5-2024

Elasticity of Orders in Quadratic Rings of Integers

Jared Kettinger
Clemson University

Elasticity of Orders in Quadratic Rings of Integers

A Project
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master's
Mathematics

---

by
Jared Kettinger
May 2024

Accepted by:
Dr. James Coykendall, Committee Chair
Dr. Ryann Cartor
Dr. Robert Dicks

Abstract

This project explores elasticity in quadratic rings of integers, specifically, those of the form $\mathbb{Z}[p\omega]$ where p is a rational prime which remains prime in $\mathbb{Z}[w]$. For these rings, we establish an upper bound on the elasticity which is attained in many cases. We also prove that this upper bound is an equality in the case when the ring of integers is a unique factorization domain. During this process, we also prove theorems about the class group of quadratic rings of integers and develop a useful method for calculating a constant similar to the Davenport constant.

Acknowledgments

First, thank you to Ryann Cartor and Robert Dicks for their willingness to be in my committee, taking the time to understand my work, and helping me along the way. I look forward to further work with you both. Thank you also to my family for supporting me through this time. Finally, a special thank you to my advisor, Dr. Jim Coykendall. Your patience and time have been invaluable, and your mastery of the material inspiring. It has been a privilege to work with and learn from you.

Table of Contents

Chapter 1

Introduction

1.1 Motivation and Background

Understanding factorization in rings of integers has lead to surprising solutions to a number of seemingly unrelated questions about the rational integers. For example, the primes which can be expressed as a sum of two squares can be determined by looking at their factorizations in the Gaussian integers. Also, Fermat's Last Theorem was proven for many values of n by considering factorizations in rings of integers of cyclotomic number fields.

The elasticity of all rings of integers was determined by Valenza [10] and Narkiewicz [6]. There proofs rely heavily on the fact that rings of integers are Dedekind domains. Hence, all ideals in these rings factor uniquely into prime ideals. Looking at how the ideals generated by elements factor into primes is very telling of how the elements themselves factor. A natural next step would be to consider the elasticity of all orders in rings of integers. Unfortunately, apart from the ring of integers itself, all other orders fail to be Dedekind. This follows immediately from the fact that they fail to be integrally closed. Hence, we lose this desirable factorization property for ideals. However, we can still take advantage of the overlying Dedekind domain by considering elements of a given order as elements of their respective ring of integers. In this paper, we will see how the factorization of an element in the overlying ring of integers can tell us a great deal about its factorization in the order.

1.2 Notation

- $\mathcal{O}_K$ - The ring of integers of the number field K.
- $\mathbb{Z}[\omega]$ - The ring of integers of $\mathbb{Q}[\sqrt{d}]$. Where d is a square-free integer and

$$\omega = \begin{cases} \sqrt{d} & d \equiv 2, 3 \ mod\ 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \ mod\ 4 \end{cases}$$

- $N(a+b\omega) = (a+b\omega)(a+b\bar{\omega})$ is the norm of an element in a quadratic ring of integers where $\bar{\omega}$ is the complex conjugate.
- p is a rational prime unless otherwise stated.
- $\mathbb{Z}[n\omega] = \{a+bn\omega | a, b \in \mathbb{Z}\}$ - the order of $\mathbb{Z}[\omega]$ with conductor $n\mathbb{Z}[\omega]$.
- $\rho(R)$ - The elasticity of the domain R.
- F^* - The non-zero elements of a field F.
- Irr(R) - The irreducible elements of the domain R.
- $U(R)$ - The units of the domain R
- $\left(\frac{d}{p}\right)$ - The Legendre symbol
- $\mathbb{Z}_p$ - The finite field of p elements.

1.3 Definitions

Let us start with an introduction to rings of integers and orders. While these theorem are given for arbitrary rings of integers, this paper will focus exclusively on the quadratic case.

Definition 1.3.1. An *algebraic number field* is a field extension of the rationals of finite degree. A *quadratic field* is a degree 2 field extension of the rationals.

Definition 1.3.2. [5] If $R \subseteq T$ are rings, the ring $\bar{R}_T = \{t \in T |\ f(t) = 0$ for some monic polynomial$f(x) \in R[x]\}$ is called the *integral closure of R in T*. If $T = K$ is the quotient field of R, then $\bar{R} := \bar{T}_K$ is called the *integral closure of R*. If $R = \bar{R}$, we say that R is *integrally closed*.

Definition 1.3.3. The *ring of integers* of a number field K is the integral closure of $\mathbb{Z}$ in K.

Example 1.3.4. $\mathbb{Z}[i]$ is the ring of integers of the quadratic field $\mathbb{Q}(i)$.

Definition 1.3.5. [9] An *order* $\mathcal{O}$ of a ring of integers $\mathcal{O}_K$ is a subring which is also a $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

It is important to note that orders are often equivalently defined as subrings with the same quotient field as the ring of integers — sometimes referred to as the maximal order. Thus, as $\mathbb{Z} \subseteq \mathcal{O} \subseteq \mathcal{O}_K$, we see that the integral closure of any order must be $\mathcal{O}_k$. Hence, an order is integrally closed if and only if it is the entire ring of integers. Notably, this implies an order is Dedekind if and only if it is the entire ring of integers.

Definition 1.3.6. The *conductor* of an order $\mathcal{O} \subseteq \mathcal{O}_K$ is the set $\{\alpha \in \mathcal{O}_\mathcal{K} | \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$. Notably, the conductor is also the largest ideal shared by $\mathcal{O}$ and $\mathcal{O}_K$.

It is important to note that the conductor of an arbitrary ring extension may be zero, but the conductor of an order is always non-zero. The conductor is has great import with respect to factorization as ideals relatively prime to the conductor retain unique factorization into primes in the order. As we will see, this allows us to put an upper bound on the elasticity of elements outside the conductor.

Definition 1.3.7. [4] Let R be a domain with quotient field K. An $R-$submodule $I \subseteq K$ is a *fractional ideal* if there exists a nonzero $a \in R$ such that $aI \subseteq R$. The ideal $\{x \in K | xI \subseteq R\}$ is called the *inverse* of I and is denoted I^{-1}. A fractional ideal is called *invertible* if $II^{-1} = R$.

Example 1.3.8. Consider the domain $\mathbb{Z}$ with quotient field $\mathbb{Q}$. The ideal $3\mathbb{Z} \subseteq \mathbb{Z}$ has inverse $\frac{1}{3}\mathbb{Z}$, and $(3\mathbb{Z})(\frac{1}{3}\mathbb{Z}) = \mathbb{Z}$, so we conclude it is invertible.

Definition 1.3.9. [5] Let R be a domain with quotient field K. We define $Inv(R) := \{I \mid I \text{ is an invertible ideal of } R\}$ and $Prin(R) := \{xR \mid x \in K \setminus \{0\}\}$. Then, the quotient group $Cl(R) := Inv(R)/Prin(R)$ is called the *class group* of R. If $|Cl(R)| = n \leqslant \infty$, then n is called the *class number* of R.

We will often consider a specific prime ideal P in a given class. Multiplication by the ideal's "conjugate" $\bar{P}$ (defined below) can be a very useful technique.

Definition 1.3.10. If $P = \langle x_\alpha \rangle_{\alpha \in \Delta}$ is an ideal of $\mathbb{Z}[\omega]$, then $\bar{P} = \langle \bar{\alpha} \rangle_{\alpha \in \Delta}$ where $\alpha = a + b\omega \Rightarrow \bar{\alpha} = a + b\bar{\omega}$.

Now, factorization in rings of integers is intimately related to the class group of the ring. Understanding this relationship motivates the following definition.

Definition 1.3.11. Let G be a finite, abelian group. We call a *G–sequence* $\{g_1, g_2, \ldots, g_n\}$ of (not necessarily distinct) elements of G a *0–sequence* if $g_1 + g_2 + \cdots + g_n = 0$.

Definition 1.3.12. The *Davenport Constant* of a group G is the smallest n s.t. any $G-$sequence of length n must have a $0-$subsequence. Equivalently, we may define the Davenport Constant as the length of the longest $0-$sequence with no proper $0 - subsequence$.

Finally, we give the definition of elasticity.

Definition 1.3.13. [4] Let R be an atomic domain. The *elasticity* of a nonzero, nonunit $r \in R$ is defined as

$$\rho(r) = sup\Big\{ \frac{n}{m} \,|\, r = \alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m \Big\}$$

where $\alpha_i, \beta_j \in Irr(R)$ for all i, j.

Similarly, the *elasticity* of the domain R is defined as

$$\rho(R) = sup\Big\{ \frac{n}{m} \,|\, \alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m \Big\}$$

where $\alpha_i, \beta_j \in Irr(R)$ for all i, j.

1.4 Theorems

We begin with some theorems on the Davenport constant.

Theorem 1.4.1. If G is a finite, abelian group, then $D(G) \leqslant |G|$.

Proof. Let $|G| = n$ and $\{g_1, \ldots, g_n\}$ be a $G-$sequence of length n. Consider the n partial sums

$$\begin{gathered} g_1 = k_1 \\ g_1 + g_2 = k_2 \\ \vdots \\ g_1 + g_2 + \cdots g_n = k_n \end{gathered}$$

If the $k_i \neq k_j$ whenever $i \neq j$, then $n = |G|$ implies $0 = k_i = g_1 + g_2 + \cdots + g_i$ for some $1 \leqslant i \leqslant n$, so $\{g_1, \ldots, g_n\}$ has a $0-$subsequence. If not, $k_i = k_j$ for some $i \neq j$. without loss of generality assume $i < j$. Subtracting the i^{th} equation from the j^{th} yields $g_{i+1} + \cdots + g_j = 0$, so once again $\{g_1, \ldots, g_n\}$ has a $0-$subsequence. $\square$

It is natural to ask if this bound is sharp, and if so, under what conditions is it achieved? The following theorem answers both of these questions.

Theorem 1.4.2. If G is a finite abelian group, $D(G) = |G| \iff G$ is cyclic.

Proof. ($\Rightarrow$) Assume $D(G) = |G| = n$. Then, there exists a $G-$sequence $\{g_1, \ldots, g_{n-1}\}$ of length n with no $0-$subsequence. We want to show $g_i = g_j$ for all $1 \leqslant i, j \leqslant n-1$. Note, by possible reordering, it is sufficient to show $g_1 = g_2$. Assume for the purpose of contradiction that $g_1 \neq g_2$. Consider the $n-1$ partial sums

$$\begin{gathered} g_1 = k_1 \\ g_1 + g_2 = k_2 \\ \vdots \\ g_1 + g_2 + \cdots g_{n-1} = k_{n-1} \end{gathered}$$

Because $\{g_1, \ldots, g_{n-1}\}$ has no $0-$subsequence, it must be the case that $k_i \neq 0$ for all $1 \leqslant i \leqslant n-1$. For the same reason, we must have $k_i \neq k_j$ for all $i \neq j$. Otherwise, assuming without loss of generality that $i < j$, $k_j - k_i = k_{i+1} + \cdots + k_j = 0$ would be a $0-$subsequence. Thus, each non-zero value of G must be attained by some k_i. Now, by our assumption, $k_1 = g_1 \neq g_2$. This implies $k_i = g_1 + g_2 + \cdots + g_i = g_2$ for some $2 \leqslant i \leqslant n-1$, but then $g_1 + g_3 + \cdots + g_i = 0$. $\Rightarrow\Leftarrow$ So we conclude $g_i = g_j$ for all $1 \leqslant i, j \leqslant n-1$.

Therefore, we have a $G-$sequence $\{g, g, \ldots, g\}$ of length $n-1$ with no $0-$subsequence. Hence, the element g must have order at least $n = |G|$, so G is cyclic.

($\Leftarrow$) Let G be a cyclic group of order n, and let α be a generator of G. Then, the $G-$sequence $\{\alpha, \alpha, \ldots, \alpha\}$ of n copies of α has no proper $0-$subsequence. Thus, $D(G) \geqslant n = |G|$, so by Theorem 1.4.1., $D(G) = |G|$.

$\square$

We proceed with some important theorems related to rings of integers and their orders.

Theorem 1.4.3. Let R be an integral domain that is not a field. TFAE:

1. All (fractional) ideals of R are invertible.
2. R is integrally closed, Noetherian, and 1-dimensional.
3. All ideals of R can be uniquely factored into prime ideals.

A domain satisfying one, hence all, of these conditions is called *Dedekind*.

The following result is due to Narkiewicz and relies heavily on the fact that rings of integers are Dedekind domains. With respect to factorization theory, the key property of Dedekind domains is that all ideals factor uniquely into prime ideals. By scrutinizing how principal ideals factor in these domains, we can learn a lot about how the elements which generate these ideals factor as well.

Theorem 1.4.4. [6] Let $\mathcal{O}_K$ be a ring of integers with class group G. Then

$$\rho(\mathcal{O}_K) = \begin{cases} \frac{D(G)}{2} \leqslant \frac{|G|}{2} & \text{if } |G| \neq 1 \\ 1 & \text{if } |G| = 1 \end{cases}$$

In this paper we will exclusively consider quadratic rings of integers. As we will see, these rings are especially well-behaved. One of the key features of these rings of integers which will prove useful is that the conductors of their orders are always principal.

Theorem 1.4.5. [5] Any quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

Proof. Let F be a quadratic ring of integers, that is, $[F : \mathbb{Q}] = 2$. Take some $\alpha \in F \setminus \mathbb{Q}$. Then, $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq F$ and $[F : \mathbb{Q}] = 2$ implies $\mathbb{Q}(\alpha) = F$. Now, $[\mathbb{Q}(\alpha), \mathbb{Q}] = 2$ implies α is the root of a an irreducible quadratic polynomial over $\mathbb{Q}$. Hence, $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ for some $a, b, c \in \mathbb{Q}$ where $b^2 - 4ac \neq 0$ as $\alpha \notin \mathbb{Q}$. Thus,

$$F = \mathbb{Q}(\alpha) = \mathbb{Q}(\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}) = \mathbb{Q}(\sqrt{b^2 - 4ac}) = \mathbb{Q}(\sqrt{d})$$

where $d = b^2 - 4ac$. We may also assume without loss of generality that d is squarefree because if $d = n^2 \cdot k$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{n^2 k}) = \mathbb{Q}(n\sqrt{k}) = \mathbb{Q}(\sqrt{k})$

□

Theorem 1.4.6. [9] If $\mathbb{Z}[\omega]$ is a quadratic ring of integers, any order is of the form $\mathbb{Z}[n\omega]$ with conductor $n\mathbb{Z}[\omega]$ for some $n \in \mathbb{Z}$.

Theorem 1.4.7. [3] For a ring of integers $\mathcal{O}_K$ and a given order $\mathcal{O}$ with conductor f, there is an isomorphism between the invertible ideals of $\mathcal{O}$ relatively prime to f and the ideals of $\mathcal{O}_K$ relatively prime to f.

Remark: For a ring of integers $\mathcal{O}_K$ and a given order $\mathcal{O}$ with conductor f, the ideals relatively prime to the conductor in both domains form multiplicatively closed sets. We denote the subgroup of $Cl(\mathcal{O}_K)$ generated by these ideals as $I_K(f)$. Similarly, we write $I(\mathcal{O}, f)$ to denote the subgroup of the class group of $\mathcal{O}$ generated by the invertible ideals relatively prime to the conductor in $\mathcal{O}$.

Theorem 1.4.8. [3] The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism $I_K(f) \xrightarrow{\cong} I(\mathcal{O}, f)$, and the inverse map is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.

This theorem is extremely important because it tells us that ideals relatively prime to the conductor have unique factorization. As a consequence, by the same construction as [10], in the order $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$, the elasticity of the elements away from the conductor is bounded above by $\frac{D(Cl(\mathbb{Z}[n\omega]))}{2}$.

Finally, the following theorems hold for Dedekind domains in general. They will be very useful in constructing examples and proving theorems in the results section of this paper.

Theorem 1.4.9. [5] Let $\mathbb{Z}[\omega]$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$ where d is square-free in $\mathbb{Z}$. Then an odd prime $0 \neq p \in \mathbb{Z}$ remains prime in $\mathbb{Z}[\omega] \iff \left(\frac{d}{p}\right) = -1$.

Theorem 1.4.10. [5] Let $\mathbb{Z}[\omega]$ be the ring of integers of $\mathbb{Q}[\sqrt{d}]$ - d a square-free integer. Note, $f(x) = x^2 - d$ is the minimal polynomial of $\sqrt{(}d)$ over $\mathbb{Z}[x]$. In $\mathbb{F}_p[x]$, suppose $f(x) = \bar{f}_1(x)^{e_1} \cdot \bar{f}_2(x)^{e_2}$. Then, if $P_i = (p, \bar{f}_i(\sqrt{d}))$, $p\mathbb{Z}[\omega] = P_1^{e_1} P_2^{e_2}$.

Theorem 1.4.11. [7] Let R be a Dedekind domain and $A, B \subseteq R$ ideals. Then, $A \subseteq B \iff B|A$.

Proof. ($\Rightarrow$) If $A \subseteq B$, then $AB^{-1} \subseteq BB^{-1} = R$. Thus, $AB^{-1} = P_1 P_2 \cdots P_n$ for some $P_i \in Spec(R), 1 \leqslant i \leqslant n$. Multiplying by B, we get $A = P_1 P_2 \cdots P_n \cdot B$, so $B|A$.

($\Leftarrow$) If $B|A$, then there is some ideal $C \subseteq R$ such that $A = BC \subseteq B$. □

Chapter 2

Results

2.1 UFDs

In this section, we consider orders $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ where the overlying quadratic ring of integers is assumed to be a UFD. This is extremely useful because any element $\beta \in \mathbb{Z}[n\omega]$ is also an element of $\mathbb{Z}[\omega]$ and thus has a unique factorization into primes: $\beta = \pi_1 \cdots \pi_k$, $\pi_i \in \mathbb{Z}[\omega]$. Thus, given any factorization of $\beta = \gamma_1 \cdots \gamma_m$, $\gamma_j \in \mathbb{Z}[n\omega]$, by uniqueness, each $\gamma_j = \pi_{i_1} \cdots \pi_{i_r}$. That is, every factorization of β in $\mathbb{Z}[\omega]$ can be attained by grouping together elements of the prime factorization in $\mathbb{Z}[\omega]$ to form irreducibles in $\mathbb{Z}[n\omega]$. Hence, we can determine the elasticity of β in $\mathbb{Z}[n\omega]$ by grouping these primes as coarsely and finely as possible. The theorems presented in this section prior to the ultimate result (Theorem 2.1.7.) should be viewed with this goal in mind.

As a motivating example, consider the Gaussian integers $\mathbb{Z}[i]$ and the order $\mathbb{Z}[7i] \subseteq \mathbb{Z}[i]$. $\mathbb{Z}[i]$ is a UFD, so the element 490 factors *uniquely* into primes as $490 = 7 \cdot 7(1+i)(1-i)(1+2i)(1-2i)$. Now, we want to group these elements to form irreducibles of $\mathbb{Z}[7i]$. One possible grouping is $[7][7][(1+i)(1-i)][(1+2i)(1-2i)] = 7 \cdot 7 \cdot 2 \cdot 5$. Another option is $[7(1+i)(1-2i)][7(1-i)(1+2i)] = (21-7i)(21+7i)$. The fact that these elements are all irreducible in $\mathbb{Z}[7i]$ follows from the fact that the prime factorization in $\mathbb{Z}[i]$ is unique, and there is no way to partition the primes we have grouped together to give a factorization in $\mathbb{Z}[7i]$. For example, looking at $[7(1+i)(1-2i)]$, $(1+i)(1-2i) = 3-i \notin \mathbb{Z}[7i]$. Also, despite $7(1+i)$ and $7(1-2i)$ being in $\mathbb{Z}[7i]$, this leaves us with a factor which is not — $1+i$ or $1-2i$. Thus, we have irreducible factorizations of lengths 2 and 4, so $\rho(490) \geqslant \frac{4}{2} = 2$ in $\mathbb{Z}[7i]$.

Lemma 2.1.1. Let $\mathbb{Z}[\omega]$ be a quadratic ring of integers and p prime. If $\pi_1 = a + pb\omega \in \mathbb{Z}[p\omega]$ and $\pi_2 = c + d\omega \in \mathbb{Z}[\omega] \setminus \mathbb{Z}[p\omega]$, then $\pi_1\pi_2 \in \mathbb{Z}[p\omega] \iff \pi_1 \in p\mathbb{Z}[\omega]$.

Proof.

$$\pi_1\pi_2 = (a + pb\omega)(c + d\omega) = ac + ad\omega + p(b\omega(c + d\omega))$$
$$= ac + ad\omega + p(x + y\omega) = ac + px + (ad + py)\omega \in \mathbb{Z}[p\omega]$$
$$\iff p|(ad + py)$$
$$\iff p|ad \text{ (in } \mathbb{Z})$$
$$\iff p|a \text{ or } p|d$$
$$\iff a + pb\omega = \pi_1 \in p\mathbb{Z}[\omega] \text{ or } c + d\omega = \pi_2 \in \mathbb{Z}[p\omega]$$

But we assumed $\pi_2 \notin \mathbb{Z}[p\omega]$. Hence, $\pi_1\pi_2 \in \mathbb{Z}[p\omega] \iff \pi_1 \in p\mathbb{Z}[\omega]$.

□

Remark: For the remainder of this section, we will assume $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}[\sqrt{d}]$ ($d < -3$), and p prime such that $\left(\frac{d}{p}\right) = -1$.

The assumption $d < -3$ is made to guarantee that the only units in our ring of integers are ± 1. This ensures that $U(\mathbb{Z}[n\omega]) = U(\mathbb{Z}[\omega])$ for any order. Also, Theorem 1.4.9. tells us that the assumption $\left(\frac{d}{p}\right) = -1$ is equivalent to assuming p remains prime (and thus irreducible) in our ring of integers. This is desirable in its own right, but we will also take advantage of the fact that this implies $\mathbb{Z}[\omega]/(p)$ is a field.

Theorem 2.1.2. Assume $\mathbb{Z}[\omega]$ is a UFD and $\beta \in \mathbb{Z}[p\omega]$ with prime factorization $p^n\pi_1 \cdots \pi_k$ such that $(\pi_i, p) = 1$ in $\mathbb{Z}[\omega]$. For a fixed j, assume $\pi_j \in \mathbb{Z}[p\omega]$. Then, if $\gamma_1 \cdots \gamma_m$ is an irreducible factorization of β in $\mathbb{Z}[p\omega]$, $\pi_j = \gamma_t$ for some $1 \leqslant t \leqslant m$.

Proof. without loss of generality we will prove the statement for $\pi_1 \in \mathbb{Z}[p\omega]$.

Assume $\pi_1 \in \mathbb{Z}[p\omega]$. Note, $\pi_1 \notin p\mathbb{Z}[\omega]$ as $(\pi_1, p) = 1$.

Let $\beta = \alpha_1\alpha_2 \cdots \alpha_n$ be an irreducible factorization of β in $\mathbb{Z}[p\omega]$. As π_1 is prime and $\pi_1|\beta$, without loss of generality $\pi_1|\alpha_1$ as an element of $\mathbb{Z}[\omega]$. Thus, by the uniqueness of the prime factorization of β in $\mathbb{Z}[\omega]$, $\alpha_1 = \pi_1 \cdot (p^r\pi_{i_1} \ldots \pi_{i_l})u$ where $u \in U(\mathbb{Z}[\omega]) = U(\mathbb{Z}[p\omega]) = \{\pm 1\}$.

If $r \geqslant 1$, then $(p^r\pi_{i_1} \cdots \pi_{i_l})u \in \mathbb{Z}[pi]$, and thus α_1 is not irreducible. Hence, we assume $r = 0$.

So we consider $\alpha_1 = \pi_1 \cdot (\pi_{i_1} \dots \pi_{i_l})u$. If $(\pi_{i_1} \cdots \pi_{i_l})u \notin \mathbb{Z}[p\omega]$, by Lemma 2.1.1, $\pi_1 \notin p\mathbb{Z}[i] \Rightarrow \pi_1 \cdot (\pi_{i_1} \dots \pi_{i_l})u = \alpha_1 \notin \mathbb{Z}[pi]$. $\Rightarrow\Leftarrow$

So, $(\pi_{i_1} \dots \pi_{i_l})u \in \mathbb{Z}[p\omega]$, but $\alpha_1 = \pi_1 \cdot (\pi_{i_1} \cdots \pi_{i_l})u$ is irreducible in $\mathbb{Z}[p\omega]$, so $(\pi_{i_1} \dots \pi_{i_l})u \in U(\mathbb{Z}[p\omega])$.

Thus, $\pi_1 = \alpha_1$ up to a unit, so π_1 appears in every irreducible factorization of β. □

The importance of this is as follows. To determine the elasticity of $\mathbb{Z}[p\omega]$, Theorem 2.1.2. tells us we need only consider elements in the conductor - $p\mathbb{Z}[\omega]$. This is because ideals relatively prime to the conductor retain unique factorization into prime ideals due to Theorem 1.4.6.—in particular, principal ideals generated by elements not in the conductor. Thus, these elements behave in the order as they do in the ring of integers. That is, their elasticity is bounded above by $\frac{D(Cl(\mathbb{Z}[p\omega]))}{2} \leqslant \frac{|Cl(\mathbb{Z}[p\omega])|}{2} = \frac{(p+1)\cdot|Cl(\mathbb{Z}[\omega])|}{2} = \frac{p+1}{2}$ when $\left(\frac{d}{p}\right) = -1$. The inequality and equality are due to Theorem 2.1 and [2] respectively. As we will soon see, elements in the conductor will achieve an upper bound which exceeds this value. Theorem 2.1.2. allows us to narrow our search even further.

Take any $\gamma \in p\mathbb{Z}[\omega]$ with prime factorization $\gamma = p^r\pi_1\pi_2\cdots\pi_m$, $r \geqslant 1$ in $\mathbb{Z}[\omega]$ where $(p, \pi_i) = 1$. If $\pi_1 \in \mathbb{Z}[p\omega]$, we let $\delta = p^r\pi_2\cdots\pi_m$ which is also in $p\mathbb{Z}[\omega]$ as $r \geqslant 1$. We may write $\rho(\delta) = \frac{n_1}{n_2}$ where n_1 and n_2 are the lengths of the longest and shortest irreducible factorizations of β in $\mathbb{Z}[p\omega]$ respectively. Theorem 2.1.2. implies that every irreducible factorization of γ is of the form $\pi_1\delta_1\cdots\delta_t$ where $\delta_1\cdots\delta_t$ is an irreducible factorization of δ. Thus, $\rho(\gamma) = \frac{n_1+1}{n_2+1} \leqslant \frac{n_1}{n_2} = \rho(\delta)$.

Therefore, we only need to consider elements of $p\mathbb{Z}[\omega]$ of the form $p^r\pi_1\cdots\pi_N$ where the π_i's are irreducibles of $\mathbb{Z}[\omega]$ not in $\mathbb{Z}[p\omega]$. To do this, we will need the following definitions.

Definition 2.1.3. Let $\mathcal{O}_K$ be a ring of integers and $\mathcal{O} \subseteq \mathcal{O}_K$ an order. We say define an $\mathcal{O}_k$ − *sequence* to be a sequence $\{\pi_1, \dots, \pi_n\}$ of (not necessarily distinct) elements in $Irr(\mathcal{O}_K)$. We say an $\mathcal{O}_k-$sequence $\{\pi_1, \dots, \pi_n\}$ is an $\mathcal{O}$ − *sequence* if $\pi_1 \cdots \pi_n \in \mathcal{O}$.

Definition 2.1.4. We define the *generalized Davenport constant* of an order $\mathcal{O} \subseteq \mathcal{O}_K$ to be the largest n such that there exists an $\mathcal{O}-$sequence of length n with no $\mathcal{O}-$subsequence. We denote the generalized Davenport constant of an order $\mathcal{O}$ as $\bar{D}(\mathcal{O})$.

The language used in these definitions is very similar to that of the Davenport constant, and that is no coincidence. Not only are these constants similarly defined, but they are intimately related for the orders we are studying as we will see in the proof of the following theorem.

Theorem 2.1.5. $\bar{D}(\mathbb{Z}[p\omega]) = p$

Proof. We begin by noting $\mathbb{Z}[\omega]/(p) \cong \mathbb{F}_p[\omega]$ via the map $[a+b\omega] \longrightarrow \hat{a}+\hat{b}\cdot\hat{\omega}$, where the coefficients and ω are reduced mod (p), and $\mathbb{F}_p$ is the finite field of p elements (note: they must be isomorphic because they are both finite fields of order p^2). $\mathbb{Z}[\omega]/(p)$ is a field because p is prime and thus (p) is prime, and prime ideals in $\mathbb{Z}[\omega]$ are maximal because rings of integers are Dedekind — in particular, 1-dimensional. Also, $\mathbb{F}_p[\hat{\omega}]$ is the splitting field of $\hat{\omega}$ over $\mathbb{F}_p$ because $\left(\frac{d}{p}\right) = -1$.

Now, considering $\mathbb{Z}[\omega]/(p)$, the elements of $\mathbb{Z}[p\omega]$ comprise the cosets of (p) of the form $[a + 0 \cdot \omega]$, which have isomorphic image $\mathbb{F}_p$ under the map defined above. Thus, we can identify $\mathbb{Z}[p\omega] \subseteq \mathbb{Z}[\omega]$ with $\mathbb{F}_p \subseteq \mathbb{F}_p[\hat{\omega}]$. Reducing coefficients mod p, we see that $\pi_1 \cdots \pi_N$ has no $\mathcal{O}$-subproduct iff $\hat{\pi}_1 \cdots \hat{\pi}_n$ has no subproduct in $\mathbb{F}_p$. In other words, $\bar{D}(\mathbb{Z}[p\omega])$ is the largest N such that there is a product in $\mathbb{F}_p[\hat{\omega}]$ with no subproduct in $\mathbb{F}_p$. Also, because $\mathbb{F}_p[\hat{\omega}]$ has no zero-divisors, this is equivalent to finding the largest N such that there is a product in $\mathbb{F}_p[\hat{\omega}]^*$ with no subproduct in $\mathbb{F}_p^*$.

Now, $\mathbb{F}_p[\hat{\omega}]$ and $\mathbb{F}_p$ are finite fields, so $\mathbb{F}_p[\hat{\omega}]^*$ and $\mathbb{F}_p^*$ are abelian, multiplicative groups with $\mathbb{F}_p^* \subseteq \mathbb{F}_p[\omega]^*$. Thus, $G = \mathbb{F}_p[\hat{\omega}]^*/\mathbb{F}_p^*$ forms a finite, abelian group. Hence, finding the longest product in $\mathbb{F}_p[\omega]^*$ with no subproduct in $\mathbb{F}_p^*$ is equivalent to finding the longest $G-$sequence with no $0-$subsequence. Notice, this is just $D(G) - 1$. By the primitive element theorem, we know $\mathbb{F}_p[\omega]^*$ is cyclic, so G is also cyclic. Thus, by Theorem 2.2,

$$D(G) - 1 = |G| - 1 = \frac{|\mathbb{F}_p[\hat{\omega}]^*|}{|\mathbb{F}_p^*|} - 1 = \frac{p^2-1}{p-1} - 1 = p$$

So we conclude the generalized Davenport constant constant of $\mathbb{Z}[p\omega] \subseteq \mathbb{Z}[\omega]$ is p. □

Theorem 2.1.6. If $\beta \in p\mathbb{Z}[\omega]$ has prime factorization $p\pi_1 \cdots \pi_N$ in $\mathbb{Z}[\omega]$, then β is irreducible in $\mathcal{O} = \mathbb{Z}[p\omega] \iff \{\pi_1, \pi_2 \ldots, \pi_N\}$ has no $\mathcal{O}-$subsequence.

Proof. ($\Rightarrow$) We proceed by contraposition. Assume $\pi_1 \cdots \pi_N$ has a $\mathcal{O}-$subproduct. without loss of generality say $\pi_1 \cdots \pi_k \in \mathbb{Z}[p\omega]$. Then, $\beta = (\pi_1 \cdots \pi_k) \cdot (p\pi_{k+1} \cdots \pi_N)$ where $\pi_1 \cdots \pi_k, p\pi_{k+1} \cdots \pi_N \in \mathbb{Z}[p\omega]$ are both non-zero, non-units. Thus, β is not irreducible in $\mathbb{Z}[p\omega]$.

($\Leftarrow$) Assume $\pi_1 \cdots \pi_N$ has no $\mathcal{O}-$subproduct. Assume for the purpose of contradiction that β is not irreducible. Then, by the uniqueness of the prime factorization, β factors non-trivially in

$\mathbb{Z}[p\omega]$ as $(u_1 \cdot p\pi_{i_1} \cdots \pi_{i_n})(u_2 \cdot \pi_{j_1} \cdots \pi_{j_m})$ where $u_1, u_2 \in U(\mathbb{Z}[p\omega])$. But this implies $\pi_{j_1} \cdots \pi_{j_m}$ is a $\mathcal{O}-$subproduct of $\pi_1 \cdots \pi_N$ which is a contradiction. Thus, β is irreducible in $\mathbb{Z}[p\omega]$

□

The following is the central result of this paper.

Theorem 2.1.7. Let $\mathbb{Z}[\omega]$ be the ring of integers of $\mathbb{Q}[\sqrt{d}]$ where $d < -3$ and p be a prime such that $\binom{d}{p} = -1$. If $\mathbb{Z}[\omega]$ is a UFD, $\rho(\mathbb{Z}(p\omega)) \leqslant 1 + \frac{p}{2}$.

Proof. Let $\alpha \in p\mathbb{Z}[\omega]$ with prime factorization $p^k\pi_1 \cdots \pi_M$ $(k \geqslant 1)$ in $\mathbb{Z}[\omega]$. Recall, by Theorem 2.1.2. we may assume without loss of generality $\pi_i \notin \mathbb{Z}[p\omega], (\pi_i, p) = 1$. Because of this assumption, we know the finest irreducible factorization of α possible in $\mathbb{Z}[p\omega]$ would have the form $p^k(\pi_1\pi_2)\cdots(\pi_{M-1}\pi_M)$ if M is even, and $p^k(\pi_1\pi_2)\cdots(\pi_{M-2}\pi_{M-1}\pi_M)$ if M is odd. So we get a factorization of length $k + \lfloor \frac{M}{2} \rfloor$.

Case 1: $M < kp$. We know that every irreducible factor of α can contain at most one factor of p. Thus, every irreducible factorization has length at least k, so

$$\rho(\alpha) \leqslant \frac{k + \lfloor \frac{M}{2} \rfloor}{k} \leqslant \frac{k + \frac{M}{2}}{k} < \frac{k + \frac{kp}{2}}{k} = 1 + \frac{p}{2}$$

Case 2: $M \geqslant kp$. Now, any irreducible factorization of α must take the form

$$(p\pi_{1,1} \cdots \pi_{1,n_1}) \cdots (p\pi_{k,1} \cdots \pi_{k,n_k})(\pi_{k+1,1} \cdots \pi_{k+1,n_{k+1}}) \cdots (\pi_{t,1} \cdots \pi_{t,n_t})$$

By Theorems 2.1.5. and 2.1.6., $n_i \leqslant p$ for $1 \leqslant i \leqslant k$. Also, each $\beta = (\pi_{j,1} \cdots \pi_{j,n_j}) \in \mathbb{Z}[p\omega] \backslash p\mathbb{Z}[\omega]$. So,

$$\rho(\beta) \leqslant \frac{D(Cl(\mathbb{Z}[p\omega]))}{2} \leqslant \frac{|Cl(\mathbb{Z}[p\omega])|}{2} = \frac{p+1}{2}$$

Using the factorizations $(\pi_{j,1} \cdots \pi_{j,n_j})(\bar{\pi}_{j,1} \cdots \bar{\pi}_{j,n_j}) = (\pi_{j,1}\bar{\pi}_{j,1}) \cdots (\pi_{j,n_j}\bar{\pi}_{j,n_j})$, we find $\frac{n_j}{2} \leqslant \rho(\beta) \leqslant \frac{p+1}{2} \Rightarrow n_j \leqslant p+1$ for $k+1 \leqslant j \leqslant t$. This is sufficient to determine that the length of any given factorization is at least $k + \lceil \frac{M-kp}{p+1} \rceil$. Hence,

$$\rho(\alpha) \leqslant \frac{k + \lfloor \frac{M}{2} \rfloor}{k + \lceil \frac{M-kp}{p+1} \rceil} \leqslant \frac{k + \frac{M}{2}}{k + \frac{M-kp}{p+1}} = \frac{2k + M}{2k + \frac{2M-2kp}{p+1}} = (p+1)\frac{2k+M}{2k+2M}$$

which is maximized when M is minimized. So $M \geqslant kp$ implies

$$\rho(\alpha) \leqslant (p+1)\frac{2k+kp}{2k+2kp} = \frac{p+1}{2} \cdot \frac{2+p}{1+p} = 1 + \frac{p}{2}$$

So $\rho(\alpha) \leqslant 1 + \frac{p}{2}$. As we have noted, the elasticity of elements away from the conductor is bounded above by $\frac{D(Cl(\mathbb{Z}[p\omega]))}{2} \leqslant \frac{|Cl(\mathbb{Z}[p\omega])|}{2} = \frac{p+1}{2} \leqslant 1 + \frac{p}{2}$ (see [2]). Thus, $\rho(\mathbb{Z}[p\omega]) \leqslant 1 + \frac{p}{2}$.

□

We strongly suspect that this inequality is in fact equality.

Proposition: If each class of $\mathbb{Z}[\omega]/(p)$ contains an irreducible element, $\rho(\mathbb{Z}(p\omega)) = 1 + \frac{p}{2}$.

If this is the case, we can construct an element which achieves the upper bound as follows. Let $\gamma \in \mathbb{Z}[\omega]$ such that it's image $\hat{\gamma}$ is a primitive element of $\mathbb{F}_p[\hat{\omega}]$. Then, $[\hat{\gamma}]$ generates $\mathbb{F}_p[\hat{\omega}]^*/\mathbb{F}_p^*$, so γ^p has no $\mathcal{O}$-subproduct. Because all the elements of $[\gamma] \in \mathbb{Z}[\omega]/(p)$ have this property, we may assume γ is irreducible. Let $\delta = (p\gamma^p)(p\bar{\gamma}^p) = p^2(\gamma\bar{\gamma})^p$. Then, $\rho(\delta) \geqslant \frac{2+p}{2} = 1 + \frac{p}{2}$, so we achieve our upper bound.

Example 2.1.8. It is well known that there are only finitely many imaginary quadratic UFDs. This statement dates back to Gauss. Let us consider $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}] = \mathbb{Z}[\omega]$ and $\mathbb{Z}[5\omega] \subseteq \mathbb{Z}[\omega]$ $(p = 5)$. This ring is actually a Euclidean domain with its norm being a Euclidean function [8]. It is easy to verify that $\left(\frac{-7}{5}\right) = -1$. Now, we are interested in finding a prime $\alpha \in \mathbb{Z}[\omega]$ such that $[\hat{\alpha}]$ generates $\mathbb{F}_5[\hat{\omega}]^*/\mathbb{F}_5^*$. Note, $|\mathbb{F}_5[\hat{\omega}]^*/\mathbb{F}_5^*| = 6$, so this is equivalent to finding an $\alpha \in \mathbb{Z}[\omega]$ such that $\hat{\alpha}^n \notin \mathbb{F}_5^*$ for $1 \leqslant n \leqslant 5$. By Lagrange's theorem, it is sufficient to check up to $n = 3$. In this case, $\omega = \frac{1+\sqrt{-7}}{2}$ satisfies these conditions. First, $N(\omega) = \omega \cdot \bar{\omega} = 2$, so ω is irreducible and thus prime as $\mathbb{Z}[\omega]$ is a UFD. Also, $\hat{\omega}^2 = -2 + \frac{1+\sqrt{-7}}{2} \equiv 3 + \frac{1+\sqrt{-7}}{2} \bmod 5\mathbb{Z}[\omega] \notin \mathbb{F}_5^*$, and $\hat{\omega}^3 = -2 - \frac{1+\sqrt{-7}}{2} \equiv 3 + 4\frac{1+\sqrt{-7}}{2} \bmod 5\mathbb{Z}[\omega] \notin \mathbb{F}_5^*$. Therefore, the element $[5 \cdot \omega^5][5 \cdot \bar{\omega}^5] = 5^2 \cdot 2^5$ has elasticity $\frac{2+5}{2} = 1 + \frac{5}{2}$ achieving the upper bound from Theorem 2.1.7.

Before we move on to some more general results, we give a few notes on the assumptions in Theorem 3.7. As we noted, the reason for the assumption $d < -3$ is that we want the units of the ring of integers and the order to be the same. This is because the proof relies in many instances on the uniqueness of the prime factorization of elements in $\mathbb{Z}[\omega]$. If $\mathbb{Z}[\omega]$ contains units that $\mathbb{Z}[p\omega]$ does not, our analysis changes. The following example illustrates how.

Example 2.1.9. Consider the Guassian integers $\mathbb{Z}[i]$ and the order $\mathbb{Z}[19i]$ which have units $\{\pm 1, \pm i\}$ and $\{\pm 1\}$ respectively. Note $\mathbb{Z}[i]$ is a UFD. Now, $2 + 3i$ generates $\mathbb{F}_{19}[i]^*$, so as an element of $\mathbb{Z}[i]$,

$(2+3i)^{19}$ has no $\mathcal{O}$-subproduct. However, $19 \cdot (2+3i)^{19}$ is not irreducible in $\mathbb{Z}[19i]$ as Theorem 2.1.6. would seem to imply. This is because, considering the coefficients mod 19, $(2+3i)^{10} \in i\mathbb{F}_{19}$, so $19 \cdot (2+3i)^{19}$ factors non-trivially in $\mathbb{Z}[19i]$ as $[i(2+3i)^{10}] \cdot [19(2+3i)^9(-i)]$. This happens because $\pm i$ are units in $\mathbb{Z}[i]$ but not $\mathbb{Z}[19i]$. The same can be said for any primitive element γ because γ^{10} will always be in $i\mathbb{F}_{19}^*$ as this subgroup contains all elements of order 2. Regardless, with some minor modifications to the proof above, one can show that $\rho(\mathbb{Z}[pi]) = \frac{p+3}{4}$ for $p \equiv 3 \bmod 4$. The details are left as an exercise to the reader.

2.2 Non-UFDs

Now that we no longer have unique factorization of elements, the approach from the previous section is obviously inappropriate, but many of the techniques remain helpful here. This is because while losing unique prime factorization of elements, we retain it for ideals. This is a principal reason why the study of rings of integers is so rich - the fact that they are Dedekind. Unfortunately, while orders conserve a number of properties of rings of integers, they fail to be Dedekind as they are not integrally closed (omit of course the maximal order $\mathcal{O}_K$). So we need to be careful about making distinctions between ideals of $\mathcal{O}_K$ and $\mathcal{O}$.

Conjecture 2.2.1. Let $\mathbb{Z}[\omega]$ be the ring of integers of $\mathbb{Q}[\sqrt{d}]$ where $d < -3$ and p prime such that $\left(\frac{d}{p}\right) = -1$. If $\mathbb{Z}[\omega]$ is a non-UFD, $\rho(\mathbb{Z}(p\omega)) = 1 + p \cdot \frac{D(Cl(\mathbb{Z}[\omega]))}{2} = 1 + p \cdot \rho(\mathbb{Z}[\omega])$.

Note that the first equality is identical to the UFD case as $D(Cl(\mathbb{Z}[\omega])) = 1$, and thus we recover $1 + \frac{p}{2}$ from Theorem 3.7. The second equality, which once again is due to Narkiewicz [6], holds only in the non-UFD case. We now endeavour to motivate this conjecture, starting with $1 + p \cdot \rho(\mathbb{Z}[\omega])$ as an upper bound.

One of the major difficulties presented in the non-UFD case is the elasticity of elements away from the conductor. Theorem 1.4.10. tells us that the ideals generated by these elements can be factored into prime ideals. Thus, using the same techniques as [10], we know that the elasticity of these elements is bounded above by $\frac{D(Cl(\mathbb{Z}[p\omega]))}{2}$. We would like to get this bound in terms of $D(Cl(\mathbb{Z}[\omega]))$. However, without knowing anything about the structure of $Cl(\mathbb{Z}[p\omega])$, the best we can do is $\frac{D(Cl(\mathbb{Z}[p\omega]))}{2} \leqslant \frac{|Cl(\mathbb{Z}[p\omega])|}{2} = \frac{(p+1)\cdot|Cl(\mathbb{Z}[\omega])|}{2}$. In the UFD case, this is not an issue because $\frac{(p+1)\cdot|Cl(\mathbb{Z}[\omega])|}{2} = \frac{1+p}{2}$ which is exceeded by elements in the conductor. However, in the non-UFD case where $|Cl(\mathbb{Z}[\omega])| \geqslant 2$ (see [1]), $\frac{(p+1)\cdot|Cl(\mathbb{Z}[\omega])|}{2} \geqslant 1 + \frac{p\cdot|Cl(\mathbb{Z}[\omega])|}{2} \geqslant 1 + p \cdot \rho(\mathbb{Z}[\omega])$, so the elasticity

of elements away from the conductor may exceed that of those in the conductor depending on the structure of $Cl(\mathbb{Z}[p\omega])$. In the cases where $\frac{D(Cl(\mathbb{Z}[p\omega]))}{2}$ does not exceed $1 + p \cdot \rho(\mathbb{Z}[\omega])$, it can be shown using similar techniques to the proof of Theorem 2.1.7. that the latter is an upper bound on the elasticity of the order. The proof is excluded here for brevity.

Now, the second question is if or when this upper bound is achieved. In order to find an element which achieves this upper bound, we would need an element in $\mathbb{Z}[\omega]$ which has irreducible factorizations

$$\gamma_1\gamma_2 = \beta_1\beta_2 \cdots \beta_d$$

with the following properties:

1. $d = D(Cl(\mathbb{Z}[\omega])$
2. $\beta_i \in \mathbb{Z}[p\omega] \ \forall \ 1 \leqslant i \leqslant d$
3. $[\gamma_1], [\gamma_2]$ generate $\mathbb{F}_p[\omega]^*/\mathbb{F}_p^*$

Property 1 can always be achieved by the following process. Let $\{[I_1], \ldots, [I_d]\}$ be a $0-$sequence of $Cl(\mathbb{Z}[\omega])$ with no proper $0-$subsequence, and let P_i, Q_i be a prime ideals in classes $[I_i], [I_i]^{-1}$ respectively for each i. Then, $(\gamma_1)(\gamma_2) = P_1P_2 \cdots P_d \cdot Q_1Q_2 \cdots Q_d = P_1Q_1 \cdot P_2Q_2 \cdots P_dQ_d = (\delta_1)(\delta_2) \cdots (\delta_d)$. Thus, $\gamma_1\gamma_2 = \beta_1\beta_2 \cdots \beta_d$ are equivalent irreducible factorizations up to a unit. For the details of the constructions, see [6].

This construction is especially encouraging because it does not rely on our choice of prime ideals from each class. It is well known that there are infinitely many prime ideals in each class for rings of integers, so our hope is that if we choose our primes wisely, we will be able to satisfy conditions 2 and 3 as well. The following theorem, while being interesting in it's own right, also shows us that we will be able to achieve condition 2 without putting any further restrictions on our choice of P_i in the case when $d \equiv 2, 3 \bmod 4$.

Theorem 2.2.2. Let P be a prime ideal in the quadratic ring of integers $\mathbb{Z}[\sqrt{d}]$. Then, $[\bar{P}] = [P^{-1}]$.

Proof. P is prime, so it lies over some rational prime p. That is, $P \cap \mathbb{Z} = p\mathbb{Z}$. Hence, $p \in P$, so $p\mathbb{Z}[\sqrt{d}] \subseteq P$, and $\mathbb{Z}[\sqrt{d}]$ is Dedekind, so this implies P divides $p\mathbb{Z}[\sqrt{d}]$. Now, if $P = p\mathbb{Z}[\sqrt{d}]$, then we are done because $\bar{P} = P$, and P is principal, so $[\bar{P}] = [P] = [P^{-1}]$.

If $P \neq p\mathbb{Z}[\sqrt{d}]$, then p is not prime in $\mathbb{Z}[\sqrt{d}]$ as it is Dedekind and thus 1-dimensional. Hence, by Theorem 1.4.10., $\left(\frac{d}{p}\right) = 1$, so $x^2 - d$ splits over $\mathbb{F}_p$ into $(x-a)(x+a)$ (note $a^2 = -d \Rightarrow (-a)^2 = -d$).

Thus, by Theorem 1.4.10., $p\mathbb{Z}[\sqrt{d}] = (p, a-\sqrt{d})(p, a+\sqrt{d}) = Q\bar{Q}$. By the uniqueness of prime factorization, $P = Q$ without loss of generality. Thus, $P\bar{P} = p\mathbb{Z}[\sqrt{d}]$ is principal, so $[\bar{P}] = [P^{-1}]$ $\square$

This is a wonderful result because it shows us that for any choice of P, there is a prime ideal Q in $[P^{-1}]$ such that PQ is generated by an element of $\mathbb{Z}[p\sqrt{d}]$ - specifically of $\mathbb{Z}$. Thus, in the case when $d \equiv 2, 3 \bmod 4$, we can achieve conditions 1 and 2 without putting any restriction on our choice of P_i.

Our last task is to show that we can choose P_i such that condition 3 is satisfied. It is important to note first that if $(\gamma_1) = P_1 P_2 \cdots P_d$ such that $[\gamma_1]$ generates $\mathbb{F}_p[\omega]^*/\mathbb{F}_p^*$, then $(\gamma_2) = \bar{P}_1\bar{P}_2\cdots\bar{P}_d = (\bar{\gamma}_1)$. Hence, $[\gamma_2] = [\bar{\gamma}_1]$ also generates $\mathbb{F}_p[\omega]^*/\mathbb{F}_p^*$ because $(\bar{\gamma}_1)^n \in \mathbb{F}_p^* \Rightarrow (\bar{\gamma_1^n}) \in \mathbb{F}_p^* \Rightarrow \gamma_1^n \in \mathbb{F}_p^*$. Thus, we need only find primes such that $[\gamma_1]$ generates. To this point, we have been unable to prove or disprove that this is possible in general. However, if we once again assume that every class of $\mathbb{Z}[\omega]/(p)$ contains an irreducible element, the three properties imply the the element $[p\cdot\gamma_1^p][p\cdot\gamma_2^p] = p^2\delta_1^p\delta_2^p\cdots\delta_d^p$ has an elasticity of at least $\frac{2+p\cdot d}{2} = 1 + p\cdot\rho(\mathbb{Z}[\omega])$ – our desired upper bound.

Example 2.2.3. Let us consider the ring $\mathbb{Z}[\sqrt{-14}]$ and the order $\mathbb{Z}[11\cdot\sqrt{-14}]$ ($p = 11$). Now, the Minkowski bound for this ring of integers is $\frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{(56)} \approx 4.764 < 5$, so $Cl(\mathbb{Z}[\sqrt{-14}]$ is generated by the prime factors of (2) and (3). Now, $\left(\frac{-14}{2}\right) = 0$ and $\left(\frac{-14}{3}\right) = -1$, so 2 ramifies and 3 splits in $\mathbb{Z}[\sqrt{-14}]$. Let $(2) = \mathcal{P}_2^2$ and without loss of generality $(3) = \mathcal{P}_3\hat{\mathcal{P}}_3$. Note, $\mathcal{P}_2$ and $\mathcal{P}_3$ are not principal as they have norms 2 and 3, and $N(\alpha) = a^2 + 14b^2 = 2, 3$ have no integral solutions. Thus, $[\mathcal{P}_2]$ has order 2 in $Cl(\mathbb{Z}[\sqrt{-14}])$.

Now, consider the equation $(2+\sqrt{-14})(2-\sqrt{-14}) = 2\cdot 3^2$. Thus, as ideals, $(2+\sqrt{-14})(2-\sqrt{-14}) = \mathcal{P}_2^2\mathcal{P}_3^2\hat{\mathcal{P}}_3^2$. Now, as 2 and 3 clearly do not divide $(2\pm\sqrt{-14})$, without loss of generality we have $(2+\sqrt{-14}) = \mathcal{P}_2\mathcal{P}_3^2$ by the uniqueness of the prime factorization. Hence, $[\mathcal{P}_3]^2 = [\mathcal{P}_2]^{-1}$, so $Cl(\mathbb{Z}[\sqrt{-14}])$ is generated by $[\mathcal{P}_3]$, and $[\mathcal{P}_3]^2 = [\mathcal{P}_2]^{-1} = [\mathcal{P}_2]$ is not principal, but $[\mathcal{P}_3]^4 = [\mathcal{P}_2]^2$ is, so $Cl(\mathbb{Z}[\sqrt{-14}]) \cong \mathbb{Z}_4$ and $D(Cl(\mathbb{Z}[\sqrt{-14}])) = 4$.

Now, to find a candidate element, we need to find an element in $[\mathcal{P}_3]$. The most natural choice would be $\mathcal{P}_3$ itself. Now, $x^2 + 14$ factors as $(x+1)(x-1)$ over $\mathbb{F}_3$, so by Theorem 1.4.10., $(3) = (3, \sqrt{-14}+1)(3, \sqrt{-14}-1) = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$. Thus, without loss of generality $\mathcal{P}_3 = (3, 1+\sqrt{-14})$. Now, $(5+2\sqrt{-14})(5-2\sqrt{-14}) = (3)^4 = \mathcal{P}_3^4\hat{\mathcal{P}}_3^4$, and clearly $3 \nmid (5\pm\sqrt{-14})$, so without loss of generality $(5+2\sqrt{-14}) = \mathcal{P}_3^4$. However, this will not yield an element of elasticity

$1+11\cdot\rho(\mathbb{Z}[\sqrt{-14}])$ because $[5+2\sqrt{-14}]$ has order 6 in $\mathbb{F}_{11}[\sqrt{-14}]^*/\mathbb{F}_{11}^*$ (note: $(5+2\sqrt{-14})^3 = -715+38\sqrt{-14} \equiv 0+5\sqrt{-14} \bmod 11$). Thus, we need to find another prime ideal in $[\mathcal{P}_3]$. Fortunately, for rings of integers, we know there are infinitely many primes in each class.

Consider the equation $(1+\sqrt{-14})(1-\sqrt{-14}) = 3\cdot 5$. Now, x^2+14 factors as $(x+1)(x-1)$ over $\mathbb{F}_5$ as well, so $(5) = (5, 1+\sqrt{-14})(5, 1-\sqrt{-14}) = \mathcal{P}_5\bar{\mathcal{P}}_5$. Thus, $(1+\sqrt{-14})(1-\sqrt{-14}) = 3\cdot 5 = \mathcal{P}_3\hat{\mathcal{P}}_3\mathcal{P}_5\bar{\mathcal{P}}_5$. Now, neither 3 nor 5 divide, so without loss of generality $(1+\sqrt{-14}) = \mathcal{P}_3\mathcal{P}_5$. Hence, $[\mathcal{P}_5] = [\mathcal{P}_3]^{-1}$. Note, as $[\mathcal{P}_3]$ and $[\mathcal{P}_3]^{-1}$ have the same order, the distinction is insignificant for our purposes.

Using an identical argument and the equation $(9+\sqrt{-14})(9-\sqrt{-14}) = 19\cdot 5$ we find that the prime factors (19) also have order 4. Now, x^2+14 factors as $(x-9)(x+9)$ over $\mathbb{F}_{19}$, so $(19) = (19, 9+\sqrt{-14})(19, 9-\sqrt{-14}) = \mathcal{P}_{19}\bar{\mathcal{P}}_{19}$. Finally, we know $\mathcal{P}_{19}^4$ is principal, and the generator has norm 19^4, so we solve $a^2+14b^2 = 19^4$ to find $(325+42\sqrt{-14})(325-42\sqrt{-14}) = (19)^4 = \mathcal{P}_{19}^4\bar{\mathcal{P}}_{19}^4$. As, $19 \nmid (325+42\sqrt{-14})$, we conclude $(325+42\sqrt{-14}) = \mathcal{P}_{19}^4$, and a direct calculation shows that $[325+42\sqrt{-14}]$ generates $\mathbb{F}_{11}[\sqrt{-14}]^*/\mathbb{F}_{11}^*$. Therefore, the element $[11\cdot(325+42\sqrt{-14})^{11}][11\cdot(325-42\sqrt{-14})^{11}] = 11^2\cdot 19^{44}$ has elasticity $\frac{2+44}{2} = 1+11\cdot\frac{4}{2} = 1+11\cdot\frac{D(CL(\mathbb{Z}[\sqrt{-14}]))}{2} = 1+11\cdot\rho(\mathbb{Z}[\sqrt{-14}])$ achieving our desired upper bound.

Chapter 3

Conclusion

We have analyzed what happens when we relax the UFD assumption. A natural next step is to consider what happens when we relax the assumption that our order is of prime index. While calculating the generalized Davenport constant in this case appears to be a relatively tame problem, analyzing elements in the conductor becomes much more difficult. This is because Theorem 2.1.1. fails to hold in general, so we will have to develop some new techniques to analyze this case further. Beyond the quadratic case, the problem becomes even harder as conductors fail to be principal in general. Thus, to explore elasticity in such orders, we would likely need to take a more ideal-driven approach.

There is a deep connection between factorization and cryptography. For example, RSA, a very famous cryptosystem, relies on the difficulty of factoring the product of two large primes. It would also be interesting to explore if this work can be used to create a cryptosystem..

Bibliography

[1] Leonhard Carlitz. A characterization of algebraic number fields with class number two. *Proceedings of the American Mathematical Society*, 11(3):391–392, 1960.

[2] H. Cohn. *Advanced Number Theory*. Dover Books on Mathematics. Dover Publications, 2012.

[3] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. Third Edition with Solutions*. AMS Chelsea Publishing. American Mathematical Society, 2022.

[4] James Coykendall. Theory of factorization. `https://jcoyken.people.clemson.edu/factorization.pdf`.

[5] Jim Coykendall. Elasticity properties preserved in the normset. *Journal of Number Theory*, 94(2):213–218, 2002.

[6] W Narkiewicz. A note on elasticity of factorizations. *Journal of Number Theory*, 1(51):46–47, 1995.

[7] Władysław Narkiewicz and Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers*, volume 57. Springer, 1974.

[8] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[9] Pace Nielson. An introduction to orders of number fields. `https://kskedlaya.org/Math254B/Orders.pdf`.

[10] Robert J Valenza. Elasticity of factorization in number fields. *Journal of Number Theory*, 36(2):212–218, 1990.