2018-07-01

Euclidean Domains

Vandy Jade Tombs
Brigham Young University

Euclidean Domains

Vandy Jade Tombs

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Pace Peterson Nielsen, Chair
David Alan Cardon
Darrin M. Doud

Department of Mathematics

Brigham Young University

ABSTRACT

Euclidean Domains

Vandy Jade Tombs
Department of Mathematics, BYU
Master of Science

In the usual definition of a Euclidean domain, a ring has a norm function whose codomain is the positive integers. It was noticed by Motzkin in 1949 that the codomain could be replaced by any well-ordered set. This motivated the study of transfinite Euclidean domains in which the codomain of the norm function is replaced by the class of ordinals. We prove that there exists a (transfinitely valued) Euclidean Domain with Euclidean order type for every indecomposable ordinal. Modifying the construction, we prove that there exists a Euclidean Domain with no multiplicative norm.

Following a definition of Clark and Murty, we define a set of admissible primes. We develop an algorithm that can be used to find sets of admissible primes in the ring of integers of $\mathbb{Q}(\sqrt{d})$ and provide some examples.

Keywords: k-stage Euclidean domain, indecomposable ordinal, multiplicative norm, (transfinitely valued) Euclidean domain, admissible primes

Acknowledgments

I would like to thank my advisor, Pace Nielsen, for his guidance, encouragement, and direction in every part of this project. A special thanks to Darrin Doud for having answers to my many questions and to David Cardon for all his help in Algebraic Number Theory. I would also like to thank my husband for his love and support.

Contents

Chapter 1. Introduction and History

1.1 Introduction

One might recall the following definition of Euclidean domains from an introductory abstract algebra class.

Definition 1.1.1. An integral domain R is a *Euclidean domain* if there exists a function, called a *Euclidean norm*, $\varphi : R \to \mathbb{Z}_{\geq 0}$ such that for all non-zero $n, d \in R$ either $d \mid n$ or there exists some $q \in R$ satisfying $\varphi(n - qd) < \varphi(d)$.

Generalizing this definition, Motzkin in [9], noted that the codomain of the Euclidean norm need not be restricted to the natural numbers, but instead could be any well-ordered set, which led to the following definition.

Definition 1.1.2. Let W be a well-ordered set. A *transfinitely valued Euclidean domain* is an integral domain R where there exists a function $\varphi : R \to W$, such that for all $n, d \in R - \{0\}$, there exists some $q \in R$ satisfying either $\varphi(n - qd) < \varphi(d)$ or $n - qd = 0$. As before, we say that φ is a *Euclidean norm* on R.

Throughout, we will consider W to be some fixed ordinal and thus all Euclidean norms are assumed to have codomain in Ord, the class of all ordinals. See Section 1.2 for review of ordinal numbers. We will refer to transfinitely valued Euclidean domains as Euclidean domains. If we restrict to the finitely valued case, we will emphasize this fact.

The definition for transfinitely valued Euclidean domains does not differ much from the definition for finitely valued ones, and it might not be readily apparent why we want to consider these more general norms. However, there are many reasons that this concept is useful. First, we note that the class of transfinitely valued Euclidean domains is strictly larger than class of finite Euclidean domains. To see this we first define the *Euclidean order* *type* of a Euclidean domain R to be

$$\min\{\alpha \in \mathrm{Ord} : \varphi(R \setminus \{0\}) \subseteq \alpha\}$$

where φ ranges among all possible Euclidean norms on R. Finite Euclidean domains have two possible order types: $\omega^0 = 1$ when R is a field and $\omega^1 = \omega$ when R is a non-field. Hiblot in [5] and Nargata in [10] independently found examples of Euclidean domains with Euclidean order type of ω^2. In Section 2.2, we completely classify all possible Euclidean order types (this work also appears in [3]).

Another reason it is useful to consider transfinitely valued Euclidean domains is that this definition shares many of the same properties as finitely valued ones. Recall that a ring R is a *principal ideal domain* (PID) if every ideal is generated by a single element (such an ideal is called *principal*). It is well known that finitely valued Euclidean domains are PID's, but it is also true of transfinitely valued Euclidean domains.

Proposition 1.1.3. *Euclidean domains are PIDs.*

Proof. We will show that every ideal is principal. Consider an ideal I in a Euclidean domain R. If $I = (0)$ then we are done. So let I be non-zero, and choose $d \in I$ to be some non-zero element of minimal norm. Clearly $(d) \subseteq I$, so we need only show the reverse containment. Let $a \in I$ and write $a = qd + r$ with $r = 0$ or $\varphi(r) < \varphi(d)$, then $r = a - qd \in I$. By the minimality condition of d, we have $r = 0$, hence $a = qd \in (d)$. Thus $I = (d)$. $\square$

Another similarity between transfinitely valued Euclidean domains and finite ones is that the division algorithm terminates in finite time.

There are other generalizations of Euclidean domains. For example, one may generalize the division algorithm in the following way. Suppose for all $a, b \in R$, either $b \mid a$, or there exists a q_1 such that $a = q_1 b + r_1$ with $\varphi(r_1) < \varphi(b)$, or there exists $q_1, q_2 \in R$ such that

$$a = q_1 b + r_1, \quad b = q_2 r_1 + r_2.$$

and $\varphi(r_2) < \varphi(b)$. Then we can still carry out a division algorithm on pairs (a, b) since, after finite number of steps, we can produce a remainder with smaller norm. We call rings satisfying this condition 2-*stage Euclidean.* To generalize this further, we loosely follow definitions in [4].

Definition 1.1.4. Let R be an integral domain.

(1) For $a, b \in R$, and $k \in \mathbb{Z}_{\geq 1}$, a *k-stage division chain* starting from the pair (a, b) is a sequence of equations in R

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k. \end{aligned}$$

Such a division chain is said to be *terminating* if the last remainder r_k is 0.

(2) If there is a function $N : R \to \mathrm{Ord}$ (we call N a norm) and for every pair (a, b) with there exists a k-stage division chain starting from (a, b) for some $1 \leq k \leq n$ such that the last remainder r_k is either 0 or satisfies $N(r_k) < N(b)$ then R is said to be *n-stage Euclidean* with respect to N.

We say R is *ω-stage* or *quasi-Euclidean* if for every pair (a, b) there is a terminating k-stage division chain for some $k \in Z_{\geq 1}$.

Unlike Euclidean domains, k-stage Euclidean domains are not necessarily PIDs.

Example 1.1.5. Consider the ring of algebraic integers, denoted by R. We will show that R is 2-stage Euclidean but not a PID. To do this, we will follow the proof of Vaserstein in [12] to show that given any two relatively prime algebraic integers a and b, there exists an algebraic integer q such that $a - qb$ is a unit.

First note that if $b = 0$ then letting $q = 0$, we have $R(a + qb) = Ra = Ra + Rb = R$. Otherwise, we can find a natural number n such that $(-a)^n \in 1 + Rb$. Such an n must exist since the multiplicative group R/Rb is torsion and $a \notin Rb$. Thus there must exist an $r \in R$ such that

$$br = (-a)^n - 1.$$

Since $Ra^{n-1} + Rb^{n-1} = R$, we can find $c, d \in R$ such that

$$-r = c(-a)^{n-1} + db^{n-1}.$$

Choose $q \in R$ satisfying the monic polynomial $x^n + cx^{n-1} + d = 0$. Then $(a + qb - a)^n + bc(a + qb - a)^{n-1} + db^n = 0$. This implies

$$(-a)^n + bc(-a)^{n-1} + db^n = -\sum_{k=1}^{n} \binom{n}{k} (bq + a)^k (-a)^{n-k} - \sum_{k=1}^{n-1} \binom{n-1}{k} (bq + a)^k (-a)^{n-1-k}$$

Thus

$$\begin{aligned} 1 &= 1 + b(r + (-a)^{n-1}c + b^{n-1}d) \\ &= 1 + br + bc(-a)^{n-1} + b^n d \\ &= 1 + (-a)^n - 1 + bc(-a)^{n-1} + b^n d \\ &= (-a)^n + bc(-a)^{n-1} + b^n d \in R(a + qb). \end{aligned}$$

Hence the set of algebraic integers is 2-stage Euclidean.

To see that R is not a PID, consider the ideal $I = (2^{1/n} : n \in \mathbb{N})$.

However, using an argument similar to that in 1.1.3, we see that any finitely generated ideal in a k-stage Euclidean ring is principal. A ring which satisfies every finitely generated ideal is principal are called *Bezout domains*.

Recall that a *unique factorization domain* (UFD) is an integral domain such that every element factors uniquely into a product of irreducibles up to associates and order. It is well-known that Euclidean domains are UFDs and the typical proof only uses the following facts,

- every element factors into indecomposables, and
- for any pair (a, b) with $b \neq 0$ there is a terminating division chain.

Using these two facts, we have proved the following proposition.

Proposition 1.1.6. *Let R be a ω-stage Euclidean domain such that every element of R factors into indecomposables. Then R is a UFD.*

Corollary 1.1.7. *Let R be a k-stage Euclidean domain for some $k \in \mathbb{Z}_{\geq 1}$ such that every element of R factors into indecomposables. Then R is a UFD.*

The k-stage Euclidean domains are related to a notion introduced by Cohn (see [2]). Recall an elementary matrix with coefficients in an integral domain R is a square matrix of one of three types:

- a diagonal matrix with entries that are units in R,
- a matrix with differs from the identity matrix by the presence of a single nonzero element off the diagonal, or
- a permutation matrix.

Note that elementary matrices are invertible. Also recall that $GL_n(R)$ is the set of $n \times n$ invertible matrices with coefficients in R, meaning those matrices whose determinants are units in R.

Cohn in [2] gave the following definition.

Definition 1.1.8. A domain R is called GE_n if $GL_n(R)$ is generated by $n \times n$ elementary matrices.

The following proposition was noticed and proved by Cooke in [4].

Proposition 1.1.9. *An ω-stage Euclidean domain in GE_n for every n.*

Proof. We work by induction on n. First, we note that every domain is GE_1. Now suppose that R is ω-stage Euclidean and GE_{n-1}. In order to show that R is GE_n, we just need to show that every invertible $n \times n$ matrix is reducible to the identity by elementary row operations. Let $M \in GL_n(R)$. Then the $\det(M)$ is a unit of R. Expanding the determinant down the first column shows that the entries in the first column of M must generate R. Let

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

be the first column of M.

Consider α_1 and α_2. We may add any multiple of α_1 to α_2 without altering any of the other entries in the column. By assumption, α_1 and α_2 have a terminating division chain. Hence by successive row operations, we may reduce M so that the first column becomes

$$\begin{pmatrix} \delta_1 \\ 0 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}$$

where δ_1 is the next to last remainder in the division chain of α_1 and α_2. Now do this for δ_1 and α_3 and call the next to last remainder of the division chain of δ_1 and α_3, δ_2. Continue until $\alpha_3, \ldots, \alpha_n$. Then δ_n is a unit of R since $(\delta_n) = (\alpha_1, \ldots, \alpha_n) = R$. Hence we have reduced the first column of M to

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Let M_{11} be obtained by deleting the first column and row of M. Then after making the above reductions, M_{11} is invertible. Thus by inductive hypothesis, M_{11} can be reduced to the identity by elementary row operations (which will not affect the first column or row), so M is row equivalent to the matrix

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & & 1 \end{pmatrix}$$

which is clearly able to be reduced to the identity. □

Example 1.1.10. Let R be the ring of integers of $\mathbb{Q}(\sqrt{-19})$. Cohn showed in [2] that R is not GE_n for any $n \geq 2$. Thus by Propositions 1.1.9, R is not ω-stage Euclidean. However, R is a PID, thus there does exist a PID which is not ω-stage Euclidean.

1.2 Review of Ordinals

Recall that a set is totally ordered if there is a relation $\leq$ which is reflexive, anti-symmetric, transitive and any two elements are comparable. A *well-ordering* is a total ordering on a set for which every non-empty subset has a least element. Equivalently, a totally ordered set is well-ordered if there is no infinitely decreasing sequence. The ordinals are a generalization of the natural numbers, which describe the order type of a well-ordered set. The first infinite ordinal is ω which describes the order type of the natural numbers.

It is not necessary that a non-empty well-ordered set has a maximum element. If a well-ordered set does have a maximum element, then the ordinal describing that set is said to be a successor ordinal. Any non-zero ordinal which is not a successor ordinal is a limit ordinal. For example, the ordinal ω is a limit ordinal. Equivalently, α is a limit ordinal if whenever an ordinal γ is less than α, then there exists an ordinal β such that $\gamma < \beta < \alpha$.

If S and T are two disjoint well-ordered sets with order type α and β respectively, then the order type of $S \cup T$ is $\alpha + \beta$. If the sets are not disjoint then one set may be replaced with an order isomorphic set. Note that this addition is not commutative. To see this consider the set $\{a < b < c\}$ with order type 3 and the natural numbers. Then the ordinal $3 + \omega$ describes the order type of the set $\{a < b < c < 0 < 1 < ...\}$, which after relabeling, also has order type ω. However, the ordinal $\omega + 3$, which describes the set $\{0 < 1 < 2 < ... < a < b < c\}$, is not equivalent to ω, since $\omega + 3$ is a successor ordinal and ω is a limit ordinal.

We may also define ordinal multiplication. For any two well-ordered sets S and T with order type α and β respectively, the order type of $S \times T$ is $\alpha \cdot \beta$. Note that this multiplication is not commutative. We may also define ordinal exponentiation. We will do this inductively, meaning given ordinals α and β we define $\alpha^0 = 1$, $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$, and if β is a limit ordinal, we define α^β to be the limit of α^γ for all $\gamma < \beta$.

Every ordinal γ can be written uniquely in *Cantor normal form*

$$\gamma = \omega^{\alpha_1} n_1 + \omega^{\alpha_2} n_2 + \cdots + \omega^{\alpha_k} n_k = \sum_{i=1}^{k} \omega^{\alpha_i} n_i$$

where $\alpha_1 > \alpha_2 > \cdots > \alpha_k$ are ordinals, the coefficients $n_1, n_2, \ldots, n_k$ are positive integers and $k \in \omega$. Since ordinal addition is not commutative, summation will be written from left to right as in the equality above.

An ordinal is *indecomposable* if it is nonzero and cannot be written as a sum of two smaller ordinals. An example would be ω. In fact, all indecomposable ordinals are of the form ω^α for some ordinal α.

Let γ, δ be two ordinals. After adding zero coefficients to their Cantor normal form (as necessary), we may write $\gamma = \sum_{i=1}^{k} \omega^{\alpha_i} m_i$ and $\delta = \sum_{i=1}^{k} \omega^{\alpha_i} n_i$ where $\alpha_1 > \alpha_2 > \cdots > \alpha_k$

are ordinals, each m_i, n_i are non-negative integers and $k \in \omega$. The *Hessenburg sum* of γ and δ is the ordinal

$$\gamma \oplus \delta = \sum_{i=1}^{k} \omega^{\alpha_i}(m_i + n_i)$$

The Hessenburg sum is commutative and cancellative.

1.3 Motzkin Sets

The Euclidean Algorithm provides a way to move from one denominator to 'simpler' denominator. Using the divisibility relation, we can measure the simplicity of a denominator. The simplest denominators would be those that divide every element in R (i.e. $x \in R$ is such that $x \mid y$ for all $y \in R$). We can then recursively assign complexities with respect to this relation, leading to the following definition.

Definition 1.3.1. Given any ring R and any ordinal α, define a *Motzkin set*

$$\begin{aligned} E_\alpha(R) := \{d \in R : \text{ if } n \in R \text{ then } d \,|\, n \text{ or there exists } q \in R \text{ and } \beta < \alpha \\ \text{such that } n - qd \in E_\beta(R)\}. \end{aligned}$$

For example, the first few Motzkin sets are as follows:

$$\begin{aligned} E_0(R) &= \{d \in R : \text{ if } n \in R \text{ then } d \,|\, n\} = U(R) \\ E_1(R) &= \{d \in R : \text{ if } n \in R \text{ then } d \,|\, n \text{ or there exists } q \in R \text{ and } \beta < \alpha \\ &\qquad \text{such that } n - qd \in E_0(R)\}. \end{aligned}$$

Notice that $E_0(R)$ contains the simplest denominators, the units of the ring. The set $E_1(R) - E_0(R)$, called the set of *universal side divisors* of R, are next in simplicity. Notice that 0 will be the most complex element of R since $0 \nmid r$ for any non-zero $r \in R$. This preserves the typical order of ideals by set containment.

Example 1.3.2. We will determine the Motzkin sets for $\mathbb{Z}$.

We have $U(\mathbb{Z}) = \{-1, 1\} = E_0(\mathbb{Z})$. For $E_1(\mathbb{Z})$, we need to determine what integers have a remainder of ± 1 or 0 when dividing another integer. The only integers to satisfy this property are ± 2 and ± 3. Hence $E_1(\mathbb{Z}) = \{\pm 2, \pm 3\} \cup E_0(\mathbb{Z})$. Inductively, we see that $E_\alpha(\mathbb{Z}) = \{x \in \mathbb{Z} : |x| < 2^{\alpha+1}\} - \{0\}$. For $\alpha = \omega$, we have $0 \in E_\alpha(R)$. Thus, the first ordinal where $\mathbb{Z} = E_\alpha(R)$ is ω.

The next three results are some known properties of Motzkin sets that were first noted in [11] without proof.

Proposition 1.3.3. *For any ordinals $\alpha < \beta$, and for any ring R we have that $E_\alpha(R) \subseteq E_\beta(R)$.*

Proof. Let $\alpha < \beta$ and let R be any ring. Given $d \in E_\alpha(R)$ then for every $n \in R$, there exists $q \in R,\ \gamma < \alpha$ such that $n - qd \in E_\gamma(R)$ thus $d \in E_\beta(R)$ since $\gamma < \alpha < \beta$. $\square$

Remark 1.3.4. This means the $E_\alpha(R)$'s form a non-decreasing chain of subsets of R.

$$E_0(R) \subseteq E_1(R) \subseteq ... \subseteq E_\omega(R) \subseteq E_{\omega+1}(R) \subseteq ...$$

This chain is strictly increasing until it stabilizes. For every ring, there exists $\alpha \in \mathrm{Ord}$ such that $E_\alpha(R) = E_{\alpha+1}(R)$ where $\alpha \leq |R|$.

Proposition 1.3.5. *Let R be a ring. If $E_\alpha(R) = E_{\alpha+1}(R)$ for some ordinal α then $E_\alpha(R) = E_\beta(R)$ for all $\beta > \alpha$.*

Proof. Let R be a ring and suppose that $E_\alpha(R) = E_{\alpha+1}(R)$ for some ordinal α. We work by induction on β to show that $E_\alpha(R) = E_\beta(R)$ for all $\beta \geq \alpha$. Assume that for all $\alpha \leq \gamma < \beta$, that $E_\alpha(R) = E_\gamma(R)$. By Proposition 1.3.3, we know that $E_\alpha(R) \subseteq E_\beta(R)$. It remains to show the reverse inclusion. Let $d \in E_\beta(R)$ where $\beta > \alpha + 1$. Let n be arbitrary. If $d|n$ there is nothing to show, otherwise, there exists $q \in R$, $\gamma < \beta$ so that $n - qd \in E_\gamma(R)$. We may assume that $\alpha \leq \gamma < \beta$, then $E_\gamma(R) = E_\alpha(R)$ by inductive hypothesis, thus $n - qd \in E_\alpha(R)$ which implies that $d \in E_{\alpha+1}(R)$ and thus $d \in E_\alpha(R)$. $\square$

Proposition 1.3.6. *If $E_\alpha(R) = R$ for some ordinal α then R is a PID.*

Proof. Suppose that $E_\alpha(R) = R$ for some ordinal α. We will show that every ideal $I \leq R$ is principal. Let $I \leq R$ be an ideal of R. We may suppose that $I \neq (0)$. Since $E_\alpha(R) = R$ there is a smallest ordinal β such that $I \cap E_\beta(R) \neq \emptyset$. Fix $x \in I \cap E_\beta(R)$ with $x \neq 0$. Clearly, $(x) \subseteq I$. To show reverse inclusion, let $y \in I$. Since $x \in E_\beta(R)$, then either $x \mid y$, which implies $y \in (x)$ or there exists $q \in R, \gamma < \beta$ such that $y - qx \in E_\gamma(R)$, contradicting minimality of β. Thus $I = (x)$ and R is a PID. $\square$

Remark 1.3.7. In the next Section, we will see that if R satisfies Proposition 1.3.6 then R is also a Euclidean domain.

Chapter 2. Transfinitely Valued Euclidean Domains can have Arbitrary Indecomposable Order Type

2.1 Minimal Euclidean Norm

Throughout this section, we assume that R is a domain and that $R = E_\alpha(R)$ for some ordinal α. Define $\tau : R \to \mathrm{Ord}$ by the following rule,

$$\tau(x) = \min\{\alpha \in \mathrm{Ord} : x \in E_\alpha(R)\}$$

Proposition 2.1.1. *τ defined above is a Euclidean norm on R.*

Proof. Let $n, d \in R$ and assume that $d \nmid n$. Since $R = E_\alpha(R)$ for some ordinal α, we have $d \in E_\beta(R)$ for $\beta < \alpha$. Choose β to be minimal. Since $d \in E_\beta(R)$, there exists $q \in R$ such that $n - qd \in E_\gamma(R)$ for some $\gamma < \beta$. Thus $\tau(n - qd) < \gamma < \beta = \tau(d)$. $\square$

Motzkin observed in [9] that τ defined above is minimal among all Euclidean norms of R, meaning if φ is any Euclidean Norm on R then $\tau(x) \leq \varphi(x)$ for all $x \in R$. We will call such a Euclidean norm on a domain R the *minimal Euclidean norm.* It is easy to see that the minimal Euclidean norm satisfies $\tau(x) \leq \tau(xy)$, with equality if and only if $y \in U(R)$ or $x = 0$. Lenstra noted the following proposition (see [8], Proposition 2.1), which gives another definition for the minimal Euclidean norm.

Proposition 2.1.2. *A Euclidean norm φ on R is the minimal Euclidean norm if and only if for all $x \in R$ and for ordinals $\gamma < \alpha$, there exists $y \in R - (x)$ such that $\varphi(z) \geq \gamma$ for every $z \in y + (x)$.*

The following property was noticed and proved by Lenstra (see [8], Proposition 3.4); however, because of the usefulness of this theorem, we will also include it.

Lemma 2.1.3. *Given $x, y \in R \setminus \{0\}$, $\tau(xy) \geq \tau(x) \oplus \tau(y)$.*

Proof. We work by induction on $\tau(xy)$. Suppose, by way of contradiction, that $\tau(xy) < \tau(x) \oplus \tau(y)$ then, interchanging x and y if necessary, we may assume $\tau(xy) \leq \gamma \oplus \tau(y)$ for some $\gamma < \tau(x)$. By Proposition 2.1.2, there exists $r \in R - (x)$ such that for all $s \in r + (x)$, $\tau(s) \geq \gamma$. Now choose $sy \in ry + (xy)$ so that $\tau(sy) \leq \tau(xy)$, then $s \in r + (x)$ and $\tau(s) \geq \gamma$. Thus $\tau(sy) \leq \tau(xy) \leq \gamma \oplus \tau(y)$. But, by inductive assumption, we should have $\tau(sy) \geq \tau(s) \oplus \tau(y) \geq \gamma \oplus \tau(y)$. $\square$

Motzkin noticed the following Proposition in [9]. For completeness we provide the proof here.

Proposition 2.1.4. *R is a Euclidean domain if and only if $E_\alpha(R) = R$ for some ordinal α.*

Proof. The forward direction follows immediately from Proposition 2.1.1. For the converse, suppose that R is a Euclidean domain with Euclidean norm φ. We claim that $d \in E_{\varphi(d)}(R)$. We work by induction on $\varphi(d)$. Since R is a Euclidean domain, there exists $q \in R$ such that $\varphi(n - qd) < \varphi(d)$ or $n - qd = 0$. By the inductive hypothesis $n - qd \in E_{\varphi(n-qd)}(R)$ which implies that $d \in E_{\varphi(d)}(R)$. Since φ maps R to Ord, and is defined on all of R, we have that $E_\alpha(R) = R$ for some ordinal. (see also [8] pg 11) $\square$

Corollary 2.1.5. *A domain R is a finite Euclidean domain if and only if $E_\omega(R) = R$*

Proposition 2.1.6. *Let R be a domain. If α is the smallest ordinal such that $E_\alpha(R) = R$ then α is an indecomposable ordinal.*

Proof. Write the Cantor normal form for α as $\omega^{\beta_1} c_1 + \omega^{\beta_2} c_2 + \cdots + \omega^{\beta_k} c_k$ where $k \in \omega$, $k \geq 2, c_i \in \mathbb{Z}_{>0}$ and $\beta_1 > \beta_2 > \cdots > \beta_k \geq 0$ are ordinals. Assume by way of contradiction, that α is not indecomposable. Then, since $E_\omega(R) = R$, there exists some $r \in R$ such that $\tau(r) = \omega^{\beta_1}$ but then by Theorem 1, we have $\tau(r^{c_1+1}) \geq \tau(r) \oplus \cdots \oplus \tau(r) = \omega^{\beta_1}(c_1 + 1) > \alpha$, a contradiction. $\square$

Recall that the *Euclidean order type* of R is $\min_{\varphi}\{\alpha \in \mathrm{Ord} : \varphi(R \setminus \{0\}) \subseteq \alpha\}$ where φ ranges among all possible Euclidean norms on R. Since τ defined above is the minimal Euclidean norm on a domain R and by Proposition 2.1.4, we may also define the Euclidean order type to be the first ordinal α such that $R = E_{\alpha}(R)$. Alternatively, the Euclidean order type is defined to be $\tau(0)$. By Proposition 2.1.6, we see that the Euclidean order type must be an indecomposable ordinal.

2.2 Euclidean Domain with Arbitrary Indecomposable Order Type

The purpose of this section is to prove the following theorem.

Theorem 2.2.1. *For every ordinal α, there exists a Euclidean Domain with Euclidean order type of ω^{α}.*

To prove this, we construct such a Euclidean Domain. First, fix an arbitrary ordinal α. Let F be a field and define $R_0 = F[x_{\{\beta\},0} : 0 < \beta < \omega^{\alpha}]$, where the elements of $\{x_{\{\beta\},0}\}_{0<\beta<\omega^{\alpha}}$ are independent indeterminates over F. For any $r \in R_0 \setminus F$, define

$$\mathrm{Sub}(r) = \{\beta \in \mathrm{Ord} : \beta \text{ is an element of the first index of some variable in the support of } r\}. \tag{2.2.2}$$

For example, if $r = x_{\{1\},0}x_{\{2\},0} - x^3_{\{3\},0}$ then $\mathrm{Sub}(r) = \{1, 2, 3\}$.

Next, we define a function $\varphi : R_0 \setminus \{0\} \to \mathrm{Ord}$ by letting $\varphi(p) = \max(\mathrm{Sub}(p))$ for any prime $p \in R_0$, and set

$$\varphi(r) = \bigoplus_{i=1}^{n} \varphi(p_i), \text{ where } r = u\prod_{i=1}^{n} p_i \text{ is a prime factorization of } r \text{ with } u \in F \setminus \{0\} \tag{2.2.3}$$

We also define $\varphi(u) = 0$ for $u \in F \setminus \{0\}$. Returning to our previous example, if $r = x_{\{1\},0}x_{\{2\},0} - x^3_{\{3\},0}$, then it is prime, so $\varphi(r) = 3$. Note that since R_0 is a polynomial ring over a field, it is a U.F.D., thus prime factorizations are unique and φ is well-defined.

Now we define,

$$S_0 = \{(n, d) \in R_0 \times R_0 : \gcd(n, d) = 1 \text{ and } \varphi(n) \geq \varphi(d) \geq 1\}.$$

The elements of S_0 are those for which we will adjoin a new quotient q such that $\varphi(n-qd) < \varphi(d)$. Thus we define

$$R_1 = R_0[x_{\{\beta\},1}, y_{T,1,n,d} : 0 < \beta < \omega^\alpha, (n, d) \in S_0]$$

where $T = T(n, d) := \mathrm{Sub}(n) \cup \mathrm{Sub}(d) \cup \{0\}$. We want $q = y_{T,1,n,d}$ to act as a quotient for the pair (n, d). Since $n - qd$ is a monic irreducible polynomial over q, it is prime in R_1, which we will call a *special prime*, with corresponding *special variable* q. For any $r \in R_1 \setminus F$, define $\mathrm{Sub}(r)$ exactly as in (2.2.2). For reducible elements $r \in R$, we will extend φ to R_1 in the obvious way, (i.e. write r in its prime factorization $r = u \prod_{i=1}^n p_i$ where $u \in F$ and each p_i is a prime then $\varphi(r) = \bigoplus_{i=1}^n \varphi(p_i)$) and for primes $p \in R_1$, we extend φ by the rule

$$\varphi(p) = \begin{cases} \max\{\beta \in T : \beta < \varphi(d)\} & \text{if } p \text{ is a special prime with special variable } q \\ \max(\mathrm{Sub}(p)) & \text{otherwise} \end{cases} \tag{2.2.4}$$

Notice that if $p \in R_0$ that $\varphi(p)$ agrees with its previous definition on R_0, thus we have truly extended φ to R_1.

We now recursively define rings R_j for each $j < \omega$ and extend φ to R_j. Similar to passing from R_0 to R_1, if we have defined some R_i ($i \geq 1$) and have extended φ to R_i so that (2.2.4) holds, we define

$$S_i = \{(n, d) \in R_i \times R_i : \gcd(n, d) = 1 \text{ and } \varphi(n) \geq \varphi(d) \geq 1\}$$

and let

$$R_{i+1} = R_i[x_{\{\beta\},i+1}, y_{T,i+1,n,d} : 0 < \beta < \omega^\alpha, (n, d) \in S_i\}$$

where T is defined as above. Note that each $q = y_{T,i+1,n,d}$ is a special variable for exactly one special prime $n - qd$ (up to unit multiples). As done previously, we define $\mathrm{Sub}(r)$ on R_{i+1} exactly as in (2.2.2) and extend φ to R_{i+1} using (2.2.4), completing the recursive construction. Note that in our extension of φ, we have defined φ in terms of its previous values which causes no problems since if $n - qd \in R_{j+1}$ is a special prime then $d \in R_j$, thus this recursion stops in finite time.

Lastly, we let $R_\infty = \cup_{j=0}^{\infty} R_j$ and let U be the set of elements which are products of special primes (including empty products) with φ-value of 0 and non-zero elements of F (i.e. $U = \{r \in R_\infty : \varphi(r) = 0\}$). Let $R = U^{-1}R_\infty$. For $r \in R$, write $r = u^{-1}r'$ where $u \in U$ and $r' \in R_\infty$ and extend φ to R by $\varphi(r) = \varphi(u^{-1}r') = \varphi(r')$. We will now show that R has the desired properties.

Lemma 2.2.5. *The map φ is a Euclidean norm on R.*

Proof. Let $n, d \in R$ with $d \neq 0$ and assume $d \nmid n$. We want to find some $q \in R$ such that $\varphi(n - qd) < \varphi(d)$. Since multiplying by units does not change the value of φ, may assume neither n nor d has any special prime factors from U. If $\varphi(n) < \varphi(d)$, then we can take $q = 0$. Thus we reduce to the case when $\varphi(n) \geq \varphi(d)$. Let $r = \gcd(n, d)$. We may write $n = n'r$ and $d = d'r$ for some $n', d' \in R_\infty$ with $\gcd(n', d') = 1$. Note that $d' \neq 1$ or else d would divide n thus $\varphi(d') \geq 1$. By the definition of φ, we have

$$\varphi(n') \geq \varphi(d'). \tag{2.2.6}$$

Let $q = y_{T,i,n,d}$, where i is chosen large enough so that $n', d' \in R_{i-1}$, then $\varphi(n' - qd') < \varphi(d')$ by the first case of (2.2.4). Thus we have

$$\varphi(n - qd) = \varphi(r(n' - qd')) = \varphi(r) \oplus \varphi(n' - qd') < \varphi(r) \oplus \varphi(d') = \varphi(d). \tag{2.2.7}$$

$\square$

Lemma 2.2.8. *The map φ is the minimal Euclidean Norm τ on R.*

Proof. We work by induction to show that $\varphi(d) = \tau(d)$ for all $d \in R \setminus \{0\}$. First, $\varphi(d) = 0$ if and only if d is a unit, which occurs if and only if $\tau(d) = 0$. This covers the base case. Now let $\beta \geq 1$. Assume, inductively that for all $r \in R \setminus \{0\}$ that satisfies $\varphi(r) < \beta$, that $\varphi(r) = \tau(r)$.

Assume by way of contradiction, that $\beta := \tau(d) < \varphi(d)$ for some $d \in R \setminus \{0\}$. By Lemma 2.1.3, the definition of φ and the fact that $\tau(r) \leq \varphi(r)$ for all $r \in R \setminus \{0\}$, we need only consider the case that d is irreducible. We know that $d \in R_j$ for some $j < \omega$. Set $n := x_{\{\beta\},j+1}$. Then $d \nmid n$. Thus we can find $q \in R$ where $\tau(n - qd) < \tau(d) = \beta$. By inductive hypothesis, we know that $\varphi(n - qd) = \tau(n - qd)$. After clearing denominators, we get

$$un - q'd = r \tag{2.2.9}$$

for some $u, q', r \in R_\infty$ with $u \in U$ and $\varphi(r) < \beta$. If u and q' share a factor then we can remove that factor from both sides of (2.2.9), thus we may assume that u and q' share no common factors. Since d is irreducible with positive φ-norm, it also shares no factors with u.

Also, if $n \,|\, q'd$ then $n \,|\, r$ which would imply that $\varphi(r) \geq \varphi(n) = \beta$, a contradiction. Thus we have that un and $q'd$ share no common factors in R_∞ and by (2.2.9) the same is true for any two polynomials un, $q'd$ and r.

Let $\psi : R_\infty \to R_\infty$ be the unique ring homomorphism fixing F and all variables in R_∞ except $\psi(n) = 0$. Note that n does not appear as a monomial in d since $d \in R_j$, thus $\psi(d) = d$, hence after applying ψ to (2.2.9) we get $-\psi(q')d = \psi(r)$. Thus $d \,|\, \psi(r)$. Since $d \nmid r$, we have that $\psi(r) \neq r$. Thus n must appear in some irreducible factor of r, say r_1. Note that r_1 must be special or else $\varphi(r) \geq \varphi(r_1) \geq \beta$, which is a contradiction. Thus r has a special variable which has β in its first index and its second index is greater than j. Let $q_1 = y_{T_1,k_1,n_1,d_1}$ be a special variable that is either in r or u such that $\beta \in T_1$ and $k_1 > j$ is maximal with respect to these properties.

Suppose that q_1 appears in an irreducible factor of r' of r but not as a corresponding special variable. The factor r' cannot be special by maximality of k_1 but then $\varphi(r) \geq \varphi(r') \geq \beta$ which is a contradiction. Thus if q_1 occurs in an irreducible factor of r, it must occur in a special prime as the corresponding special variable.

On the other hand, if q_1 appears in some irreducible of u, then since every such factor is special and k_1 is maximal, q_1 is the corresponding special variable.

Since $\gcd(u, r) = 1$, we have that q_1 must occur in exactly one prime factor (not counting multiplicity) of u or r (not both) and only as the corresponding special variable. Further, $k_1 > j$ thus q_1 does not appear in a factor of d. Thus the only way for (2.2.9) to hold is if q_1 appears in q'.

First, consider the case that q_1 appears in r. We can write $r = s(n_1 - q_1 d_1)^m$ for some integer $m \geq 1$ maximal with respect to $s \in R_\infty$. Thus r in (2.2.9) as a polynomial in the variable q_1, has leading term of $(-1)^m d_1^m s$. However, the only place where q_1 appears on the left side of (2.2.9) is in q' and thus the left hand side of (2.2.9) has leading term divisible by d. Thus $d \,|\, d_1^m s$. Since $\gcd(d, r) = 1$ and d is irreducible, we must have $d \,|\, d_1$ which implies $\varphi(d_1) \geq \varphi(d)$. Since $\beta \in T_1$ and $\beta < \varphi(d)$, by (2.2.4), we have that $\varphi(r) \geq \varphi(n_1 - q_1 d_1) \geq \beta$, which contradicts $\varphi(r) < \beta$.

Finally, consider the case when q_1 occurs in u. By the same argument as the previous paragraph we have that $d \,|\, d_1$ thus $\varphi(d_1) \geq \varphi(d) > \beta$. Since $1 \in T_1$ and $\beta < \varphi(d)$, by (2.2.4), we have that $\varphi(u) \geq \varphi(n_1 - q_1 d_1) \geq \beta \geq 1$, which contradicts $\varphi(u) = 0$ completing the proof of our claim and thus proving that $\varphi(d) = \tau(d)$. □

We have now shown that φ is the minimal Euclidean norm on R, hence the Euclidean order type of R is

$$\{\varphi(x) : x \in R \setminus \{0\}\}.$$

We have that $\varphi(1) = 0$ and $\varphi(x_{\{\beta\},0}) = \beta$ so this set contains every ordinal less than ω^α. Also, any ordinal that appears in the first index of any of the variables is less than ω^α. Since the Euclidean order type must be indecomposable, the Euclidean order type of R must be ω^α.

2.3 Finitely Valued Euclidean Domain With No Multiplicative Norm

It has been a long standing question (see, for example [7]) whether every finitely valued Euclidean domain has some *multiplicative Euclidean norm*, meaning a Euclidean norm $\psi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Modifying the ring we constructed in Section 2.2, we prove that there is a finitely-valued Euclidean domain with no multiplicative Euclidean norm. We modify the construction in the following ways.

1. Fix $\alpha = 1$ so that the ring will be a finitely valued Euclidean domain.
2. Restrict F to have characteristic 0.
3. At the initial stage of the construction, adjoin one more variable $z = z_{\{1\},0}$
4. Redefine φ to be
$$\varphi(r) = \varphi(z^k) \oplus \bigoplus_{i=1}^{n} \varphi(p_i) \tag{2.3.1}$$
where $r = uz^k \prod_{i=1}^{n} p_i$ is a prime factorization, $u \in F \setminus \{0\}$, and $z^k \,||\, r$, with $\varphi(z^k) = k^k$ for each integer $k \geq 1$. Thus φ still satisfies (2.2.3) except on powers of z. The definition of φ remains the same on primes.
5. At the recursive stages of the construction, we expand the set S_i by allowing pairs $(n, d) \in R_i \times R_i$ that satisfy $\gcd(n, d) = 1$ and $\varphi(n) < \varphi(d)$ if $z \,|\, n$. This produces new special primes and special variables, which are subject to the previous conditions.

With these changes, Lemma 2.2.5 still holds with the following adjustments to the proof. No changes are needed when (2.2.6) holds. We need only consider the case when $\varphi(n) \geq \varphi(d)$ and $\varphi(n') < \varphi(d')$, which can only occur when $z \,|\, r$ and $z \,|\, n'$. In this case there is still a special variable $q = y_{T,i,n',d'}$ due to the expansion of S_i. Since $\gcd(n', d') = 1$, we have that $z \,|\, d'$ thus $z \nmid (n' - qd')$. Thus by (2.3.1), equation (2.2.7) still holds thus φ is a Euclidean Norm on our new ring R.

Now we will show that Lemma 2.2.8 still holds. In the second paragraph, in order to reduce to the case that d is irreducible, we must now use 2.3.1, which allows for the possibility that $d = z^k$ for some $k \geq 2$. We need only consider this case since the original will remain unchanged. The proof proceeds as previously until we reach the point $d \,|\, d_1^m$. (We need only deal with the case that $r - s(n_1 - q_1 d_1)^m$ for some $m \geq 1$, since the case with q_1 in u is similar). Since $d \,|\, d_1^m$ we have $z \,|\, d_1$. Looking at 2.2.9 as a polynomial in the variable q_1, we have that the leading coefficient of the right hand side is $-mn_1^{m-1} d_1 s$. The leading coefficient of the left hand side of 2.2.9 is divisible by d. Since $m \neq 0$ and F has characteristic 0, we have $d \,|\, (n_1^{m-1} d_1 s)$. Since $z \,|\, d_1$ and $\gcd(n_1, d_1)$, $d_1 \,|\, d$ and the rest of the proof proceeds as in Lemma 2.2.8.

Now that φ is the minimal norm, we may now prove the main theorem of this Section.

Theorem 2.3.2. *There is a finitely valued Euclidean domain with no multiplicative Euclidean norm.*

Proof. Let $\psi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ be any Euclidean norm on R. Set $k := \psi(z)$. Note that since z is not a unit, we must have $k \geq 1$. Fix $\ell \in \mathbb{N}$ large enough so that $k^\ell < \ell^\ell$. If ψ was multiplicative, we would have

$$\psi(z^\ell) = \psi(z)^\ell = k^\ell < \ell^\ell = \varphi(z^\ell)$$

which contradicts the fact that φ is the minimal Euclidean norm. $\square$

2.4 Consequences

Lenstra in [8] on page 34, notices for $\mathbb{Z}$ and $k[x]$ where k is a field, that the following is true. If $\psi : R \setminus \{0\} \to \mathrm{Ord}$ is a map which is not an algorithm (a technical definition in [8]) then there exists a finite subset $E \subseteq R \setminus \{0\}$ such that there is no norm $\varphi : R \setminus \{0\} \to \mathrm{Ord}$ with $\psi|_E = \varphi|_E$. Lenstra then remarks that he does not know how generally true this is.

Modifying our construction, there is a finitely-valued ring which contains a finite set E where a map ψ does not agree with any norm on E but remains a norm.

Let φ be the minimal norm defined in Section 2.2. To begin, let $E = \{d_1, \ldots, d_k\}$ with where $\varphi(d_j) = 1$. Define $\psi : R \setminus \{0\} \to \omega$ to satisfy $\psi = \varphi$ except $\psi(d_j) = 2$. Let S_i be as previously defined and define

$$V_i = \{(d_j, r) \in E \times R_i : \gcd(d_j, r) = 1, \varphi(r) = 2\}.$$

Then at the recursive stage of the construction define

$$R_{i+1} = R_i[x_{\{\beta\},i+1}, y_{T,i+1,n,d}, y'_{T,i+1,d_j,r} : \beta < \omega, (n, d) \in S_i, (d_j, r) \in V_i].$$

Take R_∞, U and R to be as defined in Section 2.2. Then φ as defined in 2.2.3 with $\varphi(d_j - y'r) = 0$ is still a norm by the proof given in Lemma 2.2.5. Then since φ is a norm, in order to show that ψ is a norm, we need only consider the case when d_j is a numerator and $\varphi(d) = 2$ where d is the divisor of d_j. Then $\psi(d_j) = \psi(d)$. But then we have some $y' \in R$ where $\psi(d_j - y'd) = \varphi(d_j - y'd) = 0$ thus ψ is a norm.

Chapter 3. Admissible Primes

3.1 Definitions and Theorems

Through out this section, let R be a PID with quotient field K. Following Clark and Murty in [1], we make the following definition.

Definition 3.1.1. A set $\{\pi_1, \pi_2, \ldots, \pi_n\}$ of distinct non-associate prime elements of R is said to be *admissible* if for any $\beta = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_n^{a_n}$, where each a_i is a non-negative integer, every co-prime residue class of β can be represented by a unit of R. We say that a single prime π is *admissible* if $\{\pi\}$ is admissible.

Remark 3.1.2. Note that $\{\pi_1, \pi_2, \ldots, \pi_n\}$ forms an admissible set if and only if the unit group of R maps onto $\left(R/(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_n^{a_n})\right)^*$ for any choice of a_i $(1 \leq i \leq n)$.

The usefulness of admissible primes can be seen in the following theorem of Clark and Murty (see [1] pg 153).

Theorem 3.1.3. *Let R be a PID whose quotient field K is a totally real Galois extension of $\mathbb{Q}$ of degree n_k. Suppose that an admissible set of $|n_k - 4| + 1$ primes of R can be found, then R is a Euclidean Domain.*

Hence, we may use these admissible set of primes to determine when the ring of integers of certain number fields are Euclidean. Our main interest was to find examples of primes that would be admissible (see Section 3.2). Before we present our algorithm for finding admissible primes in the ring of integers of $\mathbb{Q}(\sqrt{d})$ where d is a positive square-free integer, we note the following proposition of Clark and Murty (see [1] pg 160). Because our algorithm in Section 3.2 relies heavily upon this proposition, we will include the proof.

Theorem 3.1.4. *Let R be a PID whose quotient field K is a totally real Galois extension of $\mathbb{Q}$ of degree n_k. Suppose that $\pi_1, \pi_2, \ldots, \pi_n$ are non-ramified prime elements of residue class degree one in R not lying above 2. If $\pi_1^2\pi_2^2\cdots\pi_n^2$ is such that every co-prime residue class can be represented by a unit, then $\{\pi_1, \pi_2, \ldots, \pi_n\}$ is an admissible set of primes.*

Proof. We expand on the proof of Clark and Murty. We will use induction to show if the unit group $U(R)$ maps onto $\left(R/(\pi_1^2\pi_2^2\cdots\pi_n^2)\right)^*$ then $U(R)$ maps onto $\left(R/(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_n^{a_n})\right)^*$ for each $a_i \leq 2$ as i ranges from 1 to n.

Suppose that the claim has been proven for the product $\pi_1^{b_1}\cdots\pi_n^{b_n}$, for each choice of integers $b_1,\ldots,b_n$ such that $b_i \leq c_i$ for $1 \leq i \leq n$, with at least one of the inequalities strict. Without loss of generality, suppose that $c_1 \geq 3$ and consider the product $\pi_1^{c_1-1}\pi_2^{c_2}\cdots\pi_n^{c_n}$. By the inductive hypothesis, $U(R)$ maps onto $\left(R/(\pi_1^{c_1-1}\pi_2^{c_2}\cdots\pi_n^{c_n})\right)^*$. By the Chinese Remainder Theorem,

$$R/(\pi_1^{c_1-1}\pi_2^{c_2}\cdots\pi_n^{c_n}) \cong R/(\pi_1^{c_1-1}) \times \prod_{i=2}^{n} R/(\pi_i^{c_i}),$$

thus $U(R)$ maps onto

$$\left(R/(\pi_1^{c_1-1})\right)^* \times \prod_{i=2}^{n}\left(R/(\pi_i^{c_i})\right)^*.$$

Since $\left(R/(\pi^{c_1-1})\right)^*$ is a cyclic group of order $p_1^{c_1-2}(p_1-1)$ where p_1 is the prime lying above π_1, we may find $\varepsilon_1 \in U(R)$ such that $\varepsilon_1 \equiv 1 \mod \pi_i$ for every $2 \leq i \leq n$ and ε_1 is a generator for $\left(R/(\pi^{c_1-1})\right)^*$, meaning ε_1 has order $p_1^{c_1-2}(p_1-1) \mod \pi_1^{c_1-1}\pi_2^{c_2}\cdots\pi_n^{c_n}$. Notice that ε_1 is in the group $\left(R/(\pi^{c_1-2})\right)^*$ since $\gcd(\varepsilon_1,\pi_1)=1$. We have that the order of $\left(R/(\pi^{c_1-2})\right)^*$ is $p_1^{c_1-3}(p_1-1)$ thus $\varepsilon_1^{p_1^{c_1-3}(p_1-1)} \equiv 1 \mod \pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n}$ hence

$$\varepsilon_1^{p_1^{c_1-3}(p_1-1)} = 1 + k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n},$$

where $\pi_1 \nmid k$. After raising both sides to the p_1 we have,

$$\begin{aligned}
\varepsilon_1^{p_1^{c_1-2}(p_1-1)} &= \sum_{j=0}^{p_1}\tbinom{p_1}{j}(k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n})^j \\
&= 1 + p_1k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n} + \sum_{j=2}^{p_1}\tbinom{p_1}{j}(k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n})^j \\
&= 1 + \alpha k\pi_1^{c_1-1}\pi_2^{c_2}\cdots\pi_n^{c_n} + \sum_{j=2}^{p_1}\tbinom{p_1}{j}(k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n})^j
\end{aligned}$$

where $p_1 = \alpha\pi_1$ and $\pi_1 \nmid \alpha$ since π_1 is non-ramified. Notice that

$$\begin{aligned}\sum_{j=2}^{p_1} \tbinom{p_1}{j}(k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n})^j &= \sum_{j=2}^{p_1} \tfrac{(p_1-1)!}{j!(p_1-j)!}k^j\alpha\pi_1^{jc_1-2j+1}(\pi_2^{c_2}\cdots\pi_n^{c_n})^j \\ &= \sum_{j=2}^{p_1} \tfrac{(p_1-1)!}{j!(p_1-j)!}k^j\alpha\pi_1^{(j-1)c_1-2j+1}(\pi_2^{c_2}\cdots\pi_n^{c_n})^{j-1}(\pi_1^{c_1}\pi_2^{c_2}\cdots\pi_n^{c_n})\end{aligned}$$

Since $c_1 \geq 3$ we have $(j-1)c_1 - 2j + 1 \geq 3(j-1) - 2j + 1 \geq j - 2 \geq 0$. Thus

$$\sum_{j=2}^{p_1} \tbinom{p_1}{j}(k\pi_1^{c_1-2}\pi_2^{c_2}\cdots\pi_n^{c_n})^j \equiv 0 \mod \pi_1^{c_1}\pi_2^{c_2}\cdots\pi_n^{c_n}.$$

So we have

$$\varepsilon_1^{p_1^{c_1-2}(p_1-1)} \equiv 1 + k'\pi_1^{c_1-1} \mod \pi_1^{c_1}\pi_2^{c_2}\cdots\pi_n^{c_n}$$

where $\pi_1 \nmid k'$. Hence we have shown that in the group $\left(R/(\pi_1^{c_1})\right)^*$, which has order $p_1^{c_1-1}(p_1-1)$, that any power of ε_1 less that the order of the group does not give the identity which implies that ε_1 is a generator for $\left(R/(\pi_1^{c_1})\right)^*$.

We can likewise find elements $\varepsilon_i \in U(R)$ such that $\varepsilon_i \equiv 1 \mod \pi_j^{c_j}$ for $j \neq i$ and ε_i has the order $p_i^{c_i-1}(p_i-1) \mod (\pi_1^{c_1}\pi_2^{c_2}\cdots\pi_n^{c_n})$. This then shows that $U(R)$ maps onto $\left(R/(\pi_1^{c_1}\pi_2^{c_2}\cdots\pi_n^{c_n})\right)^*$. □

Remark 3.1.5. The point of this theorem is that when checking if a set of non-ramified primes are admissible, we need only to determine if the co-prime residue classes of $\pi_1^2\pi_2^2\cdots\pi_n^2$ are represented by a unit.

3.2 Finding Admissible Primes in Quadratic Extensions of $\mathbb{Q}$

Now let $K = \mathbb{Q}(\sqrt{d})$, where d is a positive square-free integer, and let $\mathcal{O}_K$ be the ring of integers of K. We will determine when $\{\pi_1, \pi_2, \ldots, \pi_n\}$ is an admissible set of primes. Let $\beta = \pi_1^2\cdots\pi_n^2$. By Theorem 3.1.4, we need only check that the co-prime residue classes of β are represented by a unit.

We first present the case where $d \equiv 2, 3 \mod 4$. An integral basis for $\mathcal{O}_K$ is $\{1, \sqrt{d}\}$. Let u be the fundamental unit of $\mathcal{O}_K$. For each co-prime residue class of β, with class representative $r = r_1 + r_2\sqrt{d}$, we would like to find a natural number m and a choice of sign such that

$$\pm(u^m) \equiv r \mod \beta.$$

This is equivalent to solving

$$\pm(u^m) - r = \beta(x + y\sqrt{d})$$

for some $m \in \mathbb{N}$, $x, y \in \mathbb{Z}$ and choice of sign. Our algorithm will iterate over the powers of the fundamental unit for a finite interval, hence, for the time being, we will let $v = \pm(u^m)$ where we have fixed m and some choice of sign. We may write

$$v = v_1 + v_2\sqrt{d}$$

for some $v_1, v_2 \in \mathbb{Z}$ and

$$\beta = b_1 + b_2\sqrt{d}$$

where $b_1, b_2 \in \mathbb{Z}$. Showing that r is represented by the unit v is equivalent to solving the following system of equations:

$$\begin{bmatrix} b_1 & db_2 \\ b_2 & b_1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} v_1 - r_1 \\ v_2 - r_2 \end{bmatrix}.$$

Solving for x, y gives

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{N_K(\beta)} \begin{bmatrix} b_1 & -db_2 \\ -b_2 & b_1 \end{bmatrix} \begin{bmatrix} v_1 - r_1 \\ v_2 - r_2 \end{bmatrix},$$

where N_K is the usual norm on $\mathcal{O}_K$, so $N_K(\beta) = b_1^2 - db_2^2$.

Notice that $x, y \in \mathbb{Z}$ if and if only

$$b_1(v_1 - r_1) - db_2(v_2 - r_2) \equiv 0 \mod N_K(\beta)$$
$$b_1(v_2 - r_2) - b_2(v_1 - r_1) \equiv 0 \mod N_K(\beta).$$

If these congruences hold, then r is represented by the unit v.

We will now determine the fixed interval that m, the power of the fundamental unit, must range over. We know that $(\mathcal{O}_K/(\beta))^*$ is a finite group, thus m must be less than the size of $(\mathcal{O}_K/(\beta))^*$. We have that

$$\left(\mathcal{O}_K/(\beta)\right)^* \cong \prod_{i=1}^{n} \left(\mathcal{O}_K/(\pi_i^2)\right)^*$$

so $|\left(\mathcal{O}_K/(\beta)\right)^*| = \prod_{i=1}^{n} |\left(\mathcal{O}_K/(\pi_i^2)\right)^*|$. Let $\left|\left(\mathcal{O}_K/(\pi_i^2)\right)^*\right| = \alpha_i$. Note that α_i is finite for each i ranging from 1 to n, thus $m \leq \mathrm{lcm_i}(\alpha_\mathrm{i})$. We have that $\left|\left(\mathcal{O}_K/(\pi_i^2)\right)^*\right| \leq \left|\mathcal{O}_K/(\pi_i^2)\right| = N_K(\pi_i^2)$ (see [6] pg 126) hence $1 \leq m \leq N_K(\beta)$.

Note, for a non-ramified split prime π_i, that $a + b\sqrt{d} \equiv r \mod \pi_i^2$ for any $a, b \in \mathbb{Z}$ and for some $r \in \mathbb{Z}$, hence we need only consider the case when r is a primitive root of $N_K(\beta)$. Algorithm 3.1 describes a function which will determine if a set of non-associate non-ramified split primes is admissible in $\mathbb{Z}[\sqrt{d}]$. See the appendix for implementation of this algorithm in Mathematica.

Algorithm 3.1 Find Admissible Primes in $\mathcal{O}_K$ of $\mathbb{Q}(\sqrt{d})$ for $d \equiv 2, 3 \mod 4$

$P = \{\pi_1, \ldots, \pi_n\}$ is a set of non-ramified primes

$u = u_1 + u_2\sqrt{d}$ is the fundamental unit

function CHECKADMISSIBLE(P, d, u_1, u_2):

  $\beta = \prod_{i=1}^{n} \pi_i^2$, $b_1 = \text{First}(\beta)$, $b_2 = \text{Second}(\beta)$

  $N = b_1^2 - db_2^2$

  $r = \text{PrimitiveRoot}(N)$

  $v_1^{(0)} = u_1$, $v_2^{(0)} = u_2$

  for $i = 0$, $i \leq N$, i=i+1 **do** ▷ This iterates over the powers of the fundamental unit

    if $b_1(v_1 - r) - db_2v_2 \ \% \ N == 0$ AND $b_2v_2 - b_2(v_1 - r) \ \% \ N == 0$ **then**

      return TRUE

    else if $-b_1(v_1 - r) + db_2v_2 \ \% \ N == 0$ AND $-b_2v_2 + b_2(v_1 - r) \ \% \ N == 0$ **then**

      return TRUE

    else

      $v_1^{(n+1)} = u_1(u_1v_1^{(n)} + u_2d) \ \% \ N$

      $v_1^{(n+1)} = u_2(u_2v_2^{(n)} + u_2d) \ \% \ N$

  return FALSE

The case when $d \equiv 1 \mod 4$ is similar. An integral basis for $\mathcal{O}_K$, in this case, is $\{1, \frac{1+\sqrt{d}}{2}\}$. Let u be the fundamental unit of $\mathcal{O}_K$. For each co-prime residue class of β, with class representative $r = r_1 + r_2(\frac{1+\sqrt{d}}{2})$, we would, again, like to find a natural number n and a choice of sign such that

$$\pm(u^n) \equiv r \mod \beta.$$

This is equivalent to solving

$$\pm(u^n) - r = \beta\big(x + y(\tfrac{1+\sqrt{d}}{2})\big)$$

for some $m \in \mathbb{N}$, $x, y \in \mathbb{Z}$ and choice of sign. Our algorithm will iterate m over the interval

1 to $N_K(\beta)$, hence, for the time being, we will let $v = \pm(u^m)$ where we have fixed m and some choice of sign. We may write

$$v = v_1 + v_2\left(\tfrac{1+\sqrt{d}}{2}\right)$$

for some $v_1, v_2 \in \mathbb{Z}$ and

$$\beta = b_1 + b_2\left(\tfrac{1+\sqrt{d}}{2}\right)$$

where $b_1, b_2 \in \mathbb{Z}$. Showing that r is represented by the unit v is equivalent to solving the following system of equations:

$$\begin{bmatrix} b_1 + \frac{b_2}{2} & \frac{2b_1+b_2(1+d)}{4} \\ \frac{b_2}{2} & \frac{b_1+b_2}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} v_1 - r_1 + \frac{u_2}{2} - \frac{r_2}{2} \\ \frac{v_2}{2} - \frac{r_2}{2} \end{bmatrix}.$$

Solving for x, y gives

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{N_K(\beta)} \begin{bmatrix} b_1 + b_2 & -b_1 - \frac{b_2(1+d)}{2} \\ -b_2 & 2b_1 + b_2 \end{bmatrix} \begin{bmatrix} v_1 - r_1 + \frac{u_2}{2} - \frac{r_2}{2} \\ \frac{v_2}{2} - \frac{r_2}{2} \end{bmatrix}.$$

Notice that, if the following congruences hold, then r is represented by the unit v.

$$(b_1 + b_2)(v_1 - r_1 + \tfrac{v_2}{2} - \tfrac{r_2}{2}) - \left(b_1 + \tfrac{b_2(1+d)}{2}\right)\left(\tfrac{u_2}{2} - \tfrac{r_2}{2}\right) \equiv 0 \mod N_K(\beta)$$
$$b_1(v_1 - r_1 + \tfrac{v_2}{2} - \tfrac{r_2}{2}) + (2b_1 + b_2)\left(\tfrac{v_2}{2} - -\tfrac{r_2}{2}\right) \equiv 0 \mod N_K(\beta).$$

3.3 Results and Further Research

Clark and Murty proved that in $\mathbb{Z}[\sqrt{14}]$ no three primes can form an admissible set primes. We were interested to see how frequently an individual prime in $\mathbb{Z}[\sqrt{14}]$ was admissible. Figure 3.1 shows that 61.25 % of the first 80 non-ramified, split primes are admissible. We also found pairs of primes which formed admissible sets together. For example,

$\{3+\sqrt{14}, 5+2\sqrt{14}\}$ is a set of admissible primes.

Admissible Primes Among Non-Ramified Primes in $\mathbb{Z}[\sqrt{14}]$

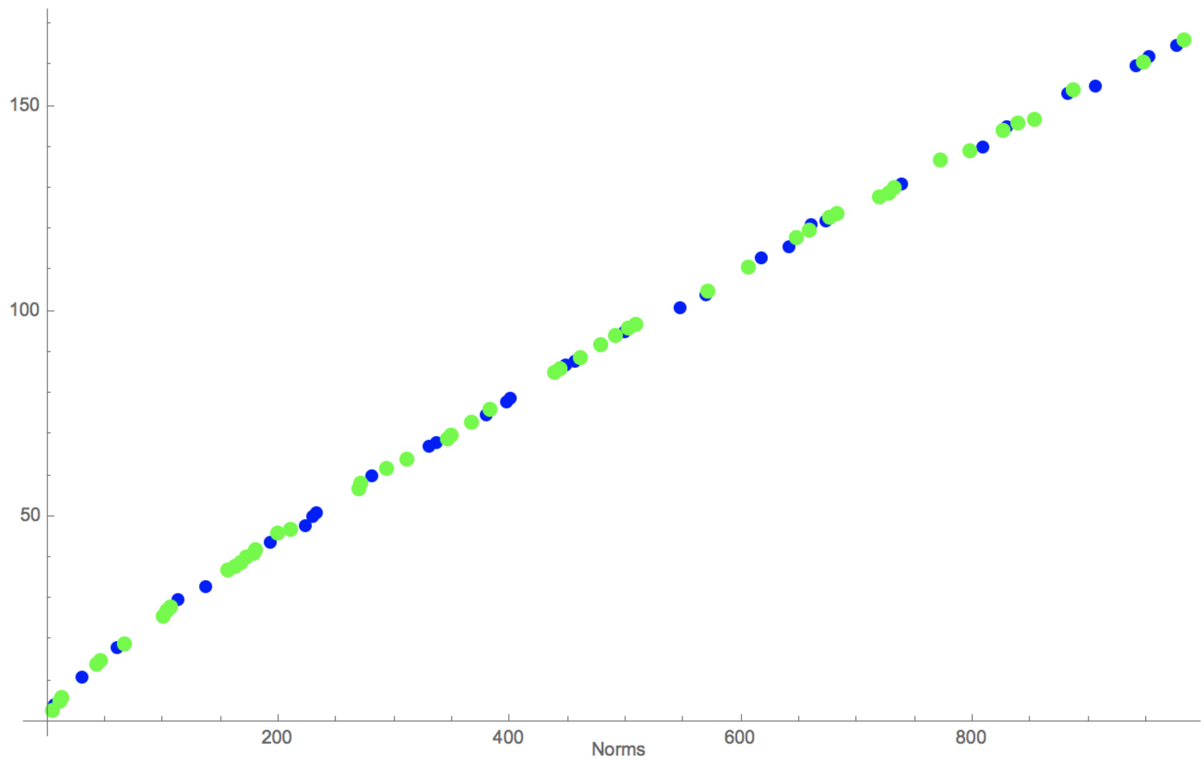

Figure 3.1: The blue dots are the norms of the first 80 non-ramified, split primes in $\mathbb{Z}[\sqrt{14}]$ and the green dots are the admissible primes. 61.25 % of the first 80 non-ramified, split primes in $\mathbb{Z}[\sqrt{14}]$ are admissible primes.

We we also ran our algorithm on $\mathbb{Z}[\sqrt{2}]$, and in this case 60.52 % of the first 76 non-ramified, split primes were admissible (see Figure 3.2). Thus we do not initially see a significant distinction between the frequency of primes being admissible for rings which are norm-Euclidean ($\mathbb{Z}[\sqrt{2}]$) and rings which are not norm-Euclidean ($\mathbb{Z}[\sqrt{14}]$).

Admissible Primes Among Non-Ramified Primes in $\mathbb{Z}[\sqrt{2}]$

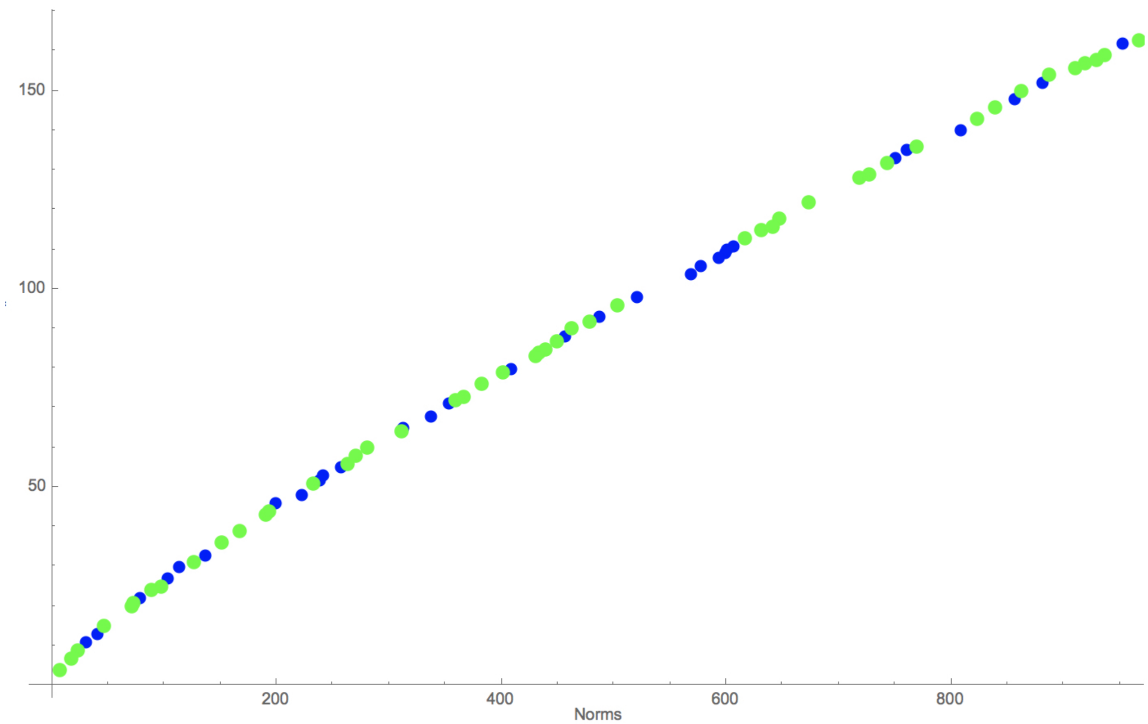

Figure 3.2: The dots are the norms of the first 76 non-ramified, split primes in $\mathbb{Z}[\sqrt{2}]$ and the green dots are the admissible primes. 60.52 % of the first 76 non-ramified, split primes in $\mathbb{Z}[\sqrt{2}]$ are admissible primes.

Bibliography

[1] David A. Clark and M. Ram Murty, *The Euclidean algorithm for Galois extensions of* **Q**, J. Reine Angew. Math. **459** (1995), 151–162. MR 1319520

[2] P. M. Cohn, *On the structure of the* GL_2 *of a ring*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 30, 5–53. MR 0207856

[3] Chris C. Conidis, Pace P. Nielsen, and Vandy Tombs, *Transfinitely valued euclidean domains have arbitrary indecomposable order type*, Submitted (2017).

[4] George E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I*, J. Reine Angew. Math. **282** (1976), 133–156. MR 0406973

[5] Jean-Jacques Hiblot, *Correction à une note sur les anneaux euclidiens*, C. R. Acad. Sci. Paris Sér. A-B **284** (1977), no. 15, A847. MR 0435058

[6] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723

[7] Franz Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Exposition. Math. **13** (1995), no. 5, 385–416. MR 1362867

[8] H. W. Lenstra, Jr., *Lectures on euclidean rings*, `https://www.math.leidenuniv.nl/~hwl/PUBLICATIONS/pub.html`, 1974, pp. 1–93.

[9] Th. Motzkin, *The Euclidean algorithm*, Bull. Amer. Math. Soc. **55** (1949), no. 12, 1142–1146. MR 0032592

[10] Masayoshi Nagata, *On Euclid algorithm*, C. P. Ramanujam—a tribute, Tata Inst. Fund. Res. Studies in Math., vol. 8, Springer, Berlin-New York, 1978, pp. 175–186. MR 541021

[11] Pierre Samuel, *About Euclidean rings*, J. Algebra **19** (1971), no. 2, 282–301. MR 0280470

[12] L. N. Vaserstein, *Bass's first stable range condition*, Proceedings of the Luminy conference on algebraic K-theory (Luminy, 1983), vol. 34, 1984, pp. 319–330. MR 772066

Appendix A. Mathematica Implementation of Algorithm 3.1

```
In[1]:= (*
return an unramified prime with norm of the nth prime or 0 if no
 such prime exists;
n: nth prime you would like to solve for;
*)
findprime[n_, d_] := Module[{sol},
  sol = Solve[s^2 - d*t^2 == Prime[n] && s > 0 && t > 0, {s, t}, Integers];
  If[sol == {},
   sol = Solve[s^2 - d*t^2 == -Prime[n] && s > 0 && t > 0, {s, t}, Integers];
  ];
  Simplify[sol /. C[1] → 0]
 ]
prime[n_, d_] := Module[{M, f},
  If[findprime[n, d] == {}, Return[{0, 0}];, f = findprime[n, d]];
  M = {s, t} /. f[[1]];
  {M[[1]], M[[2]]}
 ]

(*
Z[√d] with fundamental unit fund1+fund2√d;
range: this is the range of the prime position which you desire
  to see if a prime in the d exists;
example: to check the first 3 primes write {1,3}
*)
admissibleprimes[d_, fund1_, fund2_, lowerRangeLimit_, upperRangeLimit_] :=
 Module[{j, p1, p2, p, normp, S, i, b, b1, b2, normb, r, n, u1, u2, u,
   ClassGood, endNloop, T, u1p, u2p, AdmissiblePrimes, AdmissiblePrimeNorms,
   PrimePosition, k, m, prime1},
  AdmissiblePrimes = {}; (*primes in d which are admissible*)
  AdmissiblePrimeNorms = {}; (*norms of the admissible primes*)
  PrimePosition = {}; (*the when the admissible prime was found
   in the while loop*)
  (*This for loop runs through the primes of Z and then uses the
   findprime function to find a ramified prime to test for admissiblity*)
  For[j = lowerRangeLimit, j < upperRangeLimit, j ++,
   prime1 = prime[j, d];
   {p1, p2} = prime1;
   If[IntegerQ[p1] == False || IntegerQ[p2] == False,
    p = 0,
    p = p1 + p2 * Sqrt[d]
   ];
```

```
normp = AlgebraicNumberNorm[p, Extension -> Sqrt[d]];
If[p ≠ 0,
 (*In Clark and Murty's paper
  "The Euclidean algorithm for Galois extensions of Q" (pg 160)
  they prove that it is enough to show that every relativily
  prime residue class of p and p^2 can be represented by a
  unit. This for loop tests p and p^2 to see if every coprime
  residue class can be represented by a unit*)
 S = {};
 b = p^2; (*this is the element for which we are testing
   admissiblity. We can write b = b₁+b₂√d*)
 b1 = First[Expand[b]]; (*b₁ of b = b₁+b₂√d*)
 b2 = (Expand[b] - b1) / Sqrt[d]; (* b₂ of b = b₁+b₂√d *)
 normb = AlgebraicNumberNorm[b, Extension -> Sqrt[d]];
 r = PrimitiveRoot[Abs[normb]];
 (* generator of class that we are testing to see if it can
  be reprensented by a unit*)
 n = 1;
 u1 = fund1;
 u2 = fund2;
 u = u1 + u2 √d; (*fundamental unit*)
 ClassGood = 0;
 (* 0: the class was not represented by a unit,
 1: class was represented by a unit*)
 endNloop = Abs[normb]; (* we only need to check powers of the
  fundamental unit up to the norm of b*)
 (* this while loop checks to see if the class can be represented
  by a unit by solving the system of equations of integer
  solutions for x and y;
 (b₁  d(b₂)) (x) = (u₁-r)
 (b₂    b₁ ) (y)   ( u₂ );
 b = b₁+b₂√d (element we are testing for admissiblity);
 x+y√d is a general element;
 ±u^n = u₁+u₂√d is a power of the fundamental unit;
 Which has integer solutions iff b₁(u₁-r)-d(b₂u₂)=0 mod norm(b)
     and b₁u₂-b₂(u₁-r)=0 mod norm(b);
 *)
 While[n ≤ endNloop,
  If[(Mod[b1 * (u1 - r) - d * b2 * u2, normb] == 0 &&
     Mod[-b2 * (u1 - r) + b1 * u2, normb] == 0) ,
   ClassGood = 1; (*the class was represented*)
   n = endNloop, (*we don't need to keep checking*)
   (*this tests to see is -u^n is a representative if u^n is not*)
   If[Mod[b1 * (-u1 - r) + d * b2 * u2, normb] == 0 &&
     Mod[-b2 * (-u1 - r) - b1 * u2, normb] == 0,
```

```
     ClassGood = 1; (*the class was represented*)
     n = endNloop (*we don't need to keep checking*)
    ]
   ];
   u1p = Mod[fund1 * u1 + (fund2 * d) * u2, normb];
   (*first position of next power of fund unit mod norma*)
   u2p = Mod[fund2 * u1 + fund1 * u2, normb];
   (*second position of next power of fund unit mod norma*)
   u1 = u1p; (*reset u1 to next power*)
   u2 = u2p; (*sete u2 to next power*)
   n = n + 1;
  ];
  If[ClassGood == 1, AppendTo[S, b];
   AppendTo[PrimePosition, j];
   AppendTo[AdmissiblePrimeNorms, Prime[j]];
   AppendTo[AdmissiblePrimes, p];
  ]
 ];
];
Return[{AdmissiblePrimes, AdmissiblePrimeNorms, PrimePosition}];
]
```