Fall 2018

Lenstra-Hurwitz Cliques In Real Quadratic Fields

Daniel S. Lopez
San Jose State University

LENSTRA-HURWITZ CLIQUES IN REAL QUADRATIC FIELDS

A Thesis

Presented to

The Faculty of the Department of Mathematics and Statistics

San José State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Daniel S. Lopez

December 2018

The Designated Thesis Committee Approves the Thesis Titled

LENSTRA-HURWITZ CLIQUES IN REAL QUADRATIC FIELDS

by

Daniel S. Lopez

APPROVED FOR THE DEPARTMENT OF MATHEMATICS AND STATISTICS

SAN JOSÉ STATE UNIVERSITY

December 2018

Dr. Jordan Schettler	Department of Mathematics & Statistics
Dr. Slobodan Simić	Department of Mathematics & Statistics
Dr. Wasin So	Department of Mathematics & Statistics

ABSTRACT

LENSTRA-HURWITZ CLIQUES IN REAL QUADRATIC FIELDS

by Daniel S. Lopez

Let K be a number field and let $\mathcal{O}_K$ denote its ring of integers. We can define a graph whose vertices are the elements of $\mathcal{O}_K$ such that an edge exists between two algebraic integers if their difference is in the units $\mathcal{O}_K^\times$. Lenstra showed that the existence of a sufficiently large clique (complete subgraph) will imply that the ring $\mathcal{O}_K$ is Euclidean with respect to the field norm. A recent generalization of this work tells us that if we draw more edges in the graph, then a sufficiently large clique will imply the weaker (but still very interesting) conclusion that K has class number one. This thesis aims to understand this new result and produce further examples of cliques in rings of integers. Lenstra, Long, and Thistlethwaite analyzed cliques and gave us class number one through a prime element. We were able to extend and generalize their result to larger cliques through prime power elements while still preserving our desired property of class number one. Our generalization gave us that class number one is preserved if the number field K contained a clique that is generated by a prime power.

DEDICATION

I dedicate my work to my mother, my family and my community. We all belong in math.

ACKNOWLEDGEMENTS

First I would like to thank my advisor Dr. Jordan Schettler for his endless support, patience, and mentoring through my endeavors here at San José State University. I am more than honored to have him solidify what it is to be a mathematician, an educator and a friend. I'd also like to thank Dr. Wasin So and Dr. Slobodan Simić for being a part of my committee and being patient with me in the classroom.

Dr. Bem Cayco, Dr. Maciejewski, and Dr. Hsu thank you for your support and wisdom while tackling classes and teaching at the same time. I will forever cherish my time spent here learning how to be a great educator. To all my friends from here at San José State and from home thank you for the laughs, the time we shared on the phone, in office hours, in class, out eating/drinking, or in the library. These have been some of the best years of my life, I will forever cherish our friendship.

Last but not least, I would like to thank my Mom, my brother Julio, my brother Jovann and my girlfriend Elizabeth. Without their unconditional love and support, these last few years would not have been possible. Everything I am and will be is thanks to you all.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

CHAPTER 1

INTRODUCTION

1.1 Motivation

The classification of quadratic fields having a Euclidean ring of integers is a major unsolved problem in number theory. Weinberger showed back in 1973 that, assuming the generalized Riemann hypothesis, a quadratic number field which has infinitely many units in its rings of integers is in fact Euclidean if and only if it is a principal ideal domain. However, since there are principal ideal domains which are not norm-Euclidean, then there should be examples of rings of integers which are just Euclidean and not norm-Euclidean. The first such known example was $\mathbb{Q}(\sqrt{69})$. This opened the exploration to finding more quadratics which satisfy this property.

Lenstra and Hurwitz made some remarkable contributions in number theory by looking for new techniques to show when a given field is Euclidean. Hurwitz toyed with the idea of a field being Euclidean with the sufficient condition that its ring of integers must contain many elements, all of whose difference are units. In [Len77], Lenstra showed that we could view these sets as graphs where the points would connect if the difference is a unit in its respected ring of integers. Lenstra's major result involves a condition on the size of the subgraph in this graph, which allowed for a new technique of proving fields to be Euclidean.

From here, Long and Thistlethwaite [LT16] built on the work of Lenstra to show that a less constrained condition can be used to prove that the quadratic field has

class number one. This analysis is promising in the study of finding quadratic fields of class number one since we believe that there is an infinite number of real quadratic fields with class number one as conjectured by Gauss [Neu99].

1.2 Background

In this section, we introduce basic concepts in group theory, field theory, number theory and graph theory. More importantly, we familiarize ourselves with some of the important objects, notations and examples that help us throughout the course of the thesis.

1.2.1 Group Theory

A non-empty set G with an *associative* binary operation, where there is an identity and every element has an *inverse* is called a *group*. An *abelian* group has the added structure of also being commutative.

Example 1 (General Linear Group)**.** The following collection of matrices is a group under matrix multiplication:

$\mathrm{GL}(n, \mathbb{R}) = \{n \times n \text{ invertible matricies}\}$.

More specifically we can look at

$$\mathrm{GL}(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

Both of these sets can be shown to be groups; however, neither of them are abelian groups. We are at liberty to choose the following set of numbers apart from $\mathbb{R}$ and preserve the group structure of GL: $\mathbb{Q}, \mathbb{C},$ or $, \mathbb{Z}_p$ where p is a prime number.

If H is a subset of G and H itself is a group under the operation of G then we say that H is a *subgroup of* G. An important type of subgroup is one called *normal*. Normal subrougs happen when the left and right cosets are the same ($aH = Ha$) for all a in G, this is denoted by $H \triangleleft G$.

Example 2 (Special Linear Group)**.** In our previous example we claimed that $\mathrm{GL}(n, \mathbb{F})$ is a group, where F is any of the fields mentioned above; now we look at one of its most important subgroups:

$\mathrm{SL}(n, F) = \{n \times n \text{ matrices with determinant } 1\}$.

We will now show that $\mathrm{SL}(n, \mathbb{R}) \triangleleft Gl(n, \mathbb{R})$.

Proof. First we need to show that $\mathrm{SL}(n, \mathbb{R})$ is a subgroup. Let $A, B \in \mathrm{SL}(n, \mathbb{R})$, we have that

$$\det(A) = \det(B) = 1. \tag{1.1}$$

Now in order for $AB \in \mathrm{SL}(n, \mathbb{R})$, it must be that $\det(AB) = 1$.

Indeed:

$$\det(AB) = \det(A)\det(B) = 1. \tag{1.2}$$

Similarly, we need for $A^{-1} \in \mathrm{SL}(n, \mathbb{R})$:

$$\det(A^{-1}) = \det(A)^{-1} = 1. \tag{1.3}$$

Since all matrices in $\mathrm{SL}(n, \mathbb{R})$ are invertible, then we observe that it is a subgroup of $\mathrm{GL}(n, \mathbb{R})$.

Now, all that is left to show is that it $\mathrm{SL}(n, \mathbb{R})$ normal. It suffices to show that the conjugate ABA^{-1} is in $\mathrm{SL}(n, \mathbb{R})$ when $A \in \mathrm{GL}(n, \mathbb{R})$ and $B \in \mathrm{SL}(n, \mathbb{R})$. Since, matrix multiplication is closed, we have that

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B) = 1. \tag{1.4}$$

Therefore, $\mathrm{SL}(n, \mathbb{R}) \triangleleft \mathrm{GL}(n, \mathbb{R})$ □

1.2.2 Algebraic Number Theory

From the study of groups, we naturally will progress to the study of rings and furthermore fields. A *ring* is a nonempty set with two binary operations, such that for all a, b, c in $\mathbb{R}$:

(1) $a + b = b + a$,

(2) $(a + b) + c = a + (b + c)$,

(3) There is an additive zero.

(4) There is an additive inverse.

(5) $a(bc) = (ab)c$,

(6) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

A *field* has more structure than a ring. A field is a commutative ring with unity (a multiplicative identity) where every non zero element is a unit, i.e., has a multiplicative inverse.

Example 3. A basic example of a *field* $\mathbb{Q}$ is

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \ \& \ b \neq 0 \right\}.$$

Definition 4. If K is a field containing the subfield F, then K is said to be and *extension* of F and is denoted as K/F.

Definition 5. A *number field* K is a finite extension of $\mathbb{Q}$.

Example 6. One of the basic number fields that we are familiar with are the *Gaussian Integers* which is the rational numbers adjoined with i (the imaginary unit):

$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

Definition 7. More generally, another example of a number field is the *quadratic field* denoted as followed

$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}$ and d is a square-free integer$\}$.

Now, for a ring we look at a special case called *the ring of integers* denoted as $\mathcal{O}_K$; which is given by a number field K. This ring is defined as the set of elements $\alpha \in K$ such that α satisfies a monic polynomial with coefficients in $\mathbb{Z}$ or equivalently, there exists a monic $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. For an $\alpha \in \mathcal{O}_K$, there is a unique monic polynomial with integers coefficients, called the *minimal polynomial*, which divides every $f(x) \in \mathbb{Z}[x]$ for which α is a root. As an abelian group

$$\mathcal{O}_K \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}},$$

where $n = [K : \mathbb{Q}]$ is the degree of the number field (see [Neu99]).

Definition 8. An *embedding* of a number field K is a injective ring homomorphism $\varphi\colon K \to \mathbb{C}$. We say an embedding φ is *real* (resp. *complex*) if $\varphi(K) \subseteq \mathbb{R}$ (resp. $\varphi(K) \not\subseteq \mathbb{R}$). The complex embeddings come in complex conjugate pairs, and we call a real embedding (resp. a pair of complex embeddings) a *real place* (resp. *complex place*). Since the number of embeddings of K is the same as its degree $n = [K : \mathbb{Q}]$, we have

$$n = r + 2s,$$

where $r = \#$real places and $s = \#$complex places.

Example 9. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $f(x) = x^3 - 2$ is the monic polynomial satisfied by $\sqrt[3]{2}$. However, when we look at all the possible solutions of $f(x)$ in $\mathbb{C}$ we get the added roots:

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \omega\sqrt[3]{2}, \quad \alpha_3 = \omega^2\sqrt[3]{2} \quad \text{where } \omega = e^{2\pi i/3}$$

The embeddings are generated by:

$$\sigma_1 : \alpha \mapsto \sqrt[3]{2} \quad \sigma_2 : \alpha \mapsto \omega\sqrt[3]{2} \quad \sigma_3 : \alpha \mapsto \omega^2\sqrt[3]{2}$$

Notice that α_2 and α_3 are conjugate pairs so we get two embeddings one real and one complex. Since the degree of the minimal polynomial is 3 the statement above $n = 3 = 1 + 2(1)$ holds.

Definition 10. Given a number field K of degree n, let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of embeddings and choose a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\mathcal{O}_K$. The *discriminant* of K is defined as

$$\Delta_K = (\det(M))^2,$$

where M is the $n \times n$ matrix whose entry in the ith row and jth column is $\sigma_i(\alpha_j)$. This Δ_K is independent of the choice of $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. We also get a *field norm* $N_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ defined by

$$\alpha \mapsto \prod_{i=1}^{n} \sigma_i(\alpha).$$

Note that if $\alpha \in \mathcal{O}_K$, then $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ (See Chapter 6 on [Neu99]).

In addition, to the additive structure of the ring of integers $\mathcal{O}_K$ of a number field K, it is also important to look at the group of units of $\mathcal{O}_K$ denoted as $\mathcal{O}_K^\times$. There is an associated structure theorem here as well.

Theorem 11 (Dirichlet)**.** *For a number field K, we have*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \oplus T,$$

where $r = \#$real places, $s = \#$complex places, and the torsion part T is isomorphic to $\mu(K)$, the (finite) group of roots of unity in K.

Example 12. Let K be a *quadratic number field*, i.e., $[K : \mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ for some squarefree integer $d \neq 1$. If $d > 0$, then $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ and we say that K

is *real*. If $d < 0$, then $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}i$ and we say K is *imaginary*. It can be shown (see Chapter 13 in [IR90]) that

$$R_d := \mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \end{cases}$$

and

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

The 2 embeddings of $\mathbb{Q}(\sqrt{d})$ are just inclusion map $\mathbb{Q} \hookrightarrow \mathbb{C}$ and the 'conjugate embedding' map $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. This conjugate embedding map is just complex conjugation for an imaginary quadratic number field. So there are either exactly two real places and no complex places (when $d > 0$) or exactly one complex place and no real places (when $d < 0$). The field norm can be written explicitly here as

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2$$

for any $a, b \in \mathbb{Q}$. If $\alpha \in R_d$, then $\alpha \in R_d^\times$ is and only if

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = \pm 1,$$

but this has only finitely many solutions for imaginary quadratic number fields. In fact, we have $R_{-1}^\times = \{\pm 1, \pm i\}$, $R_{-2}^\times = \{\pm 1\}$, $R_{-3}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, and $R_d^\times = \{\pm 1\}$ for $d < -3$. This ties back in with Dirichlet's theorem since the $\mathbb{Z}$-rank of $R_d^\times$ should be $r + s - 1 = 0 + 1 - 1 = 0$. On the other hand, for real quadratic number fields, there are always infinitely many units since $r + s - 1 = 2 + 0 - 1 = 1$, and, moreover,

$$\mu(\mathbb{Q}(\sqrt{d})) = \{\pm 1\} \text{ (for } d > 0),$$

so

$$R_d^\times = \{\pm\varepsilon^n : n \in \mathbb{Z}\},$$

where the *fundamental unit* ε is the unique smallest unit $u > 1$ such that $u = a + b\sqrt{d}$ and $a, b > 0$.

Definition 13. We say that an integral domain R is a *unique factorization domain* or *UFD*, if every non-zero element may be factored uniquely as a product of irreducible elements, up to ordering and associate (i.e., differ by a unit multiple).

Just as groups have the notion of normal subgroups (which allow the definition of quotient groups), rings R have certain subrings we call ideals, the analog of a normal subgroup. A subring I in R is an *ideal* if $rx, xr \in I$ for all $r \in R$ and $x \in I$. If an ideal J of a given ring R is generated by a single element $a \in R$ we say that J is a *principal ideal* generated by a and write $J = (a)$. The structure of ideals and principal ideals in a ring R is intimately related to the ring being a UFD or not, as we will see below.

Example 14. It turns out that if given a ring R is a UFD, then its polynomial ring $R[x]$ in one variable is also a UFD. Looking at the ring $\mathbb{Z}$ of integers, which is a UFD (by the fundamental theorem of arithmetic), its polynomial ring is given as follows:

$$\mathbb{Z}[x] = \left\{ a_n x^n + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{Z} \text{ for all } i \right\}.$$

In this case, $\mathbb{Z}[x]$ being a UFD means that any non-zero polynomial with integer coefficients can be factored uniquely (up to order) into a product of monic irreducible polynomials. However, unlike the integers $\mathbb{Z}$ in which every ideal is principal, there are ideals which require more than one generator; for instance, the ideal $(2, x)$ is a non-principal prime ideal. Note that rings of integers $\mathcal{O}_K$ in a number field can can be encoded as quotients of $\mathbb{Z}[x]$. For example, $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i] = R_{-1}$ and $\mathbb{Z}[x]/(x^2 + x + 1) \cong \mathbb{Z}[\omega] = R_{-3}$.

If we have an integral domain R in which every ideal is principal, then R is called a *principal ideal domain* or *PID*. A very important result is that if a ring R is a PID, then it is also a UFD. The proof is omitted here, but see, for example, Chapter 8, Section 3 in [DF91]. The main tool for proving that an integral domain R is a PID is to establish a "division algorithm" for R in which the remainder is controlled by some notion of size in the ring.

Definition 15. R is said to be a *Euclidean domain* if there exists a function f from the nonzero elements of R to the non-negative integers $\{0, 1, 2, 3, \dots\}$ such that if $a, b \in R$ with $b \neq 0$, then there are $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(b)$.

From here we get a few strong and important results.

Theorem 16. *If R is a Euclidean domain, then R is a PID. (Chapter 8 section 3 in[DF91])*

Remark 17. Even though Euclidean implies PID, there are number rings which are PIDs that are not Euclidean, e.g., R_{-19}.

Theorem 18. *Let R be a PID and $a, b \in R$. Then a and b have a greatest common divisor d (unique up to unit multiple) and the ideal (a, b) generated by a, b is equal to (d).(Chapter 8 section 2 in [DF91])*

Corollary 19. *If R is a PID and $p \in R$ is irreducible, then p is prime.*

Remark 20. It is also true that irreducible implies prime in a UFD. In fact, if R is a Noetherian [i.e., every ideal is finitely generated] integral domain in which every irreducible is prime, then R is a UFD.

For the ring of integers $\mathcal{O}_K$ in a number field K, it can be shown that $\mathcal{O}_K$ is a UFD if and only if it is a PID.(Chapter 1 in [Neu99]) When looking at quadratic

number fields K, we have the option to choose the real or imaginary. The real case turns out to be more interesting since there are only finitely R_d with $d < 0$ which are UFDs, but Gauss conjectured (and numerical evidence supports) that there are infinitely many R_d with $d > 0$ which are UFDs:

$$d = 2, 3, 5, 7, 11, 13, 14, 17, 19, 21, 22, \ldots$$

The conjecture remains open, but we think roughly 76% of primes $p \equiv 1 \pmod 4$ have R_p a UFD. Among these, which are Euclidean? Dedekind showed that R_d is *norm- Euclidean* (i.e., R_d is a Euclidean domain with respect to N, the absolute value of the field norm) for

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 13.$$

In 1927, Dickson claimed that this list is actually complete. However, Perron observed that Dickson's argument worked only for imaginary quadratic fields. Over the next twenty years, the quadratic number rings which are norm-Euclidean were then completely characterized for the list above plus the following:

$$d = 6, 7, 11, 17, 19, 21, 29, 33, 41, 57, 73.$$

From here, Weinberger showed that, assuming some strong but widely believed conjectures, if the ring of integers $\mathcal{O}_K$ of an number field K contains infinitely many units, then $\mathcal{O}_K$ is Euclidean if and only if it is a PID. The emphasis then is on general Euclidean domains which are not norm-Euclidean since there are examples of real quadratic number rings which are Euclidean and not norm-Euclidean one of these is R_{69}[Cla97]. In fact, according the conjecture of Gauss, there should be infinitely many such examples.

Definition 21. For a number field K, the *fractional ideal* generated by $\alpha, \beta \in K$ is

defined by

$$(\alpha, \beta) := \{\alpha x + \beta y : x, y \in \mathcal{O}_K\}.$$

We say that a fractional ideal (α, β) is *principal* if $(\alpha, \beta) = (\gamma) := \gamma\mathcal{O}_K$ for some $\gamma \in K$.

Theorem 22. *Let K be a number field. Then the set J_K of fractional ideals is a group under multiplication defined by*

$$I \cdot J = \left\{ \sum_{k=1}^{m} i_k j_k : i_k \in I, j_k \in J \right\}.$$

Moreover, the subset $P_K \subseteq J_K$ of principal fractional ideals is a subgroup.

Definition 23. Given a number field K, we define the *class group* C_K of K as the quotient group $C_K = J_K/P_K$. The *class number* of K is then defined as the cardinality $h_K = |C_K|$ (which turns out to be finite, Chapter 12 [IR90]).

Theorem 24. [*Neu99*] *The following are equivalent for a number field K:*

(1) the class number of K is trivial, i.e. $h_K = 1$,

(2) $J_K = P_K$,

(3) every ideal in $\mathcal{O}_K$ is principal,

(4) $\mathcal{O}_K$ UFD.

Definition 25. If $K/\mathbb{Q}$ is a Galois extension $|Aut(K/\mathbb{Q})| = [K : \mathbb{Q}]$, and $\alpha \in K$, then the field norm of α is the product of all the Galois conjugates of α:

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{g \in Gal(K/\mathbb{Q})} g(\alpha).$$

Example 26. Consider the quadratic field $\mathbb{Q}(\sqrt{2})$. We can quickly recall that the Galois group K over $\mathbb{Q}$ has order $d = 2$ and is generated by the function that sends $\sqrt{2}$ to $-\sqrt{2}$. Thus

$$N_{K/\mathbb{Q}}(1+\sqrt{2}) = (1+\sqrt{2})(1-\sqrt{2}) = -1.$$

Remark 27. When the number field K is clear from context, we write N for the absolute value of the field norm and also to denote the norm of an integral ideal: $N(I) = |\mathcal{O}_K/I|$. With this notation, we have $N((\alpha)) = N(\alpha)$ (i.e., the norm of a principal ideal is the absolute value of the field norm of any generator.)

Comment: note that some number rings are Euclidean with respect the absolute value N of the field norm, while there are some which are Euclidean but not norm-Euclidean R_{14}

Definition 28. Let K be a number field of degree n. The *Minkowski constant* for K is defined as

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}, \tag{1.5}$$

where s is the number of complex places of K and Δ_K is the discriminant of $\mathcal{O}_K/\mathbb{Z}$.

Theorem 29. *Let K be a number field. Then for every ideal class $\mathfrak{c} \in C_K$, there is an integral ideal $I \in \mathfrak{c}$ such that*

$$N(I) \leq M_K.$$

Corollary 30. *For a number field K, the class group C_K is finite and is generated by the prime ideals of norm at most M_K.*

Example 31. Consider $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\Delta_K = 4(-5) = -20$, so

$$M_K = \sqrt{20}\left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \approx 2.847.$$

There is only one prime ideal with norm less than 3, namely the ideal

$$\mathfrak{P} = (1 + \sqrt{-5}, 2),$$

which lies above 2. This ideal is not principal, but $\mathfrak{P}^2 = (2)$, so

$$C_K \cong \mathbb{Z}/2\mathbb{Z}.$$

1.2.3 Graph Theory

The big purpose of all our algebraic structure is to unravel a connection between graphs and the issue with class number one. To further give a pictorial view of the results it is important that we understand the foundations and language of graph theory. This will give an actual visual representation of the relationship between one another.

Definition 32. A *Graph* G is a triple consisting of a *Vertex set* $V(G)$, an *Edge set* $E(G)$ and a relation that associated with each edge two vertices's (not necessarily distinct) and its endpoints.

In the following three examples we will see how a few graphs interact through their vertices and edges. We will see a directed graph (Figure 1.1), a labeled simple graph (Figure 1.2) and unlabled simple graph (Figure 1.3).

Example 33.

$$V_1(G) = \{1, 2, 3, 4\}, \qquad E_1(G) = \big\{(1, 2), (2, 1)(2, 3), (3, 2), (3, 1), (3, 4), (4, 3), (4, 4)\big\}.$$

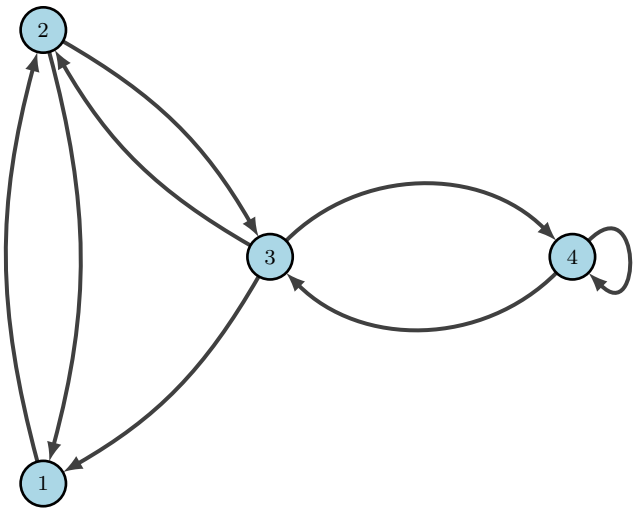

Figure 1.1: A Directed Graph

This graph has a couple of different features in the sense that we have edges going in two directions i.e. $1 \mapsto 2$ and $2 \mapsto 1$

Example 34.

$$V_2(G) = \{a_1, a_2, a_3, a_4, a_5\}, \quad E_2 = \big\{\{a_1, a_2\}, \{a_2, a_3\}, \{a_3, a_4\}, \{a_4, a_2\}, \{a_1, a_5\}\big\}.$$

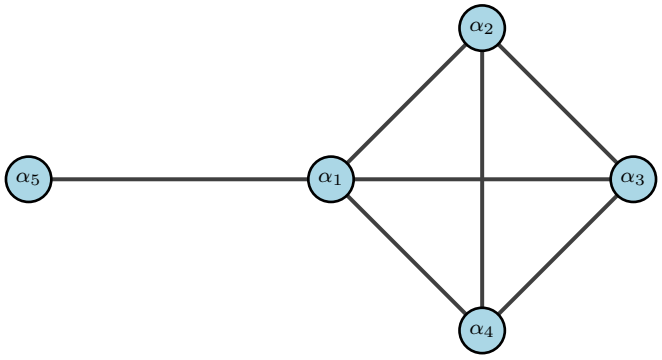

Figure 1.2: A Labeled Simple Graph

Graphs will not always show a labeling; however, one can choose the proper labeling to define both a vertex set and edge set, as shown below:

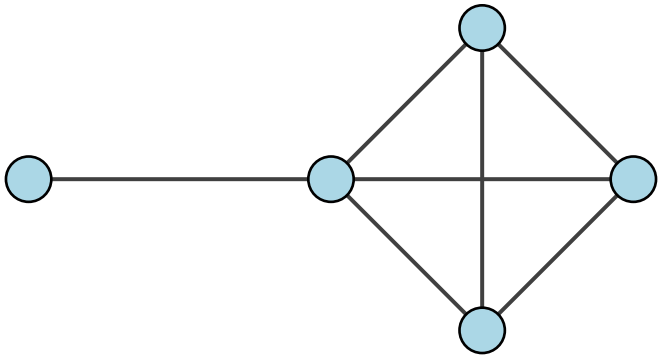

Figure 1.3: An Unlabeled Simple Graph

The main difference between Figure 1.1 and Figure 1.2 is the type of graphs; the first one is a more general graph that includes bidirectional edges. While the second one is what we call a *Simple graph* where it has no loops or multiple edges. We usually define a simple graph by treating the edge set as a set of unordered pairs of vertices $\{a_1, a_2\} = \{a_2, a_1\}$. We will from now on make the following assumptions that all the graphs we will be dealing with are simple. In addition, we will also refer to the edge as product of two vertices instead of an unordered pair i.e. $\alpha_1\alpha_2 = \alpha_2\alpha_1 \in E(G)$.

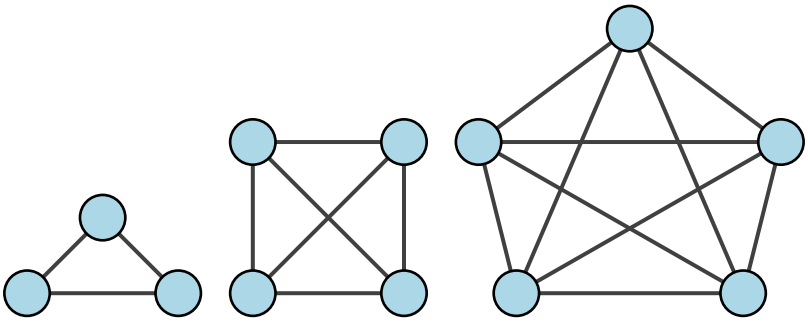

Figure 1.4: Complete Graphs on 3, 4, 5 Vertices

Definition 35. A *Complete graph* is a graph where all vertices are pairwise adjacent. Geometrically, all vertices have one edge between each other. As seen on Figure 1.4

Definition 36. The *complement* $\overline{G}$ of a simple graph G is the simple graph with the vertex set $V(G)$ and the edge set $uv \in E(\overline{G})$ if and only if $uv \notin E(G)$.

Definition 37. A *clique* in a graph is a set of pairwise adjacent vertices. An *independent* set in a graph is a set of pairwise nonadjacent vertices. We will denote the clique of a graph as $c(G)$ and the clique number to be the size of $c(G)$ namely $\omega(G) = |c(G)|$. It is important to notice that a given clique is also a complete subgraph of G. In addition, cliques are not unique as you will see on Figure 1.5. Another key feature is that a maximal clique of G, is the set of points in which produces the largest complete subgraph of G as we will see in Figure 1.5.

Example 38. Consider the following:

$$V(G) = \{u, v, w, x, y\}, \qquad E(G) = \{uv, uy, vw, wx, xy, xu\},$$
$$E(\overline{G}) = \{uw, vx, vy, wy\}.$$

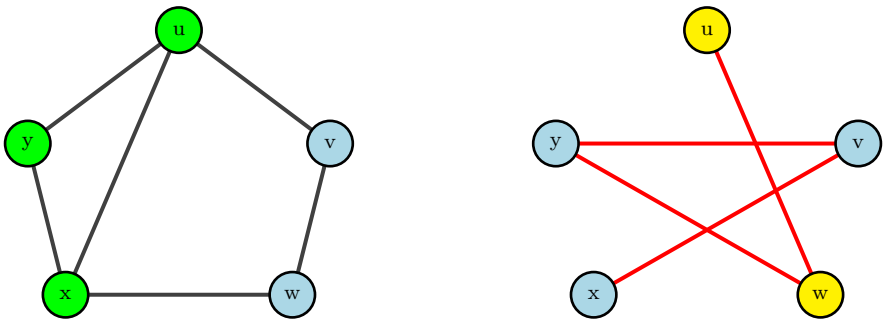

Figure 1.5: A Simple Graph with its clique and its Complement

We can now see the following:

$$c(G) = \{u, x, y\}, \qquad c(\overline{G}) = \{u, x\} \text{ or } \{v, y\}$$

Thus we have that $\omega(G) = 3$ while $\omega(\overline{G}) = 2$.

Definition 39. A *subgraph* of a graph G is a graph H such that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. On the other hand, an *induced subgraph* is a subgraph obtained by deleting a set of vertices Denoted as $G[T]$.

Example 40. We will see the difference between the induced subgraph (Figure 1.8) and a subgraph (Figure 1.7) of the Petersen graph (Figure 1.6).

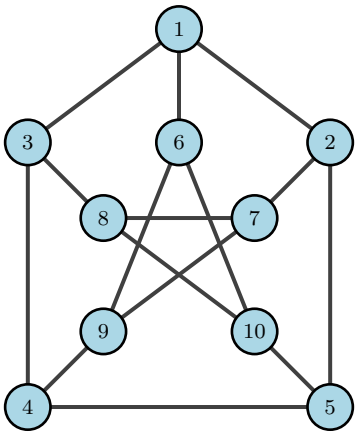

Figure 1.6: Peterson graph

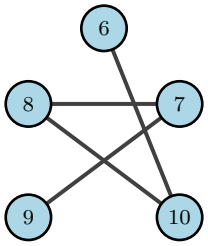

Figure 1.7: Subgraph H where $V(H) \subset V(G)$ and $E(H) \subset E(G)$

,

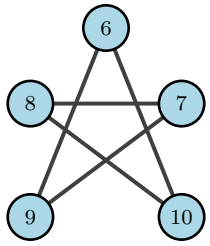

Figure 1.8: Induced subgraph where $V(K) = \{6, 7, 8, 9, 10\}$.

The big difference between the two types of subgraphs is that the verticies of the induced subgraph must connect in the same fashion as they did in the original graph G. Whereas, the subgraph just need to include some subset of the edge set. [Wes01]

In addition, to graphs with a finite vertex set there are sets where the vertex set is infinite.

Definition 41. If a graph G has a vertex set $\mathbb{N} = \{1, 2, 3, 4 \dots\}$ then we refer to this graph as *countably infinite*. If each vertex in the graph has a finite amount of edges coming out, then we call the graph *locally finite.*

The graphs we will be looking at will be countably simple graphs that are locally finite, this allows us to use all of our properties, definitions and examples on a local level.[Wil96]. Two of the more common examples are of the Infinite Ladder graph (Figure 1.9) and of the Infinite path graph (Figure 1.10)

Example 42.

$$V(G) = \left\{v_i, u_k, v'_j, u'_l \text{ such that } i, k, j, l \in \mathbb{N} \bigcup \{0\}, \text{ and } j, l \neq 0\right\}$$

$$E(G) = \begin{cases} (v_i, v_k) \text{ or } (u_i, u_k) & \text{if } k = i + 1 \\ (v'_j, u'_l) \text{ or } (v_i, u_k) & \text{if } i = k \text{ or } j = l \\ (v'_j, v'_l) \text{ or } (u'_j, u'_l) & \text{if } j = l + 1 \\ (v_0, v'_1), (u_0, u'_1). \end{cases}$$

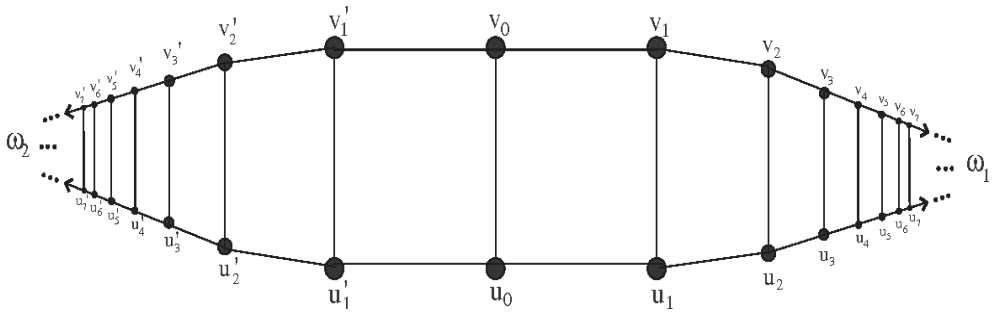

Figure 1.9: Infinite Ladder Graph

Example 43.

$$V(G) = \mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3 \dots\}$$

$$E(G) = \{(i, j) : \text{ if } |i - j| = 1, \text{ where } i, j \in \mathbb{Z}\}$$

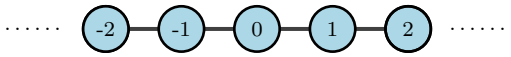

Figure 1.10: Infinite Path Graph

CHAPTER 2

UNIT CLIQUES, PRIME CLIQUES, AND CLASS NUMBER 1

2.1 Lenstra's Paper

In his famous 1997 paper [Len77], Hendrik Lenstra did some rigorous analysis on number fields K to establish some sufficient conditions for the ring of integers $\mathcal{O}_K$ to be Euclidean. The foundation of his work came from the ideas of Hurwitz [Hur19]. The method Lenstra used is based on exploiting the algebraic structure of a field. In essence, Lenstra's method arose to a sufficient condition of the number field K and its ring of integers $\mathcal{O}_K$ to contain elements where the differences of them are actually units.

Definition 44. We define a graph $\mathcal{U}_K$ from the ring of integers $\mathcal{O}_K$ as follows. The vertex set of $\mathcal{U}_K$ is just $\mathcal{O}_K$ and elements $\alpha, \beta \in \mathcal{O}_K$ are connected by an edge if and only if $\alpha - \beta \in \mathcal{O}_K^\times$. We call $\mathcal{U}_K$ the *unit graph* for $\mathcal{O}_K$. Let $\omega(\mathcal{U}_K)$ denote the clique number of this graph, i.e., the size of any maximal clique.

Lemma 45. *Suppose K is a number field and let M be a rational integer greater than the Minkowski constant M_K. Fix any subset $\{\alpha_1, \alpha_2, \ldots, \alpha_M\} \subseteq \mathcal{O}_K$. Then for every $\xi \in K$, there is a $\tau \in \mathcal{O}_K$ such that*

$$N((\alpha_i - \alpha_j)\xi - \tau) < 1$$

for some distinct $i, j \in \{1, 2, \ldots, M\}$.

Theorem 46. *Let K be a number field of degree n. Suppose that*

$$\omega(\mathcal{U}_K) > M_K$$

where M_K is the Minkowski constant for K as in Equation 1.5. Then $\mathcal{O}_K$ is norm Euclidean.

Proof. Take $\omega = \omega(\mathcal{U}_K)$ and let $\{\alpha_1, \alpha_2, \ldots, \alpha_\omega\}$ be a maximum clique in $\mathcal{U}_K$. Let $\xi \in K$ be arbitrary. To show that $\mathcal{O}_K$ is norm Euclidean, it suffices (since N is multiplicative) to prove that $N(\xi - q) < 1$ for some $q \in \mathcal{O}_K$. Since $\omega > M_K$, we may apply Lemma 45 to get $N((\alpha_i - \alpha_j)\xi - \tau) < 1$ for some $\tau \in \mathcal{O}_K$ and some distinct $i, j \in \{1, 2, \ldots, \omega\}$. Here $\alpha_i - \alpha_j \in \mathcal{O}_K^\times$ since $\{\alpha_1, \alpha_2, \ldots, \alpha_\omega\}$ is a clique in $\mathcal{U}_K$, so $N(\alpha_i - \alpha_j) = 1$ and $(\alpha_i - \alpha_j)^{-1} \in \mathcal{O}_K$. Together, this implies

$$1 > N((\alpha_i - \alpha_j)\xi - \tau) = N(\alpha_i - \alpha_j)N(\xi - \tau(\alpha_i - \alpha_j)^{-1}) = N(\xi - q)$$

with $q = \tau(\alpha_i - \alpha_j)^{-1} \in \mathcal{O}_K$ as needed. □

Remark 47. If one is interested in showing class number 1 in a particular example, then there are drawbacks to Lenstra's approach. In particular, there are Euclidean number rings that are not norm Euclidean; there are only finitely many quadratic number fields which are norm Euclidean. Nevertheless, there should be infinitely many quadratic number fields with class number 1 [Neu99] .

2.2 Work of Long and Thistlethwaite

Darren Long and Morwen Thistlethwaite built on the findings of Lenstra in [LT16]. Their key insights included (1) formally viewing the $\mathcal{U}_K$ as a graph (and drawing more edges to get larger clique sizes) and (2) establishing a more relaxed sufficient condition to show K has class number one (i.e., $\mathcal{O}_K$ is a PID, not necessarily norm-Euclidean). In order to achieve this less restricted condition we have to allow more edges on our graph, which is done by letting the difference of elements be either units or certain prime elements:

Definition 48. Let K be a number field and ρ be a prime element in $\mathcal{O}_K$. We say that ρ is a *Lenstra-Hurwitz prime* if the natural map $\mathcal{O}_K \to \mathcal{O}_K/(\rho) = F$ restricts to a surjection $\mathcal{O}_K^\times \to F^\times$ on units. We define a supergraph $\mathcal{L}_K$ of $\mathcal{U}_K$ as follows. The

vertex set of $\mathcal{L}_K$ is still just $\mathcal{O}_K$, but now elements $\alpha, \beta \in \mathcal{O}_K$ are connected by an edge if and only if $\alpha - \beta \in \mathcal{O}_K^\times$ or $\alpha - \beta$ is a Lenstra-Hurwitz prime. We call $\mathcal{L}_K$ the *Lenstra-Hurwitz graph* for $\mathcal{O}_K$. Again, let $\omega(\mathcal{L}_K)$ denote the clique number of this graph.

Long and Thistlethwaite give a generalization of Lemma 45 for the graph $\mathcal{L}_K$.

Lemma 49. *Suppose K is a number field and that $\{\alpha_1, \alpha_2, \ldots, \alpha_M\} \subseteq \mathcal{O}_K$ forms a clique in $\mathcal{L}_K$ where $M > M_K$. Then there is a finite set of units $\{u_1, u_2, \ldots, u_T\}$ such that for every $\xi \in K$, there is a $\tau' \in \mathcal{O}_K$ where either*

$$N(\xi - \tau') < 1$$

or

$$N((\alpha_i - \alpha_j)(\xi - \tau') - u_t) < 1$$

for some distinct $i, j \in \{1, 2, \ldots, M\}$ and some $t \in \{1, 2, \ldots, T\}$.

Proof. Let $\xi \in K$. By Lemma 45, we can find an integer $\tau \in \mathcal{O}_K$ such that $N((\alpha_i - \alpha_j)\xi - \tau) < 1$ for some distinct $i, j \in \{1, 2, \ldots, M\}$. Since $\{\alpha_1, \alpha_2, \ldots, \alpha_M\}$ forms a clique in $\mathcal{L}_K$, we know that $\alpha_i - \alpha_j$ is either a unit or a Lenstra-Hurwitz prime. If $\alpha_i - \alpha_j \in \mathcal{O}_K^\times$, then $N((\alpha_i - \alpha_j)^{-1}) = 1$, so we could quickly deduce:

$$N(\xi - \tau(\alpha_i - \alpha_j)^{-1}) = N((\alpha_i - \alpha_j)^{-1})N((\alpha_i - \alpha_j)\xi - \tau) = N((\alpha_i - \alpha_j)\xi - \tau) < 1$$

Now setting $\tau' = \tau(\alpha_i - \alpha_j)^{-1} \in \mathcal{O}_K$ gives the first conclusion.

Now assume $\alpha_i - \alpha_j = \rho$ is a Lenstra-Hurwitz prime. Consider the projection $\pi : \mathcal{O}_K \to \mathcal{O}_K/(\rho) = F$. This leads us to two cases: where τ lies in the kernel (i.e., $\pi(\tau)$ is zero) or where $\pi(\tau)$ is not zero.

Case 1: Suppose that $\pi(\tau)$ is 0, which implies that $\tau = \rho\tau'$ for some $\tau' \in \mathcal{O}_K$. Then we get

$$1 > N(\rho\xi - \tau) = N(\rho\xi - \rho\tau') = N(\rho)N(\xi - \tau') > N(\xi - \tau'),$$

so again this gives the first conclusion.

Case 2: If $\pi(\tau)$ is not 0, then $\pi(\tau) \in F^\times$ since F is a field. Since ρ is a Lenstra-Hurwitz prime, we know that the map $\pi : \mathcal{O}_K^\times \to F^\times$ is onto. Thus $\pi(\tau) = \pi(u)$ for some unit $u \in \mathcal{O}_K^\times$. Then we get that $\tau = u + \rho\tau'$ for some $\tau' \in \mathcal{O}_K$. We can now proceed

$$1 > N(\rho\xi - \tau) = N(\rho\xi - (u + \rho\tau')) = N(\rho(\xi - \tau') - u)$$

which gives us the second conclusion. The finite list of $\{u_1, \ldots, u_T\}$ is provided by choosing a transversal of units of each of the homomorphism $\mathcal{O}_K \to \mathcal{O}_K/(\rho)$ and taking the union of this collection. □

Theorem 50. *Let K be a number field. If $\omega(\mathcal{L}_K) > M_K$, then K has class number one.*

Proof. The proof of this theorem depends on a few important results. However, Proposition 2.3 from [LT16] is the glue that holds the proof together. This proposition is the following well-known fact:

> K has class number one if and only if for each $\xi \in K$ there is a matrix $A \in \mathrm{SL}(2, \mathcal{O}_K)$ such that $A \cdot \xi = \infty$

Here the action is given by linear fractional transformations, i.e., if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\xi = \alpha/\beta$ where $\alpha, \beta \in \mathcal{O}_K$, then

$$A \cdot \xi = \frac{a\alpha + b\beta}{c\alpha + d\beta}$$

The strategy for proving the theorem is now outlined as follows. First, note that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot 0 = \infty$$

and

$$\begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \cdot \alpha = 0$$

for any integer $\alpha \in \mathcal{O}_K$. Thus it suffices to show that any $\xi = \alpha/\beta$ can be sent to a field element γ/δ with a strictly smaller denominator: $N(\delta) < N(\beta)$. Now by Lemma 49, we have either

$$N(\xi - \tau') < 1$$

or

$$N(\rho(\xi - \tau') - u) < 1$$

for some integers $\tau', \rho \in \mathcal{O}_K$ and some unit $u \in \mathcal{O}_K^\times$. In the first case,

$$\begin{pmatrix} 0 & -1 \\ 1 & -\tau' \end{pmatrix} \cdot \xi = \frac{-\beta}{\alpha - \beta\tau'}$$

where

$$N(\alpha - \beta\tau') = N(\beta(\xi - \tau')) < N(\beta)$$

as needed. In the second case,

$$\begin{pmatrix} \rho u^{-1} - 1 & \tau'(\rho u^{-1} + 1) + 1 \\ \rho u^{-1} & -\rho u^{-1}\tau' - 1 \end{pmatrix} \cdot \xi$$

is the quotient of integers in $\mathcal{O}_K$ with denominator $\rho u^{-1}\alpha - \beta(\rho u^{-1}\tau' + 1)$ where

$$\begin{aligned} N(\rho u^{-1}\alpha - \beta(\rho u^{-1}\tau' + 1)) &= N(\beta)N(\rho u^{-1}(\xi - 1\tau') - 1) \\ &= N(\beta)N(\rho(\xi - \tau') - u) < N(\beta) \end{aligned}$$

as needed here. □

Example 51. [LT16] First consider $\mathbb{Q}(\sqrt{5})$. We already know that this field is not only a PID but infact Euclidean. Thus, we can find a maximum clique of size 4 in $\mathcal{U}_K$ namely:

$$\left\{0, 1, \frac{1+\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}\right\}.$$

However, we can find a larger Lenstra-Hurwitz clique of size 16:

$$\left\{0, 1, -1, -2, 1-\sqrt{5}, -1-\sqrt{5}, 2+\sqrt{5}, -2-\sqrt{5}, \frac{1}{2}(-1-\sqrt{5}), \frac{1}{2}(-3-\sqrt{5}),\right.$$
$$\left.\frac{1}{2}(3+\sqrt{5}), \frac{1}{2}(-3-3\sqrt{5}), \frac{1}{2}(-5-3\sqrt{5}), \frac{1}{2}(-5-\sqrt{5}), \frac{1}{2}(-7-3\sqrt{5}), \frac{1}{2}(-11-5\sqrt{5})\right\}.$$

CHAPTER 3

PRIME POWER CLIQUES AND AN EXPLICIT EXAMPLE

Definition 52. Let K be a number field. For each $n \in \mathbb{N}$, we define the *nth prime power graph* $\mathcal{P}_K^{(n)}$ as follows. The vertex set of $\mathcal{P}_K^{(n)}$ is $\mathcal{O}_K$, and elements $\alpha, \beta \in \mathcal{O}_K$ are connected by an edge if and only if $\alpha - \beta$ is either a unit or generates an ideal $(\alpha_i - \alpha_j) = \mathfrak{p}^m$ where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ with $m \leq n$. Further, we define the *nth Lenstra-Hurwitz graph* $\mathcal{L}_K^{(n)}$ as having vertex set $\mathcal{O}_K$ again and where elements $\alpha, \beta \in \mathcal{O}_K$ are connected by an edge if and only if $\alpha - \beta$ is either a unit or is an associate of ρ^m, where ρ is a prime in $\mathcal{O}_K$ with a surjective map on units $\mathcal{O}_K^\times \to (\mathcal{O}_K/(\rho^m))^\times$ and $m \leq n$.

Note, that this creates a hierarchy of cliques where the smallest correspond to Lenstra's unit graph:

$$\omega(\mathcal{U}_K) \leq \omega(\mathcal{L}_K) \leq \omega(\mathcal{P}_K^{(1)})$$

and

$$\omega(\mathcal{L}_K^{(n)}) \leq \omega(\mathcal{L}_K^{(n+1)}) \leq \omega(\mathcal{P}_K^{(n+1)}) \leq \omega(\mathcal{P}_K^{(\infty)})$$

for any positive integer n. The significance of the $\mathcal{L}_K^{(n)}$ graph is that large cliques will still imply class number one. We prove this here by establishing the following generalization of Lemma 49.

Lemma 53. *Suppose K is a number field and that $\{\alpha_1, \alpha_2, \ldots, \alpha_M\} \subseteq \mathcal{O}_K$ forms a clique in $\mathcal{L}_K^{(2)}$ where $M > M_K$. Then there is a finite set of units $\{u_1, u_2, \ldots, u_T\}$ such that for every $\xi \in K$, there is a $\tau' \in \mathcal{O}_K$ such that either*

$$N(\xi - \tau') < 1$$

or

$$N(d_{i,j}(\xi - \tau') - u_t) < 1$$

where $d_{i,j}|\alpha_i - \alpha_j$ in $\mathcal{O}_K$ for some distinct $i, j \in \{1, 2, \ldots, M\}$ and some $t \in \{1, 2, \ldots, T\}$.

Proof. Let $\xi \in K$. By Lemma 45, we can find an integer $\tau \in \mathcal{O}_K$ such that $N((\alpha_i - \alpha_j)\xi - \tau) < 1$ for some distinct $i, j \in \{1, 2, \ldots, M\}$. Since $\{\alpha_1, \alpha_2, \ldots, \alpha_M\}$ forms a clique in $\mathcal{L}_K^{(2)}$, we know that $\alpha_i - \alpha_j$ is either a unit or ρ or an associate of ρ^2 for some Lenstra-Hurwitz prime. The first two cases are already handled by Lemma 49, so we assume $\alpha_i - \alpha_j = \mu\rho^2$ for some $\mu \in \mathcal{O}_K^\times$ where the map on units $\mathcal{O}_K^\times \to (\mathcal{O}_K/(\rho^2))^\times$ is onto. There are three subcases here. First, suppose $\rho^2|\tau$, i.e., $\tau = \rho^2\tau'$. Then

$$1 > N(\mu\rho^2\xi - \rho^2\tau') = N(\rho^2)N(\xi - \mu^{-1}\tau')$$

which gives the first conclusion. Now suppose $\rho \nmid \tau$. Then τ is a unit mod ρ^2. So $\tau = u + (\alpha_i - \alpha_j)\tau'$ for some $u \in \mathcal{O}_K^\times$ and some $\tau' \in \mathcal{O}_K$, and this gives the second conclusion. Finally, assume that $\rho|\tau$ but $\rho^2 \nmid \tau$. Then $\tau = \rho\tau'$ where $\rho \nmid \tau' \in \mathcal{O}_K$. We have surjection $\mathcal{O}_K^\times \to (\mathcal{O}_K/(\rho^2))^\times \to (\mathcal{O}_K/(\rho))^\times$, so $\tau' = u + \tau''\rho$, which gives

$$1 > N(\mu\rho^2\xi - \rho(u - \tau''\rho)) > N(\mu\rho(\xi - \tau''\mu^{-1}) - u)$$

which gives the second conclusion with $d_{i,j} = \mu\rho|\mu\rho^2 = \alpha_i - \alpha_j$. □

By the same techniques used in the proof of Theorem 50, we get the following corollary.

Corollary 54. *Let K be a number field. If $\omega(\mathcal{L}_K^{(2)}) > M_K$, then K has class number one.*

Long and Thistlethwaite prove the following result about clique sizes in real quadratic fields.

Theorem 55. *Let $d \geq 6$ be a squarefree integer and set $K = \mathbb{Q}(\sqrt{d})$. Then $\omega(\mathcal{P}_K^{(1)}) \leq 8$ when 2 remains prime in R_d and $\omega(P_K^{(1)}) \leq 4$ when 2 splits or ramifies in R_d.*

Example 56. Let $K = \mathbb{Q}(\sqrt{173})$. To compute the Minkowski constant M_K, we must first find Δ_K. Since $173 \equiv 1 \pmod 4$ we get $\Delta_K = 173$, so from here we can compute $M_K = \frac{2!}{2^2}\sqrt{173} \approx 6.58$. This means that to establish class number one, it suffices to find a clique in $\mathcal{L}_K$ of size 7 or more. Long and Thistlethwaite give such a clique, namely

$$\left\{0, \frac{-77+3\sqrt{173}}{2}, -25+2\sqrt{173}, -12+\sqrt{173}, 13-\sqrt{173}, \frac{27+\sqrt{173}}{2}, \frac{53-\sqrt{173}}{2}\right\}.$$

Note that cliques are translation invariant so we can always assume that a clique contains 0. This example is important since $\mathbb{Q}(\sqrt{173})$ is not norm-Euclidean, so Lenstra's method would not work to show class number one here. It is not known if there is clique in $\mathcal{L}_K$ of size 8. However, one can find cliques of size eight in $\mathcal{P}_K^{(\infty)}$. We give an example here of a such a clique:

$$\left\{0, \frac{13+\sqrt{173}}{2}, \frac{171+13\sqrt{173}}{2}, 13+\sqrt{173}, \frac{355+27\sqrt{173}}{2}, \right.$$
$$\left. \frac{197+15\sqrt{173}}{2}, 434+33\sqrt{173}, 605+46\sqrt{173}\right\}$$

The code used to generate this example was written in SAGE and is included in our Appendix.

CHAPTER 4

CONCLUSION

The main body of our work was to further improve the methods implemented by Lenstra, Long, and Thistlethwaite. In specific, Corollary 54, which we proved, generalized all of the previously known results. Prior to this Lenstra, Long, and Thistlethwaite had only proved that class number one was given only with unit cliques or prime cliques, refer to Theorem 50. This new and very powerful result,that we have proved, is useful in the computation of clique sizes for our prime power cliques. Furthermore, the code we produced, as seen in Appendix A, allow us to produce, compute, and verify the existence of these cliques. We could see the fruits of our code in Example 56. It would be a long and tedious construction if we actually tried to construct all of these computations by hand. The problems are that not only is it hard to produce every prime ideal and prime power ideal for our real quadratic field but having to check that the differences of each and every combination of elements exist in one of these ideals is nearly impossible to do by hand.

We conclude our work by leaving the reader with a few open problems. Can we generalize our work and preserve class number 1 if we allow $\omega(\mathcal{L}_K^{(n)}) > M_K$ for any $n > 2$? One of the major unanswered questions is as to whether or not there are infinitely many real quadratic fields of class number one. The framework to prove this result, to which we contributed to in this thesis, is quite significant to solving this previous conjecture. The conjecture is believed to be true and the creation of our prime power cliques gives hope that it is.

BIBLIOGRAPHY

[Cla97] David A. Clark, *Which is euclidean but not norm-euclidean*, manuscripta mathematica (1997), no. 2, 327–330.

[DF91] David S. Dummit and Richard M. Foote, *Abstract algebra*, Prentice-Hall, 1991.

[Hur19] Adolf Hurwitz, *Der Euklidische Divisonssatz in einem endlichen algebraischen Zahlkörper*, Math Z. **3** (1919), 123–126.

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[Len77] H. W. Lenstra, *Euclidean number fields of large degree*, Inventiones Math. **38** (1977), 237–254.

[LT16] D. D. Long and Morwen B. Thistlethwaite, *Lenstra-hurwitz cliques and the class number one problem*, Journal of Number Theory **162** (2016), 564–577.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999, Translated from German by Norbert Schappacher.

[Wes01] Douglas B. West, *Introduction to graph theory*, second ed., Prentice-Hall, 2001.

[Wil96] Robin J. Wilson, *Introduction to graph theory*, fourth ed., Prentice Hall, 1996.

APPENDIX A

SAGE CODE

The following is the Sage code that was created for the computations of our prime power cliques.

```
sage: K.<a> = QuadraticField(173)
sage: U=UnitGroup(K)
sage: U.gens_values()
[-1, 1/2*a + 13/2]
sage: E = 1/2*a + 13/2
sage: E.norm()
-1
sage: list = [E^n for n in range(-4,4)]
sage: list
[-2223/2*a + 29239/2,
85*a - 1118,
-13/2*a + 171/2,
1/2*a - 13/2,
1,
1/2*a + 13/2,
13/2*a + 171/2,
85*a + 1118]
sage: P=Primes()
sage: L=[]
```

```
sage: for j in range(20):
...       p = P.unrank(j);
...       if kronecker(173,p)==-1:
...           L = L+[p, p^2];
...       else:
...           b = Integer(Mod(173,p).sqrt());
...           I = K.ideal([b+a,p]);
...           J = K.ideal([b-a,p]);
...           Igen = I.gens_reduced()[0];
...           Jgen = J.gens_reduced()[0];
...           L  = L+[Igen, Igen^2, Jgen, Jgen^2];
sage: L = [1]+L
sage: M = []
sage: for j in L:
...       M = M + [j*i for i in list]
sage: prematrix=[];
sage: for i in range(len(M)-1):
...       row = [];
...       for j in range(len(M)-1):
...           if j <= i:
...               row = row + [0];
...           else:
...               gen = M[i]-M[j];
...               n = Integer(abs(norm(gen)));
...               if n.is_prime_power():
...                   row = row + [1];
```

```
...                else:
...                    row = row + [0];
...       prematrix = prematrix + [row];
...
sage: postmatrix = matrix(prematrix)
sage: AdjMat = postmatrix + postmatrix.transpose()
sage: G = Graph(AdjMat); G
Graph on 471 vertices
sage: G.clique_maximum()
[14, 22, 38, 46, 62, 222, 254, 286, 302, 318, 334]
sage: [0, M[5], M[6], M[13], M[94], M[109], M[158], M[166]]
[0,
1/2*a + 13/2,
13/2*a + 171/2,
a + 13,
27/2*a + 355/2,
15/2*a + 197/2,
33*a + 434,
46*a + 605]
```