On Euclidean Ideal Classes

by

Hester K. Graves

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in the University of Michigan
2009

Doctoral Committee:

Assistant Professor Nicholas Adam Ramsey, Chair
Professor Jeffrey C. Lagarias
Associate Professor Mattias Jonsson
Assistant Professor Christopher J. Hall
Lecturer Melvyn Levitsky
Professor Christopher M. Skinner, Princeton University

This is dedicated to the memory of my father, who always believed I could do this.

Acknowledgments

This dissertation was not written in a vacuum. It started when Chris Skinner gave me Treatman's article "Euclidean Systems," which sparked my interest in Euclidean ideal classes. Jeff Lagarias then gave me Harper and Murty's articles. After I told Nick that I was interested in working on a version of Motzkin's Lemma for Euclidean ideal classes, he realized it would be a good idea to try to adapt their methods to the situation.

Once I knew the problem I was working on, there were many people who were willing to talk to me about my research. I would like to thank M. Ram Murty, Mel Hochster, Djordje Milicevic, Don Lewis, Toby Stafford, Chelsea Walton, Kelli Talaska, Dave Anderson, Ryan Kinser, Marie Snipes, and my fellow number theory students for their time and attention. Among the number theory students, I would particularly like to thank Leo Goldmakher, Ben Weiss, and John Bober for their friendship, comraderie, and assistance. I would also like to thank Malcolm Harper for his help and encouragement, as well as giving me a copy of his thesis. Jeffrey Lagarias has been an invaluable resource throughout, reading my work and giving me suggestions. I appreciate him being my "cheerleader."

My readers have gone above and beyond the call of duty. Nick Ramsey and Chris Hall have gone over my thesis with a fine-tooth comb. Chris Skinner has made useful comments throughout. Someone recently quoted to me that twenty-five percent of math dissertations are wrong. I am lucky to have had so much help ensuring my work is correct.

I would like to thank my dissertation committee members. I am fortunate that each of you has played a real role in my life, outside of being on my committee. In addition, I would like to thank Tara Caldwell, Bert Ortiz, Warren Noone, and Jocelyn Rhoades for all the administrative aid that has allowed me to graduate.

I am grateful to my friends, especially Jesse Metcalf-Burton, Kelli Talaska, Brennan Dorn, Dave Anderson, Chelsea Walton, and my trivia, knitting, and math beer gangs for helping me enjoy my time here. Thanks to my family for taking the time to listen to me when I was stuck on my research, even though I was speaking an alien language. I would like to thank Richard Isaacson and Stanley Chang for their support and for helping me navigate the job market. Thanks to Loren for the constant love and tech support.

Lastly, none of this could have happened without Nick Ramsey. Many advisors meet with their graduate students a handful of times; when work was most intense, I met with Nick that often a week. He knew when to challenge me and when to reassure me. He pushed me beyond what I thought were my limits and comforted me when my father was ill. I do not know if I would have been able to graduate without him. I was not sure I wanted to do research when I started working with him, only to discover I loved talking about problems. I found myself excited to work after most of our meetings. I am glad we have other projects in the works because I have found that I love working with him. Lastly, I am so glad he spent the time teaching me how to write mathematics. I will carry the skills and insights he gave me for the rest of my life. I could not have asked any more from him.

Table of Contents

List of Figures

CHAPTER 1

INTRODUCTION

In abstract algebra courses, the first way a student learns to prove a ring is principal is by using the Euclidean algorithm. Usually, this is taught by using the norm function to prove that $\mathbb{Z}$ and $\mathbb{Z}[i]$, both rings of integers of number fields, are principal ideal domains. What is not usually covered is that the norm is not the only function that can be used as a Euclidean algorithm. In fact, there are some rings that are Euclidean but not norm-Euclidean, like the ring of integers of $\mathbb{Q}(\sqrt{69})$ ([**1**]).

Definition 1.0.1. — Given a ring R and a well ordered set W, a map $\phi : R \setminus 0 \longrightarrow W$ is a *Euclidean algorithm* as long as, for any elements a and b in R with $b \neq 0$, there exist some elements q and r in R such that

$$a = qb + r, \text{ with either } \phi(r) < \phi(b) \text{ or } r = 0.$$

Just like the norm function, any function satisfying the conditions above can be used to find the greatest common divisor of two elements, implying principality of all ideals. An integral domain with a Euclidean algorithm is called a *Euclidean domain.*

Number fields with norm-Euclidean rings of integers have an interesting property. By definition, if $\mathscr{O}_K$ is norm-Euclidean, then for any a and b in $\mathscr{O}_K$ with $b \neq 0$, there exists some q and r in $\mathscr{O}_K$ such that $\mathrm{Nm}(a - qb) = \mathrm{Nm}(r) < \mathrm{Nm}(b)$. If we divide through by the norm of b, we can then see that $\mathrm{Nm}(\frac{a}{b} - q) < 1$. There is therefore an equivalent statement that given a number field K, the ring of integers of K is norm-Euclidean if and only if for every x in K, there exists some y in $\mathscr{O}_K$ such that $\mathrm{Nm}(x - y) < 1$. Note that y is an element of $\mathscr{O}_K$ and that 1 is the norm of $\mathscr{O}_K$. In [**8**], Lenstra asked what would happen if $\mathscr{O}_K$ were replaced by some non-zero ideal C. He then defined the ideal C to be *Euclidean for the norm* if, for all $x \in K$, there exists some $y \in C$ such that

$$\mathrm{Nm}(x - y) < \mathrm{Nm}(C).$$

If C is Euclidean for the norm, then so is every other ideal in its ideal class, and in this case we will call the class $[C]$ is a *norm-Euclidean ideal class* (see Proposition 3.1.4). Interestingly enough, the ring $\mathscr{O}_K$ can have at most one norm-Euclidean ideal class ([**8**]). As before, the norm is not the only function that can be a Euclidean algorithm for an ideal. This inspired Lenstra to come up with Definition 1.0.3 below. In order to state it, though, we first need the following terminology.

Definition 1.0.2. — Let R be a Dedekind domain. A *fractional ideal* is an element in the set $\{\frac{1}{b}I \mid b \in R \setminus 0, I \text{ is an ideal of } R\}$. Henceforth, unless otherwise stated, all ideals in this paper are fractional. Ideals that are properly contained in R are called *integral ideals.* For the rest of the paper, given a Dedekind domain R, let E be the set of fractional ideals of R that contain R itself. For example, if $\frac{1}{b}I$ is in E, then b is an element of I.

Definition 1.0.3. — Let R be a Dedekind domain, let C be a non-zero ideal, let W be a well-ordered set, and let ϕ be a function from E to W. We say that ϕ is an *Euclidean algorithm for C* if, given any I in E and any x in IC, with $x \notin C$ (i.e. $x \in IC \setminus C$), there exists some $y \in C$ such that

$$\phi((x+y)^{-1}IC) < \phi(I).$$

As before, this condition depends only on the ideal class of C, so if C has a Euclidean algorithm, then we call $[C]$ an *Euclidean ideal class.*

The usual reason that people want to know whether or not a ring is a Euclidean domain is because Euclidean domains are principal ideal domains. In particular, Euclidean Dedekind domains have trivial class group. The importance of Euclidean ideal classes is that a Dedekind domain with a Euclidean ideal class has cyclic class group. In fact, if R is a Dedekind domain with Euclidean ideal class $[C]$, then $[C]$ generates the class group (see Proposition 3.1.7).

Going back to our original motivation, given a number field K with trivial class group, it makes sense to ask whether $\mathscr{O}_K$ is Euclidean or not. In 1973, Weinberger ([**11**]) proved, modulo the generalized Riemann hypothesis, that if K is a number field with trivial class group and if $\mathscr{O}_K$ has infinitely many units, then the ring $\mathscr{O}_K$ is a Euclidean domain.

This then suggests the question: when do number fields with cyclic class group have a Euclidean ideal class? Lenstra proved that if one assumes the generalized Riemann hypothesis, then for every number field with infinitely many units and cyclic class group, each generator of the class group is a Euclidean ideal class. Other than this one theorem, the author knows of no result in the literature implying that if K has a Euclidean ideal class, then it has any other Euclidean ideal classes.

Both Weinberger's and Lenstra's results assume the generalized Riemann hypothesis, so the next question to ask is whether they can be proved without assuming the Riemann hypothesis. Malcolm Harper was able to partially prove Weinberger's theorem without assuming the Riemann hypothesis by using analytic techniques and a reformulation of the Euclidean algorithm called Motzkin's construction.

1.1. Motzkin's Lemma for Elements

For the rest of this section, assume that all Euclidean algorithms are $\mathbb{N}$-valued, i.e. that the well-ordered set W in the definitions above is $\mathbb{N}$. Motzkin's construction for elements is useful because one can start with any ring and the construction will determine whether or not it has a Euclidean algorithm without one having to find such an algorithm.

Definition 1.1.1. — (Motzin's Construction for Elements) Given a domain R, let $A_0 := \{0\} \cup R^{\times}$, so it contains zero and all the units. Let

$$A_i = A_{i-1} \cup \left\{ a \in R \;\middle|\; \begin{array}{c} \forall\, x \in R,\ \exists\, y \in A_{i-1} \\ \text{such that } x - y \in (a) \end{array} \right\}$$

for $i > 0$, and let $A := \cup_{i=0}^{\infty} A_i$. If $A = R$, then let us define $\phi : A \longrightarrow \mathbb{N}$, where $\phi(x) = i$ if x is an element of $A_i \setminus A_{i-1}$.

Lemma 1.1.2. — *(Motzkin's Lemma for Elements) An integral domain R has a Euclidean algorithm if and only if every element of R is in A.*

Motzkin's construction for elements does not just determine whether or not R has a Euclidean algorithm mapping to $\mathbb{N}$; it constructs a canonical 'least' algorithm mapping to $\mathbb{N}$, the map ϕ, defined above. The only such algorithm explicitly computed in the literature is for the ring $\mathbb{Z}$. No others have been computed since the publication of Motzkin's paper in 1929. This paper includes nontrivial upper bounds for the least algorithm from $\mathbb{Z}[i]$ to $\mathbb{N}$.

Harper ([**5**]) modified Motzkin's construction for elements so that the only elements in the construction are zero, units, and primes. Harper was then able to use analytic methods to study the growth of these sets.

Definition 1.1.3. — (Harper's Construction for Elements) Given a domain R, let $B_0 = \{0\} \cup R^{\times}$, so that B_0 is the set containing zero and all the units. For i greater than zero, let

$$B_i = B_{i-1} \cup \left\{ \text{primes } p \in R \;\middle|\; \begin{array}{c} \forall\, x \in R,\ \exists\, y \in B_{i-1} \\ \text{such that } x - y \in (p) \end{array} \right\}$$

and let $B = \cup_{i=0}^{\infty} B_i$.

He also had to use Dirichlet's theorem on primes in arithmetic progressions in order to prove Lemma 1.1.4 below.

Lemma 1.1.4. — *(Harper's Lemma for Elements) Given a number field K with trivial class group, if B contains every prime element of $\mathscr{O}_K$, then $\mathscr{O}_K$ is a Euclidean domain.*

Note that every set B_i in the construction, for $i \neq 0$, is a set of primes, which lends itself to estimating its size via analytic methods and sieving techniques. Moreover, there is an intelligent way to augment B_0 so that these sets grow more quickly and the lemma still holds. The aim is to say that if one of the B_i grows quickly enough, then every prime element is contained in B and therefore the ring R is Euclidean.

Harper used the large sieve for number fields to construct general machinery that shows that if any of the B_i grows quickly enough then every prime element is contained in B and therefore R is a Euclidean domain. In particular, if we define $B_i(x)$ to be $|\{p : \mathrm{Nm}(p) \leq x, p \in B_i\}|$ and $B_i(x) >> \frac{x}{\log^2 x}$ for some positive integer i, Harper ([**5**]) shows that the ring R is Euclidean. This machinery is general enough that it can even be applied to the situation where B_0 is augmented in the manner alluded to above.

Harper then found a way to use the Gupta-Murty bound ([**5**]) to show that, in specific instances, he could force B_1 to grow quickly. He then applied the large sieve for elements to show the associated ring was a Euclidean domain. Using the Gupta-Murty bound followed by his large sieve machinery, he was able to show that $\mathbb{Z}[\sqrt{14}]$ is Euclidean, even though it is not norm-Euclidean.

Analogously, it makes sense to ask if Lenstra's result on Euclidean ideal classes can be proved without assuming the generalized Riemann hypothesis. A natural way to do this would be to try to adapt Harper's techniques to Euclidean ideal classes. Unfortunately, the constructions and tools he used do not apply to Euclidean ideal classes. In order to use them, they need to be reformulated for ideal classes.

1.2. A Motzkin-type Lemma for C

Motzkin's construction for ideal classes yields immediate results supporting Lenstra's theorem modulo the Riemann hypothesis. Everything in this section is new work.

Definition 1.2.1. — (*Motzkin's Construction for Ideals, Relative to C*) If R is a Dedekind domain and C is a non-zero ideal, let $A_{0,C} := \{R\}$, so that it is a one element set, where the one element is the ideal R. For

i greater than zero, let

$$A_{C,i} = A_{C,i-1} \cup \left\{ I^{-1} \;\middle|\; \begin{array}{c} I \text{ is an ideal contained in } R \text{ and} \\ \forall\, x \in I^{-1}C \setminus C,\ \exists\, y \in C \\ \text{such that } (x-y)^{-1}I^{-1}C \in A_{C,i-1} \end{array} \right\}$$

and let $A_C := \cup_{i=0}^{\infty} A_{i,C}$.

Lemma 1.2.2. — *(Motzkin's Lemma for Ideal Classes) Given a Dedekind domain R and a non-zero ideal C, if every ideal in E is contained in A_C, then $[C]$ is a Euclidean ideal class.*

Another variation of the construction is needed in order to apply a general machinery inspired by Harper. The new sets will consist of R and inverses of prime ideals, which lend themselves more easily to sieving techniques than generic sets of ideals that contain the entire ring.

Definition 1.2.3. — *(Harper's Construction for Ideals, Relative to C)* If R is a Dedekind domain and C is a non-zero ideal, let $B_{0,C}$ be $\{R\}$. For $i > 0$, let

$$B_{C,i} = B_{C,i-1} \cup \left\{ \mathfrak{p}^{-1} \;\middle|\; \begin{array}{c} \mathfrak{p} \subseteq R \text{ is prime, and} \\ \forall\, x \in \mathfrak{p}^{-1}C \setminus C,\ \exists\, y \in C \\ \text{such that } (x-y)^{-1}\mathfrak{p}^{-1}C \in B_{C,i-1} \end{array} \right\}$$

and let $B_C = \cup_{i=0}^{\infty} B_{C,i}$.

Lemma 1.2.4. — *(Harper's Lemma for Ideals, Relative to C) If K is a number field and $\mathfrak{p}^{-1}$ is an element of B_C for all prime ideals $\mathfrak{p}$ in $\mathscr{O}_K$, then $[C]$ is a Euclidean ideal class.*

The proof uses the Chebotarev density theorem applied to a well-chosen ray class field in an analogous fashion to the use of Dirichlet's theorem on primes in arithmetic progressions to prove Lemma 1.2.4. The set $B_{C,i}$ are more amenable to growth analysis than the sets $A_{i,C}$ are. In order to create general machinery like Harper's, however, his tools will have to be adapted to the Euclidean ideal class framework.

1.3. The Large Sieve for Elements and Ideals

The large sieve is the heart of Harper's general machinery. The usual large sieve measures how a set of finitely many elements is distributed among the congruence classes of various primes. Note below how the elements in the finite set must be non-associate. In other words, no element in the set is the product of a unit and another element in the set.

Definition 1.3.1. — Given a prime ideal $\mathfrak{p}$, $\alpha \in \mathscr{O}_K$, and a finite set of non-associated integers A, let

$$Z(\alpha, \mathfrak{p}) := |\{x \in A \mid x \equiv \alpha \pmod{\mathfrak{p}}\}| \,.$$

Now that we have Definition 1.3.1, we can state the version of the Large Sieve in [**12**]. It is sometimes called the "Statistical Version" of the Large Sieve.

Theorem 1.3.2. — ***(The Large Sieve)***
Let K be a number field, let A a finite set of non-associate algebraic integers and let P a finite set of prime ideals. If $X = \max_{x \in A} |\mathrm{Nm}(x)|$ and if $Q = \max_{\mathfrak{p} \in P} \mathrm{Nm}(\mathfrak{p})$, then

$$\sum_{\mathfrak{p} \in P} \mathrm{Nm}(\mathfrak{p}) \sum_{\alpha \in R/\mathfrak{p}} \left(Z(\alpha, \mathfrak{p}) - \frac{|\, A \,|}{\mathrm{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + X)\, |A|,$$

where the implied constant depends only on K.

The issue of associate elements comes up again with the adaptation of the large sieve to ideal classes. In order to reformulate the large sieve appropriately, we need the following definitions.

Definition 1.3.3. — For a number field K and a prime ideal $\mathfrak{p}$, we define $f(\mathfrak{p})$ to be the number of equivalence classes of elements modulo $\mathfrak{p}$ that are represented by a unit, i.e.

$$f(\mathfrak{p}) := |\{ \overline{\alpha} \in \mathscr{O}_K/\mathfrak{p} \mid (\alpha - u) \in \mathfrak{p} \text{ for some } u \in \mathscr{O}_K^{\times} \}| \,.$$

The following definition and theorem are new.

Definition 1.3.4. — Let K be a number field and let C be a non-zero ideal. Suppose A is a finite set of fractional ideals in E such that if I

and J are in A, then $[I] = [J]$. Then for any prime ideal $\mathfrak{p}$ such that $[\mathfrak{p}^{-1}] = [IC^{-1}]$ for an ideal I in A and for any α in $\mathfrak{p}^{-1}C$, we define

$$Z(\alpha, \mathfrak{p}, C) := \begin{cases} \left| \left\{ \begin{array}{c} I \in A \mid \exists\, y \in C \text{ such that} \\ (\alpha + y)^{-1}\mathfrak{p}^{-1}C = I \end{array} \right\} \right| & \alpha \notin C \\ f(\mathfrak{p}) \left| \left\{ \begin{array}{c} I \in A \mid \exists\, y \in C \text{ such that} \\ (\alpha + y)^{-1}\mathfrak{p}^{-1}C = I \end{array} \right\} \right| & \alpha \in C \end{cases}.$$

Using these definitions, we can now state the large sieve for ideal classes.

Theorem 1.3.5. — (***Large Sieve with Respect to*** C)
Let K be a number field, C a non-zero ideal in $\mathscr{O}_K$, and n an integer. Suppose A is a finite set of ideals containing $\mathscr{O}_K$ such that given two ideals I and J in A , $[I] = [J]$. Suppose P is a finite set of prime ideals $\mathfrak{p}$ such that $[\mathfrak{p}^{-1}] = [IC^{-1}]$ for any ideal I in A. If $X = \max_{I \in A} \mathrm{Nm}(I^{-1})$ and $Q = \max_{\mathfrak{p} \in P} \mathrm{Nm}(\mathfrak{p})$, then

$$\sum_{\mathfrak{p} \in P} \mathrm{Nm}(\mathfrak{p}) \sum_{\alpha \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\alpha, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + X)\, |A|\,.$$

The implied constant depends only on K and the ideal class of C.

Now that we have a reformulation of the large sieve for ideal classes, we can then develop general machinery to apply to the variation of Motzkin's construction for ideal classes. Using this, we show that if $|\{I \in B_{2,C} \mid \mathrm{Nm}(I^{-1}) \leq x\}| >> \frac{x}{\log^2 x}$, then $[C]$ is a Euclidean ideal class. As in the previous case, we can intelligently augment the set $B_{1,C}$ and the machinery is still robust enough for the result to hold.

The way Harper augmented his sets B_i in a number field K was by finding a set of 'admissible' primes, and then adding the monoid generated by $\mathscr{O}_K^\times$ and these primes to his set. He could then still use his machinery to show that if the appropriate set grows 'quickly enough,' then the ring $\mathscr{O}_K$ is Euclidean. He did this because by augmenting his set by this monoid, the sets grew more quickly and he could then use the growth of early sets to show that B itself is sufficiently large.

Our goal is to find a way to apply our ideal class machinery to specific number fields. Due to technical obstructions, we could not augment our sets by the monoids Harper used. Instead, we concentrated on the concept of an 'admissible' set of primes. After tweaking that concept, we found and proved Theorem 1.3.7.

Definition 1.3.6. — Given a number field K, we denote the size of its classgroup by h_K.

Theorem 1.3.7. — ***(The Gupta-Murty Bound with Respect to*** C***)***
Let K be a number field; let C be a non-zero ideal; let m be an integer; let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be a set of distinct prime ideals, such that each $[\mathfrak{p}_i] = [C^m]$; and let $\mathfrak{M}$ be the set

$$\left\{\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k} \mid (a_1, \dots, a_k) \in \mathbb{N}^k,\ a_1 + \cdots + a_k \equiv m \ (mod\ h_K)\right\}.$$

If $\mathfrak{p}$ is a prime ideal such that $[\mathfrak{p}] = [C^{m+1}]$, then we define

$$\Gamma_{\mathfrak{p},\mathfrak{M}} := \left|\{\overline{\alpha} \in \mathfrak{p}^{-1}C/C, \overline{\alpha} \neq \overline{0} \,\middle|\, \exists\, y \in C \text{ such that } (\alpha+y)^{-1}\mathfrak{p}^{-1}C \in \mathfrak{M}\}\right| .$$

The set of primes $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^{m+1}]$ and $\Gamma_{\mathfrak{p},\mathfrak{M}} \leq y$ is $O(y^{\frac{k+1}{k}})$.

Suppose that there exists some set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, each $[\mathfrak{p}_i] = [C]$, such that for every k-tuple $(a_1, \ldots, a_k) \in \mathbb{N}^k$ with $a_1 + \cdots + a_k \equiv 1 \pmod{h_K}$, the ideal $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$ is in $A_{1,C}$. We can then augment the set $B_{1,C}$ with the set $\mathfrak{M}$ defined in Theorem 1.3.7 above and we can still apply our machinery to conclude that if $B_{2,C}$ grows quickly enough, then C is a Euclidean ideal class.

If the ideal class $[C]$ generates the class group and we can find at least two such primes (i.e. $k \geq 2$), then we can show that

$$|\{I \in B_{2,C} \mid \mathrm{Nm}(I^{-1}) \leq x\}| >> \frac{x}{\log^2 x}$$

and therefore $[C]$ is a Euclidean ideal class.

The one remaining challenge is finding an easy criterion to test whether two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, $[\mathfrak{p}_1] = [\mathfrak{p}_2] = [C]$, indeed satisfy the condition that for any natural numbers a_1 and a_2 such that $a_1 + a_2 \equiv 1 \pmod{h_K}$, then the ideal $\mathfrak{p}_1^{-a_1}\mathfrak{p}_2^{-a_2}$ is in $A_{1,C}$. Once that condition is found and proven, the results stated earlier imply that any number field with infinitely many units[1] and two prime ideals satisfying that condition has a Euclidean ideal class.

[1] This is a condition that will be required.

CHAPTER 2

THE EUCLIDEAN ALGORITHM AND MOTZKIN'S LEMMA

Before studying Euclidean algorithms on ideals, we shall first review traditional $\mathbb{N}$-valued Euclidean algorithms on elements. Recall that the most common use of the Euclidean algorithm is showing that a ring is a principal ideal domain.

Definition 2.0.8. — Let R be a domain and let W be a well-ordered set. If ψ is a function, $\psi : R \setminus 0 \longrightarrow W$, and if for all elements a, b in R, $b \neq 0$, there exist some elements q, r in R such that $a = bq + r$, with either $r = 0$ or $\psi(r) < \psi(b)$, then ψ is a *Euclidean algorithm* on R. If R is a domain with a Euclidean algorithm, then R is a *Euclidean domain.*

Theorem 2.0.9. — *If R is Euclidean, then it is a principal ideal domain.*

Proof. — Let $\phi : R \setminus 0 \longrightarrow W$ be a Euclidean algorithm on R and let I be an ideal contained in R. If b is an element of $I \setminus 0$ with $\phi(b)$ the smallest element of $\phi(I \setminus 0)$, then given any $a \in I$, there exist $q, r \in R$

such that

$$a = bq + r, \phi(r) < \phi(b),$$

implying $r = 0$ and $b \mid a$. We therefore conclude $I = (b)$. □

The classic example of a Euclidean domain is $\mathbb{Z}$, where the absolute value is a Euclidean algorithm. The second most commonly taught example is $\mathbb{Z}[i]$, where both the norm and the square root of the norm, i.e. $\psi(a + bi) = \sqrt{a^2 + b^2}$, are Euclidean algorithms. In fact, Euclidean originally meant norm-Euclidean.

Definition 2.0.10. — If K is a number field and S is the set of field embeddings into $\mathbb{C}$, then we define the *norm* of an element x in K to be

$$\mathrm{Nm}(x) = \prod_{\sigma \in S} \sigma(x).$$

Definition 2.0.11. — Let K be a number field. If for all elements x of K, there exists some y in $\mathscr{O}_K$ such that $\mathrm{Nm}(x - y) < 1$, then $\mathscr{O}_K$ is called *norm-Euclidean*.

We can see that this is equivalent to having the norm be a Euclidean algorithm for $\mathscr{O}_K$. If x is a non-zero element of K, then it can be written as a quotient $\frac{a}{b}$, where a and b are elements of $\mathscr{O}_K$, with $b \neq 0$. If the norm is a Euclidean algorithm for $\mathscr{O}_K$, then there exist some y and r in $\mathscr{O}_K$ such that $a = yb + r$ and $\mathrm{Nm}(r) < \mathrm{Nm}(b)$. This implies that

$$\mathrm{Nm}(x - y) = \mathrm{Nm}\left(\frac{a}{b} - y\right) = \mathrm{Nm}\left(\frac{a - by}{b}\right) = \mathrm{Nm}\left(\frac{r}{b}\right) = \frac{\mathrm{Nm}(r)}{\mathrm{Nm}(b)} < 1$$

and we see that two definitions are indeed equivalent.

It was unknown until the work of David A. Clark whether there are any Euclidean integer rings that are not norm-Euclidean. In 1994 , Clark proved ([**1**]) $\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ is Euclidean but not norm-Euclidean. This means that, given a number field K, we cannot always use the norm to check whether or not $\mathscr{O}_K$ is Euclidean. Fortunately, in 1948, Theodore Motzkin ([**9**]) came up with a new way to look at Euclidean rings.

Definition 2.0.12. — (*Motzin's Construction for Elements*) Given a domain R, let $A_0 := \{0\} \cup R^\times$, so it contains zero and all the units. Let

$$A_i = A_{i-1} \cup \left\{ a \in R \;\middle|\; \begin{array}{c} \forall\, x \in R,\ \exists\, y \in A_{i-1} \\ \text{such that } x - y \in (a) \end{array} \right\}$$

for $i > 0$ and let $A := \cup_{i=0}^{\infty} A_i$. We call the sequence of nested sets A_i *Motzkin's Construction.*

If $A = R$, we define ϕ_R to be the function from $R \setminus 0$ to $\mathbb{N}$ such that $\phi_R(x)$ is i if x is an element of $A_i \setminus A_{i-1}$.

Lemma 2.0.13. — *Let R be a domain. Given an unit $u \in R^\times$ and an element $\beta \in A_i$, the element $u\beta$ is also in A_i. In other words, $uA_i = A_i$ for all i.*

Proof. — By definition, β is in A_i if every equivalence class modulo (β) is represented by an element of A_{i-1}. The ideals (β) and $(u\beta)$ are equal for any unit u, so the result holds. □

Theorem 2.0.14. — *(Motzkin's Lemma) If the domain R is equal to A, then R is a Euclidean domain.*

Proof. — Assume A equals R and let ϕ_R be the function in Definition 2.0.12. Given two elements a, b of R, $b \neq 0$, we know that either b divides a or there exists some $r \in A_{\phi_R(b)-1}$ such that $a - r$ is an element of the ideal (b). This means that there exist some $r, q \in R$ such that $a = qb + r$, where either $r = 0$ or $\phi_R(r) \leq \phi_R(b) - 1 < \phi_R(b)$. We conclude ϕ_R is a Euclidean algorithm and R is a Euclidean domain. □

Note that if R is a Euclidean domain, we need not have $R = A$ because there are Euclidean rings that have algorithms mapping to some well-ordered set W, but for which there is no $\mathbb{N}$-valued Euclidean algorithm.

Example 1. — *By Proposition 6 in* [**10**]*, the finite product of Euclidean rings is itself Euclidean, so $\mathbb{Z} \times \mathbb{Z}$ is Euclidean. On page 287 of* [**10**]*, it was shown there is no Euclidean algorithm from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{N}$.*

The real importance of Motzkin's Lemma is that one no longer needs to struggle trying to find a Euclidean algorithm in order to prove whether or not a ring R has a $\mathbb{N}$-valued Euclidean algorithm. Motzkin's Construction not only says whether or not there is a Euclidean algorithm mapping to $\mathbb{N}$, but it constructs the "least" one, if it exists (see Proposition 2.0.16 and Definition 2.0.17).

Definition 2.0.15. — Given a Euclidean ring R and a well-ordered set W, we define $\phi_W : R \longrightarrow W$, by $\phi_W(\alpha) := \inf_\phi \phi(a)$, where the infimum is taken over the set of all Euclidean algorithms from R to W.

Proposition 2.0.16. — *The map ϕ_W is a Euclidean algorithm from R to W.*

Proof. — Let α, β be elements of R, with $\beta \neq 0$. Since W is well-ordered, we know that in the set of all images of β under a Euclidean algorithm from R to W, there is a least element. This implies that there is some Euclidean algorithm ρ from R to W such that $\rho(\beta)$ is the least element in this set. By the definition of Euclidean algorithms, there exist some q, r in R such that

$$\alpha = \beta q + r, \text{ such that } r = 0 \text{ or } \rho(r) < \rho(b).$$

By the definition of ϕ_W in Definition 2.0.15, we know that

$$\phi_W(r) \leq \rho(r) < \rho(\beta) = \phi_W(\beta).$$

We therefore know that given two elements α, β of R, $\beta \neq 0$, there exist some $q, r \in R$ such that $a = bq + r$ with either $r = 0$ or $\phi_W(r) < \phi_W(\beta)$. We conclude that ϕ_W is a Euclidean algorithm from R to W. □

Definition 2.0.17. — Henceforth, we shall call ϕ_W the least algorithm from R to W. Note that it is unique.

Theorem 2.0.18. — *Given a domain R with a $\mathbb{N}$-valued Euclidean algorithm, the algorithm ϕ_R constructed in the proof of Motzkin's Lemma (Lemma 2.0.14) is the least Euclidean algorithm from R to $\mathbb{N}$. In other words, the functions $\phi_{\mathbb{N}}$ and ϕ_R are equal.*

In order to prove the theorem, we first need the following lemma.

Lemma 2.0.19. — *Let R be a domain and let ϕ be a $\mathbb{N}$-valued Euclidean algorithm for R. If $\phi(b)$ is minimal in $\phi(R)$, then b is a unit.(*[**10**]*)*

Proof. — If $\phi(b)$ is minimal in $\phi(R)$, then there exist some q and r in R such that $1 = qb + r$ and $r = 0$ or $\phi(r) < \phi(b)$. Our choice of b means that $r = 0$ and b divides 1, implying that b is a unit. □

Proof. — (Proof of Theorem 2.0.18) Let ρ be a Euclidean algorithm from R to $\mathbb{N}$, and let R_i be the set $\{0\} \cup \{\beta \in R : \rho(\beta) \leq i\}$. If β is a non-zero element of R_i, then for any α in R, there exist some $q, r \in R$ such that $\alpha = \beta q + r$, where either $r = 0$ or $\rho(r) < \rho(b)$, i.e. $r \in R_{i-1}$. This implies that $R_{i-1} \twoheadrightarrow R/(\beta)$ for all non-zero β in R_i.

We will show by induction that R_i is contained in A_i. By Lemma 2.0.19, we know that R_0 is contained in A_0. Assume that R_i is contained in A_i for all i less than k. We know from the paragraph above that $R_{k-1} \twoheadrightarrow R/(\beta)$ for all non-zero β in R_k. Since R_{k-1} is contained in A_{k-1}, this means that $A_{k-1} \twoheadrightarrow R/(\beta)$ for all non-zero β in R_k, implying said β is in A_k. We conclude tht R_k is contained in A_k.

In other words, if $\rho(\beta)$ is i, then $\phi(\beta)$ is less than or equal to i, so that $\phi_R(\beta) \leq \rho(\beta)$. We conclude that ϕ is the least Euclidean algorithm from R to W. $\square$

Example 2. — *Examples of Motzkin's Construction*

(1) *In* [**9**], *Motzkin showed that for the ring* $\mathbb{Z}$,

$$\begin{aligned} A_0 &= 0, \pm 1 \\ A_1 &= 0, \pm 1, \pm 2, \pm 3 \\ A_2 &= 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7 \\ &\vdots \\ A_i &= 0, \pm 1, \ldots \pm (2^{n+1} - 1). \end{aligned}$$

(2) *For the ring* $\mathbb{Z}[\sqrt{-5}]$, *we know that* $A_0 = 0, \pm 1$. *The norm of any principal ideal in* $\mathbb{Z}[\sqrt{-5}]$ *is of the form* $a^2 + 5b^2$. *From our computation of* A_0, *we know that any element in* $A_1 \setminus A_0$ *needs the absolute value of its norm to be less than or equal to three. The only numbers of the form* $a^2 + 5b^2$ *that are less than or equal to three are zero and one. Therefore the set* $A_1 \setminus A_0$ *is empty and* $A = \{0, \pm 1\}$. *We conclude the ring* $\mathbb{Z}[\sqrt{-5}]$ *does not have a Euclidean algorithm mapping to* $\mathbb{N}$. *This was already known, however, because the class number of* $\mathbb{Z}[\sqrt{-5}]$ *is not one.*

Note that while the norm is indeed a Euclidean algorithm for $\mathbb{Z}$ and $\mathbb{Z}[i]$, the least Euclidean algorithms from $\mathbb{Z}$ and $\mathbb{Z}[i]$ to $\mathbb{N}$ found by Motzkin's construction are not the norm.

2.1. Harper's Lemma

Malcolm Harper invented a variation of Motzkin's construction that uses only units and primes. This is useful because, like the original Motzkin's construction, it constructs sets of elements, but Harper's sets are more tractable because they consist of units and prime elements. One can use known results from analytic number theory to study the asymptotic growth of these sets of units and prime elements in order to deduce whether or not a ring has a Euclidean algorithm mapping to $\mathbb{N}$.

Definition 2.1.1. — (Harper's Construction for Elements) Given a domain R, let $B_0 = \{0\} \cup R^{\times}$, so that B_0 is the set containing zero and all the units. For i greater than zero, let

$$B_i = B_{i-1} \cup \left\{ \text{primes } p \in R \;\middle|\; \begin{array}{c} \forall\, x \in R,\ \exists\, y \in B_{i-1} \\ \text{such that } x - y \in (p) \end{array} \right\}$$

and let $B = \cup_{i=0}^{\infty} B_i$.

We defined B_0 to be equal to A_0. Thus, arguing by induction on i, each B_i is contained in the A_i from Definition 2.0.12, and so B is contained in A.

Theorem 2.1.2. — *([**5**]) If K is a number field with trivial class group and every prime element p of $\mathscr{O}_K$ is in B, then $\mathscr{O}_K$ is Euclidean.*

Proof. — We follow [**5**] in this proof. If p is a prime element, let $\lambda(p) := i$ if $p \in B_i \setminus B_{i-1}$ and then extend λ to all elements of $\mathscr{O}_K$ additively, i.e.

$\lambda(p_i^{a_1} \cdots p_n^{a_n}) = a_1\, \lambda(p_1) + \cdots + a_n\, \lambda(p_n)$. The function λ is completely additive.

Let ω count the number of divisors, counting multiplicities, so that $\omega(p_1^{a_1} \cdots p_n^{a_n}) = a_1 + \cdots + a_n$. We shall now construct a new completely additive function $\phi : R \setminus 0 \longrightarrow \mathbb{N} \times \mathbb{N}$ from the two above functions: let

$$\phi(x) := (\omega(x), \lambda(x)),$$

where $\mathbb{N} \times \mathbb{N}$ is ordered lexicographically, with the first coordinate of higher order, so that $(0,0) < (1,0)$ and $(1,11) < (2,4)$.

We will now show that ϕ is a Euclidean algorithm. Let α and β be elements of $\mathscr{O}_K$, with β not equal to zero. Note that if α is zero, then for any β in R, we know that $\alpha = 0 \cdot \beta + 0$, so our conditions are trivially satisfied.

First, suppose that $(\alpha, \beta) = \mathscr{O}_K$, so that α and β are relatively prime.

If β is a unit, then $\alpha = \beta(\beta^{-1}\alpha) + 0$, where $\beta^{-1}\alpha$ is an element of $\mathscr{O}_K$.

If β is a prime and $\lambda(\beta) = i$ then, by the construction of B, there exists some prime or unit α' in B_{i-1} so that $\alpha \equiv \alpha' \pmod{\beta}$. Note that since α' is invertible modulo (β) because β is not a unit and (α, β) is the entire ring. If α' is an unit, then there exist $q, \alpha' \in \mathscr{O}_K$ such that $\alpha = q\beta + \alpha'$, with $\phi(\alpha') = (0,0) < (1,i) = \phi(\beta)$. If α' is prime, then there exist some q, α' in R such that $\alpha = q\beta + \alpha'$, where $\phi(\alpha') \leq (1, i-1) < (1,i) < \phi(\beta)$.

Suppose β is neither prime nor a unit. By Theorem 3.1.22, there exists some q in R and some prime p such that $\alpha = q\beta + p$, where $\phi(p) = (1, \lambda(p)) < (2, 0) < \phi(\beta)$.

Second, suppose that α and β, $\beta \neq 0$, do not generate the entire ring. Because K has class number one, we know that $(\alpha, \beta) = (\delta)$, where $\delta \neq 1$. Then by the above, there exists some $q, x \in R$ such that $\frac{\alpha}{\delta} = q\frac{\beta}{\delta} + x$, where $\phi(x) < \phi(\frac{\beta}{\delta})$. Recall that ϕ is completely additive, so that $\alpha = q\beta + x\delta$, where $\phi(x\delta) = \phi(x) + \phi(\delta) < \phi(\frac{\beta}{\delta}) + \phi(\delta) = \phi(\beta)$. □

Note that while this proof constructs a Euclidean algorithm for $\mathscr{O}_K$, it constructs one from $\mathscr{O}_K$ to $\mathbb{N} \times \mathbb{N}$ rather than $\mathbb{N}$. It turns out that we can use the above algorithm to show that $\mathscr{O}_K = A$, implying that there is a Euclidean algorithm from $\mathscr{O}_K$ to $\mathbb{N}$. The following proof shows the existence of such an algorithm, but does not construct it.

Proposition 2.1.3. — *If every prime element of $\mathscr{O}_K$ is in B, then there is a Euclidean algorithm from $\mathscr{O}_K$ to $\mathbb{N}$.*

Proof. — We shall prove this by double induction on the size of ω and of λ, where the functions are constructed as above in the proof of Theorem 2.1.2. We know that $B \subset A$, so that 0, the units, and all the prime elements are contained in A.

Suppose all $x \in \mathscr{O}_K \setminus 0$ such that $\omega(x) < i$ are contained in A. Because $\mathbb{N}$ is well-ordered, there is a least element in the set $\{\lambda(x) \mid \omega(x) = i\}$. Let $\lambda(y)$ be equal to this least element, so that $\omega(y) = i$. We know from the proof of Theorem 2.1.2 that for any $\alpha \in \mathscr{O}_K$, there exists some $q, r \in \mathscr{O}_K$

such that $\alpha = qy + r$, where $\phi(r) < \phi(y)$. Since $\lambda(y)$ is minimal in the set of all x in $\mathscr{O}_K$ with $\omega(x) = i$, this implies $\omega(r) < i$ and the element r is therefore in A. We conclude that y, and every y' such that $\lambda(y') = \lambda(y)$ and $\omega(y') = i$, is in A.

We shall now induce on the size of λ. Suppose all x in $\mathscr{O}_K \setminus 0$ such that $\omega < i$, or $\omega = i$ and $\lambda < k$, are in A. Let $\lambda(y)$ be the least element in the set $\{\lambda(x) \mid \omega(x) = i, \lambda(x) \geq k\}$. Then for any α in $\mathscr{O}_K$, there exists some $q, r \in \mathscr{O}_K$ such that $\alpha = qy + r$, where $\phi(r) < \phi(y)$. Since $\lambda(y)$ is minimal in our set, either $\omega(r) < i$, implying that r is in A, or $\omega(r) = i$ and $\lambda(r) < k$, implying that r is in A. We conclude that every x such that $\omega(x) = i$ is in A, and therefore that all of R is in A. The ring therefore has a $\mathbb{N}$-valued Euclidean algorithm. $\square$

While the condition in Theorem 2.1.2 and Proposition 2.1.3 is that every prime in $\mathscr{O}_K$ is in B, the proofs actually proved the results with the weaker condition that every prime of $\mathscr{O}_K$ be in A. The reason why the results were stated in terms of B is that in the case of number fields, we can apply analytic techniques to the sets B_i in order to not only find whether or not the ring of integers is Euclidean but also to find if it has a Euclidean algorithm mapping to $\mathbb{N}$. The latter is useful since it is an open question, conjectured to be true, whether or not all Euclidean rings of integers of number fields have a Euclidean algorithm mapping to $\mathbb{N}$. In order to use these analytic methods, we must first define the sets $B_n(x)$.

Definition 2.1.4. — Let $B_n(x)$ be the the set of all prime ideals (p), p in B_n, such that $|\mathrm{Nm}(p)| \leq x$, i.e.

$$B_n(x) := \{(p) \mid p \in B_n, |\mathrm{Nm}(p)| \leq x\}.$$

Let $B_n^c(x)$ be the set of all primes ideals (p) not in $B_n(x)$ such that $|\mathrm{Nm}(p)| \leq x$, i.e.

$$B_n^c(x) := \{(p) \mid p \notin B_n, |\mathrm{Nm}(p)| \leq x\}.$$

Most of the analytic methods will study the asymptotic growth of $|\,B_n(x)\,|$ as x goes to infinity. The idea is to show that if a given $|\,B_n\,|$ is "large enough," then all primes are contained in B and there is a Euclidean algorithm mapping from $\mathscr{O}_K$ to $\mathbb{N}$. In order to do this, we will need the following definition and lemma.

Definition 2.1.5. — Given two functions, $f(x)$ and $g(x)$, we write $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Lemma 2.1.6. — *Let K be a number field and let the B_n's be as in Definition 2.1.1. If $|\,B_n(x)\,| \sim \frac{x}{\log x}$ for some n, then all primes are contained in B_{n+1}.*

Proof. — Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_K$ and let α be relatively prime to $\mathfrak{p}$. We will show there is some $q \in B_n$ such that $\alpha \equiv q \pmod{\mathfrak{p}}$.

By the Landau prime ideal theorem, the number of prime ideals with norm less than or equal to x is asymptotically equivalent to $\frac{x}{\log x}$. In other words, if $\pi(x)$ represents the number of prime ideals with norm less than or equal to x, then $\lim_{x \longrightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$.

One of the most useful density results in number theory is the quantitative version of Dirichlet's theorem on arithmetic progressions, which states that density of prime elements congruent to α modulo $\mathfrak{p}$ in a number field K with trivial class group is $\frac{1}{\mathrm{Nm}(\mathfrak{p})-1}$. More precisely, if $\pi_{\alpha,\mathfrak{p}}(x)$ is the number of prime elements q such that $q \equiv \alpha \pmod{\mathfrak{p}}$ with $\mathrm{Nm}(q) \leq x$, then $\lim_{x \longrightarrow \infty} \frac{\pi_{\alpha,\mathfrak{p}}(x)}{\pi(x)} = \frac{1}{\mathrm{Nm}(\mathfrak{p})-1}$([**7**]).

Since the set of primes $q \equiv \alpha \pmod{p}$ has positive density and the set of primes in B_n has density one in the set of all primes in $\mathscr{O}_K$, the set of primes $q \equiv \alpha \pmod{p}$ has positive density in the set B_n. There therefore exists some $q \equiv \alpha \pmod{p}$ in B_n, implying $p \in B_{n+1}$ and thus all primes are in B_{n+1}

□

We can use Lemma 2.1.6 to prove the following theorem, which is the first real result using analysis to determine whether or not a ring of integers has a Euclidean algorithm mapping to $\mathbb{N}$.

Theorem 2.1.7. — *If K is a number field, if we construct B from $\mathscr{O}_K$ as in Definition 2.1.1, and if $|\, B_n(x)\,| \sim \frac{x}{\log x}$ for some n, then $\mathscr{O}_K$ is Euclidean and has a Euclidean algorithm mapping to* $\mathbb{N}$.

Proof. — By Lemma 2.1.6, if $\mid B_n(x) \mid \sim \frac{x}{\log x}$, then all primes are in B_{n+1} and therefore all primes of $\mathscr{O}_K$ are in B. We conclude $\mathscr{O}_K$ is Euclidean by Theorem 2.1.2 and has a Euclidean algorithm mapping to $\mathbb{N}$ by Proposition 2.1.3. □

We can use the above theorem to prove an even stronger result, the main result of Harper's thesis. As we have seen in Theorem 2.1.7, it is useful to have sets of primes relating to B that we can use asymptotic results on. To prove Lemma 2.1.8, we will want to look at the asymptotics of $|B_n(x)|$.

Lemma 2.1.8. — *If K is an algebraic number field of class number one, $|\mathscr{O}_K^\times| = \infty$, and $|B_n(x)| >> \frac{x}{\log^2 x}$, then $|B_{n+1}(x)| \sim \frac{x}{\log x}$.*

Proof. — The proof will be given in Section 2.4. □

In order to prove Lemma 2.1.8, we will need to use both the large sieve inequality and the Gupta-Murty bound, so the proof will be in section 2.4. Once we prove Lemma 2.1.8, we can then prove the main theoretical result of Harper's thesis, Theorem 2.1.9 below.

Theorem 2.1.9. — *If K is a number field with class number one such that $\mid \mathscr{O}_K^\times \mid = \infty$ and if $\mid B_n(x) \mid >> \frac{x}{\log^2 x}$ for some n, then $\mathscr{O}_K$ is Euclidean and has a Euclidean algorithm mapping to* $\mathbb{N}$.

Proof. — If $\mid B_n(x) \mid >> \frac{x}{\log^2 x}$, then we know that $\mid B_{n+1}(x) \mid \sim \frac{x}{\log x}$ by Lemma 2.1.8. We then apply Lemma 2.1.6, which says that since $|B_{n+1}(x)| \sim \frac{x}{\log x}$, there is a Euclidean algorithm from $\mathscr{O}_K$ to $\mathbb{N}$. □

Theorem 2.1.9 is a very powerful result, if we are lucky enough to be dealing with a ring of integers $\mathscr{O}_K$ such that there is some n where $|B_n(x)| >> \frac{x}{\log^2 x}$. Theorems 2.1.7 and 2.1.9 concern rings such that $\mathscr{O}_K^\times$ is infinite. The cases where $\mathscr{O}_K^\times$ is finite are very different, as the following examples demonstrate.

Example 3. — (1) *As we know from example 2 in section 2 , if* $R = \mathbb{Z}[\sqrt{-5}]$*, then* $B_0 = B_i = 0, \pm 1$ *for all* i*.*

(2) *Let* $R = \mathbb{Z}$*. We can easily compute the construction in Definition 2.1.1:*

$$\begin{aligned} B_0 &= 0, \pm 1 \\ B_1 &= 0, \pm 1, \pm 2, \pm 3 \\ B_2 &= 0, \pm 1, \pm 2, \pm 3, \pm 5, \pm 7 \\ B_3 &= 0, \pm 1, \pm 2, \pm 3, \pm 5, \pm 7, \pm 11. \end{aligned}$$

After B_3*, the sets* B_i *stabilize and stop growing. This is because we can see the class of* 4 *in* $\mathbb{Z}/13\mathbb{Z}$ *cannot be represented by* $0, \pm 1, \pm 2, \pm 3, \pm 5,$ *or* ± 7*. Since* $4 + 9 = 13$*, there is no prime* p *with* $\mathrm{Nm}(p) > 11$ *such that the class of* 4 *can be represented by one the primes in* B_3*, so the sets stabilize.*

The examples above have such small B's because $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-5}]$ have finitely many units. These examples show us that Theorems 2.1.7 and

2.1.9 do indeed require that the unit group $\mathscr{O}_K^\times$ be infinite. This is further demonstrated in the following proposition.

Proposition 2.1.10. — *In every quadratic imaginary number field K, the set B does not contain every prime ideal of $\mathscr{O}_K$.*

In order to prove the proposition, we need the following definition.

Definition 2.1.11. — We define $\pi(x)$ to be the number of prime ideals in $\mathbb{Z}$ with norm less than x.

Proof. — (Of Lemma 2.1.10) It is well known that $\mathbb{Z}[i]$ and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are norm-Euclidean. For simplicity of exposition, we assume that K is neither $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, so that $|\mathscr{O}_K^\times| = 2$. By definition, the size of B_0 is three, so every prime in B_1 must have norm less than or equal to three. There are only two such primes in $\mathbb{Z}$—2 and 3—so there are at most four such primes in $\mathscr{O}_K$. Each ideal has two generators, so we know that

$$\begin{array}{rcccl} |B_0| & = & 3 & & \\ |B_1| & \leq & 3+4\pi(3) & = & 11. \end{array}.$$

The primes in B_2 have norm less than or equal to eleven, so lie above the primes 2, 3, 5, 7 or 11, i.e.

$$|B_2| \leq 3+4\pi(11) = 23.$$

Continuing as before, the primes in B_3 must lie above 2, 3, 5, 7,11, 13, 17, or 23, so

$$|B_3| \leq 3 + 4\pi(23) = 39.$$

By iterating this process via hand computation, we get the following sizes:

$$\begin{aligned}
|B_4| &\leq 3 + 4\pi(39) &= 51 \\
|B_5| &\leq 3 + 4\pi(51) &= 63 \\
|B_6| &\leq 3 + 4\pi(63) &= 75 \\
|B_7| &\leq 3 + 4\pi(75) &= 87 \\
|B_8| &\leq 3 + 4\pi(87) &= 95
\end{aligned}$$

$$\begin{aligned}
|B_9| &\leq 3 + 4\pi(95) &= 99 \\
|B_{10}| &\leq 3 + 4\pi(99) &= 103 \\
|B_{11}| &\leq 3 + 4\pi(103) &= 111 \\
|B_{12}| &\leq 3 + 4\pi(111) &= 119 \\
|B_{13}| &\leq 3 + 4\pi(119) &= 123.
\end{aligned}$$

The numbers $\pi(123)$ and $\pi(119)$ are equal so the sets stabilize and the size of B is less than or equal to 123. □

We can see that the heart of the above proof was seeing whether the sequence $h_k = 3 + 2(3-1)\pi(h_{k-1})$, $h_0 = 3$, converges. To prove that $|B|$ is finite for an imaginary quadratic number field such that $|\mathscr{O}_K| = n$, it suffices to prove the sequence $h_k = n + 1 + 2n\pi(h_{k-1})$, $h_0 = n$, converges. It is possible to see that $|B|$ is finite for all quadratic imaginary fields via hand computation in the the two remaining fields. The methods can be generalized to the Euclidean ideal class situation.

By Dirichlet's unit theorem, the only number fields that have rings of integers with finitely many units are $\mathbb{Q}$ and the quadratic imaginary fields, so it makes sense to apply Theorem 2.1.7 only to the other fields.

2.2. The Large Sieve

The large sieve is one of the most important results in analytic number theory. Several conditional results in number theory, relying on the generalized Riemann hypothesis, were later proven using the large sieve, so it makes sense to try to strengthen Weinberger's result ([**11**] by proving it without using the Riemann hypothesis via some application of the large sieve. The sieve looks at the distribution of integers into congruence classes modulo primes inside a number field K. Since every class has the same density in the integers, a randomly chosen set of primes should be more or less evenly distributed among the classes.

Definition 2.2.1. — Given a prime ideal $\mathfrak{p}$, $\alpha \in \mathscr{O}_K$, and a finite set of non-associated integers A, let

$$Z(\alpha, \mathfrak{p}) := |\{x \in A \mid x \equiv \alpha \pmod{\mathfrak{p}}\}|$$

Definition 2.2.2. — Given a prime ideal $\mathfrak{p}$ and a finite set of non-associated integers A, we define $\omega(\mathfrak{p}) := |\{[\alpha] \mid Z(\alpha, \mathfrak{p}) = 0\}|$.

Definition 2.2.3. — Given two functions $f(x)$ and $g(x)$ defined on some subset of $\mathbb{R}$, we say that $f(x) = O(g(x))$, or $f(x) << g(x)$, if there exists some positive C and some δ in the domain of f and g such that $f(x) \leq Cg(x)$ for $x > \delta$.

Using this notation, given a random set A, one would expect $Z(\alpha, \mathfrak{p})$ to be close to $\frac{|A|}{\mathrm{Nm}(\mathfrak{p})}$. The large sieve considers the difference between these two numbers over many $\mathfrak{p}$.

Theorem 2.2.4. — *(***[12]***)* ***(The Large Sieve)*** *In a number field K, given a finite set A of non-associated integers and a finite set P of non-ramifying prime ideals, with $X = \max_{x\in A} |\mathrm{Nm}(x)|$ and $Q = \max_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})$, then*

$$\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\mathrm{Nm}\mathfrak{p}} \right)^2 << (Q^2 + X) \mid A \mid .$$

The associated constant depends only on K and is independent of the choices of A and P.

Corollary 2.2.5. — *In a number field K, given a finite set A of non-associated integers and a finite set P of non-ramifying prime ideals, with $X = \max_{x\in A} |\mathrm{Nm}(x)|$ and $A = \max_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})$, then*

$$\sum_{\mathfrak{p}\in P} \frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} << \frac{Q^2 + X}{\mid A \mid}.$$

Proof. —

We know that$\displaystyle\sum_{\alpha(\text{mod }\mathfrak{p})}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2$ is bounded below by

$$\sum_{\substack{\alpha(\text{mod }\mathfrak{p}),\\ Z(\alpha,\mathfrak{p})=0}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2, \text{ which can be rewritten as } \sum_{\substack{\alpha(\text{mod }\mathfrak{p}),\\ Z(\alpha,\mathfrak{p})=0}}\left(\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2.$$

This can be rewritten again as $\omega(\mathfrak{p})\left(\frac{|A|}{\mathrm{Nm}(\mathfrak{p})}\right)^2$, so that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\omega(\mathfrak{p})\frac{\mid A\mid^2}{\mathrm{Nm}(\mathfrak{p})^2}=\sum_{\mathfrak{p}\in P}\omega(\mathfrak{p})\frac{\mid A\mid^2}{\mathrm{Nm}(\mathfrak{p})}<<(Q^2+X)\mid A\mid$$

and then lastly rewritten as

$$\sum_{\mathfrak{p}\in P}\frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})}<<\frac{Q^2+X}{\mid A\mid}.$$

□

2.3. The Gupta-Murty Bound

We need the Gupta-Murty bound in order to prove Lemma 2.1.8. In order to state the bound, we need some definitions.

Given a prime ideal $\mathfrak{p}$, let $q_{\mathfrak{p}}:\mathscr{O}_K\longrightarrow\mathscr{O}_K/\mathfrak{p}$ be the quotient map where $\mathfrak{p}$ is the kernel. Using our new notation for the quotient map, we can now define an important constant for $\mathscr{O}_K$ and $\mathfrak{p}$.

Definition 2.3.1. — Given a prime ideal $\mathfrak{p}$, we define $f(\mathfrak{p}) := |q_{\mathfrak{p}}(\mathscr{O}_K^\times)|$.

The constant $f(\mathfrak{p})$ is the size of the image of the units under the quotient group, which is not necessarily the size of the units of $\mathscr{O}_K/\mathfrak{p}$. In fact, it is bounded above by, and is frequently less than, the size of the units of $\mathscr{O}_K/\mathfrak{p}$. The constant $f(\mathfrak{p})$ is a special case of the following.

Definition 2.3.2. — Let K be a number field and $\mathfrak{p}$ a prime ideal. If $\mathfrak{M}$ is a monoid in $\mathscr{O}_K$ such that $\mathfrak{M} \cap \mathfrak{p} = \emptyset$, then $f_{\mathfrak{M}}(\mathfrak{p})$ is $|q_{\mathfrak{p}}(\mathfrak{M})|$.

The quantity $f(\mathfrak{p})$ is therefore the same as $f_{\mathscr{O}_K^\times}(\mathfrak{p})$. The type of monoid that Harper was interested in was generated by an admissible set of primes, defined below.

Definition 2.3.3. — Let $p_i, \ldots, p_k$ be a set of distint, non-associate prime elements. If, given any k-tuple $(a_1, \ldots, a_k) \in \mathbb{N}^k \setminus (0, \ldots, 0)$, the set of units $\mathscr{O}_K^\times$ surjects onto $(\mathscr{O}_K/p^{a_1} \cdots p^{a_k})^\times$, then we say $p_i, \ldots, p_k$ is an *admissible set of primes.*

Example 4. — *If $K = \mathbb{Q}$, then* $f(\mathfrak{p}) = \left\{ \begin{array}{ll} 1 & \textit{if } \mathfrak{p} = (2) \\ 2 & \textit{otherwise} \end{array} \right\}$.

Definition 2.3.4. — A set of elements $x_1, \ldots, x_n$ of K is **multiplicatively independent** if the only integer n-tuple $(a_1, \ldots, a_n)$ satisfying $x_1^{a_1} \cdots x_n^{a_n} = 1$ is $(0, \ldots, 0)$.

Example 5. — *The integers* 2, 3, *and* 5 *are multiplicatively independent in* $\mathbb{Z}$. *So are* 5 *and* 10, *but the set* 5, 10, *and* 2 *is not multiplicatively independent because* $10^1 \cdot 5^{-1} \cdot 2^{-1} = 1$.

The bound below is the version published in [**5**] and the proof given follows the proof of Lemma 6 in [**2**].

Theorem 2.3.5. — *([**4**]) If* $\mathfrak{M}$ *is a finitely-generated monoid in* $\mathscr{O}_K$ *containing* t *multiplicatively independent elements, then*

$$|\{\mathfrak{p} \mid f_{\mathfrak{M}}(\mathfrak{p}) \leq y\}| << y^{\frac{t+1}{t}},$$

where the implied constant depends on K, t, *and the generators of* $\mathfrak{M}$.

Before we can prove the bound, we need the following lemmas.

Lemma 2.3.6. — *The number of primes dividing a natural number* x, *counting multiplicities, is bounded above by* $\frac{\log x}{\log 2}$.

Proof. — If x is greater than 1, then there exists some y such that $2^{y-1} \leq x < 2^y$. The smallest integer with y prime divisors (counting multiplicities), is the 2^y since 2 is the smallest primes. Therefore, the number of prime elements dividing x is less than the number of primes dividing 2^y, which is y, so $y - 1$ is an upper bound for the number of primes dividing x. Since $\frac{\log z}{\log 2}$ is an increasing function in z, we know that $\frac{\log x}{\log 2}$ is greater than or equal to $y - 1$. □

Lemma 2.3.7. — *The number of k-tuples in $\mathbb{N}^k$ such that $a_1+\cdots+a_k \leq Y$ is $\frac{Y^k}{k!} + O(Y^{k-1})$ and is greater than $\frac{Y^k}{k!}$.*

Proof. — We will prove this by induction. The number of $a \in \mathbb{N}$ such that $a \leq Y$ is $Y+1$, which is greater than Y.

Suppose the number of k-tuples $(a_1, \ldots, a_k) \in \mathbb{N}^k$ such that $a_1 + \cdots + a_k \leq Y$ is bounded above by $\frac{Y^k}{k!} + C_{k-1}Y^{k-1}$, where C_{k-1} is positive and depends on $k-1$. The $(k+1)$-tuples $(a_1, \ldots a_{k+1})$ in $\mathbb{N}^{k+1}$ such that $a_1 + \cdots + a_{k+1} \leq Y$ can be sorted by the initial value of a_1 as $Y-0, Y-1, \ldots, Y-Y$. In order to find the number of such $(k+1)$-tuples, we need to sum the number of k-tuples that add up to or less than or equal to $0, 1, \ldots, Y$. The number of such k-tuples is thus bounded above by $\sum_{n=0}^{Y}\left(\frac{n^k}{k!} + C_{k-1}n^{k-1})\right) = \frac{1}{k!}\sum_{n=0}^{Y} n^k + \sum_{n=0}^{Y} C_{k-1}n^{k-1}$. This is bounded above by $\frac{1}{k!}\left(\frac{Y^{k+1}}{k+1} + CY^k\right) + C'Y^{k-1}$ for some positive constants C and C'. We can conclude that the number of such k-tuples is bounded above by $\frac{Y^{k+1}}{(k+1)!} + O(Y^k)$.

Repeat the above proof, but this time assume that the number of k-tuples $(a_1, \ldots, a_k) \in \mathbb{N}^k$ such that $a_1 + \cdots + a_k \leq Y$ is bounded below by $\frac{Y^k}{k!} + C_{k-1}Y^{k-1}$, where C_{k-1} is positive and depends on $k-1$. By repeating the above argument, we see that the number of such k-tuples is bounded below by $\frac{1}{k!}\left(\frac{Y^{k+1}}{k+1} + CY^k\right) + C'Y^{k-1}$ for positive constants C and C', so the number of such k-tuples is bounded below by $\frac{Y^{k+1}}{(k+1)!}$. □

Corollary 2.3.8. — *The number of integer k-tuples such that*

$$|a_1| + \cdots + |a_k| \leq Y$$

is $\frac{2^k Y^k}{k!} + O(Y^{k-1})$.

Lemma 2.3.9. — *Let K be a number field and let $x_1, \ldots, x_n$ be distinct elements in $K^\times$. For each x_i, there exists a positive constant M_i such that for any n -tuples $(a_i, \ldots, a_n)$, $(b_1, \ldots, b_n)$ in $\mathbb{N}^n$,*

$$|\mathrm{Nm}_{K/\mathbb{Q}}(x_1^{a_1} \cdots x_n^{a_n} - x_1^{b_1} \cdots x_n^{b_n}) \mid \leq CM_1^{a_1+b_1} \cdots M_n^{a_n+b_n},$$

where C is a constant depending only on K.

Proof. — (Proof due to Nick Ramsey) Suppose i is an injection, $i : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and S is is the set of field embeddings from K into $\overline{\mathbb{Q}}$. If $(a_i, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are in $\mathbb{N}^n$, then

$$|\mathrm{Nm}(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k})|=|i(\mathrm{Nm}(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k}))| \, .$$

The quantity inside the absolute value is

$$\prod_{\sigma \in S} i(\sigma(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k})).$$

Since these σ are field injections, we know that

$$\prod_{\sigma \in S} i(\sigma(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k})) = \prod_{\sigma \in S} (i(\sigma(x_1)^{a_1} \cdots \sigma(x_k)^{a_k}) - i(\sigma(x_1)^{b_1} \cdots \sigma(x_k)^{b_k})).$$

We can rewrite this as

$$\sum_{S'\subset S}(-1)^{|S\setminus S'|}\prod_{\sigma\in S'} i(\sigma(x_1)^{a_1}\cdots\sigma(x_k)^{a_k})\prod_{\sigma\notin S'} i(\sigma(x_1)^{b_1}\cdots\sigma(x_k)^{b_k}).$$

For each x_i, there exists some positive M_i such that

$$\prod_{S'}|i(\sigma(x_i))|\leq M_i$$

for all subsets S' of S and therefore if a_i is a natural number,

$$\left|\prod_{S'} i(\sigma(x_i)^{a_i})\right| \leq M_i^{a_i}.$$

This implies that

$$\left|\sum_{S'\subset S}(-1)^{|S\setminus S'|}\prod_{\sigma\in S'} i(\sigma(x_1)^{a_1}\cdots\sigma(x_k)^{a_k})\prod_{\sigma\notin S'} i(\sigma(x_1)^{b_1}\cdots\sigma(x_k)^{b_k})\right|$$

is less than or equal to

$$\sum_{S'\subset S} M_1^{a_1}\cdots M_k^{a_k}M_1^{b_1}\cdots M_k^{b_k} = \sum_{S'\subset S} M_1^{a_1+b_1}\cdots M_k^{a_k+b_k}$$

$$= 2^{|S|}M_1^{a_1+b_1}\cdots M_k^{a_k+b_k}.$$

□

We can now prove Theorem 2.3.5. The proof follows the proof in [**2**].

Proof. — (Proof of Theorem 2.3.5) Suppose that $\mathfrak{M}$ contains k multiplicatively independent elements, $x_1,\ldots,x_k$ of $\mathscr{O}_K$; suppose $\mathfrak{p}$ is a prime ideal, $x_i\notin\mathfrak{p}$ for any i, such that $f_{\mathfrak{M}}(\mathfrak{p})<y$; and that $Y=(y)^{\frac{1}{k}}$. By

Lemma 2.3.7, there are more than y k-tuples $(a_1, \ldots, a_k)$ in $\mathbb{N}^k$ such that $\sum a_i \leq Y$, so there is some pair of distinct k-tuples $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$ in $\mathbb{N}^k$ such that $x_1^{a_1} \cdots x_k^{a_k} \equiv x_1^{b_1} \cdots x_k^{b_k} \pmod{\mathfrak{p}}$. Therefore, $|\{\mathfrak{p} : f_{\mathfrak{M}}(\mathfrak{p}) < y\}|$ is less than or equal to

$$\left| \left\{ \mathfrak{p} \;\middle|\; \begin{array}{c} \exists \text{ pair of distinct } (a_1, \ldots, a_k), (b_1, \ldots, b_k) \in \mathbb{N}^k \\ \sum a_i, \sum b_i \leq Y, v_{\mathfrak{p}}(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k}) > 0 \end{array} \right\} \right| ,$$

where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation. Since $v_{\mathfrak{p}}(x_1^{a_1} \cdots x_k^{a_k} - x_1^{b_1} \cdots x_k^{b_k}) > 0$, we know that

$$v_{\mathfrak{p}}(x_1^{a_1 - b_1} \cdots x_k^{a_k - b_k} - 1) > 0$$

and the above quantity is less than or equal to

$$\left| \left\{ \mathfrak{p} \;\middle|\; \begin{array}{c} \exists \ (c_1, \ldots, c_k) \in \mathbb{Z}^k \text{ such that} \\ \sum \mid c_i \mid \leq 2Y, v_{\mathfrak{p}}(x_1^{c_1} \cdots x_k^{c_k} - 1) > 0 \end{array} \right\} \right| .$$

This last quantity is less than or equal to

$$\sum_{\substack{(c_1, \ldots, c_k) \in \mathbb{Z}^k \\ \sum \mid c_i \mid \leq 2Y}} |\{\mathfrak{p} \mid v_{\mathfrak{p}}(x_1^{c_1} \cdots x_k^{c_k} - 1) > 0\}| .$$

There are $\frac{4^k Y^k}{k!} + O(Y^{k-1})$ integer k-tuples $(c_1, \ldots, c_k)$ such that $\sum \mid c_i \mid \leq 2Y$. For each of these k-tuples $(c_1, \ldots, c_k)$ such that $\sum |c_i| \leq 2Y$, there exists a component-wise minimal k-tuple $(d_1, \ldots, d_k)$ in $\mathbb{N}^k$ such that $c_i + d_i \geq 0$ for all i. As a consequence, $\sum d_i < 2Y$. Since $v_{\mathfrak{p}}(x_1^{c_1} \cdots x_k^{c_k} - 1) > 0$ and $v_{\mathfrak{p}}(x_1^{d_1} \cdots x_k^{d_k} - 1) = 0$, we know that $v_{\mathfrak{p}}(x_1^{c_1 + d_1} \cdots x_k^{c_k + d_k} -$

$x_1^{d_1} \cdots x_k^{d_k}) > 0$. The element $x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k}$ is an element of $\mathscr{O}_K$, so the fact that

$$v_{\mathfrak{p}}(x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k}) > 0,$$

implies that $v_p(\mathrm{Nm}(x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k})) > 0$, where $\mathfrak{p}$ lies above p. Suppose that $M := \max\{M_i\}$. Lemma 2.3.9 implies that

$$|\mathrm{Nm}((x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k})| \leq CM^{c_1+\cdots+c_k+2d_1+\cdots+2d_k} \leq CM^{6Y}.$$

The number of primes p in $\mathbb{Z}$ such that

$$v_p(|\mathrm{Nm}(x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k})|) > 0$$

is bounded above by $\frac{\log(CM^{6Y})}{\log 2} = \frac{6Y \log M + \log C}{\log 2}$ by Lemma 2.3.6.

In light of the above paragraph, we know that

$$\sum_{\substack{(c_1, \ldots, c_k) \in \mathbb{Z}^k \\ \sum |c_i| \leq 2Y}} |\{\mathfrak{p} \mid v_{\mathfrak{p}}(x_1^{c_1} \cdots x_k^{c_k} - 1) > 0\}|$$

is less than or equal to

$$\sum_{\substack{(c_1, \ldots, c_k) \in \mathbb{Z}^k \\ \sum |c_i| \leq 2Y}} \left| \left\{ \mathfrak{p} \mid v_{\mathfrak{p}}(x_1^{c_1+d_1} \cdots x_k^{c_k+d_k} - x_1^{d_1} \cdots x_k^{d_k}) > 0 \right\} \right| ,$$

which is bounded above by

$$[K:\mathbb{Q}] \sum_{\substack{(c_1,\ldots,c_k)\in\mathbb{Z}^k \\ \sum|c_i|\leq 2Y}} \frac{6\log M}{\log 2}Y + \frac{\log C}{\log 2}.$$

As there are $\frac{4^k Y}{k!} + O(Y^{k-1})$ integer k-tuples $(c_1,\ldots,c_k)$ such that $\sum |c_i|\leq 2Y$, the last expression is bounded above by

$$[K:\mathbb{Q}]\left(\frac{2^{2k}Y^k}{k!} + O\left(Y^{k-1}\right)\right)\left(\frac{6\log M}{\log 2}Y + \frac{\log C}{\log 2}\right)$$

$$= \frac{3\cdot 2^{2k+1}\log M}{k!\log 2}Y^{k+1} + O(Y^k),$$

which equals

$$\frac{[K:\mathbb{Q}]3\cdot 2^{2k+1}\log M}{\log 2}y^{\frac{k+1}{k}} + O(y).$$

We conclude that $|\{\mathfrak{p}\mid f_{\mathfrak{M}}(\mathfrak{p})<y\}| << y^{\frac{k+1}{k}}$.

□

Corollary 2.3.10. — *If $\mathscr{O}_K$ has infinitely many units, then*

$$|\{\mathfrak{p}\mid \mathrm{Nm}(\mathfrak{p})\leq x, f(\mathfrak{p})\leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| << x^{1-2\epsilon}.$$

Proof. — We know if $f(\mathfrak{p})\leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}$ and if $\mathrm{Nm}(\mathfrak{p})\leq x$, then $f(\mathfrak{p})\leq x^{\frac{1}{2}-\epsilon}$. If $\mathscr{O}_K$ has infinitely many units, we know that it contains a unit of infinite order and therefore at least one multiplicatively independent unit. Apply the above theorem, we know that

$$|\{\mathfrak{p}\mid \mathrm{Nm}(\mathfrak{p})\leq x, f(\mathfrak{p})\leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| << (x^{\frac{1}{2}-\epsilon})^2 = x^{1-2\epsilon}.$$

□

2.4. The Large Sieve Applied to a Variation of Harper's Lemma

In this section, we will finally prove Lemma 2.1.8. We will start by applying the large sieve. For each ideal $\mathfrak{p}$ in $B_n(x^2)$, choose a generator π. Let A be the union of zero and the set of all of these representatives, so that $|A|$=$|B_n(x^2)|$ +1 and $X \leq x^2$. The set P will be $B_{n+1}^c(x)$, so that $Q = x$.

Lemma 2.4.1. — *If* $\mathfrak{p} \in B_{n+1}^c(x)$, *then* $f(\mathfrak{p})|\omega(\mathfrak{p})$ *and* $\omega(\mathfrak{p}) > 0$, *so that* $\omega(\mathfrak{p}) \geq f(p)$.

Proof. — If $\mathfrak{p} \in B_{n+1}^c(x)$, then there is some α such that there is no prime q in B_n such that $\alpha \equiv q \pmod{\mathfrak{p}}$. This implies $Z(\alpha, \mathfrak{p}) = 0$ and therefore $\omega(\mathfrak{p}) \geq 1$. Note that since 0 is contained in every B_i, the α's such that $Z(\alpha, \mathfrak{p}) = 0$ are not in $\mathfrak{p}$.

Let $\mathfrak{p}$ be generated by p. Recall that if p is in B_n, then $\{up \mid u \in \mathscr{O}_K^\times\} \subset B_n$. Therefore if $Z(\alpha, \mathfrak{p}) = 0$, then $Z(u\alpha, \mathfrak{p}) = 0$ for all $u \in \mathscr{O}_K^\times$. As $\alpha \notin \mathfrak{p}$, there are $f(\mathfrak{p})$ classes $[u\alpha]$, where $u \in \mathscr{O}_K^\times$. □

We will now prove Lemma 2.1.8.

Proof. — Putting together Corollary 2.2.5 and Lemma 2.4.1, we see that

$$\sum_{(p)|p \in B_{n+1}^c(x)} \frac{f(p)}{|\mathrm{Nm}(p)|} << \frac{Q^2 + X}{|A|} = \frac{2x^2}{|B_n(x^2) + 1|} << \frac{x^2}{x^2/\log^2(x^2)}.$$

This means that

$$\sum_{(p)|p\in B_{n+1}^c(x)} \frac{f(p)}{|\mathrm{Nm}(p)|} << \log^2 x,$$

and therefore

$$\log^2 x >> \sum_{\substack{(p)\ |\ p\ \in\ B_{n+1}^c(x) \\ f(p)\ >\ |\mathrm{Nm}(p)|^{1/2-\epsilon}}} \frac{f(p)}{|\mathrm{Nm}(p)|}$$

$$\geq \sum_{\substack{(p)\ |\ p\ \in\ B_{n+1}^c(x) \\ f(p)\ >\ |\mathrm{Nm}(p)|^{1/2-\epsilon}}} \frac{1}{|\mathrm{Nm}(p)|^{\frac{1}{2}+\epsilon}}$$

$$\geq \frac{1}{x^{\frac{1}{2}+\epsilon}} \left|\{\mathfrak{p} \in B_{n+1}^c(x) \mid f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}\right| .$$

Multiplying both sides by $x^{\frac{1}{2}+\epsilon}$ yields

$$x^{\frac{1}{2}+\epsilon}\log^2 x >> \left|\{\mathfrak{p} \in B_{n+1}^c(x) \mid f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}\right| .$$

Our goal is to bound $|B_{n+1}^c(x)|$, so since we already have bounded $|\{\mathfrak{p} \in B_{n+1}^c(x) \mid f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|$, we now need to bound $|\{\mathfrak{p} \in B_{n+1}^c(x) \mid f(\mathfrak{p}) \leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|$. This is easily done, however, by Corollary 2.3.10.

We therefore know that $|B_{n+1}(x)| << x^{1-2\epsilon} + x^{\frac{1}{2}+\epsilon}\log^2 x$. The limit as x goes to infinity of $(x^{1-2\epsilon})/(x/\log x)$ plus $(x^{1/2+\epsilon}\log^2 x)/(x/\log x)$ is the same as

$$\lim_{x\longrightarrow\infty} \frac{\log x}{x^{2\epsilon}} + \lim_{x\longrightarrow\infty} \frac{\log^3 x}{x^{\frac{1}{2}-\epsilon}},$$

which is clearly zero for ϵ less than $\frac{1}{2}$. We conclude that $\lim_{x \longrightarrow \infty} \frac{|B^c_{n+1}(x)|}{x/\log x} = 0$ and that $|B_{n+1}(x)| \sim \frac{x}{\log x}$.

□

CHAPTER 3

EUCLIDEAN IDEAL CLASSES

3.1. Euclidean ideal classes

In 1977, H.W. Lenstra, Jr. ([**8**]) generalized the idea of the Euclidean algorithm to ideals via the concept of the Euclidean ideal. In his paper, he defined an algorithm on ideals rather than on elements and showed that if such an algorithm exists for some ideal, then such an algorithm exists for every ideal in its ideal class, giving rise to the notion of a Euclidean ideal class.

Before starting, let us recall the following definitions.

Definition 3.1.1. — Let R be a Dedekind domain. A *fractional ideal* is an element in the set $\{\frac{1}{b}I \mid b \in R \setminus 0, I \text{ is an ideal of } R\}$. Henceforth, unless otherwise stated, all ideals in this paper are fractional. Ideals that are contained in R are called *integral ideals*. For the rest of the paper, given a Dedekind domain R, let E be the set of fractional ideals of R that contain R itself. For example, if $\frac{1}{b}I$ is in E, then b is an element of I.

Definition 3.1.2. — If C is an ideal of R, it is called *Euclidean* if there exists a function $\psi : E \longrightarrow W$, W a well-ordered set, such that for all $I \in E$ and all $x \in IC \setminus C$, there exists some $y \in C$ such that

$$\psi((x+y)^{-1}IC) < \psi(I).$$

We say ψ is a *Euclidean algorithm for C* and C is an *Euclidean ideal*.

One can easily check that if R is the ring of integers of a number field, if $I = C = R$, and if ψ is the inverse of the norm, then this is equivalent to the norm-Euclidean statement in Definition 2.0.11. In fact, this version of the definition was the motivation given in Lenstra's paper introducing the definition of Euclidean ideal classes. Further motivation is given in the introduction.

3.1.1. Properties of Euclidean algorithms with respect to C. —

Lemma 3.1.3. — *If R is a Dedekind domain, C is a non-zero ideal, and ψ is a Euclidean algorithm with respect to C, then $\psi(R)$ is the smallest value in the image of ψ and R is the only ideal in the preimage of $\psi(R)$.*

Proof. — In order to show that $\psi(R)$ is the smallest value in the image of ψ, we will show that if I is an ideal in E such that $I \neq R$, then $\psi(I)$ is not minimal. Since ψ maps to a well-ordered set, there is a least element in the image of ψ. This will imply that $\psi(R)$ must be the minimal value in the set and that R is the only element in the preimage of $\psi(R)$.

If I is an ideal in E, then for any element x in $IC \setminus C$, there exists some y in C such that $\psi((x+y)^{-1}IC) < \psi(I)$. Therefore, as long as the set $IC \setminus C$ is non-empty, there exists some ideal J such that $\psi(J) < \psi(I)$. The only ideal I in E such that $IC \setminus C$ is empty is the ideal R. Therefore, not only is $\psi(R)$ the least element in the image of ψ, but the preimage of $\psi(R)$ only has one element, the ideal R. □

After defining Euclidean algorithm on ideals, Lenstra investigated how a Euclidean algorithm for some ideal C related to the other ideals in C's ideal class.

Proposition 3.1.4. — *If ϕ is a Euclidean algorithm for C, $C \neq (0)$, then ϕ is a Euclidean algorithm for every ideal in $[C]$.*

Proof. — Let J be an ideal in $[C]$ with $J = \delta C$, where $\delta \in \mathrm{Frac}(R) \setminus 0$. Given any I in E and x in $IJ \setminus J$, we know that there exists some x' in $IC \setminus C$ such that $x = \delta x'$. As ϕ is a Euclidean algorithm for C, there exists some y' such that $\phi((x'+y')^{-1}IC) < \phi(I)$. Let $y = \delta y'$. Then

$$\phi((x+y)^{-1}IJ) = \phi(\delta^{-1}(x'+y')^{-1}I\delta C) = \phi((x'+y')^{-1}IC) < \phi(I).$$

Thus for every $x \in IJ \setminus J$, there exists some $y \in J$ such that

$$\phi((x+y)^{-1}IJ) < \phi(IJ).$$

We conclude that ϕ is a Euclidean algorithm for all J in $[C]$. □

Due to Proposition 3.1.4, we can now define the following.

Definition 3.1.5. — If there exists some Euclidean algorithm for C, then $[C]$ is called a *Euclidean ideal class.*

Lenstra's concept of the Euclidean ideal class is a generalization of traditional Euclidean algorithms. Euclidean domains are rings with $[R]$ as a Euclidean ideal class and every traditional Euclidean algorithm is a Euclidean algorithm for R, as the next proposition shows.

Proposition 3.1.6. — *A Dedekind domain R has an $\mathbb{N}$-valued Euclidean algorithm if and only if $[R]$ is a Euclidean ideal class.*

Proof. — Let R be a domain with a $\mathbb{N}$-valued Euclidean algorithm and let ϕ_R be the Euclidean algorithm in Definition 2.0.12. Recall that this is the least Euclidean algorithm mapping to $\mathbb{N}$. Since R is a Euclidean domain, it is a principal ideal domain and every integral ideal can be expressed as (a) for some $a \in R$. We will define $\rho : E \longrightarrow W$ by $\rho((\frac{1}{a})) := \phi_R(a)$, where a is a non-zero element of R. Let $I = (\frac{1}{i})$, with $i \neq 0$. Every element of $I \setminus R$ can be written as $\frac{a}{i}$, with $a \in R \setminus (i)$. Given any $a \in R \setminus (i)$, there exists some $q, r \in R$ such that $a = qi + r$ with $r \neq 0, \phi_R(r) < \phi_R(i)$. Therefore, for any $x = \frac{a}{i} \in I \setminus C$, there exists some q in R such that

$$\rho\left(\left(\frac{a}{i} - q\right)^{-1} IR\right) = \rho\left(\left(\frac{a - qi}{i}\right)^{-1}\left(\frac{1}{i}\right)\right) = \rho\left(\frac{i}{r}\frac{1}{i}\right) = \phi_R(r) < \phi_R(i) = \rho(I).$$

We conclude that ρ is a Euclidean algorithm for R and $[R]$ is a Euclidean ideal class.

Suppose that $[R]$ be a Euclidean ideal class, so there exists some map $\rho : E \longrightarrow W$ such that for all $I \in E$ and all $x \in I \setminus R$, there exists some $y \in R$ such that $\rho((x+y)^{-1}IC) < \rho(I)$. We shall define $\phi : R \setminus 0 \longrightarrow W$, by $\phi(a) := \rho((\frac{1}{a}))$. Therefore, given some $a, b \in R$, $b \neq 0$, either b divides a or $\frac{a}{b} \in (\frac{1}{b}) \setminus R$. In the latter, there exists some $q \in R$ such that

$$\rho\left(\left(\frac{a}{b} - q\right)^{-1}\left(\frac{1}{b}\right)\right) = \rho\left(\left(\frac{b}{a-qb}\frac{1}{b}\right)\right) = \rho\left(\left(\frac{1}{a-qb}\right)\right) < \rho\left(\left(\frac{1}{b}\right)\right).$$

We rename $a-qb$ as r and see that for all $a, b \in R$, $b \neq 0$, there exist some $q, r \in R$ such that $a = qb+r$ and either $r = 0$ or $\phi(r) = \phi(a-qb) < \phi(b)$. We conclude that ρ is a Euclidean algorithm for R and that R is a Euclidean domain. □

Proposition 3.1.7. — ([**8**]) *If R is a Dedekind domain and $[C]$ is a Euclidean ideal class, then the class group is $\langle [C] \rangle$.*

Proof. — If for every ideal class $[I]$ in $\mathrm{Cl}(R)$, there exists some positive integer n such that $[I][C^n] = [R]$, then the class group is cyclic and every fractional ideal has an inverse. It sufices to show that for every ideal class $[I]$ in $\mathrm{Cl}(R)$, there exists some positive integer n such that $[I][C^n] = [R]$.

Given an ideal class $[J]$, the intersection $E \cap [J]$ is non-empty. Let J be an integral ideal in $[J]$. Since $\mathrm{Nm}(J)$ is an element of J, the ideal $\frac{J}{\mathrm{Nm}(J)}$ contains R and is an element of E.

Let I be an ideal in E, $I \neq R$, implying the set $IC \setminus C$ is non-empty. Suppose that ϕ is a $\mathbb{N}$-valued Euclidean algorithm for $[C]$, so that for all

x in $IC \setminus C$, there exists some y in C such that $\phi((x+y)^{-1}IC) < \phi(I)$. If $(x+y)^{-1}IC = R$, then $[I][C] = [I][C^1] = [R]$ and $n = 1$.

For the following, assume that if $\phi(R) < \phi(I) \leq m$, then there exists some $n > 0$ such that $[IC^n] = R$. Let $\phi(J) = m + 1$, so that $JC \setminus C$ is non-empty. For every x in $JC \setminus C$, there exists some $y \in C$ such that $\phi((x+y)^{-1}JC) < \phi(J) = m + 1$ so that either $(x+y)^{-1}JC = R$ or $\phi((x+y)^{-1}JC \leq m$. In the first situation, $[I][C] = [R]$ and $n = 1$. In the second case, there exists some $k \in \mathbb{Z}^+$ such that $[(x+y)^{-1}JC][C^k] = [R]$, so that $[J][C^{k+1}] = R$ and $n = k+1$. We conclude that every ideal class $[J]$ can be written as $[C]^n$ for some $n \in \mathbb{Z}^+$, so the class group is generated by $[C]$.

In particular, if $[J] = [R]$ and $J \neq R$, the above implies that there exists some $n > 0$ such that $[JC^n] = [R]$ and thus $[C]^n = [R]$. We conclude that $\mathrm{Cl}(R)$ is finite. □

Returning to the section's introduction, recall that Lenstra's motivation was the statement of norm-Euclidean domains in Definition 2.0.11. It is natural to ask what happens when the inverse of the norm is a Euclidean algorithm for C.

Definition 3.1.8. — An ideal C is *Euclidean for the norm*, or *norm-Euclidean*, if the inverse of the norm acts as a Euclidean algorithm for the ideal class. In other words, if C is norm-Euclidean, then for all $x \in IC \setminus C$, there exists some $y \in C$ so that $\mathrm{Nm}((x+y)^{-1}IC)^{-1} < \mathrm{Nm}(I)^{-1}$, i.e. $\mathrm{Nm}((x+y)^{-1}IC) > \mathrm{Nm}(I)$. This implies that if C is Euclidean for the norm, then for all $x \in IC \setminus C$, there exists some $y \in C$ such that

$$\mathrm{Nm}(x-y) < \mathrm{Nm}(C).$$

In order to look at the following examples, we need the next definition.

Definition 3.1.9. — Given any element x in $\mathbb{C}$, we denote the open ball in $\mathbb{C}$ of radius δ centered at x by $B_\delta(x)$ and the closed ball in $\mathbb{C}$ of radius δ centered at x by $\overline{B}_\delta(x)$. The metric used is the Euclidean metric.

Example 6. — *The ideal* $(2, 1+\sqrt{-5})$ *is norm-Euclidean in the ring* $\mathbb{Z}[\sqrt{-5}]$.

Proof. — Since $\mathrm{Nm}(2, 1+\sqrt{-5}) = 2$, we must show that for every x in $\mathbb{Q}(\sqrt{-5})$, there exists some y in $(2, 1+\sqrt{-5})$ such that $\mathrm{Nm}(x-y) < 2$. In other words, if we fix an embedding of $\mathbb{Q}(\sqrt{-5})$ into $\mathbb{C}$, the distance in the complex plane between the images of x and y is less than $\sqrt{2}$. The ideal $(2, 1+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ can be viewed as a lattice in $\mathbb{C}$ with $\{2, 1+\sqrt{-5}\}$ as a basis of the ideal as a $\mathbb{Z}$-module, so every point z in $\mathbb{C}$ is contained in a fundamental domain of the lattice.

We can then view every point z in $\mathbb{C}$ as a point in the square

$$a\sqrt{5} \leq \mathrm{Im}(z) \leq (a+2)\sqrt{5},$$

$$b \leq \mathrm{Re}(z) \leq b+2$$

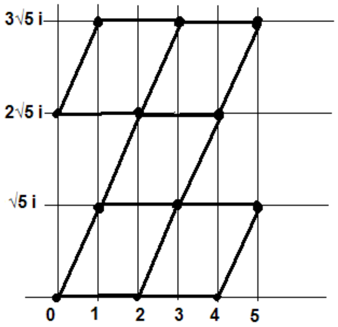

FIGURE 1. The Lattice $(2, 1+\sqrt{-5})$

for some $(b + a\sqrt{-5})$ in the ideal $(2, 1+\sqrt{-5})$, since any fundamental domain of the lattice $(2, 1+\sqrt{-5})$ is contained in two adjacent such squares. All four corners of the box are in the ideal.

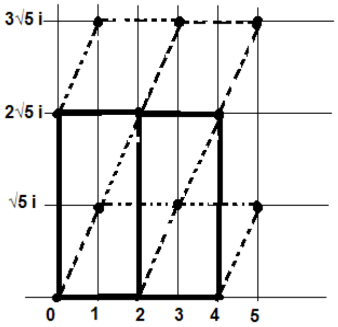

FIGURE 2. Boxes and the Lattice's Fundamental Domains

The sets $B_{\sqrt{2}}(b + a\sqrt{-5})$ and $B_{\sqrt{2}}(b + 2 + a\sqrt{-5})$ intersect inside the box at the point $b + 1 + a\sqrt{-5} + i$. Everything that is in the box that is not inside $B_{\sqrt{2}}(b + a\sqrt{-5})$ or $B_{\sqrt{2}}(b + 2 + a\sqrt{-5})$ is inside the convex hull of $b + a\sqrt{-5}$, $b + 2 + a\sqrt{-5}$, $b + a\sqrt{-5} + \sqrt{-2}$, $b + 2 + a\sqrt{-5} + \sqrt{-2}$, and $b+1+a\sqrt{-5}+i$. If every point in their convex hull is within $\sqrt{2}$ of the lattice $(2,1+\sqrt{5})$, then our condition is satisfied (See Figure 3).

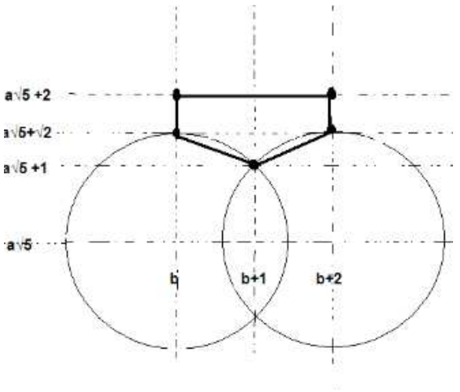

Figure 3. A Set within $\sqrt{2}$ of the Lattice

The points $b+a\sqrt{-5}+\sqrt{-2}$, $b+a\sqrt{-5}+2i$, and $b+1+a\sqrt{-5}+2i$ are all in $B_{\sqrt{2}}(b+a\sqrt{-5}+2i)$, so are all within $\sqrt{2}$ of our lattice. It remains to show that the elements of the convex hull of $b+1+a\sqrt{-5}+i$,$b+1+a\sqrt{-5}+2i$, $b+2+a\sqrt{-5}$, and $b+2+a\sqrt{-5}+\sqrt{-2}$ satisfy the condition (See Figure 4).

By symmetry, every point except $b+1+a\sqrt{-5}+i$ is contained in $B_{\sqrt{2}}(b+2+a\sqrt{-5}+2i)$.

We know that $b+1+(a+1)\sqrt{-5}$ is an element of $(2,1+\sqrt{-5})$ and that

$$|(b+1+(a+1)\sqrt{-5})-(b+1+a\sqrt{-5}+i)|=|\sqrt{-5}-i|<\sqrt{2}.$$

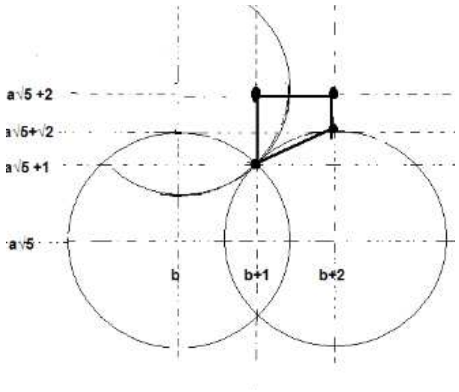

Figure 4. A Larger Set within $\sqrt{2}$ of the Lattice

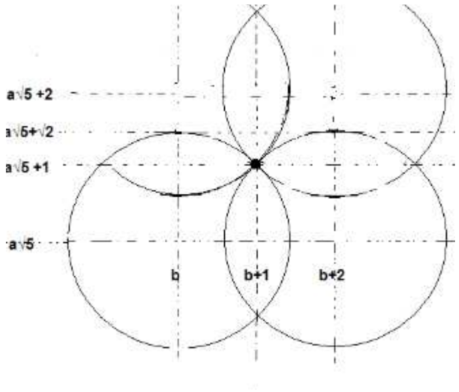

Figure 5. An Even Larger Set within $\sqrt{2}$ of the Lattice

Since the ideal $(2, 1+\sqrt{-5})$ is norm-Euclidean, it is a Euclidean ideal class and generates the class group. The ideal has order 2 so the class group has size 2.

□

Proposition 3.1.10. — *If ϕ is a Euclidean algorithm for C, then not only is it a Euclidean algorithm for every ideal J in $[C] \cap E$, but it is not a Euclidean algorithm for any ideal not in $[C] \cap E$.*

Proof. — Let $\phi : E \longrightarrow W$, W a well-ordered set, be a Euclidean algorithm for some ideal C. We know by 3.1.4 that ϕ is a Euclidean algorithm for every ideal J in $E \cap [C]$. Since W is well-ordered, there is a least element in the set $\{\phi(I) \mid I \in E, I \neq R\}$, say $\phi(I)$. Since I is not R, the set $IC \setminus C$ is non-empty and there is some element x in $IC \setminus C$. There exists some $y \in C$ such that $\phi((x+y)^{-1}IC) < \phi(I)$, implying $(x+y)^{-1}IC$ is equal to R. From this we deduce that $[C] = [I^{-1}]$, so every ideal for which ϕ is a Euclidean algorithm belongs to $[I^{-1}]$. □

Theorem 3.1.11. — *Given a Dedekind domain R, there is at most one ideal class $[C]$ that is Euclidean for any particular algorithm. If such an ideal class exists, it generates the class group $Cl(R)$.*

Proof. — We know by 3.1.10 that if ϕ is a Euclidean algorithm, it is a Euclidean algorithm for only one ideal class. We also know by 3.1.7 that any Euclidean ideal class generates the class group. □

3.1.2. Properties of IC/C. — Understanding the definition of a Euclidean algorithm with respect to C depends on understanding the ideal $(x+y)^{-1}IC$ for every I in E, every x in $IC \setminus C$, and every y in C. What is unusual about the definition of a Euclidean algorithm for C is that it associates an ideal (not necessarily principal) with an element, motivating the following definition.

Definition 3.1.12. — Let C be a non-zero ideal, let I and J be ideals in E, and let α be an element of $IC \setminus C$. The ideal J is *similar to α modulo*

IC and C, or $J \sim \alpha \pmod{IC, C}$, if J can be written as $(\alpha + y)^{-1}IC$ for some y in C.

This creates two different types of similarity classes. There are similarity classes in (a subset of) $E \cap [IC]$ associated to an element of $IC \setminus C$ and there are similarity classes in $IC \setminus C$ associated to an element of $E \cap [C]$. Given an ideal I in E, it makes sense to ask how these similarity classes relate to one another. One powerful tool is the group action of $(R/I^{-1})^{\times}$ on the set IC/C.

Note that not every ideal J in $E \cap [IC]$ is in a similarity class associated to an element of $IC \setminus C$. Some are associated to an element in C. We can see that the only ideals J in $E \cap [IC]$ that are not associated to an element in $IC \setminus C$ are the ideals J such that $J^{-1}I$ is integral.

Lemma 3.1.13. — *Let I and J be relatively prime ideals in E, $I \neq R$, such that $[J] = [I][C]$. There exists some x in $IC \setminus C$ such that $J = x^{-1}IC$.*

Proof. — We know that $J^{-1} = xI^{-1}C^{-1}$ for some x in $\mathrm{Frac}(R)$. Since $(x) = J^{-1}IC$, x is an element of IC. The ideals I and J are relatively prime and $I \neq R$, so $J^{-1}I$ is not an integral ideal, implying x is not an element of C. We conclude that x is in $IC \setminus C$. □

Lemma 3.1.14. — *Let R be a Dedekind domain such that, let C be a non-zero ideal, and let I be an ideal in E, $I \neq R$. The quotient IC/C is a free module of rank one over R/I^{-1} and the group $(R/I^{-1})^{\times}$ acts* *freely on $(IC/C) \setminus 0$. It acts freely transitively on the set of generators of IC/C as an R/I^{-1}-module.*

Proof. — Let q be the quotient map from R to R/I^{-1}; let a and b be elements of R, with $q(a)$ and $q(b)$ in $(R/I^{-1})^{\times}$; and let x be in $IC \setminus C$, so that both ax and bx are in IC and $ax - bx = (a-b)x$ is in IC. Suppose that a and b are congruent modulo I^{-1} and thus $a-b$ is in I^{-1}, implying that $(a-b)x$ is in C. We conclude that $\overline{ax} = \overline{bx}$ in IC/C and the action is well-defined.

The identity element of R/I^{-1} acts trivially on IC/C, so that $[1]\overline{x} = \overline{1x} = \overline{x}$. Since the associative and distributive laws hold in both (R/I^{-1}) and IC/C and the group action is well-defined, the quotient IC/C is indeed an R/I^{-1} module. The quotient IC/C is isomorphic to R/I^{-1} as an R/I^{-1}-module because R is a Dedekind domain, so IC/C is a free R/I^{-1} module. The rest follows from the structure as an R/I^{-1} module. □

If I^{-1} is not prime then not every class $\overline{x}$ in IC/C, $\overline{x} \neq 0$, is a generator of IC/C. It behooves us to find a condition on x that implies $\overline{x}$ is a generator of IC/C as an R/I^{-1} module.

Lemma 3.1.15. — *Let R be a Dedekind domain , let C be a non-zero ideal, and let I be an ideal in E. If x is an element of IC, then $\overline{x}$ generates IC/C as an R/I module if and only if $(x, C) = IC$. Furthermore, if $(x, C) = IC$ and ϕ is any R-isomorphism from $(IC/C)^{-1}$ to R/I^{-1}, then $[\phi(x)]$ is a unit in R/I^{-1}.*

Proof. — It is clear that the ideal C is contained in the ideal (x, C), which is itself contained in IC. Let $\overline{x}$ generate IC/C as an R/I^{-1} module. Therefore, for any z in $IC \backslash C$, there exists some $a \in R$ such that $\overline{z} = [a]\overline{x}$. This implies that there exists some y in C such that $z = ax + y$ and so IC is contained in (x, C). We conclude that (x, C) is equal to IC.

Let the ideal $(x, C) = IC$, so that x is not in$C$, and let $\overline{z}$ be any nonzero element of IC/C. There exists some a in R and some y in C such that $z = ax + y$, implying that $\overline{z} = [a]\overline{x}$. We conclude that $\overline{x}$ generates IC/C as an R/I module.

Let the function $\phi : IC/C \longrightarrow R/I^{-1}$ be an isomorphism of R/I^{-1} modules. If $\overline{x}$ generates IC/C as an R/I^{-1} module, then $\phi(\overline{x})$ generates R/I^{-1} as an R/I^{-1} module. In other words, $[\phi(x)]$ is a unit in R/I^{-1}.

□

Lemma 3.1.16. — *Let R be a Dedekind domain, let I be an ideal in E, and let x be an element of IC such that $(x, C) = IC$. If $\mathfrak{p}$ is a prime ideal such that $v_{\mathfrak{p}}(I^{-1}) \neq 0$, then $\mathfrak{p}$ and $xI^{-1}C^{-1}$ are relatively prime.*

Proof. — Let $\mathfrak{p}$ be a prime ideal and let I^{-1} be contained in $\mathfrak{p}$, implying the ring R is contained in $\mathfrak{p}I$ and C is contained in $\mathfrak{p}IC$. Suppose that the integral ideal $xI^{-1}C^{-1}$ is also contained in $\mathfrak{p}$. Then the element x would be contained in $\mathfrak{p}IC$, so the ideal (x, C) would be contained in $\mathfrak{p}IC$. This is a contradiction, so the ideals $xI^{-1}C^{-1}$ and $\mathfrak{p}$ must be relatively prime. □

3.1.3. An Analogue Dirichlet's Theorem on Prime Ideals for Euclidean Ideal Classes.

— Dirichlet's theorem on primes in arithmetic progressions is fundamental to number theory and its proof is considered by many to be the birth of analytic number theory. It was necessary for Harper's work on Euclidean rings. It will be useful to have a version of it in the Euclidean ideal class framework.

Theorem 3.1.17. — ***(Dirichlet's Theorem on Primes in Arithmetic Progressions)***
Let a and b be relatively prime elements of $\mathbb{Z}$. There are infinitely many primes p such that $p \equiv a \pmod{b}$ and the density of such primes in the set of all primes is $\frac{1}{\phi(b)}$, where ϕ is the Euler ϕ function.

The condition that a and b be relatively prime is equivalent to the condition that $\overline{a}$ is a unit in $R/(b)$, or $\overline{a}$ is in $(R/(b))^\times$. Recall from Lemma 3.1.16 that for any x in IC, the equivalence class $\overline{x}$ generates IC as an R/I^{-1} module if and only if $(x, C) = IC$. This motivates the following theorem.

Theorem 3.1.18. — *Let K be a number field and let I be an ideal in E, $I \neq R$. If x is an element of IC and $(x, C) = IC$, then the set of prime ideals $\mathfrak{p}$ such that $\mathfrak{p}^{-1} \sim x \pmod{IC, C}$ is of positive denisty in the set of all prime ideals. In other words, there is a positive density of prime ideals $\mathfrak{p}$ such that $\mathfrak{p}^{-1} = (x+y)^{-1}IC$ for some y in C.*

In order to prove this, we will need the Chebotarev density theorem. The Chebotarev denisty theorem is a generalization of Dirichlet's theorem on primes in arithmetic progressions. Instead of looking at the number of primes mapping to some α, with $(\alpha, p) = 1$, via the quotient map with kernel (p), it is concerned with prime ideals mapping to an element in $\mathrm{Gal}(K^{ab}/K)$ via the Artin map. In order to state the Chebotarev density theorem, we need the following definitions.

Definition 3.1.19. — Let K be a number field and let L be a finite extension of K. The set of all primes $\mathfrak{p}$ such that $\mathfrak{p}$ ramifies in L is $S(L)$, or the *modulus of L.* The set of all fractional ideals that are relatively prime to the primes in $S(L)$ is $\mathbb{I}^{S(L)}$.

Given an integral ideal J of K, the set of all primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(J) \neq 0$ is $S(J)$ and the set of all fractional ideals that are relatively prime to the primes in $S(J)$ is $\mathbb{I}^{S(J)}$.

With the above notation, we can now define the Artin map.

Definition 3.1.20. — Let K be a number field and let L be a finite abelian extension of K. The map $\psi_L : \mathbb{I}^{S(L)} \longrightarrow \mathrm{Gal}(L/K)$ that sends every prime ideal $\mathfrak{p}$ that is unramified in $\mathscr{O}_L$ to its associated Frobenius automorphism $(\mathfrak{p}, L/K)$ is called the *Artin map* . The map extends to the rest of $\mathbb{I}^{S(L)}$ by multiplicativity and is surjective.

We can now state the Chebotarev density theorem.

Theorem 3.1.21. — ***(Chebotarev Density Theorem)***
Let K be a number field, let L be a finite abelian extension of K, and let σ be any element of $Gal(L/K)$. There are infinitely many prime ideals that map to σ under the Artin map, and the density of the primes that map to σ under the Artin map in the set of all primes is $\frac{1}{|Gal(L/K)|}$.

As a consequence, we get the result we needed in section 2.

Theorem 3.1.22. — ***(Dirichlet's Theorem on Prime Elements in Arithmetic Progressions in Number Fields with Trivial Class Group)***
Let K be a number field with class number one and let α and β be relatively prime elements of $\mathscr{O}_K$. There is a positive density of prime elements p such that $p \equiv \alpha \pmod{\beta}$.

Proof. — Since α and β are relatively prime, the ideal (α) is an element of $\mathbb{I}^S((\beta))$. The ray class field (see following definition) $K^{S(\beta)}$ is a finite abelian extension of K, so there is a positive density of prime ideals $(\mathfrak{p})$ that map to $\psi((\alpha))$ and each ideal (p) can be written as $(1 + z\beta)(\alpha)$, for some algebraic integer z in $\mathscr{O}_K$. There therefore exists some unit u in $\mathscr{O}_K^\times$ such that $up \equiv \alpha \pmod{\beta}$. The product up is still a prime element, so the result holds. □

In order to prove Theorem 3.1.18, we shall apply the Chebotarev density theorem to a well-chosen ray class field.

Definition 3.1.23. — Given an integral ideal J, the *ray class field of modulus* J, denoted by K^J is the unique abelian extension of K such that if ψ_{K^J} is the Artin map for K^J, $\psi_{K^J} : \mathbb{I}^{S(J)} \longrightarrow \mathrm{Gal}(K^J/\mathbb{Q})$, then the kernel of ψ_{K^J} is the set of principal ideals (a) such that $v_{\mathfrak{p}}(a-1) \geq v_{\mathfrak{p}}(J)$ for all $\mathfrak{p}$ in $S(J)$. Given such a J, the ray class field always exists.

We now have all the definitions and results necessary to prove Theorem 3.1.18.

Proof. — (Proof of Theorem 3.1.18) Let $K^{I^{-1}}$ be the ray class field defined above and let x be an element of IC such that $(x, C) = IC$. We know by Lemma 3.1.16 that (x, C) is relatively prime to any prime ideal $\mathfrak{p}$ such that $\mathfrak{p}$ divides I^{-1}. The integral ideal $xI^{-1}C^{-1}$ is an element of $\mathbb{I}^{S(I^{-1})}$ by Lemma 3.1.16.

The Chebotarev density theorem implies there is a positive density in the set of all prime ideals of prime ideals $\mathfrak{q}$ in the preimage of $\psi_{K^{I^{-1}}}(xI^{-1}C^{-1})$ under the Artin map. Since the kernel of the Artin map to a ray class field is as described in Definition 3.1.23, each of these ideals $\mathfrak{q}$ can be written as $(1 + q)xI^{-1}C^{-1}$ for some q, where $v_{\mathfrak{p}}(q) \geq v_{\mathfrak{p}}(I^{-1})$ for all primes $\mathfrak{p}$ in $S(I^{-1})$. Note that $(x + xq) = (1 + q)x = \mathfrak{q}IC$, so that $x + xq$ is an element of IC. We chose x to be an element of IC, so xq is also an element of IC. As such, we know that $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(IC)$ for all primes $\mathfrak{p}$. Note that this implies that $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(C)$ for $\mathfrak{p} \notin S(I^{-1})$ because $v_{\mathfrak{p}}(I) = 0$. Since x is an element of IC, we know that $v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(IC)$ for all primes $\mathfrak{p}$. We know that $v_{\mathfrak{p}}(q) \geq v_{\mathfrak{p}}(I^{-1})$ for all primes $\mathfrak{p}$ in $S(I^{-1})$, so that $v_{\mathfrak{p}}(xq) = v_{\mathfrak{p}}(q) + v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(I^{-1}) + v_{\mathfrak{p}}(IC) = v_{\mathfrak{p}}(C)$ for primes $\mathfrak{p}$ in $S(I^{-1})$. We conclude that, because $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(C)$ for all primes $\mathfrak{p}$, xq is an element of C, so that $\mathfrak{q} = (x + qx)I^{-1}C^{-1}$, where qx is an element of C. We conclude that $\mathfrak{q}^{-1} \sim x \pmod{IC, C}$. □

We can use this to look at the more complicated situation where (x, C) is not necessarily equal to IC.

Theorem 3.1.24. — *Let $\mathscr{O}_K$ be the ring of integers of a number field K, let C be a non-zero ideal, let I be an ideal in $E(I \neq R)$, let x be an element of $IC \setminus C$, and Let L be the integral ideal $(I^{-1}, xI^{-1}C)$. There are infinitely many prime ideals $\mathfrak{p}$ such that $\mathfrak{p}^{-1} \sim x \pmod{ILC, C}$.*

Proof. — The ideals $xI^{-1}L^{-1}C^{-1}$ and $I^{-1}L^{-1}$ are relatively prime and $xI^{-1}L^{-1}C^{-1}$ is an element of $\mathbb{I}^{S(I^{-1}L^{-1})}$. Applying Chebotarev's density theorem, there is a positive density of prime ideals $\mathfrak{p}$ such that $\psi_{K^{I^{-1}L^{-1}}}(\mathfrak{p}) = \psi_{K^{I^{-1}L^{-1}}}(xI^{-1}L^{-1}C^{-1})$. By similar arguments as the last proof, $\mathfrak{p} = (1 + q)xI^{-1}L^{-1}C^{-1}$, where $\mathfrak{q}$ is an element of $I^{-1}L^{-1}$, so that $\mathfrak{p} = (x + y)I^{-1}L^{-1}C^{-1}$ for some y in C. We conclude there is a positive density of prime ideals $\mathfrak{p}$ such that $\mathfrak{p}^{-1} \sim x \pmod{ILC, C}$. □

3.2. A Motzkin-type Lemma for C

We will now prove a new criterion that determines whether a given ideal class is Euclidean or not. The criterion is a reformulation of Motzkin's construction and lemma for the Euclidean ideal class framework. Motzkin's construction for C will not only determine whether or not an ideal class $[C]$ has a Euclidean algorithm mapping to $\mathbb{N}$. If $[C]$ does have such an algorithm, then Motzkin's construction constructs one. This algorithm is the "least" Euclidean algorithm for $[C]$ that maps to $\mathbb{N}$.

Definition 3.2.1. — Motzkin's Construction for C

Given a Dedekind domain R and some non-zero ideal C, we define $A_{0,C}$ to be the set $\{R\}$. For $i > 0$, we define

$$A_{C,i} = A_{C,i-1} \cup \left\{ I \;\middle|\; \begin{array}{c} I \in E \text{ and } \forall\, x \in IC \setminus C,\ \exists\, y \in C \\ \text{such that } (x+y)^{-1}IC \in A_{C,i-1} \end{array} \right\}$$

The union $\cup_{i=0}^{\infty} A_{i,C}$ is called A_C. The sets $\{A_{i,C}\}$ and A_C are *Motzkin's Construction for C*. We define ϕ_C to be the function mapping from A_C to $\mathbb{N}$, with $\phi_C(I) = i$ if I is an element of $A_{i,C} \setminus A_{i-1,C}$.

Note that, according to this definition, the $A_{i,C}$'s are nested and the function ϕ_C is canonical.

Theorem 3.2.2. — ***(Motzkin's Lemma for*** C***)***

Let R be a Dedekind domain and let C be a non-zero ideal. If the sets A_C and E are equal, then $[C]$ is a Euclidean ideal class and ϕ_C is a Euclidean algorithm for $[C]$.

Proof. — Let I be an ideal in E and let x be an element in $IC \setminus C$. Since the ideal I is in A_C, there exists some y in C such that $(x+y)^{-1}IC$ is an element of $A_{\phi_C(I)-1,C}$. We conclude that there exists some y in C such that

$$\phi_C((x+y)^{-1}IC) \leq \phi_C(I) - 1 < \phi_C(I).$$

The function ϕ_C is thus a Euclidean algorithm for C and $[C]$ is a Euclidean ideal class. $\square$

What is interesting about this is that we do not need to initially know whether or not the class group of R is cyclic. We can start with any non-zero ideal C, and if $A_C = E$, then not only is the class group of R cyclic, but we know that $[C]$ generates the class group.

As in the traditional case (see Definition 2.0.11), it makes sense to ask if, given a well-ordered set W, there exists a least Euclidean algorithm for C.

Definition 3.2.3. — Given a Dedekind domain R with Euclidean ideal class $[C]$, let $\{\phi_i\}_{d\in D}$ be the set of all Euclidean algorithms for $[C]$ that map to W. We define $\phi_{C,W}$ to be the function mapping from E to W such that $\phi_{C,W}(J) = \min_{d\in D}\{\phi_i(J)\}$.

Lemma 3.2.4. — *If $[C]$ is a Euclidean ideal class, then $\phi_{C,W}$ is a Euclidean algorithm for $[C]$.*

Proof. — Let I be an ideal in E, $I \neq R$, and let x be an element of $IC\setminus C$. There exists a Euclidean algorithm for $[C]$, ρ, such that $\rho(I) = \phi_{C,W}(I)$. We know there exists an element y of C such that

$$\phi_{C,W}((x+y)^{-1}IC) \leq \rho((x+y)^{-1}IC) < \rho(I) = \phi_{C,W}(I),$$

so the function $\phi_{C,W}$ is a Euclidean algorithm for C. $\square$

Lemma 3.2.5. — *If R is a Dedekind domain, C is a non-zero ideal, and $A_C = E$, then $\phi_{C,\mathbb{N}}$ equals ϕ_C.*

Proof. — By Lemma 3.1.3, the least element in the image of $\phi_{C,\mathbb{N}}$ is $\phi_{C,\mathbb{N}}(R)$, so $\phi_{C,\mathbb{N}}(R) = 0$ because $\phi_{C,\mathbb{N}} \leq \phi_C$ and $\phi_C(R) = 0$.

Let I be an ideal in E. By the definition of a Euclidean ideal class for C, for any x in $IC \setminus C$, there exists some y in C such that

$$\phi_{C,\mathbb{N}}((x+y)^{-1}IC) < \phi_{C,\mathbb{N}}(I).$$

We will inductively define a chain of ideals as follows. Let $I_0 := I$. Given any $x \in I_i C \setminus C$, there exists a y such that $\phi_{C,\mathbb{N}}((x+y)^{-1}IC) < \phi_{C,\mathbb{N}}(I)$. We will define I_{i+1} to be $(x+y)^{-1}I_i C$. Note that we can only continue this process as long as $I_i \neq R$. We then have a chain of ideals $I = I_0, I_1, I_2, \ldots$ such that $\phi_{C,\mathbb{N}}(I_i) > \phi_{C,\mathbb{N}}(I_{i+1})$. The set $\mathbb{N}$ is well-ordered, so there is a least element in the set $\{\phi_{C,\mathbb{N}}(I_i)\}_{i=0}^{\infty}$. We conclude that there is some n such that $\phi_{C,\mathbb{N}}(I_n)$ is the minimal element, zero and we therefore have a chain of ideals

$$I = I_0, I_1, \ldots, I_n = R$$

such that

$$\phi_{C,\mathbb{N}}(I) > \phi_{C,\mathbb{N}}(I_1) > \cdots > \phi_{C,\mathbb{N}}(R) = 0.$$

For any I_k in this chain, $k > 0$, there exists an x in $I_{k-1}C \setminus C$ and an element y of C such that $I_k = (x+y)^{-1}I_{k-1}C$. This implies that if I_j is an element of $A_{i,C}$, then I_{j-1} is an element of $A_{i+1,C}$. Because I_n is an element of $A_{0,C}$, the ideal I is an element of $A_{n,C}$ and $\phi_C(I)$ is less than or equal to n.

The chain

$$\phi_{C,\mathbb{N}}(I) > \phi_{C,\mathbb{N}}(I_1) > \cdots > \phi_{C,\mathbb{N}}(R)$$

has $n+1$ elements in it, so $\phi_{C,\mathbb{N}}(I) \geq \phi_{C,\mathbb{N}}(R) + n = n$. Therefore $\phi_{C,\mathbb{N}}(I) \geq n \geq \phi_C(I)$, and $\phi_{C,\mathbb{N}}(I) = \phi_C(I)$. We conclude that ϕ_C and $\phi_{C,\mathbb{N}}$ are the same function. □

Example 7. — *Let $R = \mathbb{Z}$ and $C = R$.*
By definition, $A_{0,C} = R$. While the definitions are slightly different in Example 2, it still shows us that $A_{i,C} = \{(\frac{1}{j}) \mid 0 < j < 2^{i+1}\}$.

3.2.1. An Application of the Motzkin-type Lemma for C. —

Motzkin's lemma for C gives us immediate consequences that make it easier to figure out whether or not $[C]$ is a Euclidean ideal class.

Lemma 3.2.6. — *Let R be a Dedekind domain, let C be a non-zero ideal, and let I be an ideal in E, $I \neq R$. If, for all $x \in IC \setminus C$, there exists some y in C such that $(x+y)^{-1}IC$ is in A_C, then I is itself in A_C.*

Proof. — We know from lemma 3.1.14 that IC/C is finite. For each class $\overline{\alpha}$ in IC/C, let i_α be the minimum element of the set

$$\{\phi_C((\alpha + y)^{-1}IC) \mid y \in C\}.$$

Then I is an element of $A_{j,C}$, where $j = \max_{\overline{\alpha} \in IC/C}\{i_\alpha\} + 1$ and I is therefore an element of A_C. □

We can use this lemma to prove the following theorem. In our previous results, we used the existence of a Euclidean ideal class to prove a domain has cyclic class group. It makes sense, though, to ask when a domain with cyclic class group has a Euclidean ideal class.

Theorem 3.2.7. — *Let R be a Dedekind domain with cyclic class group generated by $[C]$ and let m be an integer. If the set of ideals $E \cap [C^m]$ is contained in A_C, then $[C]$ is a Euclidean ideal class.*

Proof. — Consider an ideal I in $E \cap [C^{m-1}]$ for some integer m. For each of the finitely many non-zero equivalence classes in IC/C, choose some element x_j in said class. Note that the ideal $x_j^{-1}IC$ is an element of $E \cap [C^m]$ and therefore belongs to A_C. Applying Lemma 3.2.6, the ideal I is an element of A_C and thus $E \cap ([C^{m-1}])$ is contained in A_C. By repeating this argument, we conclude that every ideal I in E that is in $[C^n]$ for some integer n is in A_C. Since $[C]$ generates the class group, this implies that every ideal in E is in A_C and $[C]$ is a Euclidean ideal class by Theorem 3.2.2 . □

3.3. A Harper-type Lemma for C

Recall that what makes Harper's construction so useful is that is deals with sets of primes and units. This allows us to use results on densities of primes, which are really results on densities of prime ideals. It therefore makes sense to try to find a variation of Motzkin's construction with respect to C that consists of sets of prime ideals.

Definition 3.3.1. — Given a Dedekind domain R and a non-zero ideal C, let $B_{0,C}$ be the one element set $\{R\}$. For i greater than zero, we define

$$B_{C,i} = B_{C,i-1} \cup \left\{ \mathfrak{p}^{-1} \;\middle|\; \begin{array}{c} \mathfrak{p} \subseteq R \text{ is prime, and} \\ \forall\, x \in \mathfrak{p}^{-1}C \setminus C,\ \exists\, y \in C \\ \text{such that } (x-y)^{-1}\mathfrak{p}^{-1}C \in B_{C,i-1} \end{array} \right\}$$

and we define B_C to be the union $\bigcup_{i=0}^{\infty} B_{C,i}$.

Theorem 3.3.2. — *Let K be a number field and let C be a non-zero ideal of $\mathscr{O}_K$. If B_C contains all ideals $\mathfrak{p}^{-1}$ such that $\mathfrak{p}$ is prime, then $[C]$ is a Euclidean ideal class.*

Proof. — The techniques of this proof follow those in [**5**], however we use Theorem 3.1.18 instead of Dirichlet's theorem on primes in arithmetic progressions.

Let ω be the function mapping from E to $\mathbb{N}$ such that $\omega(I)$ is the number of prime divisors of I^{-1}, with multiplicity. If $\mathfrak{p}$ is a prime ideal, let $\lambda(\mathfrak{p}^{-1}) := i$ if $\mathfrak{p}^{-1}$ is an element of $B_i \setminus B_{i-1}$. Extend λ to all of E by additivity. We then put the two functions together as $\phi : E \longrightarrow \mathbb{N} \times \mathbb{N}$, with $\phi(I) = (\omega(I), \lambda(I))$, and order the image $\phi(E)$ lexicographically.

Because both ω and λ are additive functions, the function ϕ is additive as well. Note that $\phi(I) = (0, 0)$ if and only if $I = \mathscr{O}_K$.

In order to prove Theorem 3.3.2, we will show that ϕ is a Euclidean algorithm with respect to C. We shall prove this by induction. Let $\mathfrak{p}$ be a prime ideal and let $\phi(\mathfrak{p}^{-1}) = (1, i)$. For any x in $\mathfrak{p}^{-1}C \setminus C$, there exists some y such that $(x + y)^{-1}\mathfrak{p}^{-1}C$ is an element of $B_{i-1,C}$, so that $\phi((x + y)^{-1}\mathfrak{p}^{-1}C) = (0, 0)$ or $\phi((x + y)^{-1}\mathfrak{p}^{-1}C) = (1, j)$, where $j < i$.

Let I be an element of E with I^{-1} not a prime ideal. Suppose that for all J such that $\phi(J) < \phi(I)$ and for all a in $JC \setminus C$, there exists some y in C such that $\phi((x + y)^{-1}JC) < \phi(J)$. Let x be an element of $IC \setminus C$. If $(x, C) = IC$, we can apply Theorem 3.1.18. There exists some $y \in C$ such that $(x + y)^{-1}IC = \mathfrak{p}^{-1}$, where $\mathfrak{p}$ is a prime ideal. Since $\phi(\mathfrak{p})$ is less than $\phi(I)$, the condition is satisfied.

Suppose that (x, C) is not equal to IC and let L be $(I^{-1}, xI^{-1}C)$. The integral ideal L contains I^{-1}, so $I^{-1}L^{-1}$ has fewer prime divisors (counting multiplicities) than I^{-1} and $\phi(IL)$ is less than $\phi(I)$. There exists some y in C such that $\phi((x + y)^{-1}ILC) < \phi(IL)$. The additivity of ϕ implies that given two ideals M and N, $\phi(MN) = \phi(M) + \phi(N)$, so $\phi((x + y)IC) < \phi(I)$ and the condition holds. We conclude that ϕ is a Euclidean algorithm for $[C]$ and that $[C]$ is a Euclidean ideal class. $\square$

If we already know that R has cyclic class group, we have an even easier criterion to determine whether or not $[C]$ is a Euclidean ideal class.

Proposition 3.3.3. — *Let R be a Dedekind domain, let m be an integer, and suppose that the class group of R is $\langle [C] \rangle$. If, for all prime ideals $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^m]$, the ideal $\mathfrak{p}^{-1}$ is an element of B_C, then $[C]$ is a Euclidean ideal class.*

In order to prove Proposition 3.3.3, we need the following lemma.

Lemma 3.3.4. — *Let $\mathfrak{p}$ be a prime ideal. If, for every element x of $\mathfrak{p}^{-1}C \setminus C$, there exists some element y of C such that $(x+y)^{-1}\mathfrak{p}^{-1}C$ is an element of B_C, then the ideal $\mathfrak{p}^{-1}$ is an element of B_C.*

Proof. — See Lemma 3.2.6. The proof is the same. □

Proof. — (Proof of Proposition 3.3.3) Let $\mathfrak{p}$ be a prime ideal such that $[\mathfrak{p}] = [C^{m+1}]$ and let x be an element of $\mathfrak{p}^{-1}C \setminus C$. We know that for all such x, the ideal (x, C) is $\mathfrak{p}^{-1}C$. Therefore, by Theorem 3.1.18, there exists some y in C such that $(x+y)^{-1}\mathfrak{p}^{-1}C$ is prime. As the ideal class of $(x+y)^{-1}\mathfrak{p}^{-1}C$ is $[C^{-m-1}][C] = [C^{-m}]$, we know that $(x+y)^{-1}\mathfrak{p}^{-1}C$ is an element of B_C and therefore that $\mathfrak{p}^{-1}$ is an element of B_C by Lemma 3.3.4. This argument shows that every inverse of a prime ideal in $[C^d]$ for any integer d is in B_C. The class group is cyclic and generated by $[C]$, so $\mathfrak{p}^{-1}$ is in B_C for all prime ideals $\mathfrak{p}$. Thus by Theorem 3.3.2, $[C]$ is a Euclidean ideal class. □

3.4. Admissible Sets of Primes with Respect to C

While our variation of Motzkin's lemma with respect to C makes it easier to apply analytic results, it is not useful computationally. We know from Proposition 3.3.3 that if K is a number field with cyclotomic class group and all of the ideals in E in a particular ideal class are contained in B_C, then $[C]$ is a Euclidean ideal class. It then makes sense to wonder whether we really need every single ideal in an ideal class–maybe we could just have many ideals from a particular ideal class. This then means it makes sense to try to determine the size of the sets $B_{C,i}$. Unfortunately, it is still hard to try to compute the sizes of the various $B_{C,i}$. In order to make computing the sizes of the $B_{C,i}$ possible, we shall try to augment one of the $B_{C,i}$ with a special set. In order to define the set, we need the following terminology.

Definition 3.4.1. — Let K be a number field and let the class group of K be $\langle [C] \rangle$. Given a set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, such that $[\mathfrak{p}_i] = [C]$ for all i, we say that the set of primes is *admissible with respect to* C if for any k-tuple $(a_1, \ldots, a_k)$ of natural numbers such that $a_1 + \cdots + a_k \equiv 1 \pmod{h_K}$, the ideal $\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k}$ is in $A_{1,C}$.

Note that the definition implies that every prime that is in an admissible set of primes with respect to C is an element of $B_{1,C}$. Any set of primes that is admissible with respect to $\mathscr{O}_K$ yields an admissible set of primes, in the sense that Clark, Murty, and Harper used (see Definition 2.3.3) ([**5**],[**6**],[**1**]), by passing to generators.

Since the inverses of the primes in an admissible set generate a monoid in E, we were inspired to formulate a version of the Gupta-Murty bound that we can apply to any admissible set of primes for C.

3.4.1. The Gupta-Murty Bound for C. — In order to prove the generalization of the Gupta-Murty bound, we will first need the following lemmas on k-tuples.

Lemma 3.4.2. — *The number of k-tuples $(a_1, \ldots, a_k)$ in $\mathbb{N}^k$ such that $\sum_{i=1}^k a_i \leq Y$ and $\sum_{i=0}^k a_i \equiv m \pmod h$ is $\frac{Y^k}{k!h} + O(Y^{k-1})$.*

Proof. — We will prove this by induction. Without loss of generality, assume that $0 \leq m \leq h-1$. We know that $|\{a \in \mathbb{N} \mid a \leq Y, a \equiv m \,(\mathrm{mod}\ h)\}| = \lfloor \frac{Y-m}{h} \rfloor = \frac{Y}{h} + C$, where C is a constant.

Suppose that $\left|\left\{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \sum_{i=0}^k a_i \leq Y, \sum_{i=0}^k a_i \equiv m \,(\mathrm{mod}\ h)\right\}\right| = \frac{Y^k}{k!h} + O(Y^{k-1})$. Then

$$\left|\left\{(a_1, \ldots, a_{k+1}) \in \mathbb{N}^{k+1} \,\middle|\, \sum_{i=0}^{k+1} a_i \leq Y, \sum_{i=0}^{k+1} a_i \equiv m \,(\mathrm{mod}\ h)\right\}\right| ,$$

equals

$$\sum_{a_{k+1}=0}^{Y} \left|\left\{(a_1, \ldots, a_k) \in \mathbb{N}^k \,\middle|\, \sum_{i=0}^{k} a_i \leq Y - a_{k-1}, \sum_{i=0}^{k} a_i \equiv m - a_{k+1} \,(\mathrm{mod}\ h)\right\}\right| ,$$

which is less than or equal to

$$\sum_{a_{k+1}=0}^{Y} \frac{(Y - a_{k+1})^k}{k!h} + C(Y - a_{k+1})^{k-1}$$

for some constant C. This last expression can be rewritten as

$$\sum_{b=0}^{Y} \frac{b^k}{k!h} + \sum_{b=0}^{Y} Cb^{k-1} \leq \frac{Y^{k+1}}{(k+1)!h} + C'Y^k + \frac{C}{k}Y^k + C''Y^{k-1}$$

for some constants C, C', and C''. We conclude that

$$\left|\left\{(a_1, \ldots, a_{k+1}) \in \mathbb{N}^{k+1} \;\middle|\; \sum_{i=0}^{k+1} a_i \leq Y, \sum_{i=0}^{k+1} a_i \equiv m \,(\mathrm{mod}\ h)\right\}\right|$$

$$= \frac{Y^{k+1}}{(k+1)!h} + O(Y^k).$$

Corollary 3.4.3. — *The number of k-tuples $(a_1, \ldots, a_k)$ in $\mathbb{Z}^k$ such that $\sum_{i=1}^{k} |a_i| \leq Y$ and $\sum_{i=0}^{k} |a_i| \equiv m \pmod{h}$ is $\frac{2^k Y^k}{k!h} + O(Y^{k-1})$.*

□

Lemma 3.4.4. — *Given a positive integer k, there exist two positive constants $C_{k,h}$ and $M_{k,h}$ such that if $Y > M_{k,h}$, then*

$$\left|\left\{(a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k} a_i \leq Y, \sum_{i=0}^{k} a_i \equiv m \,(\mathrm{mod}\ h)\right\}\right| \geq C_{k,h} Y^k.$$

The constants $C_{k,h}$ and $M_{k,h}$ depend only on k and h.

Proof. — The case where $h = 1$ was proved in Lemma 2.3.7. Henceforth, we will assume that $h \geq 2$. Lemma 3.4.4 will be proven by induction on the size of k.

In order to prove the base case $k = 1$, we will show that if $k = 1$, then

$$|\{a \in \mathbb{N} \mid a \leq Y, a \equiv m \,(\mathrm{mod}\ h)\}| \geq \frac{1}{2h} Y$$

for $Y > 4h$. Without loss of generality, assume that $0 \leq m \leq h-1$. We then know that

$$|\{a \in \mathbb{N} \mid a \leq Y, a \equiv m \pmod{h}\}|$$

is bounded below by $\lfloor \frac{Y-m}{h} \rfloor$, which is itself bounded below by $\frac{Y-m}{h} - 1 \geq \frac{Y}{h} - 2$. If $Y \geq 4h$, then $\frac{Y}{4h} - 1 \geq 0$ and $\frac{Y}{2h} - 1 \geq \frac{Y}{4h}$, so that $\frac{Y}{h} - 2 \geq \frac{Y}{2h}$. We conclude that if $Y \geq 4h$, then

$$|\{a \in \mathbb{N} \mid a \leq Y, a \equiv m \pmod{h}\}| \geq \frac{1}{2h} Y.$$

By induction, assume that if $Y \geq M_{k,h}$, then

$$\left| \left\{ (a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k} a_i \leq Y, \sum_{i=0}^{k} a_i \equiv m \pmod{h} \right\} \right| \geq C_{k,h} Y^k.$$

We know that

$$\left| \left\{ (a_1, \ldots, a_{k+1}) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k+1} a_i \leq Y, \sum_{i=0}^{k+1} a_i \equiv m \pmod{h} \right\} \right|$$

which equals

$$\sum_{a_{k+1}=0}^{Y} \left| \left\{ (a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k} a_i \leq Y - a_{k+1}, \sum_{i=0}^{k} a_i \equiv m - a_{k+1} \pmod{h} \right\} \right|$$

$$= \sum_{b=0}^{Y} \left| \left\{ (a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k} a_i \leq b, \sum_{i=0}^{k} a_i \equiv m_Y + b \pmod{h} \right\} \right|$$

$$\geq \sum_{b=M_{k,h}}^{Y} C_{k,h} b^k$$

by our hypothesis. We know that

$$\sum_{b=M_{k,h}}^{Y} C_{k,h} b^k = \sum_{b=0}^{Y} C_{k,h} b^k - \sum_{b=0}^{M_{k,h}-1} C_{k,h} b^k > \frac{C_{k,h}}{k+1} Y^{k+1} - C_{k,h} C > 0$$

for some positive constant C. For any $0 < C_{k+1,h} < \frac{C_{k,h}}{k+1}$, there exists a positive $M_{k+1,h}$ such that if $Y \geq M_{k+1,h}$, then $C_{k,h}(\frac{Y^{k+1}}{k+1} - C) > C_{k+1,h} Y^{k+1}$. We conclude that there exist positive constants $C_{k+1,h}$ and $M_{k+1,h}$ such that if $Y \geq M_{k+1,h}$, then

$$\left| \left\{ (a_1, \ldots, a_{k+1}) \in \mathbb{N}^k \;\middle|\; \sum_{i=0}^{k+1} a_i \leq Y, \sum_{i=0}^{k+1} a_i \equiv m \,(\mathrm{mod}\ h) \right\} \right| \geq C_{k+1,h} Y^{k+1}.$$

□

Now that we have stated the necessary results on k-tuples, we must first make some preliminary definitions before we can state the theorem. For the following, assume that K is a number field with cyclic class group. Let C be an ideal such that $[C]$ generates the class group of K, and let $C^{h_K} = (s)$.

Definition 3.4.5. — Let m be a non-negative integer less than h_K. Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are all prime ideals with $[\mathfrak{p}_i] = [C]$. We then define the set $\mathfrak{M}$ as $\{\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k} \mid (a_1, \cdots, a_k) \in \mathbb{N}^k, a_1 + \cdots + a_k \equiv m \text{ (mod } h_k)\}$.

Note that for any ideal I in $\mathfrak{M}$, the ideal class $[I]$ is equal to $[C^{-m}]$.

Lemma 3.4.6. — *For any ideal I in $\mathfrak{M}$ and any prime ideal $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^{m+1}]$, there exists some α in $\mathfrak{p}^{-1}C$ such that $I = \alpha^{-1}\mathfrak{p}^{-1}C$.*

Proof. — Since I and $\mathfrak{p}^{-1}C$ are in the same ideal class, there exists some α in $K^{\times}$ such that $I = \alpha^{-1}\mathfrak{p}^{-1}C$. In other words, $(\alpha) = I^{-1}\mathfrak{p}^{-1}C$. We conclude that α is in $\mathfrak{p}^{-1}C$ as I^{-1} is an integral ideal. □

Definition 3.4.7. — Given a prime $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^{m+1}]$, we define $\Gamma_{\mathfrak{p},\mathfrak{M}}$ to be the number of equivalence classes $\overline{\alpha}$ in $\mathfrak{p}^{-1}C/C \setminus 0$ such that $(\alpha + y)^{-1}\mathfrak{p}^{-1}C$ is in $\mathfrak{M}$ for some $y \in C$, i.e.

$$\Gamma_{\mathfrak{p},\mathfrak{M}} := \left|\{\overline{\alpha} \in \mathfrak{p}^{-1}C/C \mid \alpha \notin C, \alpha \sim J \text{ for some ideal } J \in \mathfrak{M}\}\right| .$$

Now that we have the appropriate terminology, we can now state the generalized Gupta-Murty bound.

Theorem 3.4.8 **(The Gupta-Murty Bound for C)**

Let K be a number field and let C be a non-zero ideal. Given a monoid $\mathfrak{M}$ as defined in 3.4.5 with $m = 1$, the size of the set of primes $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^2]$ and $\Gamma_{\mathfrak{p},\mathfrak{M}}$ is less than y is $O(y^{\frac{k+1}{k}})$, for y sufficiently large. In other words, if y is large, then

$$\left|\{\mathfrak{p} \;\middle|\; [\mathfrak{p}] = [C^2] \text{ and } \Gamma_{\mathfrak{p},\mathfrak{M}} \leq y\}\right| = O(y^{\frac{k+1}{k}}).$$

Proof. — Suppose that $y > C_{k,h}M_{k,h}^{k}$, where $C_{k,h}$ and $M_{k,h}$ are as in Lemma 3.4.4. This proof can be broken into four steps. At different points in the proof, finitely many primes will be removed from consideration.

Step 1.

Suppose $\mathfrak{p}$ is a prime ideal with $[\mathfrak{p}] = [C^2]$ such that $\mathfrak{p}$ is not in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ and $\Gamma_{\mathfrak{p},\mathfrak{M}}$ be less than or equal to y. From Corollary 3.4.4, the number of k-tuples of natural numbers such that $a_1 + \cdots + a_k \leq (\frac{y}{C_{k,h}})^{\frac{1}{k}}$ and $a_1 + \cdots + a_k \equiv 1 \pmod{h_K}$ is bounded below by $C_{k,h}(\frac{y}{C_{k,h}})^{k\frac{1}{k}} = y$. Note that since $\mathfrak{p}^{-1}$ is not in $\mathfrak{M}$, any product $\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k}$, with each a_i in $\mathbb{N}$, is similar to some α in $\mathfrak{p}^{-1}C \setminus C$ by Lemma 3.1.13. Since $\Gamma_{\mathfrak{p},\mathfrak{M}}$ is less than y, there are at least two distinct k-tuples of natural numbers $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$ such that $a_1 + \cdots + a_k \equiv 1 \equiv b_1 + \cdots + b_k \pmod{h}$, both of the sums $a_1 + \cdots + a_k$ and $b_1 + \cdots + b_k$ are less than or equal to $(\frac{y}{C_{k,h}})^{\frac{1}{k}}$, and both ideals $\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k}$ and $\mathfrak{p}_1^{-b_1} \cdots \mathfrak{p}_k^{-b_k}$ are similar to the same element of $\mathfrak{p}^{-1}C \setminus C$ modulo $\mathfrak{p}^{-1}C$ and C. In other words, there exists some α in $\mathfrak{p}^{-1}C \setminus C$ such that $\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k} = \alpha^{-1}\mathfrak{p}^{-1}C$ and there exists some y in C such that $\mathfrak{p}_1^{-b_1} \cdots \mathfrak{p}_k^{-b_k} = (\alpha + y)^{-1}\mathfrak{p}^{-1}C$.

This implies the number of prime ideals $\mathfrak{p}$, $[\mathfrak{p}] = [C^2]$ and $\mathfrak{p}^{-1} \notin \mathfrak{M}$, such that $\Gamma_{\mathfrak{p},\mathfrak{M}} < y$ is less than or equal to the number of prime ideals $\mathfrak{p}$, $[\mathfrak{p}] = [C^2]$ and $\mathfrak{p}^{-1} \notin \mathfrak{M}$, such that there exists a pair of distinct k-tuples of natural numbers $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$ such that

$$a_1 + \cdots + a_k \equiv 1 \equiv b_1 + \cdots + b_k \pmod{h},$$

both of the sums $a_1 + \cdots + a_k$ and $b_1 + \cdots + b_k$ are less than or equal to $(\frac{y}{C_{k,h}})^{\frac{1}{k}}$, and both ideals $\mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k}$ and $\mathfrak{p}_1^{-b_1} \cdots \mathfrak{p}_k^{-b_k}$ are similar to the same element of $\mathfrak{p}^{-1}C \setminus C$ modulo $\mathfrak{p}^{-1}C$ and C.

Step 2.

As each $\mathfrak{p}_i$ is in the same equivalence class as C, there exists some x_i for each i such that $\mathfrak{p}_i = x_i C$. Similarly, there exists some $x_\mathfrak{p}$ such that $\mathfrak{p} = x_\mathfrak{p} C^2$. By rewriting our ideals in terms of these elements, we have the following two equations:

$$x_1^{-a_1} \cdots x_k^{-a_k} C^{-(a_1 + \cdots + a_k)} = \mathfrak{p}_1^{-a_1} \cdots \mathfrak{p}_k^{-a_k} = \alpha^{-1}\mathfrak{p}^{-1}C = \alpha^{-1}x_\mathfrak{p}^{-1}C^{-1}$$

and

$$x_1^{-b_1} \cdots x_k^{-b_k} C^{-(b_1 + \cdots + b_k)} = \mathfrak{p}_1^{-b_1} \cdots \mathfrak{p}_k^{-b_k} = (\alpha + y)^{-1}\mathfrak{p}^{-1}C = (\alpha + y)^{-1}x_\mathfrak{p}^{-1}C^{-1}.$$

Inverting each term above yields

$$x_1^{a_1} \cdots x_k^{a_k} C^{(a_1 + \cdots + a_k)} = \alpha x_\mathfrak{p} C$$

and

$$x_1^{b_1} \cdots x_k^{b_k} C^{(b_1 + \cdots + b_k)} = (\alpha + y) x_\mathfrak{p} C.$$

Since C^{h_K} is principal and equal to (s), we can use this to rewrite the above equations as

$$x_1^{a_1} \cdots x_k^{a_k} s^{\frac{a_1 + \cdots + a_k - 1}{h_K}} C = \alpha x_\mathfrak{p} C$$

and

$$x_1^{b_1} \cdots x_k^{b_k} s^{\frac{b_1+\cdots+b_k-1}{h_K}} C = (\alpha + y) x_{\mathfrak{p}} C,$$

which implies that

$$(x_1^{a_1} \cdots x_k^{a_k} s^{\frac{a_1+\cdots+a_k-1}{h_K}}) = (\alpha x_{\mathfrak{p}})$$

and

$$(x_1^{b_1} \cdots x_k^{b_k} s^{\frac{b_1+\cdots+b_k-1}{h_K}}) = ((\alpha + y) x_{\mathfrak{p}})$$

as ideals. Choosing α and w appropriately, w a unit, we can use the above equations to see that

$$x_1^{a_1} \cdots x_k^{a_k} s^{\frac{a_1+\cdots+a_k-1}{h_K}} = \alpha x_{\mathfrak{p}}$$

and

$$x_1^{b_1} \cdots x_k^{b_k} s^{\frac{b_1+\cdots+b_k-1}{h_K}} = w(\alpha + y) x_{\mathfrak{p}}$$

as elements.

Note that the quotient of the right-hand sides is $w\frac{\alpha x_{\mathfrak{p}} + y x_{\mathfrak{p}}}{\alpha x_{\mathfrak{p}}} = w\frac{\alpha+y}{\alpha} = w(1 + \frac{y}{\alpha})$. Suppose $(y) = CJ$ and $(\alpha) = \mathfrak{p}^{-1}CI$, where J and I are integral ideals, so that $(\frac{y}{\alpha}) = \frac{CJ}{\mathfrak{p}^{-1}CI} = \frac{\mathfrak{p}J}{I}$. We know that $I \not\subset \mathfrak{p}$ since α is not in C, so that $v_{\mathfrak{p}}(\frac{y}{\alpha})$ is positive. The quotient of the left-hand sides is $x_1^{b_1-a_1} \cdots x_k^{b_k-a_k} s^{\frac{\sum b_i - \sum a_i}{h_K}}$, so that

$$x_1^{b_1-a_1} \cdots x_k^{b_k-a_k} s^{\frac{\sum b_i - \sum a_i}{h_K}} = w(1 + \frac{y}{\alpha})$$

and

$$w^{-1}x_1^{b_1-a_1}\cdots x_k^{b_k-a_k}s^{\frac{\sum b_i-\sum a_i}{h_K}}-1=\frac{y}{\alpha}$$

This implies that the $\mathfrak{p}$-valuation of

$$w^{-1}x_1^{b_1-a_1}\cdots x_k^{b_k-a_k}s^{\frac{\sum b_i-\sum a_i}{h_K}}-1$$

is positive.

Therefore, the number of prime ideals $\mathfrak{p}$, $[\mathfrak{p}]=[C^2]$ and $\mathfrak{p}^{-1}\notin\mathfrak{M}$, such that there exists a pair of distinct k-tuples of natural numbers $(a_1,\ldots,a_k)$ and $(b_1,\ldots,b_k)$ such that

$$a_1+\cdots+a_k\equiv 1\equiv b_1+\cdots+b_k \pmod{h_K};$$

both of the sums $a_1+\cdots+a_k$ and $b_1+\cdots+b_k$ are less than or equal to $(\frac{y}{C_{k,h}})^{\frac{1}{k}}$; and both ideals $\mathfrak{p}_1^{-a_1}\cdots\mathfrak{p}_k^{-a_k}$ and $\mathfrak{p}_1^{-b_1}\cdots\mathfrak{p}_k^{-b_k}$ are similar to the same element of $\mathfrak{p}^{-1}C\setminus C$ modulo $\mathfrak{p}^{-1}C$ and C is less than or equal to the number of prime ideals $\mathfrak{p}$, $[\mathfrak{p}]=[C^2]$ and $\mathfrak{p}^{-1}\notin\mathfrak{M}$, such that there exists an integer k-tuple $(c_1,\ldots,c_k)$ such that $\sum|c_i|\leq 2(\frac{y}{C_{k,h}})^{\frac{1}{k}}$; $\sum c_i\equiv 0 \pmod{h_K}$, and $v_{\mathfrak{p}}(w^{-1}x_1^{c_1}\cdots x_k^{c_k}s^{\frac{\sum c_i}{h_K}}-1)>0$.

Step 3.

Given any k-tuple $(c_1,\ldots,c_k)\in\mathbb{Z}^k$, there exists a component-wise minimal k-tuples $(d_1,\ldots,d_k)$ in $\mathbb{N}^k$ such that $c_i+d_i\geq 0$ for all i. Note that $\sum d_i\leq 2Y$. Let us define d' as $\left\lceil\frac{\sum d_i}{h_K}\right\rceil$, so that $\sum d_i+d'\equiv\sum c_i+\sum d_i+d'\equiv 0 \pmod{h_K}$.

If $v_{\mathfrak{p}}(w^{-1}x_1^{c_1}\cdots x_k^{c_k}s^{\frac{\sum c_i}{h_K}}-1)>0$, then

$$v_{\mathfrak{p}}\left(\frac{w^{-1}x_1^{c_1+d_1}\cdots x_k^{c_k+d_k}s^{\frac{d'+\sum c_i \sum d_i}{h_K}}-x_1^{d_1}\cdots x_k^{d_k}s^{\frac{d'+\sum d_i}{h_K}}}{x_1^{d_1}\cdots x_k^{d_k}s^{\frac{d'+\sum d_i}{h_K}}}\right)>0.$$

Suppose that c is an element of $\mathscr{O}_K$ such that $cC\subseteq\mathscr{O}_K$ and cx_i is in $\mathscr{O}_K$ for all i. This excludes the finitely many primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(c)>0$ from our consideration. We can then use this new notation to see that the $\mathfrak{p}$-adic valuation of

$$\left(\frac{w^{-1}x_1^{c_1+d_1}c^{c_1+c_1}\cdots x_k^{c_k+d_k}c^{c_k+c_k}s^{\frac{d'+\sum c_i+\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i+}{h_K}}}{x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'++\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}}}\right.$$

$$\left.-\frac{x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'++\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}}}{x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'++\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}}}\right)$$

is positive. We know that

$$v_{\mathfrak{p}}(x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'++\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}})=0,$$

so that the $\mathfrak{p}$-adic valuation of

$$\left(w^{-1}x_1^{c_1+d_1}c^{c_1+c_1}\cdots x_k^{c_k+d_k}c^{c_k+c_k}s^{\frac{d'+\sum c_i+\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i+}{h_K}}\right.$$

$$\left.-x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'+\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}}\right)$$

is positive. The above element is in $\mathscr{O}_K$, so the p-adic valuation of its norm is positive, where $\mathfrak{p}$ lies above p. We know the absolute value of the norm is equal to

$$|\ \mathrm{Nm}(c)|^{\ d'+\left(1+\frac{1}{h_K}\right)(\sum c_i+\sum d_i)}$$

times

$$\left|\ \mathrm{Nm}\left(w^{-1}x_1^{c_1+d_1}\cdots x_k^{c_k+d_k}s^{\frac{d'+\sum c_i+\sum d_i}{h_K}}-x_1^{d_1}\cdots x_k^{d_k}s^{\frac{d'+\sum d_i}{h_K}}\right)\right|\ .$$

Applying Lemma 2.3.9, we know that

$$\left|\ \mathrm{Nm}\left(w^{-1}x_1^{c_1+d_1}\cdots x_k^{c_k+d_k}s^{\frac{d'+\sum c_i+\sum d_i}{h_K}}-x_1^{d_1}\cdots x_k^{d_k}s^{\frac{d'+\sum d_i}{h_K}}\right)\right|$$

is less than or equal to $DM_0M_1^{c_1+2d_1}\cdots M_k^{c_k+2d_k}M_{k+1}^{\frac{2d'+2\sum d_i+\sum c_i}{h_K}}$ for some constants D, $M_0,\ldots,M_k,M_{k+1}$. Suppose that $M'=\max M_iM_j$, so the last expression is bounded above by $D(M')^{(\sum c_i+2\sum d_i+\frac{2d'+2\sum d_i+\sum c_i}{h_K}}$. If $M:=\mathrm{Nm}(c)M'$, the last expression is less than

$$DM^{(\sum c_i+2\sum d_i+\frac{2d'+2\sum d_i+\sum c_i}{h_K})}\leq D(M)^{6(1+\frac{3}{h_K})Y},$$

where $Y=(\frac{y}{C_{k,h}})^{\frac{1}{k}}$.

There are at most $\frac{\log D+6\left(1+\frac{3}{h_K}\right)(\log M)Y}{\log 2}$ prime elements p such that the p-adic valuation of the norm of

$$\left(w^{-1}x_1^{c_1+d_1}c^{c_1+c_1}\cdots x_k^{c_k+d_k}c^{c_k+c_k}s^{\frac{d'+\sum c_i+\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i+}{h_K}}\right.$$

$$\left.-\ x_1^{d_1}c^{c_1+d_1}\cdots x_k^{d_k}c^{c_k+d_k}s^{\frac{d'+\sum d_i}{h_K}}c^{\frac{d'+\sum c_i+\sum d_i}{h_K}}\right)$$

is positive by Lemma 2.3.6. There are at most

$$[K:\mathbb{Q}]\frac{\log D + 6(1+\frac{3}{h_K})(\log M)\,Y}{\log 2}$$

prime ideals $\mathfrak{p}$ such that the $\mathfrak{p}$-adic valuation of the above expression is positive.

Step 4.

There are at most $\frac{2^k}{k!hC_{k,h}}y + O(y^{\frac{k-1}{k}})$ integer k-tuples $(c_1,\ldots,c_k)$ such that $\sum|c_i| \leq 2(\frac{y}{C_{k,h}})^{\frac{1}{k}}$ and $\sum c_i \equiv 0 \pmod{h_K}$. The number of primes associated to each such k-tuple is $[K:\mathbb{Q}]\frac{\log D+6(1+\frac{3}{h_K})(\log M)\frac{y}{C_{k,h}})^{\frac{1}{k}}}{\log 2}$. We conclude that the number of prime ideals $\mathfrak{p}$, $[\mathfrak{p}] = [C^2]$ and $\mathfrak{p}^{-1} \notin \mathfrak{M}$, such that there exists an integer k-tuple $(c_1,\ldots,c_k)$ such that $\sum|c_i| \leq 2(\frac{y}{C_{k,h}})^{\frac{1}{k}}$; $\sum c_i \equiv 0 \pmod{h_K}$; and $v_{\mathfrak{p}}(x_1^{c_1}\cdots x_k^{c_k}s^{\frac{\sum c_i}{h_K}}-1) > 0$ is bounded above by

$$\left(\frac{2^k}{k!hC_{k,h}}y + C(y^{\frac{k-1}{k}})\right)\left([K:\mathbb{Q}]\frac{\log D + 6(1+\frac{3}{h_K})(\log M)(\frac{y}{C_{k,h}})^{\frac{1}{k}}}{\log 2}\right),$$

which is $O(y^{\frac{k+1}{k}})$. We conclude that the number of prime ideals $\mathfrak{p}$ such that $[\mathfrak{p}] = [C^2]$, $\mathfrak{p}^{-1} \notin \mathfrak{M}$, and $\Gamma_{\mathfrak{p},\mathfrak{M}} < y$ is $O(y^{\frac{k+1}{k}})$.

□

3.5. A Variation of Harper's Lemma for C

Definition 3.5.1. — (Variation of Harper's Construction for C) Let $\mathfrak{p}_1,\ldots\mathfrak{p}_k$ be a set of admissible primes with respect to C and let $\mathfrak{M} :=$

$\{\mathfrak{p}_1^{-a_1} \dots \mathfrak{p}_k^{-a_k} \mid a_1 + \dots + a_k \equiv 1 \pmod{h_K}, a_i \in \mathbb{N}\}$. Assuming $\mathfrak{p}$ is prime, let $B_{0,C,\mathfrak{M}} := \{\mathscr{O}_K\}$, let $B_{1,C,\mathfrak{M}} := B_{1,C} \cup \mathfrak{M} \setminus \mathscr{O}_K$, and let

$$B_{i,C,\mathfrak{M}} := \left\{ \mathfrak{p}^{-1} \;\middle|\; \begin{array}{c} \forall\, \alpha \in \mathfrak{p}^{-1}C \setminus C,\ \exists\, y \in C \\ \text{such that } (\alpha + y)^{-1}\mathfrak{p}^{-1}C \in B_{j,C,\mathfrak{M}}, \\ \text{for some } j < i, j + 1 \equiv i \pmod{h_K} \end{array} \right\}$$

for $i > 1$.

Let $B_{C,\mathfrak{M}} = \cup_{i=0}^{\infty} B_{i,C,\mathfrak{M}}$.

Note that for $i \geq 2$, $B_{i,C,\mathfrak{M}}$ consists solely of inverses of prime ideals. Also, any two ideals in $B_{i,C,\mathfrak{M}}$ are in the same ideal class, namely $[C^{-i}]$. What this variation of Motzkin's Construction does is expand the first non-trivial set with extra ideals from $A_{1,C}$ so that the early sets in this variation are larger. If Cl_K is cyclic and if one of these early sets is large enough, then we can show that $B_{C,\mathfrak{M}}$ contains all of the inverses of $\mathscr{O}_K$'s prime ideals.

Theorem 3.5.2. — ***(A Variation on Harper's Lemma for*** C***)*** *If $B_{C,\mathfrak{M}}$ contains the inverse of every prime in $\mathscr{O}_K$, then C is a Euclidean ideal class.*

Proof. — The techniques in this proof are similar to the techiniques in [**5**]. Suppose every prime $\mathfrak{p}^{-1}$ is in $B_{C,\mathfrak{M}}$. Let $\omega_{\mathfrak{M}}(I)$ be the number of prime divisors of I^{-1} that are in $\mathfrak{M}^{-1}$ and let $\omega(I)$ be the number of prime divisors of I^{-1} that are not in $\mathfrak{M}^{-1}$. Let $\lambda(\mathfrak{p}^{-1})$ be i if $\mathfrak{p}^{-1}$ is in $B_{i,C,\mathfrak{M}} \setminus B_{j,C,\mathfrak{M}}$ for all $j < i$ and extend λ to E multiplicatively. Each of the three functions is additive, so the function $\phi : E \longrightarrow \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, $\phi(I) = (\omega(I), \omega_{\mathfrak{M}}(I), \lambda(I))$ is also additive. Note that $\phi(I) = (0, 0, 0)$ if and only if $I = \mathscr{O}_K$.

We will prove by induction on the size of $\phi(I)$ that ϕ is a Euclidean algorithm for C. If $\mathfrak{p}$ is prime, than for any $\alpha \in \mathfrak{p}^{-1}C \setminus C$, there exists some y in C such that $(\alpha + y)^{-1}\mathfrak{p}^{-1}C$ is either $\mathscr{O}_K$ or the inverse of some prime $\mathfrak{q}$ such that $\lambda(\mathfrak{q}^{-1}) < \lambda(\mathfrak{p}^{-1})$. In either case, $\phi((\alpha + y)^{-1}\mathfrak{p}^{-1}C) < \phi(\mathfrak{p}^{-1})$.

Let I be an element of E, I^{-1} not prime, and suppose that for all J such that $\phi(J) < \phi(I)$ and for all $x \in JC \setminus C$, there exists some y in C such that $\phi((x + y)^{-1}JC) < \phi(J)$. Let x be an element of $IC \setminus C$. If (x, C) is IC, then there exists some y in C such that $(x + y)^{-1}IC$ is prime by Theorem 3.1.18 and $\phi((x + y)^{-1}IC) < \phi(I)$.

Let (x, C) not be equal to IC and let L be the integral ideal of maximal norm such that L contains both I^{-1} and $xI^{-1}C^{-1}$. The set of prime divisors of $I^{-1}L^{-1}$ is properly contained in the set of prime divisors of I^{-1}, so we know that both $\omega_{\mathfrak{M}}(IL) \leq \omega_{\mathfrak{M}}(I^{-1})$ and $\omega(IL) \leq \omega(I)$, but both cannot be equalities. This implies that $\phi(IL) < \phi(I)$. Since x is in I, it is also in IL. Using the inductive hypothesis, there exists some y in C such that $\phi((x + y)^{-1}ILC) < \phi(IL)$. The function ϕ is additive, so $\phi((x + y)^{-1}IC) < \phi(I)$. □

3.6. The Large Sieve for Euclidean Ideal Classes

The large sieve is at the heart of Harper's work on Euclidean rings. In order to generalize his work and examine the asymptotic growth of the sets $B_{C,i,\mathfrak{M}}$, a generalized large sieve is needed. Before the generalized version can be stated, however, we need the following definitions.

Definition 3.6.1. — For the following, given an ideal $\mathfrak{p}$, let $f(\mathfrak{p})$ be the size of the image of $\mathscr{O}_K^\times$ in $(\mathscr{O}_K/\mathfrak{p})^\times$. For each coset in the image of $\mathscr{O}_K^\times$ in $(\mathscr{O}_K/\mathfrak{p})^\times$, choose one unit that maps to that coset. Let $U(\mathfrak{p})$ be the collection of those units. Note that $|U(\mathfrak{p})|$ is $f(\mathfrak{p})$.

Recall the following definition.

Definition 3.6.2. — Given $\mathfrak{A}$, a finite set of non-associated integers, a prime ideal $\mathfrak{p}$ and some $\alpha \in R$, we define the following function

$$Z(\alpha, \mathfrak{p}) := \left|\{x \in \mathfrak{A} : x \equiv \alpha \pmod{\mathfrak{p}}\}\right| .$$

For our purposes, we want to apply the large sieve to sets of ideals, so that we look at how a finite set of ideals are distributed among the similarity classes of finite set of prime ideals, rather than how finite sets of elements are distributed among the equivalence classes of prime ideals. We will therefore look at the function $Z(\alpha, \mathfrak{p}, C)$ rather than $Z(\alpha, \mathfrak{p})$.

Definition 3.6.3. — Let C be a non-zero integral ideal and let $n \in \mathbb{Z}^+$. Let A be a finite set of distinct fractional ideals I in E, such that if I and J are in A, then $[I] = [J]$. If $\mathfrak{p}$ is a prime ideal such that $[\mathfrak{p}^{-1}] = [IC^{-1}]$

for I in A, and if β is in $\mathfrak{p}^{-1}C$, we define

$$Z(\beta, \mathfrak{p}, C) := \begin{cases} |\{I \in A \mid \exists\, y \in C \text{ such that } (\beta + y)^{-1}\mathfrak{p}^{-1}C = I\}| \\ \text{if } \beta \notin C \\ f(\mathfrak{p})\ |\{I \in A \mid \exists\, y \in C \text{ such that } (\beta + y)^{-1}\mathfrak{p}^{-1}C = I\}| \\ \text{if } \beta \in C \end{cases}$$

Definition 3.6.4. — For any I that is equivalent to C^n, $n > 0$, fix some $x_I \in K^\times$ such that $I = x_I^{-1}C^n$.

Henceforth, assume C is an integral ideal. This means $(x_I) = I^{-1}C^n$, so that x_I is an element of C^n and is therefore an integer. Note that since $[\mathfrak{p}^{-1}C] = [C^n]$, there exists some $x_\mathfrak{p}$ such that $\mathfrak{p}^{-1}C = x_\mathfrak{p}^{-1}C^n$, so that $\mathfrak{p}^{-1} = x_\mathfrak{p}^{-1}C^{n-1}$. Therefore $(x_\mathfrak{p})^{-1}C^{n-1} = \mathfrak{p}^{-1}$ and thus $x_\mathfrak{p}$ is an element of $\mathfrak{p}C^{n-1}$. We conclude $x_\mathfrak{p}$ is an integer.

Definition 3.6.5. — Given a finite set A, such that $A \subset \{I \mid I \in E \text{ and } [I] = [C^n]\}$, define $\mathfrak{A} := \{x_I \mid I \in A\}$.

Using our notation above, we can prove the following theorem.

Theorem 3.6.6. — *For C a non-zero integral ideal, $\mathfrak{p}$ a prime ideal that is relatively prime to C, and $\beta \in \mathfrak{p}^{-1}C$, we have*

$$Z(\beta, \mathfrak{p}, C) = \begin{cases} \sum_{u \in U(\mathfrak{p})} Z(u\beta x_\mathfrak{p}, \mathfrak{p}) \textit{ if } \beta \notin C \\ f(\mathfrak{p}) Z(0, \mathfrak{p}) \textit{ if } \beta \in C \end{cases}$$

In order to prove this, however, we will first need the following lemmas.

Lemma 3.6.7. — *Given two elements x and $y \in C^n$, $n \geq 0$, $x \equiv y$ $(mod\, \mathfrak{p}C^n)$ if and only if $x \equiv y$ $(mod\, \mathfrak{p})$.*

Proof. — Since $x \equiv y$ (mod $\mathfrak{p}C^n$), then $x - y$ is in $\mathfrak{p}C^n$ and is therefore in $\mathfrak{p}$, so $x \equiv y$ (mod $\mathfrak{p}$).

Conversely, suppose $x \equiv y$ (mod $\mathfrak{p}$). Then $x - y \in \mathfrak{p}$, but we also know that $x - y \in C^n$ because both $x, y \in C^n$. As $x - y$ is in both $\mathfrak{p}$ and C^n, it is in the intersection of $\mathfrak{p}$ and C^n. We know that $\mathfrak{p}$ and C are relatively prime, so $\mathfrak{p}$ and C^n are relatively prime, which means that their intersection is in fact their product. We conclude that $x \equiv y$ (mod $\mathfrak{p}C^m$). □

Lemma 3.6.8. — *Given an element y in $K^\times$, the product $yx_\mathfrak{p}$ is in $\mathfrak{p}C^n$ if and only if y is an element of C.*

Proof. — If y is in C, then $yx_\mathfrak{p}$ is an element of $(\mathfrak{p}C)(C^{n-1}) = \mathfrak{p}C^n$.

If $yx_\mathfrak{p}$ is an element of $\mathfrak{p}C^n$, then $(yx_\mathfrak{p}) = I\mathfrak{p}C^n$, for some non-zero integral ideal I. Therefore $(y) = Ix_\mathfrak{p}^{-1}C^{n-1}\mathfrak{p}C = I\mathfrak{p}^{-1}\mathfrak{p}C$ so that $(y) = IC$. We conclude $y \in IC$, which implies that $y \in C$. □

Lemma 3.6.9. — *Multiplication by $x_\mathfrak{p}$ is an isomorphism from $\mathfrak{p}^{-1}C/C$ to $C^n/\mathfrak{p}C^n$.*

Proof. — Given some β in $\mathfrak{p}^{-1}C$, we know that $x_\mathfrak{p}\beta$ is in $\mathfrak{p}C^{n-1}\mathfrak{p}^{-1}C$, which is equal to C^n, so that multiplication by $x_\mathfrak{p}$ is a map from $\mathfrak{p}^{-1}C$ to C^n. Let b be an element of C^n. Then $x_\mathfrak{p}^{-1}b$ is an element of $\mathfrak{p}^{-1}C^{1-n}C^n = \mathfrak{p}^{-1}C$, so that multiplication by $x_\mathfrak{p}$ is surjective.

By Lemma 3.6.8, the product $yx_{\mathfrak{p}}$ is in $\mathfrak{p}C^n$ if and only if y is in C, so that $x_{\mathfrak{p}}^{-1}\mathfrak{p}C^n$ is C, so the kernel of the composition of multiplication by $x_{\mathfrak{p}}$ and taking quotienting by $\mathfrak{p}C^n$ is the ideal C. The isomorphism follows. □

We can now begin the proof of Theorem 3.6.6.

Proof. — (Proof of Theorem 3.6.6) Using the elements defined above, we can rewrite the equation

$$I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$$

as

$$x_I^{-1}C^n = (\beta + y)^{-1}x_{\mathfrak{p}}^{-1}C^{n-1}C.$$

The above statement on ideals implies that

$$ux_I = \beta x_{\mathfrak{p}} + yx_{\mathfrak{p}} \text{ for some } u \in \mathscr{O}_K^{\times},$$

a statement on elements. Note that both ux_I and $\beta x_{\mathfrak{p}}$ are in C^n and that $yx_{\mathfrak{p}}$ is in $\mathfrak{p}C^n$ if and only if y is in C by Lemma 3.6.8. Therefore, the statement that there exists some

$$y \in C \text{ such that } I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$$

is equivalent to saying

$$ux_I \equiv \beta x_{\mathfrak{p}} \pmod{\mathfrak{p}C^n} \text{ for some } u \in \mathscr{O}_K^{\times}.$$

We know from Lemma 3.6.8 that this last condition is equivalent to

$$x_I \equiv u'\beta x_{\mathfrak{p}} \text{ (mod } \mathfrak{p}) \text{ for some } u' \in \mathscr{O}_K^{\times}.$$

Note that β is in C if and only if $\beta x_{\mathfrak{p}} \equiv 0(\text{mod } \mathfrak{p}C^n)$, which implies that $ux_I \equiv 0(\text{mod } \mathfrak{p}C^n)$, which is true if and only if $x_I \equiv 0(\text{mod } \mathfrak{p})$ by Lemma 3.6.7. Since there exists an element y in C such that $I = (\alpha + y)^{-1}\mathfrak{p}^{-1}C$ if and only if $x_I \equiv 0 \text{ (mod } \mathfrak{p})$,we conclude that if β is in C, then

$$Z(\beta, \mathfrak{p}, C) = f(\mathfrak{p}) \, |\{I \in A : \exists\, y \in C \text{ such that } (\beta + y)^{-1}\mathfrak{p}^{-1}C = I\}|$$

$$= f(\mathfrak{p}) \, |\{x_I \in \mathfrak{A} : x_I \equiv 0 \, (\text{mod } \mathfrak{p})\}| = f(\mathfrak{p}) Z(\beta x_{\mathfrak{p}}, \mathfrak{p}).$$

If β is not in C, this means there exists some y in C such that $I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$ if and only if $x_I \equiv u\beta x_{\mathfrak{p}}$ (mod $\mathfrak{p}$) for some $u \in \mathscr{O}_K^{\times}$. We conclude that if β is not in C, then

$$Z(\beta, \mathfrak{p}, C) = |\{I \in A : \exists\, y \in C \text{ such that } (\alpha + y)^{-1}\mathfrak{p}^{-1}C = I\}|$$

$$= |\{x_I \in \mathfrak{A} : x_I \equiv u\beta x_p \text{ for some } u \in \mathscr{O}_K^{\times}\}|$$

$$= \sum_{u \in U(\mathfrak{p})} |\{x_I \in \mathfrak{A} : x_I \equiv u\beta x_{\mathfrak{p}} \, (\text{mod } \mathfrak{p})\}| = \sum_{u \in U(\mathfrak{p})} Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}).$$

□

Now that we understand the function $Z(\beta, \mathfrak{p}, C)$ better, we can begin to get a grip on $\sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2$.

Theorem 3.6.10. — *Let C be a non-zero integral ideal, and let A be a finite collection of ideals, $A \subset E \cap [C^n]$. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{p}$ and C be relatively prime. Then*

$$\sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2 \leq \sum_{\alpha \ (mod \ \mathfrak{p})} \left(Z(\alpha, \mathfrak{p}) - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2.$$

Proof. — From the above, if β is in C, then

$$\left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2 = \left(\frac{f(\mathfrak{p}) Z(0, \mathfrak{p})}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2,$$

which equals

$$\left(Z(0, \mathfrak{p}) - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2.$$

If β is not in C, then

$$\left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2 = \left(\frac{\sum_{u \in U(\mathfrak{p})} Z(u\beta x_{\mathfrak{p}})}{f(\mathfrak{p})} - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right)^2.$$

We can rewrite the right hand side as

$$\left(\sum_{u \in U(\mathfrak{p})} \left(\frac{Z(u\beta x_{\mathfrak{p}}, \mathfrak{p})}{f(\mathfrak{p})} - \frac{\mid A \mid}{f(\mathfrak{p}) \mathrm{Nm} \mathfrak{p}} \right) \right)^2,$$

which equals

$$\frac{1}{(f(\mathfrak{p}))^2} \left(\sum_{u \in U(\mathfrak{p})} \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{\mid A \mid}{\mathrm{Nm}(\mathfrak{p})} \right) \right)^2.$$

If we apply Cauchy-Schwartz, we see that the above is less than or equal to

$$\frac{1}{(f(\mathfrak{p}))^2}\sum_{u\in U(\mathfrak{p})}f(\mathfrak{p})\left(Z(u\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2=\frac{1}{f(\mathfrak{p})}\sum_{u\in U(\mathfrak{p})}\left(Z(u\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2.$$

Summing up over all non-zero classes β in $\mathfrak{p}^{-1}C/C$, yields

$$\sum_{\substack{\beta\ (\mathrm{mod}\ C)\\ \beta\not\equiv 0\ (\mathrm{mod}\ C)}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2\leq\frac{1}{f(\mathfrak{p})}\sum_{\substack{\beta\ (\mathrm{mod}\ C)\\ \beta\not\equiv 0}}\sum_{u\in U(\mathfrak{p})}\left(Z(u\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2$$

$$=\frac{1}{f(\mathfrak{p})}\sum_{u\in U(\mathfrak{p})}\sum_{\substack{\beta\ (\mathrm{mod}\ C)\\ \beta\not\equiv 0}}\left(Z(u\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2.$$

The inner sum is independent of choice of u so that the above is equal to

$$\frac{1}{f(\mathfrak{p})}f(\mathfrak{p})\sum_{\substack{\beta\ (\mathrm{mod}\ C)\\ \beta\not\equiv 0}}\left(Z(\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2,$$

which can be further simplified to

$$\sum_{\substack{\beta\ (\mathrm{mod}\ C)\\ \beta\not\equiv 0}}\left(Z(\beta x_{\mathfrak{p}},\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}\mathfrak{p}}\right)^2=\sum_{\substack{\alpha\ (\mathrm{mod}\ \mathfrak{p}),\\ \alpha\not\equiv 0}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2$$

by Lemma 3.6.9. Finally, by considering both cases at once, we get

$$\sum_{\beta\in\mathfrak{p}^{-1}C \pmod{C}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2\leq \sum_{\alpha \pmod{\mathfrak{p}}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2.$$

□

Theorem 3.6.11. — ***(Large Sieve with Respect to*** C***)***

Let A *and* P *be finite sets of fractional ideals, with* $A\subset E\cap[C^n]$ *and* $P\subset\{\mathfrak{p}:\mathfrak{p}$ *is prime,* $[\mathfrak{p}^{-1}]=[C^{n-1}]$*. If* $X=\max_{I\in A}\mathrm{Nm}(I^{-1})$ *and* $Q=\max_{\mathfrak{p}^{-1}\in P}\mathrm{Nm}(\mathfrak{p})$*, then*

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\beta\in\mathfrak{p}^{-1}C/\mathfrak{p}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2<<(Q^2+X)|A|\,.$$

The implied constant depends only on K*, the ideal* C*, and on* n*.*

Proof. — We know from Theorem 3.6.10 that

$$\sum_{\beta\in\mathfrak{p}^{-1}C \pmod{C}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2\leq\sum_{\alpha \pmod{\mathfrak{p}}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2.$$

This means that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\beta\in\mathfrak{p}^{-1}C \pmod{C}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2$$

$$\leq\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\alpha \pmod{\mathfrak{p}}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2.$$

The maximum norm of any element in $\mathfrak{A}$ is

$$\max_{x\in\mathfrak{A}}\mathrm{Nm}(x)=\max_{I\in A}\mathrm{Nm}(x_I)=\mathrm{Nm}(C^n)X.$$

Applying the large sieve, we know that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\alpha \pmod{\mathfrak{p}}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2 << \left(Q^2+\mathrm{Nm}(C)^n X\right)\,|\mathfrak{A}|\;.$$

The sizes of A and $\mathfrak{A}$ are the same, so that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\alpha \pmod{\mathfrak{p}}}\left(Z(\alpha,\mathfrak{p})-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2 << \left(Q^2+\mathrm{Nm}(C)^n X\right)\,|A|,$$

where the implied constant only depends on the number field K. When we put this together with the earlier inequality, we see that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\sum_{\beta\in\mathfrak{p}^{-1}C \pmod{C}}\left(\frac{Z(\beta,\mathfrak{p},C)}{f(\mathfrak{p})}-\frac{\mid A\mid}{\mathrm{Nm}(\mathfrak{p})}\right)^2 << \left(Q^2+X\right)\,|A|,$$

with the implied constant now depending on both the choice of number field K, C, and n.

□

Harper did not use the large sieve in his paper, so much as a corollary of the large sieve. In order to state our version of the corollary, we need the following definition.

Definition 3.6.12. — Let $\omega(\mathfrak{p}) := \left|\{[\alpha]\in\mathfrak{p}^{-1}C/C \mid Z(\alpha,\mathfrak{p},C)=0\}\right|$.

Corollary 3.6.13. — *Let A and P be finite sets of fractional ideals, with $A\subset E\cap[C^n]$ and $P\subset\{\mathfrak{p}\mid\mathfrak{p}$ is prime, $[\mathfrak{p}^{-1}]=[C^{n-1}]\}$. If $X=$*

$\max_{I\in A}\mathrm{Nm}(I^{-1})$ *and* $Q=\max_{\mathfrak{p}^{-1}\in P}\mathrm{Nm}(\mathfrak{p})$*, then*

$$\sum_{\mathfrak{p}\in P}\frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} << \frac{Q^2+X}{|\,A\,|},$$

where the implied constant depends only on K*,* C*, and* n*.*

Proof. — We know from Theorem 3.6.11 that

$$\sum_{\beta\in\mathfrak{p}^{-1}C/C}\left(Z(\beta,\mathfrak{p},C)-\frac{|\,A\,|}{\mathrm{Nm}(\mathfrak{p})}\right)^2$$

$$\geq \sum_{\left\{\begin{array}{c}\beta\in\mathfrak{p}^{-1}C/C\\ Z(\alpha,\mathfrak{p},C)=0\end{array}\right\}}\left(Z(\alpha,\mathfrak{p},C)-\frac{|\ A\ |}{\mathrm{Nm}(\mathfrak{p})}\right)^2=\frac{|\,A\,|^2\,\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})^2}.$$

Since the quantity $\frac{|A|^2\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})^2}$ is less or equal to than

$$\sum_{\beta\in\mathfrak{p}^{-1}C \pmod{C}}\left(Z(\alpha,\mathfrak{p},C)-\frac{|\ A\ |}{\mathrm{Nm}(\mathfrak{p})}\right)^2,$$

we know that

$$\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})\frac{|\ A\ |^2\,\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})^2} << (Q^2+X)\,|A|$$

and therefore

$$\sum_{\mathfrak{p}\in P}\frac{|\ A\ |^2\,\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} << (Q^2+X)\,|A|\,.$$

We conclude that

$$\sum_{\mathfrak{p}\in P}\frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} << \frac{Q^2+X}{|A|}.$$

□

3.7. Growth results

We need the large sieve in order to look at the growth of the sets $B_{i,C,\mathfrak{M}}$. In order to do so, we need the following definition.

Definition 3.7.1. — Given the set $B_{i,C,\mathfrak{M}}$, let

$$B_{i,C,\mathfrak{M}}(x) := \{I \in B_{i,C,\mathfrak{M}} \mid \mathrm{Nm}(I^{-1}) \leq x\},$$

let

$$B^c_{i,C,\mathfrak{M}} := \{I \in E \setminus B_{i,C,\mathfrak{M}} \mid [I] = [J] \text{ for any } J \in B_{i,C,\mathfrak{M}}\},$$

and let

$$B^c_{i,C,\mathfrak{M}}(x) := \{I \in E\backslash B_{i,C,\mathfrak{M}} \mid \mathrm{Nm}(I^{-1}) \leq x, [I] = [J] \text{ for any } J \in B_{i,C,\mathfrak{M}}\}.$$

We can now state the section's main result.

Theorem 3.7.2. — *If $\mathscr{O}_K$ has a unit of infinite order, if $[C]$ generates Cl_K, and if*

$$|B_{n,C,\mathfrak{M}}(x)| >> \frac{x}{\log^2 x}$$

for some $n \in \mathbb{Z}^+$, then $E = A_C$ and $[C]$ is a Euclidean ideal class for the ring.

Proof. — First we shall prove that if

$$|B_{n,C,\mathfrak{M}}(x)| >> \frac{x}{\log^2 x},$$

then $|B_{n+1,C,\mathfrak{M}}(x)|\sim \frac{x}{h_K \log x}$. Let A be the set $B_{n,C,\mathfrak{M}}(x^2)$, let $X \leq x^2$, and let P be the set $B^c_{n+1,C,\mathfrak{M}}(x)$, so that $Q \leq x$. By Corollary 3.6.13, we know that

$$\sum_{\mathfrak{p}\in P} \frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} << \frac{Q^2+X}{\mid A \mid} << \frac{2x^2}{\frac{x^2}{\log^2(x^2)}} = \frac{2x^2}{\frac{x^2}{2\log^2(x)}} << \log^2(x).$$

Note that if I is in $B^c_{n,C,\mathfrak{M}}$, then there is some x in $IC \setminus C$ such that there is no y in C such that $(x+y)^{-1}IC$ is in $B_{n-1,C,\mathfrak{M}}$. Given any $u \in \mathscr{O}_K^\times$, we know that $(ux+uy)^{-1}IC = (x+y)^{-1}IC$ and that uy is in C. Therefore, if $Z(x,\mathfrak{p}^{-1},C)$ is zero, then so is $Z(ux,\mathfrak{p}^{-1},C)$ for any unit u. This means that if there is one x in $\mathfrak{p}^{-1}C \setminus C$ such that $Z(x,\mathfrak{p}) = 0$, then there are at least $f(\mathfrak{p})$ cosets with elements e such that $Z(e,\mathfrak{p}) = 0$, and the function $\omega(\mathfrak{p})$ is divisible by $f(\mathfrak{p})$.

If $\mathscr{O}_K$ has infinitely many units, then

$$|\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \ \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| << x^{1-2\epsilon}$$

by Theorem 2.3 and therefore

$$|\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| = o\left(\frac{x}{\log x}\right).$$

The above estimate implies that

$$\sum_{\substack{\mathfrak{p}^{-1} \,\in\, P^c(x) \\ f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}}} \frac{\omega(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} \geq \sum_{\substack{\mathfrak{p}^{-1} \,\in\, P^c(x) \\ f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}}} \frac{\mathfrak{f}(\mathfrak{p})}{\mathrm{Nm}(\mathfrak{p})} > \frac{|\{\mathfrak{p} \in B^c_{n+1,C,\mathfrak{M}} : f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}\,|}{x^{\frac{1}{2}+\epsilon}}.$$

By combining this with the first bound in the proof, we know that

$$\log^2(x) >> \frac{|\{\mathfrak{p} \in B^c_{n+1,C} : f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|}{x^{\frac{1}{2}+\epsilon}}.$$

Multiplying both sides by $x^{\frac{1}{2}+\epsilon}$ yields

$$|\{\mathfrak{p} \in B^c_{n+1,C,\mathfrak{M}} : f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| = o\left(\frac{x}{\log(x)}\right).$$

Since the size of $B^c_{n+1,C,\mathfrak{M}}(x)$ is equal to

$$|\{\mathfrak{p} \in B^c_{n+1,C}(x) \mid f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| + |\{\mathfrak{p} \in B^c_{n+1,C,\mathfrak{M}}(x) \mid f(\mathfrak{p}) \leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|,$$

we know the size of $B^c_{n+1,C,\mathfrak{M}}(x)$ is less than or equal to

$$|\{\mathfrak{p} \in B^c_{n+1,c}(x) \mid f(\mathfrak{p}) > \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| + |\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x, f(\mathfrak{p}) \leq \mathrm{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|$$

and can thus conclude $|B^c_{n+1,C,\mathfrak{M}}(x)| = o\left(\frac{x}{\log(x)}\right)$ and

$$|B_{n+1,C,\mathfrak{M}}(x)| \sim \frac{x}{h_K \log x}.$$

Suppose that $\mathfrak{p}$ is prime, that $[\mathfrak{p}] = [C^{n+2}]$, and that x is an element of $\mathfrak{p}^{-1}C \setminus C$. There is a positive density of prime ideals $\mathfrak{q}$ such that $\mathfrak{q}^{-1} = (x+y)^{-1}\mathfrak{p}^{-1}C$ for some y in C by Theorem 3.1.18. The density of primes in $[C^{n+1}]$ in the set of all primes is $\frac{1}{h_K}$, which is the same as the density of primes $\mathfrak{q}$ such that $\mathfrak{q}^{-1}$ is in $B_{n+1,C,\mathfrak{M}}$, so there exists some prime $\mathfrak{q}$ in $B_{n+1,C,\mathfrak{M}}$ such that $\mathfrak{q}^{-1} = (x+y)^{-1}\mathfrak{p}^{-1}C$ for some y in C. We conclude that $\mathfrak{p}^{-1}$ is in $B_{n+2,C,\mathfrak{M}}$.

This implies that $B_{n+2,C,\mathfrak{m}}$ is equal to $E \cap [C^{-n-2}]$. We then apply Theorem 3.3.3 and conclude that $[C]$ is a Euclidean ideal class. $\square$

INDEX

BIBLIOGRAPHY

[1] David A. Clark, “A quadratic field which is Euclidean but not norm-Euclidean,” *Manuscripta Mathematica* 83, 327-330, 1994.

[2] David A. Clark and M.Ram Murty, “The Euclidean algorithm for Galois extensions of $\mathbb{Q}$, ” *Journal fr die reine und angewandte Mathematik* 459, 151-162, 1995.

[3] Hester Graves and Nick Ramsey, “On the Harper/Graves Construction in Imaginary Quadratic Number Fields,” in preparation

[4] Rajiv Gupta and M.Ram Murty, “A Remark on Artin’s Conjecture,” *Invent. Math* 78, 127-130, 1984.

[5] M. Harper, “$\mathbb{Z}[\sqrt{14}]$ is Euclidean,” *Canad. J. Math* 56, 55-70, 2004.

[6] M. Harper and M. Ram Murty, “ Euclidean rings of algebraic integers,” *Canad. J. Math* 56, 71-76, 2004.

[7] K. Ireland and M. Rosen, “A Classical Introduction to Modern Number Theory,” Springer-Verlag, New York, NY, 1990.

[8] H.K. Lenstra, “Euclidean Ideal Classes,” *Asterique* 61, 121-131, 1979.

[9] Th. Motzkin, ”The Euclidean Algorithm,” *Bull. Amer. Math. Soc.* 55, 1142-6, 1949.

[10] P. Samuel, “About Euclidean Rings,” *Journal of Algebra* 19, 282-301, 1971.

[11] Peter J. Weinberger, ”On Euclidean rings of algebraic integers”, *Proceedings of Symposia in Pure Mathematics (AMS)* 24: 321-332, 1973.

[12] Robin J.Wilson, “The large sieve in algebraic number Fields”, *Mathematika* 16, 189-204, 1969.