,0)$, $\alpha \mapsto (0,1,0)$ and $\alpha^2 \mapsto (0,0,1)$. This map is an isomorphism of the $\mathbb{Z}$-modules $O_K$ and $\mathbb{Z}^3$, the latter of which is embedded in $\mathbb{R}^3$.

Now, let $\beta \in I \subset O_K$. Our condition that $|\beta| < \text{Len}(I)$ transforms into the geometric condition that the point $\phi(\beta)$ lies strictly between two planes: $x + \alpha y + \alpha^2 z = \pm L$. Our second condition, that $|\text{Sh}(\beta)| < \text{Len}(I)^2$, transforms into the geometric condition that the point $\phi(\beta)$ lies inside the oblique elliptic cylinder given by $(x - \alpha^2 z)^2 - \alpha(x - \alpha^2 z)(y - \alpha z) + \alpha^2(y - \alpha z)^2 < L^2$.

These conditions define a region $R$, between two planes and inside an elliptic cylinder, which is bounded and symmetric about the origin; it contains the images of 0 and of at most finitely many other elements in the ideal $I$. The ideal is reduced if and only if $\phi(\beta) \notin R$ for every non-zero $\beta \in I$.

It is thus sufficient to write conditions establishing that $R$ is empty of images of non-zero ideal elements.

First, we can ignore the line $y = z = 0$, which contains images of rationals, because it intersects the boundaries of $R$ at $(\pm L, 0, 0)$, and there are no non-zero rationals between these two points.

Now, the entire region $R$ satisfies $|z| \leq \frac{L}{\sqrt[3]{2}}$, because this is the maximum $z$-coordinate of the intersection of our elliptic cylinder with either plane. Beyond that value, no point inside the elliptical cylinder is between the planes. By symmetry, and because images of ideal elements have integer coordinates, we need only consider integer values from $z = 0$ to $z = \left\lfloor \frac{L}{\alpha^2} \right\rfloor$.

For each integer $z$ in that range, we can bound possible $y$-values with the inequalities $\alpha z - \frac{2L}{\sqrt{3}\alpha} \leq y \leq \frac{L - \alpha^2 z + \sqrt{L^2 + 2\alpha^2 z - 3\alpha^2 z^2}}{2\alpha}$. These values are, respectively, the minimum $y$-value attained by a point on the elliptic cylinder, and the maximum $y$-value of a point of intersection of the cylinder and the planes. The other condition on $y$, that $y - e \equiv 0 \pmod{c}$, simply restricts our checking to $y$ values where we find images of numbers in the ideal $I$.

For each $y$-value that we check, we wish to verify that no image of a number in the
ideal lies in region $R$ along the line corresponding to our choices of $y$ and $z$. This can be expressed by saying that the first image to the left of the right edge of $R$ is also to the left of the left edge of $R$. This is expressed as the inequality 

$$\left\lfloor \frac{q-(yb+zd)}{L} \right\rfloor < \frac{p-(yb+zd)}{L},$$

where $p$ and $q$ are the $x$-coordinates of the left and right edges of $R$, respectively. This proves the theorem. \hfill \Box

Corollary 2.9 (Lower bound). If $L < \alpha$, then $I$ is reduced.

Proof. If $L < \alpha$, then in the above theorem, the only $z$-value satisfying inequality (1) is $z = 0$. The intersection of $R$ with the plane $z = 0$ has maximum/minimum $y$-values of $\pm \frac{L}{\alpha}$, so the only integer $y$-value in our region is $y = 0$. As noted in the proof of the theorem, no images of non-zero ideal elements are found in the interior of $R$ along the line $y = z = 0$. \hfill \Box

Theorem 2.10 (Upper bound). If $L > \frac{6\sqrt{3m}}{\pi}$, then $I$ is not reduced.

Proof. The region $R$ is convex and symmetric about the origin, and we claim its volume is equal to $\frac{4\pi L^3}{3m\sqrt{3}}$. Indeed, the perpendicular distance between the planes $x + \alpha y + \alpha^2 z = \pm L$ is $\frac{2L}{\sqrt{1+\alpha^2+\alpha^4}}$, and the area of the ellipse where each plane intersects the elliptic cylinder is $\frac{2\pi L^2 \sqrt{1+\alpha^2+\alpha^4}}{3m\sqrt{3}}$.

It now follows from Minkowski’s convex body theorem (see, e.g. page 306 in [1]) that if $I$ is reduced, then $N(I) \geq \frac{\pi L^3}{6\sqrt{3m}}$, or $\frac{1}{8}$ the volume of $R$. On the other hand, since $I$ is primitive if it is reduced, we also have from our canonical form that $N(I) = acf = Lc \leq L^2$. These two inequalities are incompatible for $L > \frac{6\sqrt{3m}}{\pi}$, so we have our result. \hfill \Box

Theorem 2.11. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 = m$, for a square-free integer $m \not\equiv \pm 1 \pmod{9}$. Then the ring $\mathcal{O}_K$ contains at least one, and only finitely many, reduced ideals.

Proof. The entire ring $\mathcal{O}_K$ is always a reduced ideal, so we have at least one. By the above theorem, the length of a reduced ideal is bounded, which means its norm is also bounded, by the square of the length. Since there are only finitely many ideals of a given norm, [1, p.313] we have this result as well. \hfill \Box
The above results (2.8 - 2.10) give us a way of efficiently computing a complete list of reduced ideals in the fields we have been studying. We check for them by examining ideals of each length less than the upper bound of Theorem 2.10. For each length, we produce a list of ideals, per the results following Proposition 2.4.

Considering each ideal, those with lengths less than $\alpha$ are necessarily reduced by Corollary 2.9. For those between $\alpha$ and the upper bound, we obtain a list of pairs $(y, z)$ satisfying inequalities (1), (2) and (3), for each pair, we calculate $p$ and $q$ and check our condition from Theorem 2.8. The Python code found in the appendix executes this algorithm.

The following definition affords a different characterization of reduced ideals which will prove useful.

**Definition 2.12.** Let $I$ be an ideal (or fractional ideal) in a number field. Then $\beta \in I$ is a *minimal element of $I$* if $|\gamma| < |\beta|$ and $|\text{Sh} (\gamma)| < |\text{Sh}(\beta)|$ for $\gamma \in I$ together imply that $\gamma = 0$.

Now we can characterize reduced ideals in terms of minimal elements.

**Theorem 2.13.** Let $I$ be an ideal in a number field. Then $I$ is reduced if and only if there is some rational $q \in I$ that is a minimal element of $I$.

The proof is immediate from the definition. In particular, if $I$ is reduced, then $q = \pm L(I)$ is a minimal element.
As seen in Mollin’s *Quadratics*, the terms in a quadratic number’s continued fraction expansion can be put in correspondence with a sequence of ideals, and the eventual periodicity of these sequences corresponds to the presence of finitely many reduced ideals in an equivalence class [10, p. 44]. We now develop a corresponding notion for a class of cubic numbers.

Throughout this section, let \( \alpha \) be the cubic irrational satisfying \( \alpha^3 = m \) for some square-free integer \( m \neq \pm 1 \pmod{9} \), and let \( K = \mathbb{Q}(\alpha) \). Let \( \phi \) be the additive homomorphism defined in the proof of Theorem 2.8.

Define the functions \( \text{Val}, \text{Sh} : \mathbb{R}^3 \to \mathbb{R} \) by the formulas \( \text{Val}(x,y,z) = x + \alpha y + \alpha^2 z \) and \( \text{Sh}(x,y,z) = (x - \alpha^2 z)^2 - \alpha(x - \alpha^2 z)(y - \alpha z) + \alpha^2(y - \alpha z)^2 \). Then we have \( \text{Val}(\phi(\beta)) = \beta \) and \( \text{Sh}(\phi(\beta)) = \text{Sh}(\beta) \). Next define the function \( \text{N}(x,y,z) = \text{Sh}(x,y,z)\text{Val}(x,y,z) \). If \( (x,y,z) \in \mathbb{Z}^3 \), then we have \( \text{N}(x,y,z) = \text{N}(\phi^{-1}(x,y,z)) \).

Taking \( a \) and \( b \) positive, define the region:

\[
R_{a,b} = \{(x,y,z) \in \mathbb{R}^3 : |\text{Val}(x,y,z)| < a, \text{Sh}(x,y,z) < b\}.
\]

This region is convex and symmetric about the origin. (In this notation, the region examined in Theorem 2.8 is \( R_{L,L^2} \).)

Let \( \beta_0 = 1 \), and \( P_0 = \phi(\beta_0) = (1,0,0) \). We begin with \( R_{a_0,b_0} = R_{1,1} \), a region with the point \( P_0 \) on its boundary, and with no non-zero lattice points in its interior. To find \( P_{k+1} \), let \( a_{k+1} \) be the maximum positive number such that \( R_{a_{k+1},b_k} \) has no lattice point in its interior. Such a number is guaranteed by Minkowski’s convex body theorem. We will actually encounter two lattice points at once, because of symmetry; take \( P_{k+1} \) to be the one for which the function Val is positive. We have \( a_{k+1} = \text{Val}(P_{k+1}) \); also set \( b_{k+1} = \text{Sh}(P_{k+1}) \), and let \( \beta_{k+1} = \phi^{-1}(P_{k+1}) \).
Definition 3.1. The sequence \((\beta_k)_{k \geq 0}\) is the minimal sequence associated with \(\alpha\), and \((N_k)_{k \geq 0} = (N(P_k))\) is the norm sequence associated with \(\alpha\).

We have computer code that calculates the minimal sequence and norm sequence of \(\alpha\) given an appropriate value for \(m\). This is included in an appendix.

We note that the minimal sequence of \(\alpha\) is precisely the sequence of minimal elements of \(\mathcal{O}_K\), starting with \(\beta_0 = 1\) and proceeding through minimal elements in order of increasing absolute value. The algorithm could be modified to run backwards, by holding cylinder heights constant and increasing their widths to find new points. This would give us the rest of the positive minimal elements, those with absolute values between 0 and 1. However, as we shall see, the sequence we have defined contains all the information we need. We first note some useful facts:

Proposition 3.2. If \(\beta\) is a minimal element in the ideal (or fractional ideal) \(I\), and \(\gamma\) is another field element, then \(\gamma\beta\) is a minimal element in the ideal (or fractional ideal) \((\gamma) \cdot I\).

Proof. This follows immediately because the functions \(\text{Sh} : K \to \mathbb{R}\) and \(|\cdot| : K \to \mathbb{R}\) are both multiplicative. \(\square\)

Remark 3.3 (Dirichlet’s Unit Theorem). The unit group of \(K\), a number field of degree 3 with one real embedding and one pair of complex embeddings (i.e., a cubic field with negative discriminant), is of the form \(U_K = \{ \pm \varepsilon_0^k | k \in \mathbb{Z}\}\), where \(\varepsilon_0 \in K\) is the fundamental unit of the number field, which satisfies \(\varepsilon_0 > 1\). (See, e.g., [1, p.346,p.362].)

Now we are ready to show that the norm sequence we have defined is indeed periodic.

Theorem 3.4. The norm sequence of \(\alpha\) is periodic, and the minimal sequence has the property that \(\beta_{h+l} = \varepsilon_0 \beta_h\), where \(l\) is the period of the norm sequence, and \(\varepsilon_0\) is the fundamental unit of the field \(K = \mathbb{Q}(\alpha)\).

We note that this theorem is essentially equivalent to Proposition 2.6 from [3].

Proof. Let \(\varepsilon_0\) be the fundamental unit of \(K\). Our first observation is that, if \(\beta\) is any
minimal element, then so is $\pm \varepsilon_0^k \beta$ for $k \in \mathbb{Z}$. So, the set of minimal elements is the set of all associates (unit multiples) of minimal elements on the interval $[1, \varepsilon_0)$. Let these elements be denoted $1 = \beta_0 < \cdots < \beta_{l-1}$. We know there are only finitely many, for a lattice can only intersect a compact region (the closure of $R_{\varepsilon_0,1}$) in finitely many points. Then the minimal sequence is of the form:

$$(1 = \beta_0, \ldots, \beta_{l-1}, \varepsilon_0, \ldots, \varepsilon_0 \beta_{l-1}, \varepsilon_0^2, \ldots).$$

This sequence has the property that $\beta_{h+l} = \varepsilon_0 \beta_h$, and taking norms, this gives us that $N_{h+l} = N_h$. Thus, we have periodicity. Furthermore, we know that $N_0 = 1 = N_l = N(\varepsilon_0)$, and since $\varepsilon_0$ is the fundamental unit, we know that $N_h > 1$ for any positive $h < l$. This gives us that the period of the norm sequence is precisely $l$. \hfill \Box

Now, let $\mathcal{M}$ be the set of elements in the minimal sequence of $\alpha$ on the interval $[1, \varepsilon_0)$, and let $\mathcal{R}$ be the set of reduced principal ideals in $K$. We construct functions $F : \mathcal{M} \to \mathcal{R}$ and $G : \mathcal{R} \to \mathcal{M}$, which we will show to be inverses. This will establish a bijection between our two sets.

First, let $\gamma$ be a minimal element of $\mathcal{O}_K$ satisfying $1 \leq \gamma < \varepsilon_0$, and let $J$ be the fractional ideal generated principally by $\gamma^{-1}$. Since $J = (\gamma^{-1}) \cdot \mathcal{O}_K$, then $1 = \gamma^{-1} \gamma$ is minimal in $J$. Let $L$ be the least integer such that $I = (L)J = (\frac{L}{\gamma})$ is an integral ideal, which we note is primitive. Now, $L = L \cdot 1$ is minimal in $I$. Since $L$ is rational, then $I$ is reduced, and we set $F(\gamma) = I$.

In the other direction, let $I$ be a reduced principal ideal. Then $I = (\eta)$ for some integer $\eta > 0$. Since $I$ is reduced, we have that $L = \text{Len}(I)$ is minimal in $(\eta)$. Then $\hat{\gamma} = L \eta^{-1}$, must be minimal in $(\eta^{-1})(\eta) = \mathcal{O}_K$. Let $k = -\lceil \log_{\varepsilon_0} \hat{\gamma} \rceil$, and let $\gamma = \varepsilon_0^k \eta$. Then $\gamma$ is a minimal element in $\mathcal{O}_K$ satisfying $1 \leq \gamma < \varepsilon_0$, so we set $G(I) = \gamma$.

Since the ideal $I$ could be written as a principal ideal in more than one way, we need to check that $G$ is well-defined. However, if $I = (\eta')$, then we know that $\eta' = \eta \varepsilon^m$ for some $m$. Thus, in the above argument, we obtain a $\hat{\gamma}'$ that is an associate of $\hat{\gamma}$, and therefore an associate of the same $\gamma$. So, $G$ is well-defined.
Theorem 3.5. The functions $F$ and $G$ defined above are inverses, providing a bijection between the sets $\mathcal{M}$ and $\mathcal{R}$.

We note that this result mirrors Proposition 4.3 from [3].

Proof. First, we calculate $F(G(I))$, where $I = (\eta)$ is a reduced principal ideal with length $L$. We have that $G(I) = \gamma$ where $\gamma$ is some associate of $\hat{\gamma} = \frac{L}{\eta}$. To apply $F$, we must choose the smallest integer $L'$ such that $(L'\gamma^{-1})$ in an integer ideal. We know that $I = (\eta) = (L\hat{\gamma}^{-1}) = (L\gamma^{-1})$ is an integer ideal, and furthermore, a primitive one because it is reduced. If $L' < L$, then $I$ would not be primitive, so we have $L' = L$, and

$$F(G(I)) = F(\gamma) = \left(\frac{L}{\gamma}\right) = \left(\frac{L}{\gamma}\right) = (\eta) = I,$$

as desired.

In the other direction, we consider $G(F(\gamma))$, where $\gamma$ is a minimal element in $\mathcal{O}_K$ satisfying $1 \leq \gamma < \varepsilon_0$. Let $L$ be the least positive integer such that $I = \left(\frac{L}{\gamma}\right)$ is an integer ideal. Then:

$$G(F(\gamma)) = G\left(\left(\frac{L}{\gamma}\right)\right) = \varepsilon_0^k \frac{\text{Len}(L/\gamma)}{L/\gamma} = \varepsilon_0^k \frac{L}{L/\gamma} = \varepsilon_0^k \gamma.$$

Since $\gamma$ is in the appropriate interval, we can choose $k=0$, and this completes our proof. \qed
The norm sequences we have defined can be defined analogously for quadratic irrationals of the form $\alpha = \sqrt{m}$ for some square-free $m$, by checking closest points to the vector $(\alpha, 1)$. Indeed, if we take closest points $(x, y)$, and form the quotients $\frac{x}{y}$, we obtain the convergents of the continued fraction of $\alpha$. If instead we take norms in the field $K = \mathbb{Q}(\alpha)$ of the algebraic integers $x + y\alpha$, we obtain a norm sequence, which can also be calculated directly from the terms in the continued fraction expansion.

Two easily obtainable results are the following: The norm sequence of the number $\alpha_k^+ = \sqrt{k^2 + 1}$ for an integer $k \geq 1$ is $(1)$. The norm sequence of the number $\alpha_k^- = \sqrt{k^2 - 1}$ for an integer $k \geq 2$ is $(1, 2(k-1))$. These results follow by calculation from the known results that the continued fraction expansion of $\alpha_k^+$ is $[k, 2k]$, and the continued fraction expansion of $\alpha_k^-$ is $[k-1, 1, 2(k-1)]$. These in turn follow by direct computation: just solve the quadratic equation implied by the periodic continued fraction.

We have corresponding results for norm sequences of cubic irrationals $\alpha_k^+ = \sqrt[3]{k^3 + 1}$ and $\alpha_k^- = \sqrt[3]{k^3 - 1}$, but we cannot use the same method of proof, because we do not have anything quite like the machinery of continued fractions with which to make our calculations. However, we can establish these results by examining minimal sequences directly. We therefore establish them with the restrictions that $m = \alpha^3$ is square-free and not congruent to $\pm 1 \pmod{9}$, because we have a precise description of minimal sequences in these cases.

We have no counterexamples in cases where these conditions are not satisfied, and proving these generalizations seems to be a natural extension of this work. Another natural extension would be identifying and proving similar propositions for other classes of cubic irrationals with simple norm sequences.

The following two theorems are the cubic results, and include what these results imply about reduced ideals in cubic fields.

**Theorem 4.1.** Let $k \geq 1$ be an natural number so that $m = k^3 + 1$ is square-free and not...
congruent to $\pm 1$ modulo 9, let $\alpha^3 = m$ and let $K = \mathbb{Q}(\alpha)$. Then:

- The fundamental unit of $K$ is $\varepsilon_0 = k^2 + k\alpha + \alpha^2$.
- The norm sequence associated with $\alpha$ is $(1, 1)$.
- The only reduced principal ideal in the ring of integers of $K$ is the entire ring, $(1)$. 

**Proof.** Let $\varepsilon_0 = k^2 + k\alpha + \alpha^2$, so $\phi(\varepsilon_0) = (k^2, k, 1)$. We need to show that there is no other $\beta \in K$ satisfying $\text{Sh} \beta < 1$ and $|\beta| < |\varepsilon_0|$. Indeed, this will prove that $\varepsilon_0$ is the fundamental unit.) Equivalently, we must show that, in the determination of the minimal sequence of $\alpha$, $(k^2, k, 1) = P_1$.

First, no point in $(x, y, z) \in \mathbb{Z}^3$ with $z > 1$ can be $P_1$, which can be seen as follows: Fix $z = z_0$; the pair $(x, y)$ that minimizes the function $\text{Val}(x, y, z_0)$ on the region inside the ellipse $\text{Sh}(x, y, z_0) = 1$ is $(\alpha^2z_0 - 1, \alpha z_0 - \frac{1}{\alpha})$. At this point, we have $\text{Val} = 3\alpha^2z_0 - 2$. This value is greater than $\varepsilon_0$ for any $k$ whenever $z_0 \geq 2$. Since the minimal sequence in arranged in order of absolute value, we can restrict our attention to $z \leq 1$.

The case $z = 0$ is not a problem; because no non-zero lattice points in this plane have $\text{Sh} < 1$. Examining the plane $z = 1$, it can be shown that the only point satisfying $\text{Sh} < 1$ is $\phi(\varepsilon_0)$.

It is now clear that the period of our norm sequence is 1, and it follows by Theorem 3.5 that there is only one reduced principal ideal, which must be $(1)$. □

**Theorem 4.2.** Let $k \geq 2$ be an natural number so that $m = k^3 - 1$ is square-free and not congruent to $\pm 1$ modulo 9. Let $\alpha^3 = m$ and let $K = \mathbb{Q}(\alpha)$. Then:

- The fundamental unit of $K$ is $\varepsilon_0 = k^2 + k\alpha + \alpha^2$.
- The norm sequence associated with $\alpha = \sqrt[3]{m}$ is $(1, 3k(k - 1))$.
- The ring of integers of $K$ has two reduced principal ideals, namely $[1, \alpha, \alpha^2]$, which is principally generated by 1, and $[3k(k - 1), 3k(k - 1)\alpha, (k - 1)^2 + (k - 1)\alpha + \alpha^2]$, which is principally generated by $(k - 1)^2 + (k - 1)\alpha + \alpha^2$.

**Proof.** This proof is identical to the above proof except for one detail. When we examine the plane $z = 1$ for images of minimal elements, we find two: $\phi(\gamma) = (k^2 - 1, k, 1)$ and
$\phi(\varepsilon_0) = (k^2, k, 1)$, where $\gamma$ is the unique minimal element of $\mathcal{O}_K$ satisfying $\text{Sh}(\gamma) < 1$ and $1 < \gamma < \varepsilon_0$. The rest follows by computation. □
APPLICATION TO DIOPHANTINE APPROXIMATION

We turn now to an application in Diophantine approximation. The image of our minimal sequence under \( \phi \) is a sequence of points with decreasing shadow size. Since shadow is measured by an elliptical cylinder with the vector \( \langle \alpha^2, \alpha, 1 \rangle \) as its axis, the minimal sequence gives us lattice points that are very close to that vector. Before pursuing this idea further, let us recall some facts about “badly approximable” numbers and vectors.

Quadratic numbers are known to be badly approximable, in a way that can be quantified by calculating a “Lagrange value”. In particular, \( \alpha \) is badly approximable, if there is some positive constant \( c_0 \), depending on \( \alpha \), such that for \( c < c_0 \), there are only finitely many pairs \( (x, y) \in \mathbb{Z} \times \mathbb{N}^+ \) satisfying

\[
\frac{|x - \alpha|}{|y|} < \frac{c}{y^2},
\]

whereas, for any \( c > c_0 \), there are infinitely many. (For numbers that are not badly approximable, this \( c_0 \) would equal 0.) The constant \( c_0 \) is called the Lagrange value of \( \alpha \). (See, e.g., [4]) We can give the following formula for \( c_0 \), using the notation \( \| \alpha \| \) for the distance between \( \alpha \) and the nearest integer:

\[
c_0 = \lim \inf_{y \in \mathbb{N}^+} |y| \| \alpha y \|.
\]

In two dimensions, we can say that a vector \( \langle \alpha, \beta \rangle \in \mathbb{R}^2 \) is badly approximable if there is a \( c_0 \) such that, for \( c < c_0 \), there are only finitely many triples \( (x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^+ \) such that

\[
\max \left\{ \frac{|x - \beta|}{z}, \frac{|y - \alpha|}{z} \right\} < \frac{c}{z^{3/2}},
\]

and infinitely many such triples for any \( c > c_0 \). We can write a formula as above, and make the following definition.
**Definition 5.1.** Let \( \langle \alpha, \beta \rangle \in \mathbb{R}^2 \) be a badly approximable vector. Then the positive number:

\[
c_0 = c_0(\alpha, \beta) = \lim \inf_{z \in \mathbb{N}^+} \sqrt{z} \max \left\{ \|z \beta\|, \|z \alpha\| \right\}
\]

is the *coefficient of approximation* for the vector \( \langle \alpha, \beta \rangle \).

As Perron showed in 1921, if \( \{1, \alpha, \beta\} \) is a \( \mathbb{Q} \)-basis for a field \( K \) that is a degree 3 extension of \( \mathbb{Q} \), then the vector \( \langle \alpha, \beta \rangle \) is badly approximable \([11]\). Take \( \alpha^3 = m \) for some square-free integer \( m \not\equiv \pm 1 \pmod{9} \). We now show a method of calculating the coefficient of approximation of the vector \( \langle \alpha, \alpha^2 \rangle \).

To examine rational approximations of \( \langle \alpha, \alpha^2 \rangle \), we look at integer points close to the 3-vector \( \langle \alpha^2, \alpha, 1 \rangle \). The minimal sequence of \( \alpha \), under the map \( \phi \), provides a sequence of integer points approximating that vector. In fact, it will be sufficient to work with the subsequence of the minimal sequence given by positive integral powers of the fundamental unit, \( \varepsilon_0 \).

**Proposition 5.2.** Let \( \varepsilon_0 \) be the fundamental unit of the field \( K = \mathbb{Q}(\alpha) \), with \( \alpha^3 = m \) for some square-free integer \( m \not\equiv \pm 1 \pmod{9} \). Let \( (x_k, y_k, z_k) = \phi(\varepsilon_0^k) \) Then we have:

\[
c_1 = \lim \inf_{k \to \infty} \sqrt{z_k} \max \left\{ |x_k - \alpha^2 z_k|, |y_k - \alpha z_k| \right\} = \frac{1}{\alpha \sqrt{3(1 + \alpha + \alpha^2)}}
\]

**Proof.** We note that the images \( \phi(\varepsilon_0^k) \) are successive images of \( (1, 0, 0) \) under the transformation \( T(x, y, z) = (x, y, z)A \), where \( A \) is a matrix with rows \( \phi(\varepsilon_0) \), \( \phi(\alpha \varepsilon_0) \) and \( \phi(\alpha^2 \varepsilon_0) \). This transformation has a real eigenvalue, \( \lambda_1 = \varepsilon_0 > 1 \), and its eigenspace \( V_1 \) is generated by \( \langle \alpha^2, \alpha, 1 \rangle \) which is the vector we are approximating. The other two eigenvalues are complex, and since the determinant equals 1, \( T \) acts on their invariant subspace \( V_2 \) (the plane \( x + \alpha y + \alpha^2 z = 0 \)) via contraction and rotation.

Since we are working with powers of a unit, the images \( (x_k, y_k, z_k) \) all lie on the surface

\[
N(x, y, z) = x^3 + my^3 + m^2z^3 - 3mxyz = 1.
\]
As $k \to \infty$, we have $z_k \to \infty$, because each point lies in the cylinder $\text{Sh}(x, y, z) < 1$, and successive powers of $\varepsilon_0$ lie on planes $\text{Val}(x, y, z) = c_k$ for $c_k = |\varepsilon^k| \to \infty$. Now, for each $k$, consider the cross-section of the surface $N(x, y, z) = 1$ by the plane $z = z_k$. This gives us a closed curve with the equation:

$$x^3 + my^3 + m^2z^3 - 3mxyz_k = 1$$

Now, set $\hat{x} = z_k(x - \alpha^2z_k)$ and $\hat{y} = z_k(y - \alpha z_k)$. With this change of variables, the above equation becomes:

$$3\alpha^2 (\hat{x}^2 - \alpha \hat{x}\hat{y} + \alpha^2 \hat{y}^2) = 1 - \frac{\hat{x}^3 + m\hat{y}^3}{z_k^{3/2}}$$

Applying these transformations for each $k$, we see that, as $k \to \infty$ the term $\frac{\hat{x}^3 + m\hat{y}^3}{z_k^{3/2}} \to 0$, because both $\hat{x}$ and $\hat{y}$ remain bounded. This can be shown by examining the action of the linear transformation $T$ on the subspace where only the complex eigenvalues act. The distance between the points in our sequence and the subspace $V_1$ decreases in such a way that multiplication by $\sqrt{z}$ still results in $\hat{x}$ and $\hat{y}$ being bounded.

Thus, we conclude that the translated cross-sections converge to the ellipse:

$$\hat{x}^2 - \alpha \hat{x}\hat{y} + \alpha^2 \hat{y}^2 = \frac{1}{3\alpha^2}.$$ 

Now, when we apply the same change of variables to our formula for $c_1$, we obtain:

$$c_1 = \lim \inf_{k \to \infty} \max \{|\hat{x}_k|, |\hat{y}_k|\},$$

where $\hat{x}_k$ and $\hat{y}_k$ are the images of $x_k$ and $y_k$ under the appropriate change of variables.

Next, we note that the powers of $\varepsilon^k$ project onto a dense set on the limiting ellipse. This comes again from examining the linear map $T$. As we noted above, its action on the 2-dimensional eigenspace is a contraction and a rotation. We claim that the rotation is not periodic, i.e., no number of iterations of it equal a whole number of rotations. Indeed, they cannot, because then multiplication by that power of $\varepsilon_0$ would correspond to a linear
map with three real eigenvalues, so it would be an element of a cubic field with positive
discriminant, a contradiction. We can thus conclude that the points in our sequence will be
densely distributed if projected radially onto the limiting ellipse.

By a straightforward calculation, the minimum of \( \max\{x, y\} \) for \((x, y)\) on our limiting
ellipse equals \( \frac{1}{\alpha \sqrt{3(1+\alpha+\alpha^2)}} \).

Assembling these facts, we have that the infimum of the set \( \max\{\hat{x}_k, \hat{y}_k\} \) is, because
of density and convergence, the minimum of \( \max\{x, y\} \) on the limiting ellipse, as needed. \(\square\)

The number we have just calculated is an upper bound for \(c_0(\alpha, \alpha^2)\); we now show
that they are equal.

**Theorem 5.3.** With the same notation as above,

\[
c_0(\alpha, \alpha^2) = c_1 \left( \frac{1}{\alpha \sqrt{3(1+\alpha+\alpha^2)}} \right)
\]

**Proof.** It is clear that \(c_0 \leq c_1\); we wish to show that they are in fact equal. Consider an
arbitrary non-zero point \((x_0, y_0, z_0) \in \mathbb{Z}^3\). It lies on some surface \(N(x, y, z) = n\) where \(n\) is a
non-zero integer. (Without loss of generality, we can take \(n > 0\) by replacing \((x, y, z)\) with
\((-x, -y, -z)\) if necessary.) As above, images of this point, under repeated multiplication by
\(\varepsilon_0\), all lie on the surface \(N = n\). They can be translated by the same coordinate change in
the above theorem, and their images will converge to the ellipse:

\[
\hat{x}^2 - \alpha \hat{x} \hat{y} + \alpha^2 \hat{y}^2 = \frac{n}{3\alpha^2}.
\]

The minimum value attained by \(\max\{x, y\}\) on this ellipse is the number \(\frac{n}{\alpha \sqrt{3(1+\alpha+\alpha^2)}}\),
which cannot be less than \(c_1\). This gives us \(c_0 \geq c_1\), and so \(c_0 = c_1\), as claimed.

\(\square\)

As a comparison, we note the Lagrange values for numbers of the form \(\sqrt{m}\), as
computed from continued fraction expansions. If \(\alpha^2 = m\) where \(m\) is a non-square integer,
then the Lagrange value of \(\alpha\), using our definition from above can be computed to be \(c_0(\alpha) = \frac{1}{2\alpha}\).
APPENDIX A

Sequence Interleaving Algorithm
We wish to define a map from \((\mathbb{N}^\mathbb{N})^\mathbb{N}\) to \(\mathbb{N}^\mathbb{N}\) with the following property. Given an input which is a sequence of sequences of natural numbers, we want our output to be a sequence of natural numbers that is eventually periodic if and only if at least one of the sequences of natural numbers in the input is eventually periodic. Thus, suppose we have a sequence of sequences of natural numbers, and let \(a_{i,j}\) denote the \(j\)-th term in the \(i\)-th sequence: \(((a_{i,j})_{j \geq 1})_{i \geq 1} \in (\mathbb{N}^\mathbb{N})^\mathbb{N}\). We proceed to describe an algorithm for generating an output sequence \((b_n)_{n \geq 1} \in \mathbb{N}^\mathbb{N}\).

First, we define some terms.

**Definition A.1.** Let \(A = (a_1, \ldots, a_n)\) be an \(n\)-tuple. Suppose there is some \(k < n\) such that the relation \(a_{i+k} = a_i\) for \(i = 1, \ldots, n-k\), is satisfied. Suppose in addition that this \(k\) is minimal, i.e., that \(h < k\) implies that \(a_i \neq a_{i+h}\) for some \(i = 1, \ldots, n - h\). Then we say that \(A\) is **finite-periodic with period** \(k\), or simply **finite-periodic.** In this case, we call \((a_1, \ldots, a_k)\) the **finite-fundamental string** of \(A\).

We construct our output sequence by concatenating tuples, or blocks of terms, taken from the input sequences. We denote the blocks \(B_l\) for \(l \geq 1\), and the length of block \(B_l\) is \(2^l\). Blocks are taken from input sequences, in a diagonal fashion, checking for periodicity at each step.

Define the sequence \((i_k)_{k \geq 1} = (1, 2, 1, 2, 3, 1, 2, 3, 4, 1, 2, 3, 4, 5, \ldots)\) as our sequence of indices for the purpose of diagonalization. (Note, we can give a formula for \(i_k\) in terms of triangular numbers: Let \(T_n = \frac{n(n+1)}{2}\) be the \(n\)-th triangular number. Then, for \(T_n \leq k < T_{n+1}\), we have \(i_k = k - T_n + 1\).)

1. Begin with \(k = l = 1\); the variable \(k\) tracks our place in the indexing sequence \((i_k)\), while \(l\) is the numbering for blocks. Define a Boolean variable \(P\) to indicate whether we have detected finite-periodicity that may persist, and begin with \(P = \text{false}\).
2. Create block \(B_l\) by removing \(2^l\) terms from the beginning of the sequence \((a_{i_k,j})_j\).

We say “removing” to emphasize that any terms used as part of block \(B_l\) will not be available for any subsequent block \(B_{l+h}\). Each block taken from a sequence begins
with the first unused term.

(3) Check the value of \( P \):

(a) If \( P = \text{false} \), check whether the block \( B_l \) is finite-periodic. If so, then set \( P = \text{true} \), let \( S \) be the finite-fundamental string of \( B_l \), and proceed to step 4. If \( B_l \) is not finite-periodic, then increment \( k \) by 1 and proceed to step 4.

(b) If \( P = \text{true} \), then we need to check whether some previously detected finite-periodicity has persisted. In this case, we have a string \( S \), which is the finite-fundamental string of some concatenation of blocks \( B_h + \cdots + B_{l-1} \), with \( h < l \). We now check whether the concatenation \( B_h + \cdots + B_l \) is finite-periodic with finite-fundamental string \( S \). If it is, proceed to step 4. If it is not, set \( P = \text{false} \), increment \( k \) by 1, and proceed to step 4.

(4) Increment \( l \) by 1 and return to step 2.

Concatenating all of the blocks \( B_1 + \cdots \), we obtain a sequence of natural numbers; this is our output sequence \((b_n)\).

**Definition A.2.** The process described above, viewed as a map \( T : (\mathbb{N}^\mathbb{N})^\mathbb{N} \to \mathbb{N}^\mathbb{N} \) is called the **sequence interleaving algorithm**.

**Theorem A.3.** Given a countable family of sequences of natural numbers as input, the output of the sequence interleaving algorithm is an eventually periodic sequence if and only if some sequence in the input family is eventually periodic.

**Proof.** Indeed, suppose that \((b_n) = T(((a_{i,j}))_j)_i\) is eventually periodic, with period \( m \), fundamental string \( S \), and a pre-period of length \( r \). Choose \( l_0 \) minimal so that \( \sum_{d=1}^{l_0-1} 2^d > r \) and \( 2^{l_0} > m \). Now, in considering what happens when we reach block \( B_{l_0} \), we must consider two cases:

Suppose we have, after finishing with block \( B_{l_0-1} \), either \( P = \text{false} \) or \( P = \text{true} \) and finite-fundamental string \( S \) (or some cyclic permutation of \( S \)). In either instance, after examining block \( B_{l_0} \) in step 3 of the algorithm, we will have \( P = \text{true} \), with finite-fundamental string \( S \) (or the same cyclic permutation), and \( P \) will remain in this state because the peri-
odicity is not broken in subsequent blocks. Therefore, \( k \) will not increment again, and the rest of \( (b_n) \) will be a tail of whichever input sequence was the source of block \( B_l \). Thus, that input sequence is eventually periodic.

As a second case, suppose that the algorithm finishes with block \( B_{l_0-1} \) with \( P = \text{true} \) and finite-fundamental string \( S' \) that is different from any cyclic permutation of \( S \). In this case, we will finish block \( B_l \) with \( P = \text{false} \), and it will be in block \( B_{l_0+1} \) that we finally get \( P = \text{true} \) with finite-fundamental string \( S \), just as in the above case. In that case, whatever input sequence is the source of terms for block \( B_{l_0+1} \) is eventually periodic.

Conversely, suppose \( (b_n) \) is not eventually periodic, and suppose by way of contradiction that some input sequence \( (a_{i_0,j})_j \) is eventually periodic. Since the indicator \( P \) can only remain in a true state while the same string continues to repeat, the lack of eventual periodicity in \( (b_n) \) implies that \( P \) is in a false state infinitely often. Therefore, \( k \) is incremented infinitely often, and \( i_k = i_0 \) infinitely often, paired each time with values of \( l \) that increase without bound.

Now, if \( (a_{i_0,j})_j \) is eventually periodic, it has some pre-period length and some period. Eventually, \( i_k \) will equal \( i_0 \) often enough that the corresponding blocks use up the pre-period. Eventually after that, \( i_k \) will return to \( i_0 \) enough times that \( l \) will grow until \( 2^l \) is greater than the period of \( (a_{i_0,j})_j \). When these conditions are met, there is no way for the algorithm to leave the sequence \( (a_{i_0,j})_j \), and \( P \) will remain true, a contradiction.

In the second part of the proof, a proof by contrapositive might seem more direct, but such an approach is complicated by the fact that more than one input sequence may be periodic, so we need the assumption that \( (b_n) \) is not periodic to ensure sufficient returns to the putative periodic input.

We note that, in the case where some sequence in the input family is periodic, exactly one periodic input sequence appears, in its entirety, in the output sequence, and can be recovered by analysis of the output sequence. In the case where no input sequence is periodic, all of the input sequences appear in their entireties in the output sequence, and can be reconstructed from it.
APPENDIX B

Proof of lemma on \( \mathbb{Z} \)-modules
The following is a proof of Lemma 2.2:

**Theorem 2.2.** Let \( M = \langle u_1, u_2, u_3 \rangle \) be a free \( \mathbb{Z} \)-module of rank 3. Let \( M' \subseteq M \) be a submodule of full rank. Then we can write \( M' = \langle au_1, bu_1 + cu_2, du_1 + eu_2 + fu_3 \rangle \), with all coefficients integral. Furthermore, we can suppose without loss of generality that \( a, c, f \) are strictly positive, that \( 0 \leq e < c \) and that \( 0 \leq b, d < a \). Subject to these conditions, all six coefficients are uniquely determined.

**Proof.** Let \( M = \langle u_1, u_2, u_3 \rangle \), and let \( M' \subseteq M \) have full rank. The sets

\[
I_1 = \{ k \in \mathbb{Z} \mid ku_1 \in M' \} \\
I_2 = \{ k \in \mathbb{Z} \mid ku_2 \in M' + u_1\mathbb{Z} \} \\
I_3 = \{ k \in \mathbb{Z} \mid ku_3 \in M' + u_1\mathbb{Z} + u_2\mathbb{Z} \}
\]

are all non-zero ideals of \( \mathbb{Z} \), so put \( I_1 = (a), I_2 = (c), \) and \( I_3 = (f) \).

By the definition of \( I_1 \), we have \( w_1 = au_1 \in M' \). By the definition of \( I_2 \), we have some \( \hat{b} \in \mathbb{Z} \) such that \( \hat{w}_2 = \hat{b}u_1 + cu_2 \in M' \). Similarly, considering \( I_3 \), we have integers \( \hat{d} \) and \( \hat{e} \) so that \( \hat{w}_3 = \hat{d}u_1 + \hat{e}u_2 + fu_3 \in M' \).

Using the division algorithm, we can write \( \hat{e} = q_1c + e \), with \( 0 \leq e < c \). Similarly, we can write \( \hat{b} = q_2a + b \) with \( 0 \leq b < a \), and \( \hat{d} - q_1 \hat{b} = q_3a + d \) with \( 0 \leq d < a \). We thus obtain \( w_2 = \hat{w}_2 - q_2w_1 = bu_1 + cu_2 \) and \( w_3 = \hat{w}_3 - q_1\hat{w}_2 - q_3w_1 = du_1 + eu_2 + fu_3 \), both in \( M' \).

It is clear that \( N = \langle w_1, w_2, w_3 \rangle \subseteq M' \). For the reverse inclusion, take an element \( m \in M' \), and write \( m = k_1u_1 + k_2u_2 + k_3u_3 \) in terms of our original integral basis. Now, \( k_3 \in I_3 \), so \( k_3 = t_3f \). Subtracting \( m - t_3w_3 \), we obtain \( (k_1 - t_3d)u_1 + (k_2 - t_3e)u_2 \), another element of \( M' \). This puts \( k_2 - t_3e \in I_2 \), so \( k_2 - t_3e = t_2c \).

Finally, we subtract again, and obtain \( m - t_3w_3 - t_2w_2 = (k_1 - t_3d - t_2b)u_1 \), another element of \( M' \). This puts \( k_1 - t_3d - t_2b \in I_1 \); call it \( t_1a \). Thus, we have

\[
m = t_1w_1 + t_2w_2 + t_3w_3 \in N,
\]
as desired.

To see that the expression is unique subject to our constraints, suppose that $M'$ is also given by $M' = [w'_1, w'_2, w'_3]$, with $w'_1 = a'u_1$, $w'_2 = b'u_1 + c'u_2$, and $w'_3 = d'u_1 + e'u_2 + f'u_3$, and that the positivity and bounding constraints are satisfied by these coefficients. Examining the differences $w_i - w'_i \in M'$, we see that all six must match, proving uniqueness.

□
APPENDIX C

Python code for reduced ideals
The following Python code executes the algorithms described in Section 2 for finding all the ideals, and all the reduced ideals, in a given pure cubic field or range of fields. It only does computations in fields of the form $K = \mathbb{Q}(\alpha)$ where $\alpha^3 = m$ for some square-free rational integer $m \not\equiv 1 \pmod{9}$.

```python
import math

def isIdeal(a, b, c, d, e, m):
    N = a * c
    ideal = 1
    if (d - e ** 2) % c != 0:
        ideal = 0
    else:
        if (m - d * e) % c != 0:
            ideal = 0
        else:
            if (b * c * e - c * d - b * e ** 2) % (N) != 0:
                ideal = 0
            else:
                if (m * c * e - c * d * e) % (N) != 0:
                    ideal = 0
                else:
                    if (m * c * e - m * b + b * d * e - c * d * e ** 2) % (N) != 0:
                        ideal = 0
    return ideal
```

36
```python
def isReduced(a, b, c, d, e, m):
    alpha = math.exp(math.log(m) / 3)
    reduced = 1
    if a > alpha:
        upperZ = a / alpha**2
        z = 0
        while (z < upperZ) * (reduced == 1):
            upperY2 = math.floor((a - alpha**2 * z + math.sqrt(a**2 + 2 * a * alpha**2 * z - 3 * alpha**4 + 4 * z**2)) / (2 * alpha))
            y = math.ceil(alpha * z - 2 * a / (math.sqrt(3) * alpha))
            yStepSize = 1
            while (y <= upperY2) * (reduced == 1):
                if (y - e * z) % c == 0:
                    yStepSize = c
                    p = max(-a - (alpha**2 * z + alpha * y), (alpha**2 * z + alpha * y - math.sqrt(4 * a**2 - 3 * (alpha**2 * z + alpha * y)**2)) / 2)
                    q = min(a - (alpha**2 * z + alpha * y), (alpha**2 * z + alpha * y + math.sqrt(4 * a**2 - 3 * (alpha**2 * z + alpha * y)**2)) / 2)
                    if (math.floor((q - (y * b + z * d)) / a) > (p - (y * b + z * d)) / a) * (y**2 + z**2 > 0):
                        reduced = 0
                        y = y + yStepSize
                        z = z + 1
                y = y + yStepSize
                z = z + 1
            reduced = 0
    return reduced
```
def isSquarefree(n):
    squarefree=1
    k=2
    while (k<=math.sqrt(n))*(squarefree==1):
        if n%k**2==0:
            squarefree=0
        k=k+1
    return squarefree

m=int(input('Starting m: '))
maxM=int(input('Maximum for m: '))
while m<=maxM:
    if (isSquarefree(m)==1)*((m**2-1)%9!=0):
        alpha=math.exp(math.log(m)/3)
        print("m=",m)
    N=1
    upperL=6*math.sqrt(3)*m/math.pi
    print("Upper bound on Length =",upperL)
    reducedIdealCount=0
    a=1
    while a<upperL:
        c=1
        while c<=a:
            if a%c==0:
                b=0
                while b<a:
d=0
while d<a:
    e=0
    while e<c:
        id=isIdeal(a, b, c, d, e, m)
        if id==1:
            red=isReduced(a, b, c, d, e, m)
            if red==1:
                print("Reduced ideal I=",(int(a),b,c,d,e)," norm =",int(a)*c," N(gamma)=",int(a**2/c))
                reducedIdealCount=
                reducedIdealCount+1
                e=e+1
        d=d+1
        b=b+c
        c=c+1
    a=a+1
print("Total reduced ideals:",reducedIdealCount)
print("------------------------------------------------------------------")
print
m=m+1
APPENDIX D

Python code for minimal sequences
The following Python code generates the norm sequence of \((\alpha, \alpha^3)\), given an appropriate value for \(m = \alpha^3\) and a maximum \(z\)-value for searching.

```python
import math

def Value(x, y, z):
    Val = x + alpha * y + alpha ** 2 * z
    return Val

def Shadow(x, y, z):
    Sh = (x - alpha ** 2 * z) ** 2 - alpha * (x - alpha ** 2 * z) * (y - alpha * z) + alpha ** 2 * (y - alpha * z) ** 2
    return Sh

def Norm(x, y, z):
    N = x ** 3 + m * y ** 3 + m * 2 * z ** 3 - 3 * m * x * y * z
    return N

m = int(input('m: '))
maxZ = int(input('maximum z-value: '))
alpha = math.exp(math.log(m) / 3)
a = 1
b = 0
c = 0
bestList = [[1, 0, 0]]
Val = 1
Sh = 1
N = Val * Sh
```

41
print(bestList[0],"",Val="",Val,"",Sh="",Sh,"",N="",N)
c=c+1

while c<maxZ:
    currentBest=[]
    x0=math.floor(alpha**2*c)
    y0=math.floor(alpha*c)
    if Shadow(x0,y0,c)<Sh:
        currentBest.append([x0,y0,c])
    if Shadow(x0,y0+1,c)<Sh:
        currentBest.append([x0,y0+1,c])
    if Shadow(x0+1,y0,c)<Sh:
        currentBest.append([x0+1,y0,c])
    if Shadow(x0+1,y0+1,c)<Sh:
        currentBest.append([x0+1,y0+1,c])

    currentBest.sort(key=lambda x: Value(x[0],x[1],x[2]))

    while len(currentBest)>0:
        if Shadow(currentBest[0][0],currentBest[0][1],currentBest[0][2])<Sh:
            newBest=currentBest.pop(0)
            Val=Value(newBest[0],newBest[1],newBest[2])
            Sh=Shadow(newBest[0],newBest[1],newBest[2])
            N=Norm(newBest[0],newBest[1],newBest[2])
            print(newBest,"",Val="",Val,"",Sh="",Sh,"",N="",N)
            bestList.append(newBest)
        else:
            currentBest.remove(currentBest[0])

        c=c+1


