Singular Moduli and the Ideal Class Group

Caleb Geiger

A thesis
submitted in partial fulfillment of the
requirements for the degree of

Master of Science

University of Washington

2020

Committee:

Bianca Viray

Max Lieblich

Program Authorized to Offer Degree:
Mathematics

University of Washington

Abstract

Singular Moduli and the Ideal Class Group

Caleb Geiger

Chair of the Supervisory Committee:
Bianca Viray

Let d_1 and d_2 be discriminants of distinct quadratic imaginary orders $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$ and let $J(d_1, d_2)$ denote the product of differences of CM j-invariants with discriminants d_1 and d_2. In 2012, Lauter and Viray generalized the methods of Gross, Zagier, and Dorman to give a computable formula for $v_p(J(d_1, d_2))$ for any distinct pair of discriminants d_1, d_2 and any prime $p > 2$. Further, in the case that d_1 is squarefree and d_2 is the discriminant of any quadratic imaginary order, they gave a simple closed form. To do this, they related the question to a particular counting problem. We recap the developments of Gross-Zagier, Dorman, and Lauter-Viray before making progress on the remaining cases by considering a related counting problem.

ACKNOWLEDGMENTS

I would like to express gratitude towards my advisor, Bianca Viray, without whom this thesis would not have been possible. I would also like to thank Max Lieblich for his mentoring. I learned much from them both, and I have become a better person because of the time and effort they have invested in me.

I thank my colleagues and friends who have supported me throughout my journey. A special thanks to my office mates Ashwin, Gerardo, Kevin, Nikolas, Scott, and Zihui, as well as my academic siblings Manar, Sam, and Thomas.

Finally, I wish to thank my family and those who have helped me positively grow throughout my time writing this thesis outside of academia. In particular, my mother, who gave me constant encouragement to succeed; my father, who sparked my initial interest in the subject; my brothers, for their welcome distractions; and my sister, who inspired me to attend university. A special thanks to Camilo, Seth, and Sharat for everything that they've done, which cannot be put in bijection with a subset of the integers.

To the grad student reading this for inspiration, it may seem like everyone has it together, but the journey is challenging for everyone. This final product is the result of dozens of revisions, I didn't just wake up one day with this thesis in mind. Don't be discouraged; if I can do this, so can you.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Brief History and Motivation

Gross and Zagier in their seminal paper [GZ85, Def 1.2] introduced a function of particular note.

Definition 1.1.1. Given two arbitrary discriminants of imaginary quadratic orders, d_1 and d_2, define the function

$$J(d_1, d_2) := \prod_{\substack{\mathrm{disc}[\tau_i]=d_i, \\ \tau_i \in \mathbb{H}/\,\mathrm{SL}_2(\mathbb{Z})}} (j(\tau_1) - j(\tau_2))$$

where j is the elliptic modular function.

If the d_i are coprime discriminants of *maximal* orders, surprisingly, $J(d_1, d_2)^{\frac{8}{w_1 w_2}}$ is an integer; moreover, it is a so-called 'highly-divisible' integer, meaning it is divisible by many small primes. In the maximal case, the paper of Gross-Zagier provided a beautiful description of its factorization (which we discuss in §2.2).

Later, Dorman [Dor88] would give an algebraic proof of one of the results of Gross-Zagier about $J(d_1, d_2)$, which was originally proven analytically. In particular, he gave an expression for the powers of its prime factorization in the case of d_1 being square-free, d_2 fundamental, and $\gcd(d_1, d_2) = 1$ (his results are discussed in §2.3).

Finally, we discuss the most recent results of Lauter and Viray [LV15b]. Inspired by cryptographic applications to computing denominators of certain Igusa polynomials [LV15a] used in the construction of genus 2 curves, Lauter-Viray generalized the factorization to include arbitrary discriminants. They give a method to compute the exact prime powers dividing $J(d_1, d_2)^{\frac{8}{w_1 w_2}}$ and give an explicit expression for the powers under certain technical conditions, conjecturing the result remains true when some conditions are dropped.

The expression given relates the power of the primes dividing $J(d_1, d_2)$ to a counting of ideals in an imaginary quadratic order of fixed norm with certain properties. In an attempt to attempt to show the conjectured formula holds true, we have worked on this counting problem. In §3, we determine the number of ideals of fixed norm in an imaginary quadratic order of discriminant d, relating it to the case of a maximal order, resulting in an interesting observation. We then give a proposed direction to prove the resut of Lauter-Viray and the tools we have to complete this task.

1.2 Notation

We will use K and L to denote number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Rational prime numbers will be denoted by ℓ, p, and q with corresponding primes $\mu, \mathfrak{p}$, and $\mathfrak{q}$ being used for prime ideals of a number field lying over the corresponding rational prime. In general, we try to use *fraktur* letters when referring to ideals, e.g. $\mathfrak{a}$ and $\mathfrak{b}$. Completion with respect to a prime ideal will be denoted via a subscript; so, for example $\mathbb{Q}_\ell$ would be the ℓ-adic rationals, the fraction field of the ℓ-adic integers $\mathbb{Z}_\ell$. To distinguish localization at a prime from the former, we use parentheses, i.e., $\mathbb{Z}_{(\ell)}$ and $\mathcal{O}_{L,(\mu)}$. Since there is a *unique* imaginary quadratic order for each discriminant d, we let this order be denoted $\mathcal{O}_d := \mathbb{Z}[\tau]$, where $\tau := \frac{d+\sqrt{d}}{2}$ and $d < 0$. We may also simply use $\mathcal{O}$ if the discriminant is clear from context, and reserve D for a fundamental discriminant $\mathcal{O}_D = \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. This gives an alternate expression for $\mathcal{O}_d = \mathbb{Z}[f\frac{D+\sqrt{D}}{2}]$ where $d = Df^2$ for some integer f, which we call the *conductor* of $\mathcal{O}_d$. Finally, we denote the class group of an order, that is, the group of locally principal (invertible) ideals modulo principle ideals, by $\mathrm{Cl}(\mathcal{O}_d)$, the Picard group of the order, which is of size $h = h_{\mathcal{O}_d} = h_d$.

Chapter 2

PREVIOUS RESULTS

This section recaps some of the results of Gross-Zagier, Dorman, and Lauter-Viray, which will display the motivation of those questions that we begin to answer in §3. Proofs of the results of this section are omitted, as they exist in the respective papers of note. We do, however, try to state all the results from first principles.

2.1 Preliminaries

Let $z \in \mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be a complex number in the upper-half plane. Then there exists a certain function called the *elliptic modular function* $j \colon \mathbb{H} \to \mathbb{C}$, which gives a parameterization of homothetic lattices of the form $\mathbb{Z}[\tau]$ where $\tau \in \mathbb{H}$. That is, given $\tau, \tau' \in \mathbb{H}$, then there is some $\lambda \in \mathbb{C}^\times$ such that $\mathbb{Z}[\tau] = \lambda\mathbb{Z}[\tau']$ if and only if $j(\tau) = j(\tau')$ [Lan87, Thm 4]. Explicitly, if we define $q := e^{2\pi i z}$, j is given by a q-expansion

$$j(z) := \frac{1}{q} + 744 + 196884q + \cdots = 1/q + \sum_{n \geq 0} c_n q^n$$

for some $c_n \in \mathbb{Z}$ [Sil09].

One may define an $\mathrm{SL}_2(\mathbb{Z})$ action on the upper-half plane by linear fractional transformations. In particular, given $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ define $A \cdot z := \frac{\alpha z + \beta}{\gamma z + \delta}$. The j-function is invariant under this action.

We will be primarily interested in evaluating $j(\tau)$ where τ satisfies

$$a\tau^2 + b\tau + c = 0$$

for some $a, b, c \in \mathbb{Z}$ where the discriminant $d := \mathrm{disc}(\tau) = b^2 - 4ac < 0$. Such $j(\tau)$ are called *singular moduli*. This discriminant differs from the maximal order of $K := \mathbb{Q}(\sqrt{d})$ by

a square [Ste12, Proposition 6.2.6] called its conductor, which we will denote f.

Let $\mathcal{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$ be the imaginary quadratic order of dicsriminant d. The following are standard (rather involved) results concerning singular moduli $j(\tau)$, that can be found in such texts as [Cox13, Thm 10.23,§11] or [Neu99, Thm 6.10]:

- $j(\tau)$ is an algebraic integer of degree $h = \#\operatorname{Cl}(\mathcal{O}_d)$, the class number of $\mathcal{O}_d$, over $\mathbb{Q}$,
- $K(j(\tau))$ is the ring class field of conductor f associated to K,
- There exists an elliptic curve, E, having complex multiplication by $\mathcal{O}_d$ with j invariant $j(E) = j(\tau)$,
- and the h different conjugates of $j(\tau)$ over $\mathcal{O}_d$ are the values $j(\tau')$ where τ' run over the roots of the primitive quadratic polynomials of discriminant d.

Suppose that d_1 and d_2 are two negative, relatively prime discriminants. Define

$$J(d_1, d_2) = \prod_{\operatorname{disc}[\tau_i]=d_i} (j(\tau_1) - j(\tau_2)).$$

This product is taken over the pairs of equivalence classes of imaginary quadratic elements $[\tau_1], [\tau_2]$ modulo the $\mathrm{SL}_2(\mathbb{Z})$ action given above.

One might be wary of the finiteness of this product, and rightly so; the finiteness of the product is a consequence of the finiteness of the class group, which is a non-trivial result itself [Ste12, §7].

In reference to this J function, the papers of Gross-Zagier and Dorman are concerned only when $d_i = D_i$ are fundamental. In this case, letting w_i be the number of roots of unity in $\mathcal{O}_{d_i}$, $J(D_1, D_2)^{\frac{4}{w_1 w_2}}$ is an integer unless one of the $D_i = -4$ in which case $J(D_1, D_2)^{\frac{8}{w_1 w_2}}$ is an integer. The case where one of the discriminants is -3, say D_2, results in adjoining ζ_3 a third root a unity, giving six roots of unity, i.e., $w_2 = 6$. This ostensibly gives a cube root in the expression of $J(D_1, -3)$; however, $j(\zeta_3) = 0$, and so the product becomes

$J(D_1, -3) = \prod_{\mathrm{disc}[\tau_1]=D_1} j(\tau_1)$. Since the other fundamental discriminant is coprime, we may use a result that $K(j(\tau_1)^{1/3}) = K(j(\tau_1))$ for any of the τ_1 [Cox13, §13].

When one removes the coprime and fundamental discriminant restrictions, as [LV15b] find, the factorization results in powers which can be fractional. One could alternately consider $J(d_1, d_2)^{\frac{24}{w_1 w_2}}$ to avoid such fractional powers; however, to stay as close as possible to the statements of Gross-Zagier, we shall not do so.

2.2 Gross-Zagier

Let D_1, D_2 be coprime, fundamental discriminants and $w_i = |\mathcal{O}_{D_i}^\times|$. Letting $D = D_1 D_2$, we consider all primes ℓ where $\left(\frac{D}{\ell}\right) \neq 1$, and for such primes, we define

$$\epsilon(\ell) = \begin{cases} \left(\frac{D_1}{\ell}\right) & \text{if } (\ell, D_1) = 1, \\ \left(\frac{D_2}{\ell}\right) & \text{if } (\ell, D_2) = 1 \end{cases}$$

where $(\frac{D_i}{\ell})$ is the Jacobi symbol. We extend ϵ to $\mathbb{Z}^{\geq 0}$ by multiplicativity.

The main result of [GZ85] is the following factorization formula:

Theorem 2.2.1 ([GZ85, Thm 1.3])**.**

$$J(D_1, D_2)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{n,n' \in \mathbb{Z} \\ n,n'>0, x^2+4nn'=D}} n^{\epsilon(n')}.$$

One may rewrite this result by defining

$$F(m) = \prod_{\substack{nn'=m \\ n,n'>0}} n^{\epsilon(n')},$$

then the result can be stated

$$J(D_1, D_2)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x^2<D \\ x^2 \equiv D \bmod 4}} F\left(\frac{D - x^2}{4}\right).$$

It is not at all obvious apriori, but these $F(m)$ are powers of a single prime, namely an $\ell \mid \frac{D-x^2}{4}$. The reason for the high-divisibility is then explained in a corollary.

Corollary 2.2.2 ([GZ85, Cor 1.6]). *If ℓ is a rational prime dividing $J(D_1, D_2)^{\frac{8}{w_1 w_2}}$, then $\left(\frac{D_1}{\ell}\right) \neq 1$, $\left(\frac{D_2}{\ell}\right) \neq 1$, and ℓ divides a positive integer of the form $\frac{D-x^2}{4}$. In particular, $\ell \leq D/4$; moreover, if $D \equiv 1 \bmod 8$, then $\ell < D/8$, and if $D_1 \equiv D_2 \equiv 5 \bmod 8$, then $\ell < D/16$.*

Namely, every prime ideal containing $j(\tau_1) - j(\tau_2)$ lies in a particular, bounded collection of rational primes, which is independent of the chosen prime ideal.

2.3 Dorman

In the paper of Gross-Zagier, the authors go on to give two proofs to provide a formula for the prime factorization of the differences of two singular moduli. Whilst the proof in the case of prime discriminants used only algebraic means, an analytic proof was necessary for the composite, relatively prime case. Dorman remedied this by providing an algebraic proof of such a formula in his paper [Dor88].

Again, we let D_1, D_2 be coprime, fundamental discriminants and $w_i = |\mathcal{O}_{D_i}^\times|$. Let $K = \mathbb{Q}(\sqrt{D_1})$ and $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of K. Define

$$R(n) = \#\{\mathfrak{a} \subseteq \mathcal{O} : |\mathcal{O}/\mathfrak{a}| = n\}.$$

Extend R to $\mathbb{Q}$ by defining $R(x) := 0$ for $x \in \mathbb{Q} \setminus \{1, 2, 3, \ldots\}$.

Let H be the *Hilbert Class Field* of K, i.e., the maximal unramified extension of K. It is well-known that its Galois group $G = \mathrm{Gal}(H/K) \simeq \mathrm{Cl}(\mathcal{O})$ [Cox13, Thm 5.23]. Let χ_{D_1} be the primitive, quadratic character defined mod D_1 extended to $\mathbb{Z}$ in the standard way, i.e., start by letting

$$\chi_p(x) = \begin{cases} 0 & \text{if } p \mid x \\ 1 & \text{if there is an } a \in \mathbb{Z} : x \equiv a^2 \bmod p \\ -1 & \text{if there is no } a \in \mathbb{Z} : x \equiv a^2 \bmod p, \end{cases}$$

then one can extend this to $\chi_{D_1} : (\mathbb{Z}/D_1)^\times \to \{\pm 1\}$ by multiplication and to $\mathbb{Z}$ by residue class.

Now, if $p \nmid D_1$, define the Frobenius

$$\mathrm{Frob}(p) = \begin{cases} 1 & \text{if } p \text{ splits in } K, \\ -1 & \text{if } p \text{ remains inert in } K. \end{cases}$$

Then, given $n = up^{a_p} \in \mathbb{Z}$ where $\gcd(p, u) = 1$, we define ϵ_p by

$$\epsilon_p(n) = \begin{cases} \mathrm{sgn}(n) & \text{if } p = \infty \\ \mathrm{Frob}(p)^{a_p} & \text{if } p \nmid D_1, \\ \chi_p(u)\chi_{D_1/p}(p)^{a_p} & \text{if } p \mid D_1. \end{cases}$$

These ϵ_p are thought of as 'genus characters' of K. That is, they reflect whether or not a particular ideal is a square in the class group or not (this being its genus). Thus, we arrive at Dorman's main result:

Theorem 2.3.1 ([Dor88, Thm 1.2])**.** *Let ℓ be a rational prime with ramification index e in K. Then,*

$$\mathrm{ord}_\ell \left(J(D_1, D_2)^{\frac{4}{w_1 w_2}} \right) = \frac{1}{2e} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \rho_\ell(x) R\left(\frac{D_1 D_2 - x^2}{4\ell^n} \right)$$

where

$$\rho_\ell(x) = \begin{cases} 0 & \text{if there is a } p \mid D_1 : p \neq \ell \text{ and } \epsilon_p(x^2 - D_1 D_2) = -1 \\ 2^{\#\{p : p \mid \gcd(x, D_1)\}} & \text{otherwise.} \end{cases}$$

Notice the relationship between the powers of primes dividing $J(D_1, D_2)$ to ideals of some norm 'in a specific genus class.' The generalized version of this result, which we will talk about in the following section is the main drive behind studying the questions of §3.

Remark 2.3.2. A great portion of the proofs rely on facts surrounding embeddings of endomorphisms of elliptic curves into the endomorphisms of their reduction, which requires a decent understanding on quaternion algebras. For general understanding of quaternion algebras, we direct the reader to [Voi18], which we found to be quite useful in the understanding on the proofs.

2.4 Lauter-Viray

Finally, we shall consider d_1, d_2 to be *arbitrary* discriminants. In such a case, we lose the fact that the $\mathcal{O}_{d_i}$ are Dedekind domains, integrally closed, locally DVRs, etc. Remarkably, one can still state something of the same flavor as the results of Gross-Zagier.

Theorem 2.4.1 ([LV15b, Thm 1.1])**.** *Let d_1, d_2 be any two distinct discriminants. Then, there exists a function F that takes non-negative integers of the form $m = \frac{d_1 d_2 - x^2}{4}$ to (possibly fractional) prime powers. This function satisfies*

$$J(d_1, d_2)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x^2 \leq d_1 d_2 \\ x^2 \equiv d_1 d_2 \bmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right).$$

Moreover, $F(m) = 1$ unless either

- *$m = 0$ and $d_2 = d_1 \ell^{2k}$ for some prime ℓ, or*
- *The Hilbert symbol $(d_1, -m)_\ell = -1$ at a unique finite prime ℓ and this prime divides m.*

In both of these cases $F(m)$ is a (possibly fractional) power of ℓ.

We remark again that the fractional powers of primes occur exactly when $3 \mid d_1, d_2$. Lauter-Viray give an additional result, generalizing the work of Dorman.

Theorem 2.4.2 ([LV15b, Thm 1.5])**.** *Let d_1, d_2 be any two distinct discriminants, and let m be a non-negative integer of the form $\frac{d_1 d_2 - x^2}{4}$ and ℓ a fixed prime that is coprime to $f_1 = \mathrm{cond}(d_1)$.*

If $m > 0$ and either $\ell > 2$ or 2 does not ramify in both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, then $v_\ell(F(m))$ can be expressed as a weighted sum of the number of certain invertible integral ideals in $\mathcal{O}_{d_1}$ of norm m/ℓ^r for $r > 0$.

Moreover, if m is coprime to the conductor of d_1, then $v_\ell(F(m))$ is an integer and the weights are easily computed and constant; more precisely we have

$$v_\ell(F(m)) = \begin{cases} \frac{1}{e}\rho(m)\sum_{r\geq 1}\mathfrak{A}(m/\ell^r) & \text{if } \ell \nmid \operatorname{cond}(d_2), \\ \rho(m)\mathfrak{A}(m/\ell^{1+v(\operatorname{cond}(d_2))}) & \text{if } \ell \mid \operatorname{cond}(d_2), \end{cases} \tag{2.4.1}$$

where e is the ramification degree of ℓ in $\mathbb{Q}(\sqrt{d_1})$ and

$$\rho(m) = \begin{cases} 0 & \text{if } (d_1,-m)_p = -1 \text{ for } p|d_1, p\nmid f_1\ell, \\ 2^{\#\{p|(m,d_1):p\nmid f_2 \text{ or } p=\ell\}} & \text{otherwise,} \end{cases}$$

$$\mathfrak{A}(N) = \#\left\{ \begin{array}{ll} & \mathrm{N}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible}, \\ \mathfrak{b}\subseteq\mathcal{O}_{d_1}: & p\nmid\mathfrak{b} \text{ for all } p|(N,f_2), p\nmid \ell d_1 \\ & \mathfrak{p}^3\nmid\mathfrak{b} \text{ for all } \mathfrak{p}|p|(N,f_2,d_1), p\neq\ell \end{array} \right\}. \tag{2.4.2}$$

If $m=0$, then either $v_\ell(F(0))=0$ or $d_2 = d_1\ell^{2k}$ and

$$v_\ell(F(0)) = \frac{2}{w_1}\cdot \#\operatorname{Pic}(\mathcal{O}_{d_1}).$$

Finally, Lauter-Viray conjectures a formula for the powers of the primes dividing the J function in the case of the discriminants having coprime conductors.

Conjecture 2.4.3 ([LV15b, Conj 1.7])**.** *Let d_1 and d_2 be two distinct discriminants with relatively prime conductors. Write f for the product of the two conductors and for any prime p, let $d_{(p)} \in \{d_1, d_2\}$ be such that $p\nmid \operatorname{cond}(d_{(p)})$. Then, for any prime ℓ*

$$v_\ell(J(d_1,d_2)^{\frac{8}{w_1w_2}}) = H + \sum_{\substack{x^2<d_1d_2 \\ x^2\equiv d_1d_2 \bmod 4}} \epsilon_\ell(x) \prod_{p|m_x, p\neq\ell} \begin{cases} 1+v_p(m) & \left(\frac{d_{(p)}}{p}\right)=1, p\nmid f, \\ 2 & \left(\frac{d_{(p)}}{p}\right)=1, p|f, \text{ or} \\ & p|d_{(p)}, (d_{(p)},-m)_p = 1, p\nmid f \\ 1 & \left(\frac{d_{(p)}}{p}\right)=-1, p\nmid f, v_p(m) \text{ even or} \\ & p|d_{(p)}, (d_{(p)},-m)_p = 1, p|f, v_p(m)=2 \\ 0 & \text{otherwise,} \end{cases}$$

where $H = 0$ *unless* $d_2 = d_1\ell^{2k}$ *for some* $k > 0$*, in which case* $H = \frac{2}{w_1} \cdot \#\operatorname{Pic}(\mathcal{O}_{d_1})$*, and* $m_x := \frac{d_1 d_2 - x^2}{4}$.

$$\epsilon_\ell(x) = \begin{cases} v_\ell(m_x) & \text{if } \ell \nmid f, \ell | d_\ell \\ \frac{1}{2}(v_\ell(m_x) + 1), & \text{if } \ell \nmid f d_{(p)}, v_\ell(m) \text{ odd}, \\ 0 & \text{if } \ell \nmid d_{(p)}, v_\ell(m) \text{ even}, \\ 1 & \text{otherwise.} \end{cases}$$

Thus, we see the utility in considering a counting problem of particular invertible ideals of each norm. It is for this reason that we will shift our attention to the task of counting ideals in imaginary quadratic orders.

Chapter 3

RESULTS

As we now see that the question of factoring $J(d_1, d_2)$ is directly related to the counting of ideals, we focus our attention on the following question:

Question 3.0.1. Without the additional constraint of m being coprime to the conductor of d_1, can we give an alternate formulation of $\mathfrak{A}(N)$ so that Thm 2.4.2 still holds?

Though we do not give a solution to this problem, we make progress by counting a superset of the ideals considered in the expression of $\mathfrak{A}(N)$ in Thm 2.4.2 and discuss further steps to be taken to find the proper collection of ideals to yield the desired equality. Namely, our results consist of determining the number of integral ideals of fixed norm in an order of arbitrary discriminant, as well as the number of invertible integral ideals of fixed norm.

This problem sounds deceptively simple, especially considering the ease with which one can answer the same question when the order is maximal. We shall see that it requires quite a bit of delicacy to answer most questions when working in non-maximal orders. The main difficulty comes from the fact that we lose the factorization of ideals into a product of primes. This added complication becomes clear even in the statements of the number of ideals in each case.

The proofs of the results follow in §3.3.

3.1 Ideal Counting

Proposition 3.1.1. *Take $K = \mathbb{Q}(\sqrt{d})$ to be imaginary quadratic. Let p be a rational prime and $m \geq 0$ a non-negative integer. Then, the number of ideals of norm p^m in $\mathcal{O}_K$ is sum-*

marized by the following equality:

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K : \mathrm{N}(\mathfrak{a}) = p^m\} = \begin{cases} m+1, & \text{if } p \text{ splits,} \\ 1, & \text{if } p \text{ is inert and } 2 \mid m, \text{ or if } p \text{ is ramified,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Break into cases depending on the splitting behavior of the prime p: one has either $p = \mathfrak{p}$ is inert and is of norm p^2; $p = \mathfrak{p}^2$ and $\mathfrak{p}$ has norm p; or $p = \mathfrak{p}_1\mathfrak{p}_2$, each of which has norm p. All ideals have a unique factorization as a product of primes; so, starting in split case, we have the ideals of norm p^m will be exactly those of the form $\mathfrak{p}_1^r\mathfrak{p}_2^{m-r}$ for $r \in \{0, \ldots, m\}$, giving $m+1$ such ideals. In the inert case, the only possibility is $\mathfrak{p}^{m/2}$, requiring m to be even. In the ramified case, the only ideal is $\mathfrak{p}^m$. □

In contrast to the Dedekind case, in an arbitrary imaginary quadratic order $\mathcal{O}$ we lose the factorization into prime ideals. We do still have primary decomposition, but importantly, the localizations at prime ideals are no longer DVRs. This makes it difficult to compute the norm of the localization of our ideal.

Our first result follows:

Theorem 3.1.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field of discriminant $D < 0$ with maximal order $\mathcal{O}_K = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$, and let $\mathcal{O} = \mathbb{Z}[f\frac{D+\sqrt{D}}{2}]$ be the order of conductor f in K. Choose a rational prime p that divides the conductor f and a non-negative integer m. Let $w := v_p(f)$ and let $\epsilon = 0$ or 1 if m is odd or even, respectively. Then, if $v_p(d/4) \geq m$ then there are $\frac{p^{\lfloor \frac{m}{2} \rfloor + 1} - 1}{p-1}$ ideals of norm p^m in $\mathcal{O}$; otherwise, if $v_p(d/4) < m$ and $p \neq 2$, the number of ideals of norm p^m in $\mathcal{O}$ is summarized as follows:*

$$\#\{\mathfrak{a} \subseteq \mathcal{O} : [\mathcal{O} : \mathfrak{a}] = p^m\} = \begin{cases} \frac{p^{w+1}-1}{p-1} & \text{if } p \text{ ramifies in } \mathcal{O}_K, \\ \frac{p^{w+\epsilon}-1}{p-1} & \text{if } p \text{ is inert in } \mathcal{O}_K \\ \frac{p^{w+\epsilon}-1}{p-1} + p^w(m+1-2w-\epsilon) & \text{if } p \text{ splits in } \mathcal{O}_K. \end{cases}$$

Finally, the number of ideals of norm 2^m, assuming $v_p(d/4) < m$, is given by the following equality:

$$\#\{\mathfrak{a} \subseteq \mathcal{O} : [\mathcal{O} : \mathfrak{a}] = 2^m\} = \begin{cases} 2^{w+1} - 1 & \text{if } D \equiv 0 \bmod 8, \\ 2^{w+\epsilon} - 1 & \text{if } D \equiv 4 \bmod 8, \\ 2^{w-1+\epsilon} - 1 & \text{if } 2 \text{ is inert in } \mathcal{O}_K, w \neq 1 \\ 2^{1+\epsilon} - 1 & \text{if } 2 \text{ is inert in } \mathcal{O}_K, w = 1 \\ 2^{w+\epsilon} - 1 + 2^w(m + 1 - 2w - \epsilon) & \text{if } 2 \text{ is split in } \mathcal{O}_K \end{cases}$$

Since we're interested in invertible ideals with a certain property, we see which of the ideals found in the previous theorem are actually invertible. This will require a case-by-case analysis to determine a closed form, which gives the following result.

Corollary 3.1.3. *Using the notation of Thm 3.1.2, when $v_p(d/4) > m$, the number of invertible ideals of norm p^m in $\mathcal{O}_d = \mathbb{Z}[f\frac{D+\sqrt{D}}{2}]$ is $p^{m/2}$ if m is even and 0 if m is odd; otherwise, assuming $v_p(d/4) \leq m$, the number of ideals of norm p^m is summarized by the following equality:*

$$\#\{\mathfrak{a} \subseteq \mathcal{O} : [\mathcal{O} : \mathfrak{a}] = p^m\} = \begin{cases} p^w & \text{if } p \text{ ramifies in } \mathcal{O}_K \\ p^w + p^{w-1} & \text{if } p \text{ is inert in } \mathcal{O}_K, \ m \text{ even}, \\ (p^w - p^{w-1})(m + 1 - 2w) & \text{if } p \text{ splits in } \mathcal{O}_K \end{cases}$$

We now see how the problem is a bit more complicated than the Dedekind case, simply from the statement of the results. In particular, we remark on the fact that in the maximal case, the number of ideals of norm p^m is independent of p, which is no longer true in the non-maximal case. For some reason, the larger the prime, the more ideals lie over it.

We begin with a couple of requisites.

3.2 Preliminary Results

Proposition 3.2.1. *Let $\mathcal{O} = \mathbb{Z}[\tau] = \mathbb{Z}[\frac{d+\sqrt{d}}{2}] = \mathbb{Z}[x]/(x^2 - dx + \frac{d^2-d}{4}) = \mathbb{Z}[x]/(g(x))$. Let p be a rational prime. Denote the irreducible factors of $g(x) \bmod p$ by $\overline{g_i}(x)$. Then, the primes of $\mathcal{O}$ containing p are exactly $\mathfrak{p}_i = p\mathcal{O} + (g_i(\tau))$, where g_i is a lift of $\overline{g_i}$.*

Proof. Let $\mathfrak{p} = (p) + I$ is a prime ideal in question over (p) for some ideal I. Then we have the following isomorphism:

$$\mathcal{O}/\mathfrak{p} = \frac{\mathbb{Z}[x]/(g(x))}{(p) + I} \simeq \frac{\mathbb{Z}/p[x]/(\prod_i \overline{g_i}(x))}{\bar{I}},$$

where $\bar{I}$ is the corresponding ideal under the reduction map. In order to be an integral domain, $\bar{I}$ must contain $(\bar{g}_i)$ for some i. This implies, $\mathfrak{p} \supseteq (p, g_i)$, which is maximal; hence, $\mathfrak{p} = (p, g_i(\tau))$. □

Lemma 3.2.2. *For any prime $\mathfrak{p} \subseteq \mathcal{O} = \mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right]$, letting $\tau := (d + \sqrt{d})/2$, we have $\mathcal{O}_\mathfrak{p} \supseteq \mathbb{Z}_{(p)}[\tau]$ with equality when $\mathfrak{p}$ is not split in $\mathcal{O}$. In particular, in the non-split case, $a + b\tau \in \mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$ is invertible in $\mathcal{O}_\mathfrak{p}$ exactly when $p \nmid \mathrm{N}(a + b\tau)$.*

Proof. Since $\mathfrak{p}$ lies over (p), we know $\mathfrak{p} \cap \mathbb{Z} = (p)$. Hence, every integer coprime to p is invertible in $\mathcal{O}_\mathfrak{p}$, showing $\mathbb{Z}_{(p)} \subseteq \mathcal{O}_\mathfrak{p}$, giving the desired containment.

Now assume that p is not split. In $\mathcal{O}_\mathfrak{p}$ all elements are of the form α/β where $\alpha \in \mathcal{O}, \beta \in \mathcal{O} \setminus \mathfrak{p}$. Since in $\mathcal{O}$,

$$\beta\bar{\beta} = \mathrm{N}(\beta) = \mathrm{N}(\prod_\mathfrak{q} \beta\mathcal{O}_\mathfrak{q} \cap \mathcal{O}) = \prod_\mathfrak{q} [\mathcal{O} : \beta\mathcal{O}_\mathfrak{q} \cap \mathcal{O}] \in \mathbb{Z},$$

each $[\mathcal{O} : \beta\mathcal{O}_\mathfrak{q} \cap \mathcal{O}]$ is a power of the rational prime q over which $\mathfrak{q}$ lies, and $\mathfrak{p}$ is the *unique* prime lying over p, we know that $p \nmid \beta\bar{\beta}$. Hence, $\bar{\beta}$ is invertible in $\mathcal{O}_\mathfrak{p}$. This allows us to rewrite $\alpha/\beta = \alpha\bar{\beta}/\mathrm{N}(\beta) \in \mathbb{Z}_{(p)}[\tau]$, showing the reverse containment. □

Remark 3.2.3. The primes that split in $\mathcal{O}$ are exactly those that split in $\mathcal{O}_K$ and are prime to the conductor.

For the remainder of this section, let $\mathcal{O} = \mathbb{Z}[\frac{d+\sqrt{d}}{2}] = \mathbb{Z}[\tau]$ so that $\tau^2 - d\tau + \frac{d^2-d}{4} = 0$, take p to be a rational prime **dividing** $f = \text{cond}(d)$, and define $w := v_p(f)$.

Since we will be counting ideals of a fixed norm, we find necessary and sufficient conditions for the generators of a $\mathfrak{p}$-primary ideal to have norm p^m.

Lemma 3.2.4. *Let $g(x) = x^2 - dx + \frac{d^2-d}{4}$ so that $\mathcal{O} = \mathbb{Z}[\tau] = \mathbb{Z}[x]/g(x)$ is the quadratic imaginary order of discriminant d. Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal over some rational prime p dividing the conductor $\text{cond}(d)$. If $\mathfrak{a} \subseteq \mathcal{O}$ is a $\mathfrak{p}$-primary ideal of norm p^m for some non-negative integer m, then there exists a minimal integer k with $m/2 \leq k \leq m$ and a unique residue class $[A] \in \mathbb{Z}/p^{2k-m}$ where $g(A) \equiv 0 \bmod p^{2k-m}$, which give $\mathfrak{a} = (p^k, p^{m-k}(\tau - A))$. Conversely, any such ideal is $\mathfrak{p}$-primary of norm p^m.*

Proof. Assume that $\mathfrak{a} \subseteq \mathcal{O}$ is of norm p^m and let k be such that p^k is the minimal, non-negative integer in $\mathfrak{a}$. If $k = 0$, then $\mathfrak{a} = \mathcal{O}$ implying $m = 0$, and $(1, p^0(\tau - 0))$ certainly takes the desired form. So, we may assume $k > 0$ throughout. We write $\mathfrak{a} = (p^k) + (\alpha_i)_i$ where $\alpha_i \in \mathcal{O}$ are the remaining generators of $\mathfrak{a}$. Now, we manipulate $\mathcal{O}/\mathfrak{a}$ as follows:

$$\mathcal{O}/\mathfrak{a} = [\mathbb{Z}[x]/(g(x))]\,/(p^k, \alpha_i) = \mathbb{Z}/p^k[x]/(g(x), \alpha_i)$$

where by abuse of notation g and the α_i are now considered as polynomials in $\mathbb{Z}/p^k[x]$. Note that the minimality of p^k implies that the ideal $(g(x), \alpha_i)$ contains no non-zero constants. Now, as g is monic of degree 2, we can assume that the α_i are linear. In fact, we only need one such α_i; to see this, consider an ideal $(p^a x + a_0, p^b x + b_0) \subseteq \mathbb{Z}/p^k[x]$ with $a \leq b$ that contains no non-zero constants. Then, the difference between the second generator and p^{b-a} time the first must be zero. i.e.,

$$(p^b x - b_0) - p^{b-a}(p^a x - a_0) = p^{b-a}a_0 - b_0 \in (p^a x + a_0, p^b x + b_0)$$

is a constant in the ideal; hence, $p^{b-a}a_0 = b_0$ in $\mathbb{Z}/p^k$. However, this implies that the ideal is principal generated by $(p^a x - a_0)$. Moreover, since this principal ideal $(p^a x - a_0)$ contains no non-zero constants, it must be that $a \leq v_p(a_0)$, as multiplication by p^{k-a} would give a non-zero constant.

Thus, in our case, we may write $(g(x), \alpha_i) = (g(x), p^a(x-A))$. Now, again by the fact that we require this ideal to not contain non-zero constants, we must have that $g(A) \equiv 0 \bmod p^{k-a}$; one may see this by the fact that modding by the ideal gives relations $g(x) \equiv 0 \bmod p^k$ and $p^a(x-A) \equiv 0 \bmod p^k$, which together give $g(A) \equiv 0 \bmod p^{k-a}$.

As $[\mathcal{O} : \mathfrak{a}] = p^m$, it must be that $[\mathbb{Z}/p^k[x]/g(x) : (p^a(x-A))] = p^m$. So, we note $m/2 \leq k \leq m$, which we will use extensively throughout the proof beyond this lemma. We may, of course, compute the index $[\mathbb{Z}/p^k[x]/g(x) : (p^a(x-A))]$ directly by noting that in $\mathbb{Z}/p^k[x]/g(x)$, $x(p^a(x-A)) = (d-A)p^a(x-A))$. So, one may compute the size of the ideal $\#|(p^a(x-A))| = p^{k-a}$ by just considering its integer multiples. Hence, the index $[\mathbb{Z}/p^k[x]/g(x) : (p^a(x-A))] = p^{2k}/p^{k-a} = p^{k+a}$, which shows $a = m-k$. This computation shows the converse of the lemma, as well.

Putting this all together, we see that $\mathfrak{a} = (p^k, p^{m-k}(\tau - A))$ for some A such that $g(A) \equiv 0 \bmod p^{2k-m}$. Our final task is to show that such an ideal is unique up to choice of A mod p^{2k-m}. To do this, we begin by noticing that $\mathcal{O}$-linear combinations of the generators are exactly $\mathbb{Z}$-linear combinations.

Remark 3.2.5. This follows from an argument similar to that done in the quotient. Namely, since $k > m-k$ we have

$$\tau p^k = Ap^k + p^{2k-m}[p^{m-k}(\tau - A)]$$

and similarly

$$\begin{aligned}
\tau p^{m-k}(\tau - A) &= p^{m-k}(\tau^2 - A\tau) \\
&= p^{m-k}\left[d\tau + \left(-\frac{d^2-d}{4}\right) - A\tau\right] \\
&= p^{m-k}\left[d\tau + (A^2 - dA + Cp^{2k-m}) - A\tau\right], \text{ for some } C \in \mathbb{Z} \\
&= Cp^k + (d-A)p^{m-k}(\tau - A).
\end{aligned}$$

So, every element of our ideal is a $\mathbb{Z}$-linear combination of our generators.

Say $(p^k, p^{m-k}(\tau - A)) = (p^k, p^{m-k}(\tau - B))$ for some $A, B \in \mathbb{Z}$. Then, there are integers

a_1, a_2 such that

$$p^{m-k}(\tau - A) = a_1 p^k + a_2 p^{m-k}(\tau - B).$$

Considering the coefficients of τ, we see that $1 - a_2 = 0$, i.e., $a_2 = 1$. Reordering the integer portion, we find

$$p^{m-k}(B - A) = a_1 p^k,$$

showing that $A \equiv B \bmod p^{2k-m}$, as desired. □

Lemma 3.2.6. *For a prime p, we let r and s be non-negative integers such that $2r < s$ and u be an integer coprime to p. Then, the number of roots of $x^2 - p^{2r}u \equiv 0 \bmod p^s$ is zero when u is not a quadratic residue modulo p^{s-2r}. Otherwise, when u is a quadratic residue $\bmod p^{s-2r}$, finding the number of roots is equivalent to counting those $\mu \in \mathbb{Z}/p^{s-r}$ for which $\mu^2 \equiv 1 \bmod p^{s-2r}$. The number of such μ is explicitly given by the following:*

$$\#\{\mu \in \mathbb{Z}/p^{s-r} : \mu^2 \equiv 1 \bmod p^{s-2r}\} = \begin{cases} 2p^r & , \text{ when } p \neq 2 \\ 2^r & , \text{ when } p = 2, \text{ and } s - 2r = 1 \\ 2^{r+1} & , \text{ when } p = 2, \text{ and } s - 2r = 2 \\ 2^{r+2} & , \text{ when } p = 2, \text{ and } s - 2r \geq 3. \end{cases}$$

Proof. When $p \neq 2$, the roots of $x^2 - 1 \bmod p^{s-2r}$ are exactly ± 1, as a root is such that $p^{s-2r} \mid (x-1)(x+1)$. In particular, $p \mid (x-1)$ or $(x+1)$, and the other term will be coprime to p.

When $s - 2r \geq 3$ and $p = 2$, the roots of $x^2 - 1 \bmod 2^{s-2r}$ can by found by noticing that one of $(x-1), (x+1)$ is divisible by 2 but not 4, meaning that one of the factors of $x^2 - 1$ is divisible by 2^{s-2r-1}. Hence, $x = \pm 1$ or $2^{s-2r} \pm 1$. In the final two cases, when $s - 2r = 1$, we have the sole root, $x = 1$ and when $s - 2r = 2$, we check we only get two roots, ± 1. This gives $1, 2$, or 4 roots in the respective cases.

Now, elements of $\mathbb{Z}/p^{s-r}$ that map to these roots will be of the form $\bar{x} + yp^{s-2r}$ $1 \leq y \leq p^r$ where $\bar{x}$ is a lift of one of the roots we found mod p^{s-2r}. For each of the $1, 2$ or 4 roots we

find, such lifts are distinct, which agrees with the number claimed in the statement of the lemma. □

Lemma 3.2.7. *For any integers r and s where $r \geq 0$, the ideal $(p^r(\tau - s))\mathcal{O}_\mathfrak{p}$ contains minimal, positive integer $p^{r+v_p(\mathrm{N}(\tau-s))}$.*

Proof. Letting $k = r + v_p(\mathrm{N}(\tau - s))$, we see that $p^r(\tau - s)(\bar{\tau} - s) = p^k u$ for some $(u, p) = 1$. So, we need only show minimality. For convenience, we note that $\mathcal{O}_\mathfrak{p} = \mathbb{Z}_{(p)}[\tau] = \mathbb{Z}_{(p)}[\sqrt{d}/2]$ since $d/2 \in \mathcal{O}_\mathfrak{p}$.

We rewrite $p^r(\tau - s) = p^r(\sqrt{d}/2 + a)$ for some $a \in \mathbb{Z}_{(p)}$. Say $\beta = b_0 + b_1\sqrt{d}/2 \in \mathcal{O}_\mathfrak{p}$ is such that $p^r(\sqrt{d}/2 - a)\beta = p^\ell$ is minimal in ℓ. Since p^ℓ is in $\mathbb{Z}_{(p)}$, the coefficient on $\sqrt{d}/2$ must be zero, i.e., $p^r(b_0 + ab_1) = 0$. Hence,

$$\det \begin{bmatrix} a & 1 \\ b_0 & -b_1 \end{bmatrix} = 0.$$

That is, this matrix has rank 1 over $\mathbb{Q}$. This tells us that the conjugate of β is a $\mathbb{Z}_{(p)}$-multiple of $\sqrt{d}/2 + a = \tau - s$, giving the result. □

Lemma 3.2.8. *Given α, β, and $r \in \mathbb{Z}$ with $r \geq 0$, the ideals $p^r(\tau - \alpha)\mathcal{O}_\mathfrak{p}$ and $p^r(\tau - \beta)\mathcal{O}_\mathfrak{p}$ are equal exactly when $v_p(\mathrm{N}(\tau - \alpha)) = v_p(\mathrm{N}(\tau - \beta))$ and $\alpha \equiv \beta \bmod p^{v_p(\mathrm{N}(\tau-\alpha))}$.*

Proof. Note that the intersections with $\mathcal{O}$ are the $\mathfrak{p}$-primary ideals $(p^{r+v_p(\mathrm{N}(\tau-\alpha))}, p^r(\tau - \alpha))$ and $(p^{r+v_p(\mathrm{N}(\tau-\beta))}, p^r(\tau - \beta))$ from Lemma 3.2.7. The result follows from the uniqueness of the equivalence class of A in Lemma 3.2.4. □

We can now prove Thm 3.1.2 and Corollary 3.1.3.

3.3 Proofs

Proof. We will use the notation $\mathfrak{r}(p^m) := \#\{\mathfrak{a} \subseteq \mathcal{O} : [\mathcal{O} : \mathfrak{a}] = p^m\}$ and $\mathfrak{r}_k(p^m) := \#\{\mathfrak{a} \subseteq \mathcal{O} : [\mathcal{O} : \mathfrak{a}] = p^m, p^k \in \mathfrak{a}, \text{ and } p^{k-1} \notin \mathfrak{a}\}$. We note that in the proof of the Lemma 3.2.4 for an ideal $\mathfrak{a} = (p^k, p^{m-k}(\tau - A))$ the minimal value k must lie in $m/2 \leq k \leq m$. As

a consequence, our task will be to count the roots of $g(x) \equiv 0 \bmod p^{2k-m}$ for each k in $m/2 \leq k \leq m$. Totaling such values will then give us the desired count of ideals, i.e.,

$$\mathfrak{r}(p^m) = \sum_{m/2 \leq k \leq m} \mathfrak{r}_k(p^m).$$

Firstly, notice that with a little cosmetic work,

$$g(x) = x^2 - dx + \frac{d^2 - d}{4} = (x - d/2)^2 - d/4.$$

Now, if $p = 2$, then $4 \mid d$ and both $d/2$ and $d/4$ are integers; otherwise, if $p \neq 2$, then 2 is invertible mod p^{2k-m}, allowing us to consider $g(x + d/2) \bmod p^{2k-m}$. Hence, using the change of variables $x \mapsto x + d/2$, the ideal counting problem reduces to counting roots of $x^2 - d/4 \bmod p^{2k-m}$.

We split into two cases depending on whether or not the constant term is zero. Equivalently, we break into cases based upon $2k - m \leq v_p(d/4)$ or $2k - m > v_p(d/4)$. As we will be counting by ranging over the values of k we rewrite these conditions in terms on k, i.e., $k \leq \frac{v_p(d/4)+m}{2}$ and $k > \frac{v_p(d/4)+m}{2}$. This is because if $k \leq \frac{v_p(d/4)+m}{2}$, then $x^2 - d/4 \equiv x^2 - 0 \bmod p^{2k-m}$.

Letting $\kappa = \frac{v_p(d/4)+m}{2}$ we see,

$$\begin{aligned}\mathfrak{r}(p^m) &= \sum_{m/2 \leq k \leq m} \mathfrak{r}_k(p^m) \\ &= \sum_{m/2 \leq k \leq \kappa} \#\{x \in \mathbb{Z}/p^{2k-m} : x^2 = 0\} + \sum_{\kappa < k \leq m} \#\{x \in \mathbb{Z}/p^{2k-m} : x^2 - d/4 = 0\}.\end{aligned}$$

For the first summand, $k \leq \kappa$, in order for x to be a root, $v_p(x) \geq (2k - m)/2$. Hence, there are $p^{k-\lceil m/2 \rceil}$ possibilities for x.

Notice that if $v_p(d/4) \geq m$ then k will always be less than κ. So, the total number of ideals would be given by

$$\mathfrak{r}(p^m) = \sum_{m/2 \leq k \leq m} p^{k-\lceil \frac{m}{2} \rceil} = \frac{p^{\lfloor \frac{m}{2} \rfloor + 1} - 1}{p - 1}$$

In the event that $m > v_p(d/4)$ then there is the possibility $k > \kappa$, and the problem becomes a bit more involved.

So, we now assume $k > \kappa$. Notice that if p ramifies in the maximal order $\mathcal{O}_K = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$, $g(x + d/2) = x^2 - (f^2/4)D$ does not have a root mod p^{2k-m}. To see this, if $p \neq 2$ or $D \equiv 0 \mod 8$, then, in terms of integers, $v_p(x^2)$ is even but $v_p(d/4)$ would be odd. Moreover, when $D \equiv 4 \mod 8$ one considers $x^2 - f^2(D/4)$ where $D/4 \equiv 3 \mod 4$, which is a quadratic residue only modulo 2; however, $2k - m = 1$ when $k = \frac{1+m}{2} \leq \frac{v_p(d/4)+m}{2} = \kappa$, outside our current case, showing there are no roots when p ramifies in $\mathcal{O}_K$ and $k > \kappa$. So, if p ramifies, the total collection of such ideals can be computed by summing those $k \leq \kappa$, i.e.,

$$\mathfrak{r}(p^m) = \sum_{m/2 \leq k \leq \kappa} p^{k-\lceil \frac{m}{2} \rceil} = \frac{p^{w+\lfloor \frac{v_p(D/4)+m}{2} \rfloor - \lceil \frac{m}{2} \rceil + 1} - 1}{p-1},$$

which matches the proposed solution for each of the cases where p ramifies in $\mathcal{O}_K$.

Outside of the ramified case, we use Lemma 3.2.6. Firstly, rewrite

$$x^2 - d/4 = x^2 - p^{2w}(f^2/p^{2w})D/4 \mod p^{2k-m}.$$

When $p = 2$, using the notation of Lemma 3.2.6, we may take $r = w - 1$ and $u = f^2D/p^{2w}$, and when $p \neq 2$ we take $r = w$ and $u = f^2D/(4p^{2w})$. The number of ideals is then given by the result of the lemma.

Thus, we have found the number of ideals for each value of k. We now explicitly sum these k depending on whether p is inert or split in $\mathcal{O}_K$ to match the explicit forms given in the theorem, as we have already considered p being ramified.

Consider the case of $p \neq 2$. When p is inert, D is not a quadratic residue mod p^{2k-m}; so, we get the same sum as in the ramified case:

$$\mathfrak{r}(p^m) = \sum_{m/2 \leq k \leq \frac{v_p(d/4)+m}{2}} p^{k-\lceil \frac{m}{2} \rceil} = \frac{p^{w+\lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{2} \rceil + 1} - 1}{p-1},$$

which we simplify using the fact that $v_p(D/4) = 0$. Notice that $\lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{2} \rceil + 1 = 0, 1$ when m is odd, even, respectively; so, if we define $\epsilon = 0, 1$ when m is odd, even, we see this agrees with the theorem.

If instead p splits in $\mathcal{O}_K$, then Lemma 3.2.6 gives $2p^w$ roots for each values of k between $\kappa < k \leq m$. Again using the ϵ notation, we obtain the following total:

$$\mathfrak{r}(p^m) = \left(\sum_{m/2 \leq k \leq \frac{v_p(d/4)+m}{2}} p^{k-\lceil \frac{m}{2} \rceil} \right) + 2p^w(m - \lfloor \frac{v_p(d/4)+m}{2} \rfloor) = \frac{p^{w+\epsilon}-1}{p-1} + p^w(m+1-2w-\epsilon),$$

completing the case of $p \neq 2$.

Now, turn to the case of $p = 2$. When 2 is inert in $\mathcal{O}_K$, i.e., $D \equiv 5 \bmod 8$, we know that D is a quadratic residue only mod 2 or 4. The only case in which $2k - m = 1$ or 2 and $k > \kappa = w - 1 + \frac{m}{2}$ is when $w = 1$. In such a case, Lemma 3.2.6 tells us that we will have 1 or 2 roots when $2k - m = 1$ or 2, respectively. So, in total, if we let $\delta = 0, 1$ when $w \neq 1$ or $w = 1$, respectively, then the total number of ideals when 2 is inert in $\mathcal{O}_K$ is given by

$$\mathfrak{r}(p^m) = \left(\sum_{m/2 \leq k \leq \kappa} 2^{k-\lceil \frac{m}{2} \rceil} \right) + \delta 2^\epsilon = 2^{w+\lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{2} \rceil} - 1 + \delta 2^\epsilon = 2^{w-1+\epsilon} - 1 + \delta 2^\epsilon.$$

Finally, in much the same way, when 2 splits in $\mathcal{O}_K$, the total number of ideals is given by

$$\left(\sum_{m/2 \leq k \leq \kappa} 2^{k-\lceil \frac{m}{2} \rceil} \right) + 2^{w-1+\epsilon} + 2^{w+1}(m - \lfloor \kappa \rfloor - 1) = 2^{w+\epsilon} - 1 + 2^w(m + 1 - 2w - \epsilon)$$

where the middle term $2^{w-1+\epsilon}$ comes from the fact that $2k - m = 1$ or 2 depends on m being odd or even, respectively. □

Now, we prove the statement of Corollary 3.1.3.

Proof. Say $(p^k, p^{m-k}(\tau - A)) = \gamma \mathcal{O}_\mathfrak{p}$ for some

$$\gamma = c_1 p^k + c_2 p^{m-k}(\tau - A).$$

Being a generator, there is another element $\gamma' \in \mathcal{O}_\mathfrak{p}$ for which $\gamma\gamma' = p^{m-k}(\tau - A)$. By considering the coefficient on τ, we see that $v_p(c_2) = 0$. Hence, multiplying by a unit, we

can assume γ is actually of the form

$$\begin{aligned}\gamma &= c_1 p^k + p^{m-k}(\tau - A) \\ &= p^{m-k}(\tau - (A - c_1 p^{2k-m})) \\ &= p^{m-k}(\tau - \alpha)\end{aligned}$$

for some integer α in the same equivalence class mod p^{2k-m} as A.

Applying Lemma 3.2.7 and Lemma 3.2.8, we need to count those α where $v_p(\mathrm{N}(\tau - \alpha)) = 2k - m$, i.e., α must be a root of $g(x) \bmod p^{2k-m}$ but not a root mod p^{2k-m+1}. We break up into cases similar to the proof of the theorem in an attempt to see which lifts give us *some* non-root mod p^{2k-m+1}; namely, consider the cases of $m < v_p(d/4)$ and $m \geq v_p(d/4)$. Additionally, as we range over values of k, those k where $2k - m < v_p(d/4)$, $2k - m = v_p(d/4)$, and $2k - m > v_p(d/4)$ will be useful to consider as the counting will depend on whether $d/4 \equiv 0 \bmod p^{2k-m}$. Writing these in terms of k, we will consider $k < \frac{v_p(d/4)+m}{2}, k = \frac{v_p(d/4)+m}{2}$, and $k > \frac{v_p(d/4)+m}{2}$.

Define

$$\mathfrak{R}(p^m) := \#\{\mathfrak{a} \subseteq \mathcal{O} : \mathfrak{a} \text{ is locally principal, } [\mathcal{O} : \mathfrak{a}] = p^m\}$$

and

$$\mathfrak{R}_k(p^m) := \#\{\mathfrak{a} \subseteq \mathcal{O} : \mathfrak{a} \text{ is locally principal, } [\mathcal{O} : \mathfrak{a}] = p^m, p^k \in \mathfrak{a}, \text{ and } p^{k-1} \notin \mathfrak{a}\}.$$

Then, letting $\kappa = \frac{v_p(d/4)+m}{2}$,

$$\mathfrak{R}(p^m) = \sum_{m/2 \leq k < \kappa} \mathfrak{R}_k(p^m) + \mathfrak{R}_\kappa(p^m) + \sum_{\kappa < k \leq m} \mathfrak{R}_k(p^m),$$

where $\mathfrak{R}_\kappa(p^m) = 0$ when κ is not an integer.

When $m < v_p(d/4)$ then all values $m/2 \leq k \leq m$ will be such that the polynomial $g(x + d/2) = x^2 - d/4 \equiv x^2 \bmod p^{2k-m+1}$. If m is odd, then we see that any value x for which $x^2 \equiv 0 \bmod p^{2k-m}$ will also satisfy $x^2 \equiv 0 \bmod p^{2k-m+1}$. So, there are no such principally generated ideals when m is odd. However, when m is even, we may take those $x = p^{k-\frac{m}{2}}u$ where $u \in \{1, \ldots, p^{k-\frac{m}{2}} - 1\}$ is coprime to p.

For each k the number of such values is $\phi(p^{k-\frac{m}{2}})$, and so the total number of principal ideals will be

$$\mathfrak{R}(p^m) = \sum_{k=m/2}^{m} \phi(p^{2k-m}) = p^{m/2},$$

agreeing with the corollary. Additionally, when $m = 0$, there is a unique such ideal, and we will assume $m > 0$ from here onwards.

Assume now $m \geq v_p(d/4)$. We will work through the cases of p ramifying, remaining inert, and splitting in $\mathcal{O}_K$, and within each case, treat $p = 2$ separately.

We first work through the case of p being ramified in $\mathcal{O}_K$. For clarity, we work through the case of $p \neq 2$. For $k < \kappa$ the argument is the same as above, giving us 0 ideals when m is odd and

$$\sum_{k=m/2}^{w+\frac{m}{2}} \phi(p^{k-m/2}) = p^w$$

when m is even. Now, when $k = \kappa$, then we have to be a bit careful. Noting that this equality can only occur when m is odd, we ask which x are such that $x^2 \equiv 0 \bmod p^{2\kappa-m}$ but $x^2 - d/4 \not\equiv 0 \bmod p^{2\kappa-m+1}$. Certainly the lift of any such value remains zero, as m is odd, and since $d/4 \not\equiv 0 \bmod p^{2\kappa-m+1}$ any of the p^w roots of the former lifts to a non-root. Hence, regardless of the parity of m, we have $\mathfrak{R}(p^m) = p^w$ when $p \neq 2$.

The proof when $p = 2$ ramifies in $\mathcal{O}_K$ breaks into $D \equiv 4 \bmod 8$ and $D \equiv 0 \bmod 8$; however, $D \equiv 0 \bmod 8$ is exactly the same as $p \neq 2$ since $v_2(d/4) = 2w + 1$. So, we proceed assuming $D \equiv 4 \bmod 8$. For $k < \kappa$ we get no ideals when m is odd, and we get

$$\sum_{k=m/2}^{w+\frac{m}{2}-1} \phi(2^{k-\frac{m}{2}}) = 2^{w-1}$$

ideals when m is even. Now, when $k = \kappa$, which occurs only when m is even, the values $x = 2^{w+1}r$ for any $r \in \{0, \ldots, 2^{w-1}\}$ will be exactly the desired values. This gives 2^{w-1} additional values, totaling 2^w locally principal ideals when m is not odd. When $d/4 \not\equiv 0 \bmod 2^{2k-m}$, then $x^2 - d/4 \equiv x^2 - 2^{2w}(f^2/2^{2w})(D/4) \equiv 0 \bmod 2^{2k-m}$ has a root only when $2k-m = 2w+1$ since $D/4 \equiv 3 \bmod 4$, which is not a quadratic residue. Hence, when m is odd, we can take

$k = w + \frac{m+1}{2}$ so that $2k - m = 2w + 1$, and by lemma 3.2.6, with $s = 2w + 1, r = w$ we see that there are 2^w such roots. In any case, when p is ramified, $\mathfrak{R}(p^m) = p^w$.

Now, assume that p is inert in $\mathcal{O}_K$. Again, for convenience, we will prove $p \neq 2$ separate from $p = 2$. Assuming $p \neq 2$, we find that the number of ideals gained over those k where $2k - m < v_p(d/4)$ when m is odd is zero, and when m is even we find

$$\sum_{k=m/2}^{w+\frac{m}{2}-1} \phi(p^{k-m/2}) = p^{w-1}$$

ideals. When $k = w + m/2$, none of the lifts are roots, and so, all p^w roots give us an ideal. Noting there are no roots when $k > w + m/2$, we have $\mathfrak{R}(p^m) = p^w + p^{w-1}$ when $p \neq 2$ and m is even.

Now assume $p = 2$. Then, in much the same way, the number of ideals gained over those $k < \frac{v_p(d/4)+m}{2}$ when m is odd is zero, and when m is even we find

$$\sum_{k=m/2}^{w+\frac{m}{2}-2} \phi(2^{k-m/2}) = \begin{cases} 0 & \text{if } w = 1 \\ 2^{w-2} & \text{if } w > 1. \end{cases}$$

When $k = w - 1 + m/2$, which occurs only when m is even, we gain those $x = 2^w r$ for any r, giving an additional 2^{w-2} roots. So, regardless of the value of w, this gives $\mathfrak{R}(2^m) = 2^{w-1}$ roots when m is even and 0 otherwise.

As we are in the inert case, $D \equiv 5 \bmod 8$; hence, for $k > w-1+m/2$, $x^2 - d/4 \bmod 2^{2k-m}$ has a root only when $k = 2w - 2 + 1$ or $2w - 2 + 2$ depending on whether m is odd or even, respectively. In the odd case, all the roots are still roots after being lifted, and in the even case, none of the lifts are roots. Hence, only in the even case, we gain additional ideals. Applying lemma 3.2.6, we find an additional 2^w roots. Hence, whether or not $p = 2$, we have $\mathfrak{R}(p^m) = p^w + p^{w-1}$ when m is even and p is inert in $\mathcal{O}_K$.

Finally, we work through the case of p being split in $\mathcal{O}_K$. Starting with $p \neq 2$ and m even, we gain p^{w-1} ideals from those $k < \kappa$. When $k = \kappa$, we count those x such that $x^2 \equiv 0 \bmod p^{2w}$ but $x^2 - d/4 \not\equiv 0 \bmod p^{2w+1}$. The total number of roots mod p^{2w} is p^w, but

we have to take away those roots that are reductions of roots. Using, lemma 3.2.6, we know there are $2p^w$ roots mod p^{2w+1}, giving p^{w-1} reductions; hence, we gain $p^w - 2p^{w-1}$ ideals. Finally, for each $k > \kappa$, we gain $2p^w - 2p^{w-1}$ by a similar counting argument. Adding all of these together, we find

$$\begin{aligned}\mathfrak{R}(p^m) &= \sum_{m/2 \le k \le \kappa} \mathfrak{R}_k(p^m) + \mathfrak{R}_\kappa(p^m) + \sum_{\kappa < k \le m} \mathfrak{R}_k(p^m) \\ &= p^w + (p^w - 2p^{w-1}) + (2p^w - 2p^{w-1})(m - (w + m/2 + 1) + 1) \\ &= (p^w - p^{w-1})(m + 1 - 2w)\end{aligned}$$

When m is odd, the only roots come from those $k > \kappa$. Namely, we find $2(p^w - p^{w-1})(m - (\frac{m+1}{2} + w) + 1) = (p^w - p^{w-1})(m + 1 - 2w)$ invertible ideals, as well.

Our final case will be $p = 2$ splitting in $\mathcal{O}_K$, i.e., $D \equiv 1 \bmod 8$. When m is even, in exactly the same way as the inert case, we find $2^{w-1} = 2^w - 2^{w-1}$ ideals when $k \le \kappa = w - 1 + m/2$. If k is such that $2k - m = 1$ or 2, then lemma 3.2.6 shows us that all lifts are still roots. So, we sum over $k \ge w + 1 + m/2$, each giving $2(2^w - 2^{w-1})$ ideals to get

$$2(2^w - 2^{w-1})(m - (w + 1 + m/2) + 1) = (2^w - 2^{w-1})(m - 2w)$$

additional ideals, showing the total agrees with the $p \neq 2$ case. The case of m is odd is similar, giving

$$\mathfrak{R}(2^m) = 2(2^w - 2^{w-1})(m - (w + 1 + (m+1)/2) + 1) = (2^w - 2^{w-1})(m + 1 - 2w).$$

□

3.4 Conclusion and Future Work

Now that we have determined the number of invertible ideals in an arbitrary imaginary quadratic order, the next step would be to determine an expression for $\mathfrak{A}(N)$ from equality (2.4.2) that would satisfy the relation (2.4.1) in Lauter-Viray's theorem without their additional assumptions.

In the proof of the equality, Lauter-Viray make extensive use of the assumption that m need be coprime to the conductor of d_1. The constraints given in (2.4.2) are a necessary set of conditions for the equality to hold in general, but when m is not coprime to d_1 they appear to be too lax. As such, to determine a set of sufficient conditions, we wish to perform explicit calculations to determine the genus class of the invertible ideals, which we have yet to properly do in the case where the ideal non-trivially intersects the conductor.

Additionally, we remark (as was pointed out to us by Bianca Viray) that the number of ideals of fixed norm seems to have a relationship to the number of ideals in the maximal order. Namely, the number seems to differ by a factor of the size of one of $\mathbb{G}_a(\mathbb{Z}/p^r), \mathbb{G}_m(\mathbb{Z}/p^r)$, or $\mathbb{P}^1(\mathbb{Z}/p^r)$ for an appropriate choice of r. Whether this is merely coincidence, or if there exist some underlying maps of interest is still unclear, but it is a question that seems worth keeping in the back of our minds.

BIBLIOGRAPHY

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[Dor88] David R. Dorman. Special values of the elliptic modular function and factorization formulae. *J. Reine Angew. Math.*, 383:207–220, 1988.

[GZ85] Benedict H. Gross and Don B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[LV15a] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of igusa class polynomials. *American Journal of Mathematics*, 137(2):497–533, 2015.

[LV15b] Kristin Lauter and Bianca Viray. On singular moduli for arbitrary discriminants. *Int. Math. Res. Not. IMRN*, (19):9206–9250, 2015.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[Ste12] William Stein. Algebraic number theory, a computational approach. *preprint*, November 14, 2012.

[Voi18] John Voight. Quaternion algebras. *Version v0*, 9, 2018.