UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

ARITHMETIC IN QUATERNION ALGEBRAS AND QUATERNIONIC MODULAR FORMS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

JORDAN ISAAC WIEBE
Norman, Oklahoma
2019

ARITHMETIC IN QUATERNION ALGEBRAS AND QUATERNIONIC MODULAR FORMS

A DISSERTATION APPROVED FOR THE
DEPARTMENT OF MATHEMATICS

BY

Dr. Kimball Martin, Chair

Dr. Qi Cheng

Dr. Ameya Pitale

Dr. Alan Roche

Dr. Ralf Schmidt

For my wife

Abigail Joy Wiebe

Acknowledgments

I have had an incredible journey in mathematics, thanks to many wonderful people who have helped along the way. I would like to begin by thanking my advisory committee for their time and guidance. Ralf Schmidt guided me for much of my beginnings in mathematics, and it was his course in elliptic curves which piqued my interest in number theory — to him I am very grateful. I am also indebted to my advisor, Kimball Martin, from whom I have learned a great many things. Your patience and guidance through the vast world of number theory has been enormously appreciated. Thank you.

The wonderful community in the math department at OU is also deserving of thanks. The courses and seminars and friendship of my fellow GAs is very much appreciated. Thanks to Gordon Brown for being a wonderful colleague and friend. Many fond memories of us highlight the last seven years. The camaraderie and friendship we share has brought me great joy. Thank you.

A huge amount of thanks is due to the Life.Church communities that we have been a part of over the years, from my first year in Oklahoma at the Midwest City location, to Moore, to NW OKC, to our current Yukon cohort. So many people have prayed and guided us as Abby and I have made this incredible journey together, and to all I am eternally grateful. Many thanks to the staff teams at NW OKC and Yukon, who represented the very best of what fully devoted followers of Christ can be.

To Nate and Kala Jacobs, your constant support and friendship means the world, and despite being physically separated I know that we will always be friends. Your kindness and care truly changed my heart. Thank you.

To Don and Nancy Rice, your constant support and consistent prayer made a world of difference for Abby and me. I would not have accomplished this without you. Thank you so much for adopting me into the family. We will always be close, no matter how far apart we are.

To my parents, Don and Allison, and Cindy, thank you. Your wisdom and guidance and strength made me who I am today. Being a part of your family has meant so much to me. Thank you so much for your constant prayers and care.

To Crystal Zaragoza and Josh and Erica Czufin: you all have been the best friends anyone could ask for. Your support, encouragement, and care have made an indescribable difference. Your time and love have changed me forever, and helped me in so many ways on this journey. Thank you for sharing your family and your hearts with me. Just know...thank you. You're the best.

Finally, to my wife Abby, I am eternally indebted. We've grown so much together, and while the journey through graduate school has been sometimes painful, your constant friendship and love and sheer determination have carried me. I would not be wise without your wisdom. I would not be strong without your strength. I know that wherever we go from here, you will be by my side, kicking butt. I love you, and thank you.

Contents

Abstract

This dissertation has two parts. In the first part, we revisit the correspondence between spaces of modular forms and orders in quaternion algebras addressed first by Eichler and completed by Hijikata, Pizer, and Shemanske, using an arbitrary definite quaternion algebra with arbitrary level. We present explicit bases for orders of arbitrary level $N > 1$ in definite rational quaternion algebras. These orders have applications to computations of spaces of elliptic and quaternionic modular forms.

In the second part, we investigate the behavior of quaternionic modular forms. In particular, we calculate quaternionic modular forms of weight 2, and illustrate a use of the orders constructed in the first part. We use these forms to explore the behavior of spaces of quaternionic cusp forms of weight 2 and level N, and make a number of conjectures concerning the behavior of zeros of such quaternionic modular forms. In particular, we use dimension formulas and the action of involutions on our space to predict certain zeros of quaternionic modular forms (which we call trivial zeros), and conjecture that the ratio of the number of zerofree forms of level $\leq N$ to the number of forms with no trivial zeros tends to 1 as N goes to infinity. Finally, we analyze asymptotics of the growth rate of trivial zeros, and provide a histogram of the distribution of nontrivial zeros with respect to the degrees of factors associated to them. We also provide data on a variety of quaternionic modular forms in Appendix A.

Introduction

Let $S_k(N)$ denote the space of elliptic cusp forms of weight k on $\Gamma_0(N)$ with trivial character. Denote by B a definite quaternion algebra over $\mathbb{Q}$, and denote by $\mathcal{O}$ an order in B. In 1940, Hecke conjectured that for a prime p, a basis for $S_2(p)$ could be obtained via the theta series associated to a set of one-sided $\mathcal{O}$-ideal class representatives, where $\mathcal{O}$ is a maximal order in the definite quaternion algebra ramified at p and ∞. In 1956, Eichler [4] proved that there was indeed a basis for $S_2(p)$ taken from a more general collection of theta series associated to $\mathcal{O}$ obtained via certain arithmetically defined matrices associated to the order called Brandt matrices. Hijikata, Pizer and Shemanske [7] generalized Eichler's work to arbitrary level in 1989 by working with orders of level $N = p^r M$ in a definite quaternion algebra ramified at p and ∞. More recently, Martin [12] treated the basis problem using orders in algebras with more general discriminant.

Much of the literature on the subject of these orders involves fixing a definite quaternion algebra B ramified at p and ∞, and explicit bases for the orders involved are limited. For example, Pizer [18] presents bases for maximal orders of the definite algebras ramified at a single finite prime. Albert [1] and Ibukiyama [8] also present bases for maximal orders of definite quaternion algebras. Pacetti and Rodriguez-Villegas [15] also provide bases for orders of level p^2. More generally, orders of level N can be used to construct modular forms of level N. Note that there are other approaches to this, for instance modular symbols or an approach of Dembélé [3] which only requires the use of maximal orders. Pacetti and Sirolli [16] also compute Bass orders over a totally real field, as well as ideal class representatives (note that the orders considered here are also Bass orders). One can algorithmically construct more general orders, but explicit bases were not known. Moreover, explicit construction of non-maximal orders is also useful for computations of quaternionic modular forms via Brandt matrices, which we address in Chapter 3. Specifically, computations of these quaternionic modular forms will allow us to address questions raised in [11].

We begin by presenting the background on quaternion algebras and modular forms, including a variety of pertinent number-theoretic objects used in Chapters 2 and 3. This serves as the foundation for the subsequent chapters.

We continue in Chapter 2, presenting explicit bases for orders of arbitrary level $N > 1$ in definite rational quaternion algebras. These results have been checked for $\Delta \leq 1000$ and $N \leq 10{,}000$ in Sage via discriminant computations. Furthermore, we can construct these orders in arbitrary definite rational quaternion algebras for admissible levels N, where an admissible level N is one in which the discriminant of the quaternion algebra divides N (note that this is a necessary condition to obtain an order of level N in B). Our construction works in every case except where $v_2(N) = 2$ and the discriminant of B is even. In this case, we can construct an order with level $N = 4N'$ (with N' odd) in a quaternion algebra with even discriminant if $\prod_{p|RM_1, p\neq 2} p \equiv 1 \bmod 4$, where we have written our level as $N = RM$ for relatively prime R and M, where the discriminant of B divides R, and split M into M_1 and M_2, where the factors of M_1 are the primes in N which have odd exponent, and the factors of M_2 are the primes in N which have even exponent.

We conclude in Chapter 3 with a construction and analysis of weight 2 quaternionic modular forms over $\mathbb{Q}$. Quaternionic modular forms in certain Atkin-Lehner eigenspaces have trivial zeros. We conjecture that almost all quaternionic modular forms with no trivial zeros in fact have no zeros. To motivate our conjectures we begin by describing a construction algorithm for computing quaternionic modular forms of weight 2 and level $N \in Sq^*$, where Sq^* is the set of positive squarefree integers which are a product of an odd number of primes. We then proceed to describe data collected counting both the number of trivial zeros (for prime level) and the number of zerofree quaternionic modular forms of level $L \in Sq^* \leq N$, and connect this data to the number of forms with no trivial zeros which we can predict via dimensions of Atkin-Lehner eigenspaces calculated using results from [14]. This determines how many quaternionic modular forms have no trivial zeros. We conjecture that, for N a squarefree product of an odd number of primes, the ratio of the number of zerofree quaternionic modular forms of level $L \leq N$ to the number of forms with no trivial zeros of level $L \leq N$ tends to 1 as $N \to \infty$, and provide data for prime N up to 7500, and for nonprime level $L \in Sq^*$ up to 3000. We also compare the number of nontrivial zeros which occur for prime level to the number which occur for squarefree levels which are a product of an odd number of primes. We then expand our considerations to quaternionic modular forms of arbitrary levels which are a product of an odd number of primes, constructed via the algorithm presented in Chapter 2. Lastly, we analyze asymptotics of the growth rate of trivial zeros, and provide a histogram of the distribution of nontrivial zeros with respect to the degrees of factors associated to them.

Appendix A contains tables of cuspidal quaternionic modular forms of level $N \in Sq^* \leq 100$ for reference, along with their associated global root numbers w_f.

Chapter 1

Background

In this chapter we will gather relevant information on quadratic fields and quaternion algebras. We will also provide some useful results on the splitting of quaternion algebras, and we discuss quadratic residues and quadratic reciprocity, which are relevant to the calculations of the splitting criteria. We also present a brief description of the theory of orders in quaternion algebras and their ideal theory. For more background, Vignéras [19] is the classical source, but for a more recent source one may find Voight [20] of help.

We also describe modular forms and related results in some detail, with specific emphasis on connections with quaternion algebras via the construction of Brandt matrices. We also briefly visit the theory of old- and newforms of Atkin and Lehner [2].

1.1. Quaternions

1.1. Quadratic fields

Consider the quadratic field $K = \mathbb{Q}(\sqrt{a})$ and its ring of integers $\mathfrak{o}_K$. It is well-known that $\mathfrak{o}_K = \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right]$ and $\operatorname{disc}(K) = a$ if $a \equiv 1 \bmod 4$, and $\mathfrak{o}_K = \mathbb{Z}\left[\sqrt{a}\right]$ and $\operatorname{disc}(K) = 4a$ otherwise. We wish to use the quadratic field K to control the behavior of our order O, since we have $K \subset B = \left(\frac{a,b}{\mathbb{Q}}\right)$. Now consider the local field $K_p = \mathbb{Q}_p(\sqrt{a})$ and its behavior at p:

Lemma 1. *Let $K = \mathbb{Q}_p(\sqrt{a})$. If $p|a$ then K_p is ramified, but if $\left(\frac{a}{p}\right) = -1$ then K_p is unramified, and if $\left(\frac{a}{p}\right) = 1$ then K_p is split. For $p = 2$, if a is even then K_2 is ramified, and if $a \equiv \pm 1 \bmod 8$ then K_2 is split, but if $a \equiv \pm 3$ mod 8 then K_2 is unramified.*

1.1. Quaternion algebras

Now consider a simple algebra A. By Wedderburn's theorem, we know that any simple algebra with dimension < 4 is a field; hence, the first interesting simple algebras have dimension 4, and these are our subject of study. Recall that a quaternion algebra over $\mathbb{Q}$ is a four-dimensional central simple $\mathbb{Q}$-algebra. Note that any quaternion algebra over $\mathbb{Q}$ is either a noncommutative division algebra or the split matrix algebra $M_2(\mathbb{Q})$; we write $(a, b)_{\mathbb{Q}} = 1$ if the algebra is split, and $(a, b)_{\mathbb{Q}} = -1$ if the algebra is ramified. We can construct quaternion algebras using the Hilbert symbol $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ to denote the quaternion algebra with $\mathbb{Q}$-basis $1, i, j, k$ and multiplication satisfying

$$i^2 = a, j^2 = b, \text{ and } ij = -ji = k.$$

Indeed, any quaternion algebra can be constructed in this way for some $a, b \in \mathbb{Z}$.

The splitting behavior of our quaternion algebra is described as follows:

Lemma 2. *Suppose that p is an odd prime and $a, b \in \mathbb{Z}$ are nonzero and squarefree. Then $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is division (i.e., ramified) if and only if*

1. *$p \nmid a$, $p \mid b$, and a is a nonsquare mod p; or*

2. *$p \mid a$, $p \nmid b$, and b is a nonsquare mod p; or*

3. *$p \mid a$, $p \mid b$, and $-a^{-1}b$ is a nonsquare mod p.*

Alternatively, if $p = 2$, then we have

$$(a,2)_{\mathbb{Q}_2} = \left(\frac{a}{2}\right) = \begin{cases} +1 & \text{if } a \equiv 1, 7 \text{ mod } 8 \\ -1 & \text{if } a \equiv 3, 5 \text{ mod } 8 \end{cases}.$$

Furthermore, if both a and b are odd primes we have $(a,b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

This lemma follows from known calculations of Hilbert symbols over $\mathbb{Q}_p$.

There are 3 possibilities for the behavior of K_p, and 2 for B_p, so we have the means of describing the behavior of our quaternion algebra B with $K = \mathbb{Q}(\sqrt{a}) \subset B$ in six cases. However, in order for our quadratic field K to be contained in B, B must not ramify if K is split; in other words, we can omit one of the cases:

K_p split, B_p split	K_p ramified, B_p split	K_p unramified, B_p split
$\times$	K_p ramified, B_p ramified	K_p unramified, B_p ramified

We also note here that the Hilbert symbols defined above have many helpful properties, including $(a,b)_F \cdot (a,c)_F = (a,bc)_F$ if F is p-adic. This will prove useful for calculating the behavior of B_2, the localization of our algebra B at 2.

We will be using a number of useful facts about quadratic residue symbols, which are listed here. A quadratic residue symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases} .$$

Now if $a = p_1 \cdot \cdots \cdot p_k$, then the Kronecker symbol $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdot \cdots \cdot \left(\frac{p_k}{p}\right)$. We also have the law of quadratic reciprocity:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This allows us to relate conditions on q to conditions on p, and vice versa. Observe that the value of $(-1)^{\frac{p-1}{2}\frac{p-1}{2}}$ depends on p and q mod 4; in particular, if either p or $q \equiv 1 \bmod 4$, then $(-1)^{\frac{p-1}{2}\frac{p-1}{2}} = 1$. If both p and q are $\equiv 3 \bmod 4$, then $(-1)^{\frac{p-1}{2}\frac{p-1}{2}} = -1$. We will also note here some useful particular values of residue symbols:

1. $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 4$, and
2. $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \bmod 8$.

1.1. Orders

Recall the definition of a order in a number field K as a complete $\mathbb{Z}$-lattice in K which is also a subring of K. We expand this definition to orders in quaternion algebras as follows:

Definition 3. *Let B be an F-algebra, for F the fraction field of a Dedekind domain R. An R-lattice Λ is a finitely generated module over R, and Λ is called complete if it contains a basis for the algebra B (as a vector space). An order $\mathcal{O}$ of B is a complete R-lattice which is also a subring in A.*

Consider, for example, the quaternion algebra $B = \left(\frac{a,b}{F}\right)$ and $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$. Then $\mathcal{O}$ is an order, which naturally extends our idea of orders to quaternions. Consider the matrix representation of the quaternion algebra

$$B = \left(\frac{a,b}{\mathbb{Q}}\right) \simeq \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

where $K = \mathbb{Q}(\sqrt{a})$, with the above isomorphism given by

$$i \mapsto \begin{pmatrix} \sqrt{a} & \\ & -\sqrt{a} \end{pmatrix}, j \mapsto \begin{pmatrix} & b \\ 1 & \end{pmatrix}, k \mapsto \begin{pmatrix} & b\sqrt{a} \\ -\sqrt{a} & \end{pmatrix}.$$

We can see the natural extension of our idea of orders from rings of integers using

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathfrak{o}_K \right\},$$

where $\mathfrak{o}_K$ is the ring of integers of K.

Since the collection of all integral elements of a simple algebra does not generally form a ring, we must consider collections of elements that do, i.e. orders. The analog of the ring of integers in this context is a maximal order — an order which is maximal with respect to inclusion. If A is a commutative semisimple algebra, then A has a unique maximal order $\mathcal{O}_{\max}$, but for general quaternion algebras maximal orders are not unique.

The intersection of two maximal orders yields an Eichler order, a class of orders which correspond to

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2) : c \equiv 0 \bmod N \right\}.$$

This congruence subgroup plays an important role in the theory of modular forms, which will be discussed in the next section.

Notice that if A is split — i.e. $A \simeq M_2(F)$ — the presentation of orders differs from when $A = D$ is division. In particular, if D is a local division algebra, then $\mathcal{O} = \{\alpha \in D : v_D(\alpha) \geq 0\}$ is the unique maximal order of D. Here $v_D(\alpha) = v_F(N(\alpha))$ is the valuation on D via the norm map $N(\alpha)$.

We now develop the concept of level to differentiate between orders. Begin with B a quaternion algebra over $\mathbb{Q}$.

Definition 4. *If $\mathcal{O}$ is an order with $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_4$ as a free module,*

$$\mathit{level}(\mathcal{O}) = \mathit{disc}(\mathcal{O}) = (\det(\alpha_i \alpha_j)_{i,j})^2.$$

Moreover, for $\mathit{lev}_p(\mathcal{O})$ the local level of $\mathcal{O}$, we have $\mathit{level}(\mathcal{O}) = \prod_{p<\infty} \mathit{lev}_p(\mathcal{O})$.

This gives us a method of easily computing the level of an order, given a basis. Note that as we define level here, $\mathrm{disc}(B)$ divides $\mathrm{lev}(\mathcal{O})$. In Chapter 2, we will present local orders of level p^n in distinct cases for B split or B division.

1.1. Ideal theory of orders

Orders have a theory of ideals which will come into play in calculations of Brandt matrices and quaternionic modular forms, and we describe important details here.

Definition 5. *Let $\mathcal{O}$ be an R-order in an algebra A. A left (integral) ideal $\mathcal{I}$ in $\mathcal{O}$ is an additive subgroup of $\mathcal{O}$ such that $\mathcal{O}\mathcal{I} \subset \mathcal{I}$. A left fractional ideal $\mathcal{J}$ of $\mathcal{O}$ is a subset of the form $\alpha\mathcal{I}$ where $\alpha \in F^\times$ and $\mathcal{I}$ is an integral ideal. We refer to the set of fractional ideals of $\mathcal{O}$ as Frac$(\mathcal{O})$.*

When we refer to ideals we will henceforth mean left fractional ideals unless specified. For $\mathcal{I}, \mathcal{J} \in \mathrm{Frac}(\mathcal{O})$, we say $\mathcal{I} \equiv \mathcal{J}$ if $\mathcal{J} = \mathcal{I}\alpha$ for some $\alpha \in A^\times$. This is an equivalence relation on $\mathrm{Frac}(\mathcal{O})$, and the set of ideal classes is given by $\mathrm{Cl}(\mathcal{O})$. Moreover, define the class number $h(\mathcal{O}) = \#\mathrm{Cl}(\mathcal{O})$. Note that [18] and [17] provide formulas for the class number of orders of certain types, while a general formula is given in [6].

The representatives of the ideal classes $\{\mathcal{I}_1, \ldots, \mathcal{I}_h\}$ can be used to construct Brandt matrices (cf [18]), which provide a means of computing modular forms. Examples of such construction via Sage and Magma can be found in Section 2.6.

We can use a quaternion order $\mathcal{O}$ of level N to construct a series of Brandt matrices using the ideals of $\mathcal{O}$, which gives us a basis of elliptic modular forms of level N. This construction is introduced by Pizer in [18] and further refined in [7]. We now pivot our background to describe modular forms in view of this connection.

1.2. Modular forms

Modular forms are a fundamental tool in number theory for the study of a variety of objects, including elliptic curves and quadratic forms. We now introduce modular forms and relevant background.

1.2. Classical modular forms

Consider the Nth congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2) : c \equiv 0 \bmod N \right\},$$

which acts by linear fractional transformations on the upper half plane $\mathfrak{H}$.

Definition 6. *Fix $k \geq 0$ and $N \geq 1$. A classical (elliptic) modular form is a function $f : \mathfrak{H} \to \mathbb{C}$ which is holomorphic on $\mathfrak{H}$ and the cusps, and satisfies the modular transformation law*

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \right) = (cz + d)^k \cdot f(z).$$

The condition at the cusps essentially amounts to a growth condition as f approaches each cusp. The space of modular forms of weight k and level N is denoted by $M_k(N)$.

Since f is periodic (in particular, $f(z+1) = f(z)$), we know that f has a Fourier expansion

$$f(z) = \sum_{n \geq 0} a_n q^n, q = e^{2\pi i z}.$$

We call a_n the nth Fourier coefficient of f.

Definition 7. *The Eisenstein series of weight $k \geq 4$ is*

$$E_k(z) = \frac{1}{2\zeta(k)} \cdot \sum_{(c,d) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(cz + d)^k} \in M_k(N),$$

where $\zeta(k)$ is the Riemann zeta function.

The Eisenstein series is well-understood, but there are other modular forms which require further study.

Definition 8. *A cusp form is a modular form $f \in M_k(N)$ which vanishes at all of the cusps; i.e., the constant term a_0 of the expansion of f at each cusp is zero. Denote by $S_k(N)$ the space of cusp forms of weight k and level N.*

Generally, the space of modular forms $M_k(N)$ is spanned by the Eisenstein series and $S_k(N)$.

Definition 9. *The k-th Hecke operator T_k can be defined as follows:*

- *For primes p,*

$$(T_p f)(z) = \begin{cases} \sum a_{pn} + p^{k-1} a_{n/p} q^n & p \nmid N \\ \sum a_{pn} q^n & p \mid N \end{cases}$$

- *For prime powers,*

$$T_{p^m} f = \begin{cases} T_p T_{p^{m-1}} - p^{k-1} T_{p^{m-2}} & p \nmid N \\ (T_p)^m & p \mid N \end{cases}$$

- *For general k, we require that $T_{mn} = T_m T_n$ when $gcd(m, n) = 1$.*

The Hecke operators above were developed by Atkin and Lehner to show that $M_k(N)$ has a basis of forms satisfying $a_m(f)a_n(f) = a_{mn}(f)$ for all relatively prime $m, n \in \mathbb{N}$. In particular, there is a basis of eigenvectors — called eigenforms — for all T_k with $\gcd(N, k) = 1$ which can be normalized to give the multiplicative conditions above.

1.2. Oldforms and newforms

We outline briefly here the theory of oldforms and newforms of Atkin and Lehner. Begin by observing that if $M \mid N$, we have $\Gamma_0(N) \subset \Gamma_0(M)$, which gives us $S_k(M) \subset S_k(N)$. Furthermore, for divisors $d \mid N/M$ we can map a form f of level M to one of level N using $f(z) \mapsto f(dz)$.

Definition 10. *A cusp form $\varphi \in S_k(N)$ is called an oldform if it can be obtained from a lower level $M \mid N$ via the map $f(z) \mapsto f(dz)$ for some $d \mid N/M$. The newspace $S_k^{new}(N)$ is the orthogonal complement of the space generated by the oldforms. Lastly, we call $f \in S_k^{new}(N)$ a newform if f is a normalized eigenform for the Hecke operators T_n with n relatively prime to N.*

Observe that newforms have multiplicative Fourier coefficients, which are in fact determined by the values of $a_p(f)$ for p prime. Atkin and Lehner showed in [2] that there is a basis of newforms for $S_k^{\text{new}}(N)$, giving us a basis of forms with multiplicative Fourier coefficients. Furthermore, since distinct newforms are linearly independent, the number of newforms is $\dim(S_k^{\text{new}}(N))$. Understanding the space of newforms of level N is fundamental to understanding spaces of modular forms. We will use a decomposition of the spaces of newforms into a plus space $S_k^{\text{new},+}(N)$ and a minus space $S_k^{\text{new},-}(N)$, according the the sign of the global root number w_f of the modular form, in Chapter 3.

Chapter 2

Constructing non-Eichler orders in quaternion algebras

2.1. Introduction

In this chapter, we present an explicit basis for orders of arbitrary admissible level $N > 1$ in definite rational quaternion algebras, where an admissible level N is one in which the discriminant of the quaternion algebra divides N (this is a necessary condition to obtain an order of level N in B). These results have been checked for $\Delta \leq 1000$ and $N \leq 10,000$ in Sage. Furthermore, we present these orders in arbitrary definite rational quaternion algebras in every case except the case where $v_2(N) = 2$ and the discriminant of B is even. In this case, we can construct an order with level $N = 4N'$ (with N' odd) in a quaternion algebra with even discriminant if $\prod_{p|RM_1, p\neq 2} p \equiv 1 \bmod 4$, where we have written our level as $N = RM$ for relatively prime R and M, where the discriminant of B divides R, and split M into M_1 and M_2, where the factors of M_1 are the primes in N which have odd exponent, and the factors of M_2 are the primes in N which have even exponent.

Our result uses a careful choice of the presentation of our definite quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ via $a, b \in \mathbb{Z}$, allowing for computation of a space of modular forms of weight $2k$ and level N (see [6], [12]). Note that working with more general ramification sets in our algebra allows us to remove oldforms from the space of modular forms constructed using our order, compared to an order of the same level in an algebra with a smaller ramification set (see [15]). Moreover, our result can be used to compute quaternionic modular forms via Brandt matrices. Note that our result is for definite rational quaternion algebras, but a nearly identical argument (with different conditions mod 8) will work for indefinite quaternion algebras. The general description of our basis is somewhat complex, so for simplicity we state an explicit basis for the special case with odd level p^r:

Theorem 11. *Let B be a definite quaternion algebra with discriminant $\Delta_B = p$ odd and $N = p^r$ our level. Take*

$$a, b = \begin{cases} -q, -p & \text{if } r \text{ odd, } p \equiv 1 \bmod 4\text{, with } q \text{ nonsquare } \bmod p \text{ and } 3 \bmod 4 \\ -p, -q & \text{if } r \text{ odd, } p \equiv 3 \bmod 4\text{, with } q \text{ square } \bmod p \text{ and } 1 \bmod 8 \\ -qp, -p & \text{if } r \text{ even, } p \equiv 1 \bmod 4\text{, with } q \text{ nonsquare } \bmod p \text{ and } 3 \bmod 4 \\ -p, -q & \text{if } r \text{ even, } p \equiv 3 \bmod 4\text{, with } q \text{ square } \bmod p \text{ and } 1 \bmod 8 \end{cases}$$

Then we can represent B as $\left(\frac{a,b}{\mathbb{Q}}\right)$. Furthermore, put $f = p^r$ if r is odd, and $f = p^{r-1-v_p(b)}$ if r is even, and select x with $x^2 \equiv -p \bmod q$, and let z be given by the Euclidean algorithm for finding $y(-q) + z(2x) = 1$, u be given by using the Euclidean algorithm to write $v(q) + w(2x) = 1$, and setting $0 \le u < 2q$ such that $u \equiv vq + 2w \bmod 2q$, and z' is given by choosing $0 \le z' < 2q$ with $z' \equiv 4z \bmod 2q$.

Then the order

$$\mathcal{O} = \begin{cases} \mathbb{Z}\left\langle \frac{q+i+2zk}{2q}, \frac{2i+z'k}{2q}, \frac{f(j+k)}{2}, fk \right\rangle & \text{if } p \equiv 1 \bmod 4 \\ \mathbb{Z}\left\langle 1, \frac{1+i}{2}, \frac{f(j+uk)}{2q}, fk \right\rangle & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

has level $N = p^r$.

The above theorem splits into two cases, one where r is odd and the other where r is even. In the second case, p is ramified in K, making the construction more complicated, as well as the structure of the space of associated theta series (see [7], [12]). Our result is stated in full generality in Theorem 13.

In Section 2.2, we will embed our quaternion algebra B in $M_2(K)$, for K a quadratic field, and examine its level locally in cases based on the splitting/ramification of K_p and B_p. In Section 2.3, we will construct a global order $\mathcal{O}$ of B using the local results from the previous section, with level $N \cdot q$ for a suitable auxiliary prime q. We will construct this order in cases, based on the behavior of 2 in the quadratic field K and in the algebra B. We will also calculate the basis for this order. In Section 2.4, using a technique of Voight [21] we will lower the level of our order constructed in the previous section from $N \cdot q$ to N, and calculate the new basis for this order. In Section 2.5, we will present our general result, as well as a few special cases, including an order of level p^r for the algebra ramified at a single prime p. Finally, in Section 2.6 we will present examples of using our construction of orders to compute spaces of modular forms.

2.2. Local orders

Recall that we can embed our quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ in $M_2(K)$, where $K = \mathbb{Q}(\sqrt{a})$ as

$$B = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K = \mathbb{Q}(\sqrt{a}) \right\}.$$

The form of an order varies depending on whether K is split, ramified, or unramified, and also varies based on whether B is split or ramified. Therefore, we will examine orders in each case separately. In particular, we may consider the local algebra

$$B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K_p = K \otimes \mathbb{Q}_p \right\}$$

at each prime, and examine orders locally, split into the cases above for the behavior of K_p and B_p. Consider the following orders, referred to as residually inert orders by Voight in [20]: for finite primes that ramify in B, a residually inert order $\mathcal{O}_p$ of B_p has a quadratic extension K_p of $\mathbb{Q}_p$ and a positive integer $\nu(p)$ (odd if K_p is unramified) so that $\mathcal{O}_p = \mathfrak{o}_{K_p} + \mathfrak{P}_{B_p}^{\nu-1}$, where $\mathfrak{P}_{B_p}$ is the unique maximal ideal of the unique maximal order $\mathcal{O}_{B_p}$ of B_p. Note that these orders were called special orders by Hijikata, Pizer, and Shemanske in [6]. For our purposes, we will construct $\mathcal{O}$ to be a residually inert order for primes which ramify in B and in K (using K as our quadratic field), and to be Eichler (residually split) for primes which split in B.

For the remainder of this section, fix $a, b \in \mathbb{Z}$ squarefree and coprime.

B_p is split

Assume that B_p is split. Then the standard Eichler order $\mathcal{O}_{B_p}(n)$ of level $n = p^k$ has the form

$$\mathcal{O}_B(n) = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^k\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix},$$

and all Eichler orders of level n are conjugate to $\mathcal{O}_B(n)$.

K_p is split

If K_p is split, we have $K_p = \mathbb{Q}_p \oplus \mathbb{Q}_p$ and $\mathfrak{o}_{K_p} = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Consider the order

$$\mathcal{O}_p = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in f\mathfrak{o}_{K_p} \right\}$$

$$= \left\{ \begin{pmatrix} (x,y) & bf(z,w) \\ f(w,z) & (y,x) \end{pmatrix} : x,y,z,w \in \mathbb{Z}_p \right\}.$$

We now conjugate and simplify:

$$\begin{pmatrix} f & \\ & 1 \end{pmatrix} \begin{pmatrix} (x,y) & bf(z,w) \\ f(w,z) & (y,x) \end{pmatrix} \begin{pmatrix} \frac{1}{f} & \\ & 1 \end{pmatrix} = \begin{pmatrix} (x,y) & bf^2(z,w) \\ (w,z) & (y,x) \end{pmatrix}.$$

So we can identify these matrices with pairs of matrices $\left(\begin{pmatrix} x & bf^2z \\ w & y \end{pmatrix}, \begin{pmatrix} y & bf^2w \\ z & x \end{pmatrix} \right)$, and we have

$$\mathcal{O}_p \simeq \left\{ \begin{pmatrix} x & bf^2z \\ w & y \end{pmatrix} : x,y,z,w \in \mathbb{Z}_p \right\}.$$

This is an Eichler order of level $p^{2v_p(f)+v_p(b)}$ in $B_p = M_2(\mathbb{Q}_p)$.

K_p is ramified

Now assume that K_p is ramified. Note that $\mathfrak{o}_{K_p} = \mathbb{Z}_p[\sqrt{a}]$.

If B_p is split, then b must be a norm from $\mathfrak{o}_{K_p}^\times$, so we can write $b = u\bar{u}$ for some $u \in \mathfrak{o}_{K_p}^\times$. Making the substitution $\beta \mapsto \bar{u}^{-1}\beta$ gives us

$$B_p = \left\{ \begin{pmatrix} \alpha & u\beta \\ u^{-1}\bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K_p \right\}.$$

Consider the order

$$\mathcal{O}_p = \left\{ \begin{pmatrix} \alpha & u\beta \\ u^{-1}\bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z}_p + g\mathfrak{o}_{K_p}, \beta \in f(\mathbb{Z}_p + g\mathfrak{o}_{K_p}) \right\}.$$

Now let $\ell = \begin{pmatrix} \sqrt{a} & -\sqrt{a} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & \\ & 1 \end{pmatrix}$, and write $\alpha = x + gy + gz\sqrt{a}$ and $\beta = fp + fgq + fgr\sqrt{a}$. Then the conjugation $\ell \mathcal{O}_p \ell^{-1}$ gives us

$$\ell \begin{pmatrix} \alpha & u\beta \\ u^{-1}\bar{\beta} & \bar{\alpha} \end{pmatrix} \ell^{-1} = \frac{1}{2u^{-1}\sqrt{a}} \cdot \begin{pmatrix} u^{-1}\sqrt{a}[(\alpha + \bar{\alpha}) - (\beta + \bar{\beta})] & u^{-1}a[(\alpha - \bar{\alpha}) + (\beta - \bar{\beta})] \\ u^{-1}[(\alpha - \bar{\alpha}) - (\beta - \bar{\beta})] & u^{-1}\sqrt{a}[(\alpha + \bar{\alpha}) + (\beta + \bar{\beta})] \end{pmatrix}. \quad (2.1)$$

Now if $\alpha \in \mathbb{Z}_p + g\mathfrak{o}_{K_p}$ and $\beta \in f(\mathbb{Z}_p + g\mathfrak{o}_{K_p})$ then $\alpha + \bar{\alpha} = 2x + 2gy$, $\alpha - \bar{\alpha} = 2gz\sqrt{a}$, $\beta + \bar{\beta} = 2fp + 2fgq$, and $\beta - \bar{\beta} = 2fgr\sqrt{a}$. This gives us

$$\ell \mathcal{O}_p \ell^{-1} = \begin{pmatrix} x + gy - fp - fgq & a(gz + fgr) \\ gz - fgr & x + gy + fp + fgq \end{pmatrix}$$

$$= \begin{pmatrix} \mathbb{Z}_p & p^{v_p(a)+v_p(g)}\mathbb{Z}_p \\ p^{v_p(g)}\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} = \begin{pmatrix} \mathbb{Z}_p & p^{v_p(a)+2v_p(g)}\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}.$$

So we have an explicit conjugation of B_p to $M_2(\mathbb{Q}_p)$ that clearly expresses $\mathcal{O}_p$ as an Eichler order of level $p^{v_p(a)+2v_p(g)}$.

If $p = 2$, we must be more careful, since it is possible for 2 to be ramified in K but for $2 \nmid a$. In particular, if $a \equiv 3 \mod 4$ but $2 \nmid a$, then the order described above has $v_2(N) = 2v_2(g) + 2$. Alternatively, if $p = 2$ and $2 \mid a$, then the order described above has $v_2(N) = 2v_2(g) + 8$. Finally, if $p = 2$ and $2 \mid b$, then the order described above has $v_2(N) = 2v_2(g) + 1$.

K_p is unramified

If K_p is unramified, then $\mathfrak{o}_{K_p} = \mathbb{Z}_p[\sqrt{a}]$ unless $p = 2$ and $a \equiv 1 \mod 4$, when we have $\mathfrak{o}_{K_2} = \mathbb{Z}_2[\frac{1+\sqrt{a}}{2}]$. An identical argument as the previous section gives us

$$\mathcal{O}_p = \left\{ \begin{pmatrix} \alpha & u\beta \\ u^{-1}\bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z}_p + g\mathfrak{o}_{K_p}, \beta \in f(\mathbb{Z}_p + g\mathfrak{o}_{K_p}) \right\}.$$

with level $p^{v_p(a)+2v_p(g)}$. In this case, since K_p is unramified, we have $v_p(a) = 0$, so our level is $p^{2v_p(g)}$.

If $p = 2$ and $a \equiv 1 \mod 4$, then we have $\mathfrak{o}_{K_2} = \mathbb{Z}_2\left[\frac{1+\sqrt{a}}{2}\right]$. The basis for our order $\mathcal{O}_2$ is $\mathbb{Z}_2\langle 1, \frac{1+i}{2}, fj, f \cdot \frac{j+k}{2}\rangle$, and a quick calculation shows that $v_2(\text{disc}(\mathcal{O})) = 2v_2(f)$. So our level is $2^{2v_2(f)}$.

B_p is ramified

Assume that B_p is ramified. We again break into cases based on whether K_p is ramified or unramified.

K_p is ramified

Assume K_p is ramified. Here we use the residually inert orders defined previously. We know that $\mathfrak{P}_{B_p} = \varpi_{B_p}\mathcal{O}_{B_p}$, and $\mathfrak{P}_{B_p}^{\nu-1} = \{x \in \mathcal{O}_{B_p} : N(x) \in \mathfrak{p}^{\nu-1}\}$. Now $\mathcal{O}_{B_p}$ is the maximal order of B_p, a local division algebra, which we know is of the form

$$\mathcal{O}_{B_p} = \left\{\begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in \mathfrak{o}_{K_p}\right\}$$

if $p \neq 2$. When $p = 2$,

$$\mathcal{O}_{B_2} = \left\{\begin{pmatrix} \alpha & 2\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_2}, \beta \in \mathfrak{o}_{K_2}\right\}$$

is maximal when K_2 is unramified.

We require that $p \mid b$ if K_p is unramified, and $p \nmid b$ if K_p is ramified to obtain the maximal orders.

Now consider an element $x \in \mathcal{O}_B$:

$$x = \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} \alpha & \\ & \bar{\alpha} \end{pmatrix} + \begin{pmatrix} & b\beta \\ \bar{\beta} & \end{pmatrix}.$$

For x to be an element of our residually inert order $\mathcal{O}_p$, we need $\begin{pmatrix} \alpha & \\ & \bar{\alpha} \end{pmatrix} \in \mathfrak{o}_{K_p}$, so $\alpha \in \mathfrak{o}_{K_p}$. We also need $y = \begin{pmatrix} & b\beta \\ \bar{\beta} & \end{pmatrix} \in \mathfrak{P}_B^{\nu-1}$ to obtain level p^ν. Now $y \in \mathfrak{P}_B^{\nu-1}$ if and only if $N(y) \in p^{\nu-1}\mathbb{Z}_p$, and we know that $N(y) = -b\beta\bar{\beta}$. So we know that we need $\beta\bar{\beta} \in p^{\nu-1-v_p(b)}\mathbb{Z}_p$. Now we write $\beta = u\varpi_{K_p}^m$ for a uniformizer ϖ and a unit u. Now since K_p is ramified, we choose $\varpi_{K_p} = \sqrt{vp}$. So $\beta\bar{\beta} = u\bar{u} \cdot v^m p^m$ when K_p

is ramified. So when K_p is ramified, then if $\beta \in p^{v/2}\mathfrak{o}_{K_p}$ then $N\begin{pmatrix} & b\beta \\ \bar{\beta} & \end{pmatrix} \in p^{v+1}\mathbb{Z}_p$.

So

$$\mathcal{O}_p = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in f\mathfrak{o}_{K_p} \right\}$$

is a residually inert order with level $p^{v_p(f)+1}$, for $f \in \mathfrak{o}_{K_p}$.

K_p is unramified

If K_p is unramified, then a maximal order is given by

$$\left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in \varpi\mathfrak{o}_{K_p} \right\}.$$

Furthermore, it is well-known that all orders containing the unramified quadratic field extension are isomorphic to $\mathfrak{o}_{K_p} \oplus \varpi^n \mathfrak{o}_{K_p} j$, where ϖ is a uniformizer for K_p. We will represent these orders in this setting via an embedded in the matrix algebra as

$$\left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in \varpi^n\mathfrak{o}_{K_p} \right\}.$$

Orders of this form have level p^{2n+1}. So consider the order

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_{K_p}, \beta \in f\mathfrak{o}_{K_p} \right\}.$$

So long as $p \mid b$, this order will have level $p^{2v_p(f)+1}$.

2.3. Global order

Now that we know the form that local orders take, we can examine a global order which has prescribed level locally at each place. Our global order will be a residually inert order locally for primes $p \mid R_2$, and will be Eichler locally for primes $p \nmid R$, for $a, b \in \mathbb{Z}$ such that $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ with $a, b \in \mathbb{Z}$ squarefree. Consider the global order $\mathcal{O} \subset B = \left(\frac{a,b}{\mathbb{Q}}\right)$ given by

$$\mathcal{O} = \mathcal{O}(a, b, f, g) = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z} + g\mathfrak{o}_K, \beta \in f(\mathbb{Z} + g\mathfrak{o}_K) \right\}.$$

The localization of this order is

$$\mathcal{O}_p = \mathcal{O} \otimes_{\mathfrak{o}_{\mathbb{Q}}} \mathfrak{o}_{\mathbb{Q}_p} = \mathcal{O} \otimes \mathbb{Z}_p = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z}_p + g\mathfrak{o}_{K_p}, \beta \in f(\mathbb{Z}_p + g\mathfrak{o}_{K_p}) \right\}.$$

We require $g \in \mathbb{Z}_p^\times$ for the primes where both K_p and B_p are split, so that $\alpha \in \mathbb{Z}_p + \mathfrak{o}_{K_p} = \mathfrak{o}_{K_p}$ and $\beta \in f(\mathbb{Z}_p + \mathfrak{o}_{K_p}) = f\mathfrak{o}_{K_p}$. This yields our order from Section 2.2 with level $p^{v_p(b)+2v_p(f)}$. Our order $\mathcal{O}_p$ also has level if K_p is ramified and B_p is split, since its form locally is the same as in Section 2.2.

So this order has level $p^{1+2v_p(g)}$ if p is odd or if $p = 2$ and $a \equiv 1 \bmod 4$, and level $2^{2v_2(g)+2}$ if $p = 2$ and $a \equiv 3 \bmod 4$, and level $2^{2v_2(g)+3}$ if $p = 2$ and $2 \mid a$. Similarly, $\mathcal{O}_p$ has level if K_p is unramified and B_p is split, giving us level $p^{2v_p(g)}$ if p is odd or $p = 2$ with $a \equiv 1 \bmod 4$, and $2^{2v_2(g)+2}$ when $p = 2$ and $a \equiv 3 \bmod 4$, and $2^{2v_2(g)+3}$ when $p = 2$ and $2 \mid a$.

Locally, our order $\mathcal{O}_p$ has level if both K_p and B_p are ramified, since our order has the form of the order constructed in 2.2, since $f \in \mathfrak{o}_K$ for primes which ramify in both the field and the algebra. Lastly, requiring $g \in \mathbb{Z}_p^\times$ for the primes where K_p

is unramified and B_p is ramified allows $\mathcal{O}_p$ to have level, since $\alpha \in \mathbb{Z}_p + \mathfrak{o}_{K_p} = \mathfrak{o}_{K_p}$ and $\beta \in f(\mathbb{Z}_p + \mathfrak{o}_{K_p}) = f\mathfrak{o}_{K_p}$. This gives $\mathcal{O}_p$ level $p^{2v_p(f)+1}$. We summarize the results from Section 2.2 via the levels we can achieve locally at each prime, based on the behavior of K_p and B_p:

Figure 2.1: Distribution of levels by ramification in K and B

	K_p split	K_p ramified	K_p unramified
B_p split	$p^{2v_p(f)+v_p(b)}$	$p^{2v_p(g)+1}$	$p^{2v_p(g)}$
B_p ramified	$\times$	$p^{v_p(f)+1}$	$p^{2v_p(f)+1}$

It is important to note the parity that can be achieved in each case; in particular, for p where K_p is unramified and B_p is split, we only obtain even exponents for the local level at p. On the other hand, at p where K_p is ramified and B_p is split, or where K_p is unramified and B_p is ramified, we only obtain odd exponents for the local level at p. When both K_p and B_p are split, we obtain either odd or even exponent, with the parity determined by our selection of b in the representation of $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. We have the most freedom when both K_p and B_p are ramified, where we obtain either even or odd exponents, dependent only on the valuation of f.

Selecting a, b

Now consider our quaternion algebra B given via its discriminant Δ, and the level N we desire. Write $N = R \cdot M$ for relatively prime R and M, with primes dividing the discriminant grouped into R and the others into M. Next write $R = R_1 \cdot R_2$ and $M = M_1 \cdot M_2$, where we group the primes with odd powers into R_1 and M_1, and the primes with even powers into R_2 and M_2. Note that R_1, R_2, M_1, and M_2 are all pairwise relatively prime. Moreover, we will use $\prod'_{p|S}$ to indicate that the product should be taken over all primes $p \in S$ except $p = 2$. We wish to select $a, b \in \mathbb{Z}$ so that (i) $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ and (ii) primes dividing the level are sorted appropriately into cases which give the correct level that matches the parity of the exponent.

Proposition 12. *Suppose that B is a definite quaternion algebra over $\mathbb{Q}$ with discriminant Δ, and we wish to choose $a, b \in \mathbb{Z}$ so that $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ and so that each prime $p \mid N$ has the appropriate splitting behavior in K and B so that we can achieve local level $p^{v_p(N)}$. Then we may choose a, b in the following way (noting that $p, q,$ and r represent primes) based on our desired behavior at 2:*

1. *Suppose that $2 \nmid \Delta$ and 2 has an even exponent in N (including the case where $2 \nmid N$). If the product $\prod_{p|RM_1} p \equiv 3 \bmod 4$ then select $a := -\prod_{p|RM_1} p$ and $b := -q$ with q prime satisfying the conditions*

    - $\left(\frac{-q}{p}\right) = -1$ *for all $p \mid R$;*
    - $\left(\frac{-q}{p}\right) = 1$ *for all $p \mid M_1$;*
    - *and $q \equiv 1 \bmod 8$.*

    Alternatively, if the product $\prod_{p|RM_1} p \equiv 1 \bmod 4$ then select $a := -q \cdot \prod_{p|R_2} p$ and $b := -\prod_{p|RM_1} p$ with q prime satisfying the conditions

    - $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod_{r|R_2} r}{p}\right)$ *for all $p \mid R_1$;*
    - $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod_{r|RM_1, r\neq p} r}{p}\right)$ *for all $p \mid R_2$;*
    - $\left(\frac{q}{p}\right) = \left(\frac{-\prod_{r|R_2} r}{p}\right)$ *for all $p \mid M_1$;*
    - *If $\prod_{p|R_2} p \equiv 1 \bmod 4$, then $q \equiv 3 \bmod 4$; and if $\prod_{p|R_2} p \equiv 3 \bmod 4$, then $q \equiv 1 \bmod 4$.*

2. *Suppose that $2 \nmid \Delta$ and 2 has an odd exponent in N. Select $a := -q \cdot \prod_{p|R_2} p$ and $b := -\prod_{p|RM_1} p$ with q prime satisfying the conditions*

- $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod_{r|R_2} r}{p}\right)$ *for all* $p \mid R_1$*;*
- $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod_{r|R_1M_1, r\neq p} r}{p}\right)$ *for all* $p \mid R_2$*;*
- $\left(\frac{q}{p}\right) = \left(\frac{-\prod_{r|R_2} r}{p}\right)$ *for all* $p \mid M_1$*,* $p \neq 2$*;*
- *If* $\prod_{p|R_2} p \equiv 1 \mod 8$*, then* $q \equiv 7 \mod 8$*; if* $\prod_{p|R_2} p \equiv 3 \mod 8$*, then* $q \equiv 5 \mod$ *; if* $\prod_{p|R_2} p \equiv 5 \mod 8$*, then* $q \equiv 3 \mod$ *; and if* $\prod_{p|R_2} p \equiv 7 \mod 8$*, then* $q \equiv 1 \mod 8$.

3. *Suppose that* $2 \mid \Delta$*,* $v_2(N) \neq 2$*. Select* $a := -q \cdot \prod_{p|R_2} p$ *and* $b := -\prod_{p|RM_1} p$ *with q prime satisfying the conditions*

   - $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod'_{r|R_2} r}{p}\right)$ *for all* $p \mid R_1, p \neq 2$*;*
   - $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod'_{r|R_1M_1, r\neq p} r}{p}\right)$ *for all* $p \mid R_2, p \neq 2$*;*
   - $\left(\frac{q}{p}\right) = \left(\frac{-\prod'_{r|R_2} r}{p}\right)$ *for all* $p \mid M_1$*;*
   - *If* $v_2(N) = 1, 3$*, choose q so that* $a \equiv 5 \mod 8$*. If* $v_2(N) > 4$ *is even, then we have the following for* $a' = a/2$ *and* $b' = b/2$*:*

     - *If* $b' \equiv 1 \mod 8$*, then choose q so that* $a' \equiv 3$ *or* $5 \mod 8$.
     - *If* $b' \equiv 3 \mod 8$*, then choose q so that* $a' \equiv 1$ *or* $3 \mod 8$.
     - *If* $b' \equiv 5 \mod 8$*, then choose q so that* $a' \equiv 1$ *or* $7 \mod 8$.
     - *If* $b' \equiv 7 \mod 8$*, then choose q so that* $a' \equiv 5$ *or* $7 \mod 8$.

     If $v_2(N) > 4$ *is odd, then we have the following:*

     - *If* $b' \equiv 1 \mod 4$*, then choose q so that* $a \equiv 3 \mod 8$.
     - *If* $b' \equiv 3 \mod 4$*, then choose q so that* $a \equiv 7 \mod 8$.

4. *Lastly, suppose that* $2 \mid \Delta$ *with* $v_2(N) = 2$*. If* $\prod'_{p|RM_1} p \equiv 1 \mod 4$*, then select* $a := -q \cdot \prod'_{p|R_2} p$ *and* $b := -\prod'_{p|RM_1} p$ *with q prime satisfying the conditions*

- $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod'_{r|R_2} r}{p}\right)$ *for all* $p \mid R_1, p \neq 2$*;*
- $\left(\frac{q}{p}\right) = (-1) \cdot \left(\frac{-\prod'_{r|R_1M_1, r\neq p} r}{p}\right)$ *for all* $p \mid R_2, p \neq 2$*;*
- $\left(\frac{q}{p}\right) = \left(\frac{-\prod'_{r|R_2} r}{p}\right)$ *for all* $p \mid M_1$*;*
- *If* $\prod'_{p|R_2} p \equiv 1 \bmod 4$*, then* $q \equiv 1 \bmod 4$*; and if* $\prod'_{p|R_2} p \equiv 3 \bmod 4$*, then* $q \equiv 3 \bmod 4$.

Alternatively, if $\prod'_{p|RM_1} p \equiv 3 \bmod 4$*, we cannot construct an order with* $v_2(N) = 2$*. This is an inherent condition in the structure of the quaternion algebra* $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ *and the field* $K = \mathbb{Q}(\sqrt{a})$*, not specific to our particular construction.*

Observe that there is a hidden condition that $\left(\frac{b}{q}\right) = 1$, so that we obtain $\operatorname{disc}\left(\frac{a,b}{\mathbb{Q}}\right) = \Delta$, which we will verify. Furthermore, we will observe the behavior of 2, which will determine its behavior in our algebra.

The conditions on q amount to a finite number of modular congruences, which by Dirichlet's theorem on primes in arithmetic progressions we know have a prime solution $q \neq 2$. It is worth observing here that if we choose a and b correctly so that the correct prime factors of a and b are ramified (excluding q), and if we have the correct ramification or splitting of 2, we expect that B_q will be split due to the parity of the set of ramified primes. What we desire in selecting a and b as described above is the following picture of the distribution of primes (ignoring 2 and q):

Figure 2.2: Distribution of level factors

	K_p split	K_p ramified	K_p unramified
B_p split	$p \mid M_2$	$p \mid M_1$	$p \mid M_2$
B_p ramified	$\times$	$p \mid R$	–

In the above diagram, the primes dividing M_2 are distributed between the K_p split case and the K_p unramified case, since the parity of the exponent we can achieve in those cases is the same. In particular, according to Lemma 2 the conditions that $\left(\frac{-q}{p}\right) = -1$ for all $p \mid R$ determine that B_p is ramified for all primes $p \mid R$, and K_p is also ramified for all primes $p \mid R$. The conditions that $\left(\frac{-q}{p}\right) = 1$ for all $p \mid M_1$ determine that B_p is split for all primes $p \mid M_1$, and K_p is ramified for all primes $p \mid M_1$. These conditions are sufficient in all cases except the Case 1b, which is considered by hand. We also need that B_q is split, which is accomplished via quadratic reciprocity:

$$\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p|R} \left(\frac{p}{q}\right) \cdot \prod_{p|M_1} \left(\frac{p}{q}\right)$$

$$= \left(\frac{-1}{q}\right) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

$$= \left(\frac{-1}{q}\right) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)\left(\frac{-q}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)\left(\frac{-q}{p}\right).$$

Notice that we are using quadratic reciprocity assuming that $2 \nmid a$. If $2 \mid a$ then we have

$$\left(\frac{a}{q}\right) = \left(\frac{-2}{q}\right) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

$$= \left(\frac{-2}{q}\right) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)\left(\frac{-q}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)\left(\frac{-q}{p}\right).$$

But the prime q satisfies that $\left(\frac{-q}{p}\right) = -1$ for all factors of the first product and $\left(\frac{-q}{p}\right) = 1$ for all factors in the second product. Now there are an odd number of finite ramified primes in B, so $\prod_{p|R}\left(\frac{q}{p}\right) = -1$. Thus we have

$$\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right) \cdot (-1) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)$$

in the case where $2 \nmid a$, and

$$\left(\frac{a}{q}\right) = \left(\frac{-2}{q}\right) \cdot (-1) \cdot \prod_{p|R} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right) \cdot \prod_{p|M_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{-1}{p}\right)$$

in the case where $2 \mid a$. In order for B_q to be split we need $\left(\frac{a}{q}\right) = 1$, which means that we need

$$1 = \left(\frac{-1}{q}\right) \cdot (-1) \cdot \prod_{p|RM_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \prod_{p|RM_1} \left(\frac{-1}{p}\right)$$

for $2 \nmid a$ and

$$1 = \left(\frac{-2}{q}\right) \cdot (-1) \cdot {\prod_{p|RM_1}}' (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot {\prod_{p|RM_1}}' \left(\frac{-1}{p}\right).$$

for $2 \mid a$. These two conditions interact with the behavior of 2 in K and in B, which means that we must consider their behavior together.

Case 1: $2 \nmid \Delta$ **and** $v_2(N)$ **is even**

Suppose we are in Case 1, where by hypothesis $2 \nmid \Delta$ and 2 has an even exponent in N. Furthermore, suppose that the product $\prod_{p|RM_1} p \equiv 3 \bmod 4$, so that we select $a := -\prod_{p|RM_1} p$ and $b := -q$, with $q \equiv 1 \bmod 8$. This gives us $a \equiv 1 \bmod 4$ and $b \equiv 7 \bmod 8$, so $(a, b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = 1$. Furthermore,

$$\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right) \cdot (-1) \cdot \prod_{p|RM_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \prod_{p|RM_1} \left(\frac{-1}{p}\right)$$

$$= 1 \cdot (-1) \cdot \prod_{p|R} \left(\frac{-1}{p}\right) \cdot \prod_{p|M_1} \left(\frac{-1}{p}\right) = -1 \cdot \prod_{p|RM_1} \left(\frac{-1}{p}\right).$$

Now since $\prod_{p|RM_1} p \equiv 3 \mod 4$, an odd number of the p are $\equiv 3 \mod 4$. Therefore $\prod_{p|RM_1} \left(\frac{-1}{p}\right) = -1$, so $\left(\frac{a}{q}\right) = 1$ as desired. Furthermore, $a \equiv 1 \mod 4$ so 2 is not ramified in K. This gives us

Figure 2.3: Distribution of level factors and q, Case 1a

	K_p split	K_p ramified	K_p unramified
B_p split	$2, q, p \mid M_2$	$p \mid M_1$	$p \mid M_2$
B_p ramified	$\times$	$p \mid R$	$-$

Alternatively, suppose that the product $\prod_{p|RM_1} p \equiv 1 \mod 4$, so that we select $a := -q \cdot \prod_{p|R_2} p$ and $b := -\prod_{p|RM_1} p$. Then $b \equiv 3 \mod 4$, and we choose $q \mod 4$ so that $a \equiv 1 \mod 4$. This gives us $(a, b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = 1$ (so B_2 is split) and K_2 is not ramified. Furthermore, we have

$$\left(\frac{b}{q}\right) = \left(\frac{-\prod_{p|RM_1} p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p|RM_1} \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p|R_1} \left(\frac{p}{q}\right) \cdot \prod_{p|R_2} \left(\frac{p}{q}\right) \cdot \prod_{p|M_1} \left(\frac{p}{q}\right)$$

$$= \left(\frac{-1}{q}\right) \cdot \left[\prod_{p|RM_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right] \cdot \left[\prod_{p|R_1} \left(\frac{-\prod_{p'|R_2} p'}{p}\right) \cdot (-1)\right]$$

$$\cdot \left[\prod_{p|R_2} \left(\frac{-\prod_{p'|R_1M_1} p'}{p}\right) \cdot (-1)\right] \cdot \left[\prod_{p|M_1} \left(\frac{-\prod_{p'|R_2} p'}{p}\right)\right]$$

via quadratic reciprocity and our assumptions on the values of $\left(\frac{q}{p}\right)$. Now since $a \equiv 1 \mod 4$, we have $\prod_{p|RM_1} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$. Moreover, we can factor the -1's out of the products above by observing that there are an odd number of primes dividing R, so we have an odd number of -1's, giving us a -1 factor. We can also expand the products in the residue symbols above to obtain

$$\left(\frac{-1}{q}\right)\cdot(-1)\cdot\left[\prod_{r\mid R_1}\left(\frac{-1}{r}\right)\cdot\prod_{p\mid R_2}\left(\frac{p}{r}\right)\right]$$

$$\cdot\left[\prod_{r\mid R_2}\left(\frac{-1}{r}\right)\cdot\prod_{p\mid R_1M_1}\left(\frac{p}{r}\right)\right]\cdot\left[\prod_{r\mid M_1}\left(\frac{-1}{r}\right)\cdot\prod_{p\mid R_2}\left(\frac{p}{r}\right)\right].$$

The products above can be written as

$$\left(\frac{-1}{q}\right)\cdot(-1)\cdot\left[\prod_{p\mid RM_1}\left(\frac{-1}{p}\right)\right]\cdot\left[\prod_{p\mid R_2,r\mid R_1}\left(\frac{p}{r}\right)\right]\cdot\left[\prod_{p\mid R_1,r\mid R_2}\left(\frac{p}{r}\right)\right]$$

$$\cdot\left[\prod_{p\mid M_1,r\mid R_2}\left(\frac{p}{r}\right)\right]\cdot\left[\prod_{p\mid R_2,r\mid M_1}\left(\frac{p}{r}\right)\right].$$

Notice that we have some quadratic reciprocity here; in particular, we have $\left(\frac{p}{r}\right)\cdot\left(\frac{r}{p}\right)$ for all pairs $p \mid R_1$ and $r \mid R_2$, as well as all pairs $p \mid R_2$ and $r \mid M_1$. Furthermore, since $\prod_{p\mid RM_1} p \equiv 1 \bmod 4$, we have $\prod_{p\mid RM_1}\left(\frac{-1}{p}\right) = 1$. So we obtain

$$\left(\frac{b}{q}\right)=\left(\frac{-1}{q}\right)\cdot(-1)\cdot\left[\prod_{p\mid R_2,r\mid R_1}(-1)^{\frac{p-1}{2}\frac{r-1}{2}}\right]\cdot\left[\prod_{p\mid R_2,r\mid M_1}(-1)^{\frac{p-1}{2}\frac{r-1}{2}}\right].$$

Now we know that $\prod_{p\mid RM_1} p \equiv 1 \bmod 4$, so we have the following cases:

1. $R_1 \equiv 1 \bmod 4$, $R_2 \equiv 1 \bmod 4$, and $M_1 \equiv 1 \bmod 4$;

2. $R_1 \equiv 1 \bmod 4$, $R_2 \equiv 3 \bmod 4$, and $M_1 \equiv 3 \bmod 4$;

3. $R_1 \equiv 3 \bmod 4$, $R_2 \equiv 1 \bmod 4$, and $M_1 \equiv 3 \bmod 4$;

4. $R_1 \equiv 3 \bmod 4$, $R_2 \equiv 3 \bmod 4$, and $M_1 \equiv 1 \bmod 4$.

Furthermore, notice that to obtain $a \equiv 1 \bmod 4$, in the first and third cases above we require $q \equiv 3 \bmod 4$, and in the second and fourth we require $q \equiv 1 \bmod 4$. Now observe that to obtain $(-1)^{\frac{p-1}{2}\frac{r-1}{2}} = -1$, we need both p and r to be $\equiv 3 \bmod 4$. Moreover, to get -1 out of each of the products above, there need to be an odd number of $p \equiv 3 \bmod 4$ *and* $r \equiv 3 \bmod 4$. So we can use the above cases to evaluate $\left(\frac{b}{q}\right)$. In Case 1, $\left(\frac{b}{q}\right) = (-1)(-1)(1)(1) = 1$ as desired; similarly, in Case 2 $\left(\frac{b}{q}\right) = (1)(-1)(1)(-1) = 1$; in Case 3 $\left(\frac{b}{q}\right) = (-1)(-1)(1)(1) = 1$; finally in Case 4 $\left(\frac{b}{q}\right) = (1)(-1)(-1)(1) = 1$.So B_q is split in all cases. Thus we have the following distribution of primes:

Figure 2.4: Distribution of level factors and q, Case 1b

	K_p split	K_p ramified	K_p unramified
B_p split	$2, p \mid M_1, M_2$	q	$p \mid M_2$
B_p ramified	$\times$	$p \mid R_2$	$p \mid R_1$

Case 2: $2 \nmid \Delta$ **and** $v_2(N)$ **is odd**

Suppose now that we are in Case 3, where by hypothesis $2 \nmid \Delta$ and 2 has an odd exponent in N. We select $a := -q \cdot \prod_{p|R_2} p$ and $b := -\prod_{p|RM_1} p$ with $q \bmod 8$ so that $a \equiv 1 \bmod 8$. Then $2 \mid b$. In this scenario we have

$$\left(\frac{b}{q}\right) = \left(\frac{-\prod_{p|RM_1} p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p|RM_1} \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p|R_1} \left(\frac{p}{q}\right) \cdot \prod_{p|R_2} \left(\frac{p}{q}\right) \cdot \prod_{p|M_1} \left(\frac{p}{q}\right)$$

This gives us $\left(\frac{b}{q}\right) = 1$ as in the previous case. Moreover, in both cases, since $2 \mid b$ we have 2 non-ramified in K. Since $2 \mid b$, $(a,b)_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (a,b')_{\mathbb{Q}_2}$ for $b' = b/2$. Then $(a,b')_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b'-1}{2}} = 1$ since $a \equiv 1 \bmod 4$, and $(a,2)_{\mathbb{Q}_2} = 1$ since $a \equiv 1 \bmod 8$. Thus B_2 is split. So we have the following distribution of primes:

Figure 2.5: Distribution of level factors and q, Case 2

	K_p split	K_p ramified	K_p unramified
B_p split	$q, p \mid M_2$	$2, p \mid M_1$	$p \mid M_2$
B_p ramified	$\times$	$p \mid R_2$	R_1

Case 3: $2 \mid \Delta$ **and** $v_2(N) \neq 2$

Suppose that we are in Case 3, where by hypothesis $2 \mid \Delta$. We select $a := -q \cdot \prod_{p \mid R_2} p$ and $b := -\prod_{p \mid RM_1} p$ with q mod 8 so that 2 ramifies in B . Furthermore, we have the requirements mod p so that the $p \mid R$ are ramified in B and the $p \mid M$ are split in B. Now we have

$$\left(\frac{b}{q}\right) = \left(\frac{-\prod_{p \mid RM_1} p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p \mid RM_1} \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p \mid R_1} \left(\frac{p}{q}\right) \cdot \prod_{p \mid R_2} \left(\frac{p}{q}\right) \cdot \prod_{p \mid M_1} \left(\frac{p}{q}\right)$$

As before, we obtain $\left(\frac{b}{q}\right) = 1$. So B_q is split as desired. Since b is even, B ramifies at 2 if and only if a is nonsquare mod 8. In the case $v_2(N) = 1$ or 3, $a \equiv 5 \mod 8$, while in the case $v_2(N) > 4$ and odd, $a \equiv 3 \mod 4$. In all cases it is nonsquare. Furthermore, K_2 is non-ramified when $2 \nmid R_2$, and K_2 is ramified when $2 \mid R_2$.

Case 4: $2 \mid \Delta$ **and** $v_2(N) = 2$

It is important to observe that our order at 2 behaves differently depending on whether a and b are both odd, or $2 \mid a$, or $2 \mid b$. The behavior also depends on a mod 4. In particular, if we desire $v_2(N) = 2$, we must select a and b as follows:

Both a and b must be $\equiv 3 \mod 4$, so that $v_2(\mathrm{disc}(K)) = 2$, and so that $(a, b)_{\mathbb{Q}_2} =$

$(-1)^{\frac{a-1}{2}\frac{b-1}{2}} = -1$. Furthermore, since we can only choose $a = -\prod'_{p|RM_1} p$, $b = -q$ or $a = -q \cdot \prod'_{p|R_2} p$, $b = -\prod'_{p|RM_1} p$, we therefore need $\prod'_{p|RM_1} p \equiv 1 \bmod 4$. This is an inherent condition in the structure of the quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ and the field $K = \mathbb{Q}(\sqrt{a})$, not specific to our particular construction. If this product is $\equiv 1 \bmod 4$, we select $a = -q \cdot \prod'_{p|R_2} p$ and $b = -\prod'_{p|RM_1} p$ with q so that $a \equiv 3 \bmod 4$. Alternatively, if $\prod'_{p|RM_1} p \equiv 3 \bmod 4$, we cannot create an order with $v_2(N) = 2$ if Δ is even.

Special Cases

In some cases, we prefer to restrict our quaternion algebra to simpler scenarios which are common or particularly useful. In particular, our general construction above can be reduced to two helpful cases: (1) where $\Delta = p$, i.e., where B ramifies at a single prime, and (2) where K_p is unramified wherever B_p is ramified.

Case 1: $\Delta = p$

Suppose that $\Delta = p$, so our quaternion algebra only ramifies at one place p, and furthermore suppose that $N = p^k$. Then if $p \neq 2$, we can use Case 1 from above to obtain the following:

If $p \equiv 3 \bmod 4$ then select $a := -p$ and $b := -q$ with q satisfying $\left(\frac{-q}{p}\right) = -1$ and $q \equiv 1 \bmod 8$. If $p \equiv 1 \bmod 4$, then choose $a := -qp$ and $b := -p$ for even exponents of p, and $a := -q$ and $b := -p$ for odd exponents of p. In both scenarios, choose q satisfying $\left(\frac{q}{p}\right) = -1$ and $q \equiv 3 \bmod 4$. In both cases, there is a hidden condition that $\left(\frac{b}{q}\right) = 1$ so that $\Delta = p$ as desired.

In the first case, both 2 and q are split in K, and p is ramified in both the field and the algebra. In the second case, 2 is split in K, q is ramified in K and split in B, and p is ramified in B and either ramified or unramified in K (depending on p mod 4).

Then the order

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_K, \beta \in p^{k-1}\mathfrak{o}_K \right\}$$

has level qp^k. Now the level we have achieved is close to what we desired, but there is an additional q. In a subsequent section we will take care of this and revisit our order.

Case 2: K_p unramified for $p \mid \Delta$

Suppose that $R = R_1$, so all primes which ramify in B have odd exponents in the level N. Then we can select $a = -q$ and $b = -\prod_{p \mid RM_1} p$ with the following conditions on q:

1. $\left(\frac{-q}{p}\right) = -1$ for all $p \mid R$
2. $\left(\frac{-q}{p}\right) = 1$ for all $p \mid M_1$
3. If $2 \mid M_2$, then we require $q \equiv 3 \mod 4$.
4. If $2 \mid M_1$, then we require $q \equiv 7 \mod 8$
5. If $2 \mid R$, then we require $q \equiv 3 \mod 8$.

Conditions 1 and 2 determine that our quaternion algebra is ramified for all $p \mid R$, and split for all $p \mid M_1$, with the exception of $p = 2$. We must verify that 2 behaves as desired in B, and that B splits at q. Now we have

$$\left(\frac{b}{q}\right) = \left(\frac{-1}{q}\right) \cdot \prod_{p \mid RM_1} \left(\frac{-q}{p}\right) \cdot \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

if $2 \nmid b$, and

$$\left(\frac{b}{q}\right) = \left(\frac{-2}{q}\right) \cdot \prod_{p \mid RM_1}{}' \left(\frac{-q}{p}\right) \cdot \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

if $2 \mid b$. In either case, we obtain $\left(\frac{b}{q}\right) = 1$ as desired.

In the case where b is odd, a is odd as well, so $(a,b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$. In the first case, $b \equiv 3 \mod 4$, and $a \equiv 1 \mod 4$, so $(-1)^{\frac{a-1}{2}\frac{b-1}{2}} = 1$ as desired. In the second case, $b \equiv 1 \mod 4$, so $(-1)^{\frac{a-1}{2}\frac{b-1}{2}} = 1$ as desired. Thus 2 is split in B in both cases. Furthermore, $a \equiv 1 \mod 4$ is required in both cases so that 2 is not ramified in K. In the other case, where b is even, we use $(a,b)_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (a,b')_{\mathbb{Q}_2}$ (for $b' = b/2$). Now in both cases, $a \equiv 1 \mod 4$, so this yields $(a,b)_{\mathbb{Q}_2} = 1$ as desired. So 2 is split in B.

Now if $2 \mid R$, then we have

$$\left(\frac{b}{q}\right) = \left(\frac{-2}{q}\right) \cdot {\prod_{p \mid RM_1}}' \left(\frac{p}{q}\right) = \left(\frac{-2}{q}\right) \cdot {\prod_{p \mid RM_1}}' \left(\frac{-q}{p}\right) \cdot \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

$$= \left(\frac{-2}{q}\right) \cdot {\prod_{p \mid RM_1}}' \left(\frac{-1}{p}\right) \cdot \left({\prod_{p \mid RM_1}}' (-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}.$$

If $\prod'_{p \mid RM_1} p \equiv 1 \mod 4$, an even number of the p are $\equiv 3 \mod 4$, so $\prod'_{p \mid RM_1} \left(\frac{-1}{p}\right) = 1 = \prod'_{p \mid RM_1} (-1)^{\frac{p-1}{2}}$, so this reduces to $\left(\frac{b}{q}\right) = \left(\frac{-2}{q}\right) \cdot 1 \cdot 1 = \left(\frac{-2}{q}\right)$. Therefore $q \equiv 3 \mod 8$ is sufficient.

Alternatively, if $\prod'_{p \mid RM_1} p \equiv 3 \mod 4$, an odd number of the p are $\equiv 3 \mod 4$, so $\prod'_{p \mid RM_1} \left(\frac{-1}{p}\right) = -1 = \prod'_{p \mid RM_1} (-1)^{\frac{p-1}{2}}$, so this reduces to $\left(\frac{b}{q}\right) = \left(\frac{-2}{q}\right) \cdot -1 \cdot (-1)^{\frac{q-1}{2}} = (-1) \cdot \left(\frac{-2}{q}\right) \cdot (-1)^{\frac{q-1}{2}}$. Therefore $q \equiv 3 \mod 8$ is sufficient.

In both of the cases above, $2 \mid b$, so we use $(a,b)_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (a,b')_{\mathbb{Q}_2}$ (for $b' = b/2$). Now if $2 \mid R$, we desire B_2 to be ramified. Now in the first case, $\prod'_{p \mid RM_1} p \equiv 1 \mod 4$, so $b' \equiv 3 \mod 4$. So $(a,b)_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (a,b')_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (-1)^{\frac{a-1}{2}}$. Observe that if $q \equiv 3 \mod 8$, then $a \equiv 5 \mod 8$, and either yields $(a,b)_{\mathbb{Q}_2} = -1$ as desired. So 2 ramifies in B. In the second case, $\prod'_{p \mid RM_1} p \equiv 3 \mod 4$, so

$b' \equiv 1 \bmod 4$. So $(a,b)_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (a,b')_{\mathbb{Q}_2} = (a,2)_{\mathbb{Q}_2} \cdot (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = (a,2)_{\mathbb{Q}_2}$. Observe that if $q \equiv 3 \bmod 8$, then $a \equiv 5 \bmod 8$, and either yields $(a,b)_{\mathbb{Q}_2} = -1$ as desired. So 2 ramifies in B. Furthermore, we desire that 2 is unramified in K, so we need $q \equiv 3 \bmod 4$. Therefore, we need $q \equiv 3 \bmod 8$.

Now we have selected a, b so that $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, This gives us

Figure 2.6: Distribution of level factors and q, K_p unramified

	K_p split	K_p ramified	K_p unramified
B_p split	$p \mid M_1, p \mid M_2$	q	$p \mid M_2$
B_p ramified	$\times$	$-$	$p \mid R$

.

Now the order

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z} + g\mathfrak{o}_K, \beta \in f(\mathbb{Z} + g\mathfrak{o}_K) \right\}$$

has level qN for

$$f = \epsilon \cdot {\prod_{p \mid R}}' p^{\frac{v_p(N)-1}{2}} \cdot \prod_{\substack{p \mid M_2, \\ \left(\frac{a}{p}\right)=1}} p^{v_p(N)/2}, \quad g = \prod_{\substack{p \mid M_2, \\ \left(\frac{a}{p}\right)=-1}} p^{v_p(N)/2} \cdot \prod_{p \mid M_1} p^{\frac{v_p(N)-1}{2}},$$

with

$$\epsilon = \begin{cases} 2^{\frac{v_2(N)-3}{2}} & \text{if } v_2(N) \geq 3 \text{ odd} \\ 2^{\frac{v_2(N)}{2}-2} & \text{if } v_2(N) \geq 3 \text{ even} \\ 1 & \text{else.} \end{cases}$$

Now the level we have achieved is close to what we desired, but there is a q factor separating us from our ultimate goal. In a subsequent section we will take care of this and revisit our order.

Basis for $\mathcal{O}$

We know that $\mathfrak{o}_K$ has basis $1, \sqrt{a}$ if $a \equiv 3 \bmod 4$, and $1, \frac{1+\sqrt{a}}{2}$ if $a \equiv 1 \bmod 4$. In the first case, $\mathbb{Z} + g\mathfrak{o}_K$ has basis $1, g\sqrt{a}$ and $f(\mathbb{Z} + g\mathfrak{o}_K)$ has basis $f, fg\sqrt{a}$; in the second case, $\mathbb{Z} + g\mathfrak{o}_K$ has basis $1, g\left(\frac{1+\sqrt{a}}{2}\right)$ and $f(\mathbb{Z} + g\mathfrak{o}_K)$ has basis $f, fg\left(\frac{1+\sqrt{a}}{2}\right)$. So a basis for

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathbb{Z} + g\mathfrak{o}_K, \beta \in f(\mathbb{Z} + g\mathfrak{o}_K) \right\}$$

is

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} g\sqrt{a} & \\ & -g\sqrt{a} \end{pmatrix}, \begin{pmatrix} & fb \\ f & \end{pmatrix}, \text{ and } \begin{pmatrix} & fgb\sqrt{a} \\ -fg\sqrt{a} & \end{pmatrix}$$

in the case where $a \equiv 3 \bmod 4$, and

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} g\left(\frac{1+\sqrt{a}}{2}\right) & \\ & g\left(\frac{1-\sqrt{a}}{2}\right) \end{pmatrix}, \begin{pmatrix} & fb \\ f & \end{pmatrix}, \text{ and } \begin{pmatrix} & fgb\left(\frac{1+\sqrt{a}}{2}\right) \\ fg\left(\frac{1-\sqrt{a}}{2}\right) & \end{pmatrix}$$

in the case where $a \equiv 1 \bmod 4$. Using the fact that

$$\begin{pmatrix} \sqrt{a} & \\ & -\sqrt{a} \end{pmatrix} \cdot \begin{pmatrix} & b \\ 1 & \end{pmatrix} = \begin{pmatrix} & b\sqrt{a} \\ -\sqrt{a} & \end{pmatrix}$$

we can convert these elements from their matrix representations to the standard representations using $1, i, j$, and k. We also observe that since $f \in \mathfrak{o}_K$, then we will obtain powers of the factors of a, encoded by h (a squarefree integer). Notice that locally when p is ramified in K–so that $\mathcal{O}_p$ is a residually inert order–we have basis

$$\mathcal{O}_p = \mathbb{Z}\langle 1, i, p^{v_p(h)} \cdot fj, fk\rangle,$$

with level $p^{2v_p(f)+2}$ when p is ramified in B. This allows us to simplify our description of f to be in $\mathbb{Z}$ rather than in $\mathfrak{o}_K$, by incorporating a third, squarefree integer h to do globally what the p did locally here. So, if $a \equiv 3 \bmod 4$, our basis becomes

$$\mathcal{O} = \mathbb{Z}\langle 1, gi, fhj, fgk\rangle.$$

Alternatively, if $a \equiv 1 \bmod 4$, our basis becomes

$$\mathcal{O} = \mathbb{Z}\left\langle 1, g\left(\frac{1+i}{2}\right), fhj, fg\left(\frac{hj+k}{2}\right)\right\rangle.$$

We can calculate the discriminant of $\mathcal{O}_p$ by observing that if $p \neq 2$ we have $\mathcal{O}_p = \mathbb{Z}_q\langle 1, gi, fgh \cdot j, fk\rangle$ and $\operatorname{disc}(\mathcal{O}_p) = \sqrt{\det(\alpha_i \alpha_j)} = ab \cdot f^2 g^2 h$. If $p = 2$, then $\operatorname{disc}(\mathcal{O}_2) = 4$ if $a \equiv 3 \bmod 4$, and $\operatorname{disc}(\mathcal{O}_2) = 1$ if $a \equiv 1 \bmod 4$. If $2 \mid a$, then $\operatorname{disc}(\mathcal{O}_2) = 8$.

2.4. Lowering the level

In Section 2.3 you may notice that the prime q was used to manipulate our quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ so that we obtained the discriminant Δ as we desired, as well as distributing the primes in R_1, R_2, M_1 and M_2 properly to obtain the desired parity for each exponent. Furthermore, q was often used to manipulate the behavior of 2 in both the quadratic field $K(\sqrt{a})$ and B to obtain the desired behavior of 2 in the level. The selection of q played a central role in achieving these results, yet as you may note from the distributions of primes in each of the cases from the previous section the behavior of K_q and B_q is such that while B_q is always split we can obtain at minimum a level of q for the localization of our order $\mathcal{O}_q$. So to obtain our desired level N, we must lower the level of $\mathcal{O}_q$ from q to 1, which in turn lowers the level of $\mathcal{O}$ from qN to N. Observe that since we have chosen $q \neq 2$, $\mathcal{O}_q$ has basis $1, i, j, k$ in all cases. This allows us to apply a technique from Voight ([21]) to find a maximal order $\mathcal{O}'_q$ containing $\mathcal{O}_q$. From [21], Algorithm 7.10, we will compute a q-maximal order containing $\mathcal{O}$ by adjoining a special element to our order. Now in Cases 1a, 2, and 3, $q \mid b$, and in Cases 1b $q \mid a$. Now since q is odd, we are in Step 2 of the algorithm, where we swap i for j or k so that $\mathrm{ord}_q(a) = 0$. So in Cases 1a, 2, and 3 $q \nmid a$, so we do not need to swap anything. If we are in Cases 1b, we swap i for j locally, which globally swaps gi and fj. In both of these cases, $\mathrm{ord}_q(b) = 1$ and (after swapping if necessary) $\left(\frac{a}{q}\right) = 1$, so next we solve $x^2 \equiv a \bmod q$ for $x \in \mathbb{Z}/q\mathbb{Z}$ and adjoin $q^{-1}(x-i)j$ locally. In order to adjoin this element globally to $\mathcal{O}$ without altering $\mathcal{O}_p$ ($p \neq q$) we adjoin $fgq^{-1}(x-i)j$ globally in Cases 1a, 2, and 3, and we adjoin $fgq^{-1}(x-j)i$ globally in Cases 1b.

Adjoining $fgq^{-1}(x-i)j$ globally to our order does not affect the order at places $p \neq q$, since $q \in \mathbb{Z}_p^\times$ and $x \in \mathbb{Z}_p$, so we have

$$fgq^{-1}(x-i)j = fgq^{-1}(xj-k) = q^{-1}(xg(fj) - fgk) \in \mathcal{O}_p$$

for all $p \neq q$. Similarly, adjoining $fgq^{-1}(x-j)i$ globally to our order does not affect the order at places $p \neq q$ since

$$fgq^{-1}(x-j)i = fgq^{-1}(xi+k) = q^{-1}(xf(gi) + fgk) \in \mathcal{O}_p$$

for all $p \neq q$. In particular,

$$\mathbb{Z}_p\langle 1, gi, fhj, fgq^{-1}(x-i)j\rangle = \mathbb{Z}_p\langle 1, gi, fhj, fg(xj-k)\rangle$$

$$= \mathbb{Z}_p\langle 1, gi, fhj, gx(fj) - fgk\rangle = \mathbb{Z}_p\langle 1, gi, fhj, fgk\rangle = \mathcal{O}_p$$

and

$$\mathbb{Z}_p\langle 1, gi, fhj, fgq^{-1}(x-j)i\rangle = \mathbb{Z}_p\langle 1, gi, fhj, fg(xi+k)\rangle$$

$$= \mathbb{Z}_p\langle 1, gi, fhj, fx(gi) + fgk\rangle = \mathbb{Z}_p\langle 1, gi, fhj, fgk\rangle = \mathcal{O}_p.$$

Therefore we have $\mathcal{O} = \mathbb{Z}\langle 1, gi, fhj, fgk\rangle \subset \mathcal{O}' = \mathbb{Z}\langle 1, gi, fhj, fgq^{-1}(x-i)j\rangle$. On the other hand, away from q, $\mathcal{O}'_p = \mathcal{O}_p$; at q, $\mathcal{O}_q \subset \mathcal{O}'_q$ with $\mathcal{O}'_q$ maximal as desired, since

$$\mathbb{Z}_q\langle 1, gi, fhj, fgq^{-1}(x-i)j\rangle = \mathbb{Z}_q\langle 1, i, j, q^{-1}(x-i)j\rangle$$

and

$$\mathbb{Z}_q\langle 1, gi, fhj, fgq^{-1}(x-j)i\rangle = \mathbb{Z}_q\langle 1, i, j, q^{-1}(x-j)i\rangle.$$

So since $\mathcal{O}'$ is unchanged from $\mathcal{O}$ for $p \neq q$, while $\mathcal{O}'$ has level 1 at q whereas $\mathcal{O}$ has level q, we have level$(\mathcal{O}) = R_1R_2 \cdot M_1M_2 = N$ as desired.

So globally if $a \equiv 3 \mod 4$ we can compute our basis as

$$\mathcal{O}' = \begin{cases} \mathbb{Z}\langle 1, gi, \frac{fgh(j+xk)}{q}, fk\rangle & \text{if } q \mid b \\ \mathbb{Z}\langle 1, \frac{gh(i+tk)}{q}, fgj, fk\rangle & \text{if } q \mid a \end{cases},$$

where $t \in \mathbb{Z}$ comes from the Euclidean algorithm for writing

$$1 = s(q) + t(hx). \tag{2.2}$$

However, if $a \equiv 1 \mod 4$, so $\mathcal{O}$ has basis

$$\mathcal{O} = \mathbb{Z}\left\langle 1, g \cdot \frac{1+i}{2}, fhj, fg \cdot \frac{hj+k}{2} \right\rangle,$$

we must calculate the basis obtained by adjoining $q^{-1}(x-i)j$ or $q^{-1}(x-j)i$ to $\mathcal{O}$ by using the Hermite normal form. The Hermite normal forms give us a basis for our order:

$$\mathcal{O}' = \begin{cases} \mathbb{Z}\left\langle 1, \frac{g(1+i)}{2}, \frac{fgh(j+uk)}{2q}, fk \right\rangle & \text{if } q \mid b \\ \mathbb{Z}\left\langle \frac{q+gi+2gzk}{2q}, \frac{g(2i+z'k)}{2q}, \frac{f(hj+gk)}{2}, fgk \right\rangle & \text{if } q \mid a \end{cases},$$

where u is given by using the Euclidean algorithm to write $v(q) + w(2x) = 1$, and setting $0 \le u < 2q$ such that

$$u \equiv vq + 2w \mod 2q, \tag{2.3}$$

z is given by the Euclidean algorithm for writing

$$y(-q) + z(2x) = 1, \tag{2.4}$$

and where z' is given by choosing $0 \le z' < 2q$ with

$$z' \equiv 4z \mod 2q. \tag{2.5}$$

2.5. Main result

In Section 2.3 we constructed orders of level qN, and in the previous section we lowered the level of our order at q from q to 1. Therefore we have the following:

Theorem 13. *Select a, b to represent our quaternion algebra as stated in Proposition 12, and put*

$$f = \epsilon \cdot {\prod_{p \mid R_1}}' p^{\frac{v_p(N)-1}{2}} \cdot {\prod_{p \mid R_2}}' p^{v_p(N)/2-1} \cdot \prod_{\substack{p \mid M_2, \\ \left(\frac{a}{p}\right)=1}} p^{v_p(N)/2},$$

$$g = \prod_{\substack{p \mid M_2, \\ \left(\frac{a}{p}\right)=-1}} p^{v_p(N)/2} \cdot \prod_{p \mid M_1} p^{\frac{v_p(N)-1}{2}}$$

and

$$h = \begin{cases} \prod_{p \mid R_2} p^{1-v_p(b)} & \text{if } v_2(N) \neq 2 \\ {\prod_{p \mid R_2}}' p^{1-v_p(b)} & \text{if } v_2(N) = 2 \end{cases} \quad \text{with } \epsilon = \begin{cases} 2^{\frac{v_2(N)-3}{2}} & \text{if } v_2(N) \geq 3 \text{ odd} \\ 2^{\frac{v_2(N)}{2}-2} & \text{if } v_2(N) \geq 3 \text{ even} \cdot \\ 1 & \text{else} \end{cases}$$

and select $x \in \mathbb{Z}$ with $x^2 \equiv a \bmod q$ if $q \mid b$, and $x^2 \equiv b \bmod q$ if $q \mid a$. Then the order

$$\mathcal{O} = \begin{cases} \mathbb{Z}\left\langle \frac{q+gi+2gzk}{2q}, \frac{g(2i+z'k)}{2q}, \frac{f(hj+gk)}{2}, fgk \right\rangle & \text{if } q \mid a \text{ and } a \equiv 1 \bmod 4 \\ \mathbb{Z}\langle 1, \frac{gh(i+tk)}{q}, fgj, fk \rangle & \text{if } q \mid a \text{ and } a \equiv 3 \bmod 4 \\ \mathbb{Z}\left\langle 1, \frac{g(1+i)}{2}, \frac{fgh(j+uk)}{2q}, fk \right\rangle & \text{if } q \mid b \text{ and } a \equiv 1 \bmod 4 \\ \mathbb{Z}\langle 1, gi, \frac{fgh(j+xk)}{q}, fk \rangle & \text{if } q \mid b \text{ and } a \equiv 3 \bmod 4 \end{cases}$$

has level N in B, with u given by (2.3)*, z given by* (2.4)*, z' given by* (2.5)*, and t given by* (2.2).

Theorem 11 follows from descending Theorem 13 to $\Delta = p$.

When $\Delta \mid R_1$–i.e. when K_p is unramified for all $p \mid \Delta$–Theorem 13 descends to:

Theorem 14. *When we select a, b to represent our quaternion algebra as stated in Section 2.3, we choose*

$$f = \epsilon \cdot \prod_{p|R} p^{\frac{v_p(N)-1}{2}} \cdot \prod_{\substack{p|M_2,\\ \left(\frac{a}{p}\right)=1}} p^{v_p(N)/2}, \quad g = \prod_{\substack{p|M_2,\\ \left(\frac{a}{p}\right)=-1}} p^{v_p(N)/2} \cdot \prod_{p|M_1} p^{\frac{v_p(N)-1}{2}}$$

with

$$\epsilon = \begin{cases} 2^{\frac{v_2(N)-3}{2}} & \text{if } v_2(N) \geq 3 \text{ odd} \\ 2^{\frac{v_2(N)}{2}-2} & \text{if } v_2(N) \geq 3 \text{ even} \\ 1 & \text{else} \end{cases},$$

and select $x \in \mathbb{Z}$ with $x^2 \equiv a \bmod q$ if $q \mid b$, and $x^2 \equiv b \bmod q$ is $q \mid a$. Then the order

$$\mathcal{O} = \begin{cases} \mathbb{Z}\left\langle \frac{q+gi+2gzk}{2q}, \frac{g(2i+z'k)}{2q}, \frac{f(j+gk)}{2}, fgk \right\rangle & \text{if } a \equiv 1 \bmod 4 \\ \mathbb{Z}\langle 1, \frac{g(i+tk)}{q}, fgj, fk \rangle & \text{if } a \equiv 3 \bmod 4 \end{cases}$$

has level N in B, with z given by (2.4)*, z' given by* (2.5)*, and t given by* (2.2).

These results have been checked for $\Delta < 1000$ and $N < 10,000$ by constructing the order prescribed above in Sage and computing its discriminant, matching it to the level N. Note that I have provided the code for the general construction of an order with level N detailed in my result, available at `http://math.ou.edu/~jwiebe/`.

2.6. Examples

Now that we have our order $\mathcal{O}$ of level N, we can use it to construct spaces of modular forms of level N using Brandt matrices (or theta series); see [18], [6] when B has prime discriminant, and see [12] for arbitrary B. Note that there are other approaches to this, including a technique of Dembélé [3] which only requires the use of maximal orders. However, our result also allows us to compute quaternionic modular forms via Brandt matrices, and also solves the quaternionic analog of the classical problem of finding bases for orders in number fields.

We conclude by presenting examples of finding bases of orders, and indicate how this is used to compute modular forms of matching level.

Example 15 ($\Delta = 3$ and $N = 27$)**.**

Suppose that $\Delta = 3$ and $N = 27$. We can compute the class number (see [18]), and obtain $H = 2$. We can compute a, b and $\mathcal{O}$ using the case outlined in Section 2.3 to obtain $a = -3$, $b = -73$ and use Theorem 13 to obtain

$$\mathcal{O} = \mathbb{Z}\left\langle 1, \frac{1+i}{2}, \frac{3j + 309k}{146}, 3k \right\rangle.$$

Using Magma we obtain the following via `M:=BrandtModule(O)` and `HeckeOperator(M,p)`:

$$T_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$T_4 = \begin{pmatrix} -5 & 6 \\ 3 & -2 \end{pmatrix}, \quad T_5 = \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix}, \quad T_6 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$T_7 = \begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}, \quad T_8 = \begin{pmatrix} 32 & 64 \\ 32 & 64 \end{pmatrix}, \ldots$$

which yield the Eisenstein series with $a_p = p + 1$ for $p \neq 3$, as well as the cusp form

$$f = q - 2q^4 - q^7 + 5q^{13} + \ldots.$$

These are both modular forms of weight 2 and level 27, whose pth Fourier coefficient is an eigenvalue of the Hecke operator T_p above ($p \neq 3$).

Example 16 ($\Delta = 7$ and $N = 49$)**.**

Suppose that $\Delta = 7$ and $N = 49$. We can compute a, b and $\mathcal{O}$ using (again) the case outlined in Section 2.3 to obtain $a = -7$, $b = -11$ and use Theorem 13 to obtain

$$\mathcal{O} = \mathbb{Z}\left\langle 1, \frac{1+i}{2}, \frac{7(j-5k)}{22}, k \right\rangle.$$

Using Magma as in the previous example gives us

$$T_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{pmatrix},$$

$$T_4 = \begin{pmatrix} 3 & 4 & 0 & 0 \\ 4 & 3 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 4 & 3 \end{pmatrix}, T_5 = \begin{pmatrix} 0 & 0 & 3 & 3 \\ 0 & 0 & 3 & 3 \\ 3 & 3 & 0 & 0 \\ 3 & 3 & 0 & 0 \end{pmatrix}, \quad T_6 = \begin{pmatrix} 0 & 0 & 6 & 6 \\ 0 & 0 & 6 & 6 \\ 6 & 6 & 0 & 0 \\ 6 & 6 & 0 & 0 \end{pmatrix},$$

$$T_7 = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \quad T_8 = \begin{pmatrix} 6 & 9 & 0 & 0 \\ 9 & 6 & 0 & 0 \\ 0 & 0 & 6 & 9 \\ 0 & 0 & 9 & 6 \end{pmatrix}, \ldots$$

which yield the Eisenstein series with $a_p = p + 1$ for $p \neq 7$, as well as the cusp form

$$f = q + q^2 - q^4 - 3q^8 - 3q^9 + 4q^{11} + \ldots$$

These are both modular forms of weight 2 and level 49, whose pth Fourier coefficient is an eigenvalue of the Hecke operator T_p above ($p \neq 7$). Note that [7] provides a number of examples in Section 10 of similar calculations to ours, and in fact we may verify our results in this example by considering Example 10.5.

Example 17 ($\Delta = 70$ and $N = 2 \cdot 5^2 \cdot 7^5 \cdot 11 \cdot 23^2$)**.**

Suppose that $\Delta = 70$ and $N = 2 \cdot 5^2 \cdot 7^5 \cdot 11 \cdot 23^2$. Since $2 \mid \Delta$ and $v_2(N) = 1$, we are in Case 3, where we select $a = -q \cdot \prod_{p|R_2} p$ and $b = -\prod_{p|RM_1} p$. Our conditions on q we compute as:

1. $\left(\frac{q}{7}\right) = (-1) \cdot \left(\frac{-5}{7}\right)$; and
2. $\left(\frac{q}{5}\right) = (-1) \cdot \left(\frac{-7 \cdot 11}{5}\right)$; and
3. $\left(\frac{q}{11}\right) = \left(\frac{-5}{11}\right)$.

We also choose $q \equiv 7 \bmod 8$ so that $a \equiv 5 \bmod 8$. So this gives us a set of congruences where q is nonsquare $\bmod 7$, a square $\bmod 5$, and nonsquare $\bmod 11$. So if $q \equiv 7 \bmod 8$, $q \equiv 3 \bmod 7$, $q \equiv 2 \bmod 5$, and $q \equiv 2 \bmod 11$, we obtain $q = 1487$. So $a = -1487 \cdot 5$ and $b = -2 \cdot 5 \cdot 7 \cdot 11$. This gives us

$B = \left(\frac{-7435,-770}{\mathbb{Q}}\right)$ with $\Delta = 70$ as desired. Then $f = 23 \cdot 7^2$, $g = 1$, and $h = 1$. Now we need to find x so that $x^2 \equiv -770 \bmod 1487$, which gives us $x = 593$. Next we use the extended Euclidean algorithm to compute $d = y(-1487) + z(2 \cdot 593)$, which gives us $z = 1156$. Then $c = 2z = 2312$. So now we can construct our order:

$$O = \mathbb{Z}\left\langle \frac{1487 + i + 2 \cdot 578k}{2974}, \frac{i + 1156k}{1487}, \frac{1127j + 1127k}{2}, 1127k \right\rangle.$$

This order has level $N = 4889996650 = 2 \cdot 5^2 \cdot 7^5 \cdot 11 \cdot 23^2$ as desired.

Chapter 3

Zeros of quaternionic modular forms

3.1. Introduction

Modular forms are a fundamental tool in number theory for the study of a variety of objects, including elliptic curves and quadratic forms. As discussed in 1, classical modular forms are functions on the upper half plane $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im(z)} > 0\}$ obeying a certain set of transformation properties; equivalently, one can characterize classical modular forms as functions on the hyperbolic plane that behave well under the action of specific discrete subgroups of isometries. One can also expand on the idea of modular forms to functions on $\mathfrak{H}^n$ (yielding Hilbert modular forms) or on the Siegel upper half-space (yielding Siegel modular forms). Here we will study modular forms on quaternion algebras, and use certain behavior connected to the Atkin-Lehner eigenvalues associated to the forms to predict zeros of such forms. In particular, we will investigate the behavior of zeros of quaternionic modular forms of a given level which can be predicted to occur by a combination of analysis of the plus and minus spaces $S_k^{\mathrm{new},\pm}(N)$ and the action of the σ_p on the forms, where σ_p represents the involution given by right multiplication on $\mathrm{Cl}(\mathcal{O})$ by a uniformizer ϖ_p of O_p. This behavior is tied to a nonvanishing result for the L-functions of the elliptic cusp forms associated with our quaternionic modular forms. This nonvanishing phenomena will be examined in more detail in a joint paper with Kimball Martin in the future.

Let $S_k^{\text{new}}(N)$ denote the new subspace of weight k elliptic cusp forms on $\Gamma_0(N)$ — i.e., the space of forms which are not obtained from lower level modular forms. We can decompose the newspace above into the (full) plus and minus spaces $S_k^{\text{new},\pm}(N)$, subspaces generated by newforms with global root number — the $\pm$ in the functional equation of their L-functions — equal to ± 1. We can refine this decomposition further by observing that newforms with Atkin-Lehner eigenvalue $+1$ or -1 for each prime $p \mid N$ generate subspaces of the full plus/minus spaces, which we denote by $S_2^{\text{new},\epsilon_M}(N)$, using the notation of sign patterns in [14]. In this chapter, we construct and analyze quaternionic modular forms over $\mathbb{Q}$. Define Sq^* to be the set of squarefree integers which are the product of an odd number of primes, necessary to create a maximal order O with level N because the discriminant of our quaternion algebra must have the same (odd number of) prime factors as our level N. We begin by describing a construction algorithm for computing quaternionic modular forms of level $N \in Sq^*$. We then proceed to describe data collected counting both the number of zeros and the number of zerofree quaternionic modular forms of level $L \leq N$, compared with the dimension of the minus spaces $S_2^{\text{new},\epsilon_M}(N)$ to determine the behavior of the nontrivial zeros of quaternionic modular forms — that is, the zeros which are not the result of the action of the σ_p on the minus spaces $S_2^{\text{new},\epsilon_M}$. We conjecture that the ratio of the total number of zerofree quaternionic modular forms of level $L \in Sq^* \leq N$ to the total number of forms with no trivial zeros tends to 1 as $N \to \infty$, and provide data for prime N up to 7500 and nonprime $N \in Sq^*$ up to 3000 by using [14] to calculate the dimensions of such $\pm$ spaces, along with the involutions on the space of quaternionic modular forms. We also compare the number of nontrivial zeros which occur for prime level to the number which occur for level $N \in Sq^*$. We also expand our considerations to quaternionic modular forms of arbitrary level, constructed via the algorithm presented in Chapter 2. We conclude by analyzing asymptotics of the growth rate of trivial zeros, and provide a histogram of the distribution of nontrivial zeros with respect to the degrees of factors associated to them.

We begin in Section 3.2 by defining quaternionic modular forms and the cusp space $S(\mathcal{O})$. We present an algorithm for computing quaternionic modular forms of level $N \in Sq^*$ in Section 3.3. We proceed in Sections 3.4 and 3.5 to calculate dimensions of the plus and minus spaces of $S_k^{\text{new}}(N)$ using [14], which we use to calculate the number of trivial zeros of a given quaternionic modular form of prime level N, as well as to calculate the number of zeros for all forms of prime level N. This allows us to analyze the number of nontrivial zeros with respect to the size of the minus space of $S_k^{\text{new}}(N)$ (the space of forms with no trivial zeros), whose ratio we expect to tend towards 1 as $N \to \infty$. We establish our conjecture for prime level, and give relevant data illustrating this limit. In Section 3.5, we use the dimension formulas of [14] and results of [11] to calculate the number of forms of level $N \in Sq^*$ which we expect to be zerofree (i.e., forms which have no trivial zeros), and compare the predicted number to the actual value given via the previous data. This yields our final conjecture that the ratio of the total number of zerofree forms of level $L \in Sq^* \leq N$ to the number of forms with no trivial zeros of level $L \in Sq^* \leq N$ tends to 1 as $N \to \infty$. We continue in Section 3.6 by connecting our construction of orders of general level presented in Chapter 2 to our discussion on quaternionic modular forms, and present examples of quaternionic modular forms with general level N. We conclude with an analysis of the growth rate of the number of nontrivial zeros, as well as the number of forms with nontrivial zeros, and a histogram relating nontrivial zeros to the degree of the associated factors.

3.2. Quaternionic modular forms

Let $\mathcal{O}$ be be an order in a definite rational quaternion algebra B.

Definition 18. *A quaternionic modular form of level $\mathcal{O}$ and weight 2 is a complex-valued function φ on the set $Cl(\mathcal{O})$ of right $\mathcal{O}$-ideal classes. Let $M(\mathcal{O})$ denote the space of quaternionic modular forms.*

Note that we can view quaternionic modular forms as functions $\varphi : \hat{B}^\times \to \mathbb{C}$ which are left $B^\times$-invariant and right $\hat{\mathcal{O}}^\times$-invariant to better see their arithmetic connections.

For $F = \mathbb{Q}$, things become simpler because we have $F^\times \mathfrak{o}_p^\times F_\infty^\times \simeq \mathbb{A}_F$, giving us quaternionic eigenforms which correspond to elliptic cusp forms with trivial central character. Moreover, we define the Eisenstein space $\mathrm{Eis}(\mathcal{O})$ of $M(\mathcal{O})$ to be the subspace of constant functions on $\mathrm{Cl}(\mathcal{O})$.

Definition 19. *The normalized inner product on $M(\mathcal{O})$ is given by*

$$\langle \varphi, \varphi' \rangle = \sum_{i=1}^{h} \frac{\varphi(x_i)\overline{\varphi(x_i)}}{w_i},$$

where $w_i = |\mathcal{O}_\ell(x_i)^\times|$, the size of the unit group of the left order of $\mathcal{O}$ with respect to x_i.

Let $\mathbb{1}$ denote the constant function 1 on $\mathrm{Cl}(\mathcal{O})$. The cusp space $S(\mathcal{O})$ of $M(\mathcal{O})$

is given by

$$S(\mathcal{O}) = \{\varphi \in M(\mathcal{O}) : \langle \varphi, \mathbb{1} \rangle = 0\};$$

i.e., the subspace of forms which satisfy

$$\frac{1}{w_1}\varphi(x_1) + \cdots + \frac{1}{w_h}\varphi(x_h) = 0.$$

Observe that the definition above is for quaternionic modular forms over $\mathbb{Q}$. The general definition requires a more sophisticated inner product and that cusp forms to be orthogonal to the entire Eisenstein subspace $\mathrm{Eis}(\mathcal{O})$.

Note that the Jacquet-Landlands correspondence, in the setting of automorphic representations, gives us the isomorphism

$$S_2(\mathcal{O}) \simeq S_2^{\mathrm{new}}(N),$$

where $\mathrm{lev}(\mathcal{O}) = N$ and $S_2^{\mathrm{new}}(N)$ is the space of elliptic modular forms. This isomorphism respects the action of the Hecke operators T_p for $p \nmid N$. Also note that the action of the ramified Hecke operators T_p on $S_2(\mathcal{O})$ corresponds to the action of $T_p = -W_p$ on $S_2^{\mathrm{new}}(N)$ under the Jacquet-Langlands correspondence for the Atkin-Lehner operator W_p.

This correspondence shows the number-theoretic connections quaternionic modular forms have to modular forms of other varieties, and is used to obtain the dimension formulas we will in Sections 3.4 and 3.5, as well as in future work on a nonvanishing result of the L-function of the elliptic modular form f associated to our quaternionic modular form φ.

3.3. Computing bases of quaternionic modular forms

We calculate quaternionic modular forms over $\mathbb{Q}$ via the following algorithm:

```
// Input:  Level N, squarefree product of odd number of primes
// Output: S={quaternionic modular forms of level N},
           total number of zeros of S,
           total number of zerofree forms of S
function mod-form-data(N):
    B:=BrandtModule(N)
    while CharPoly(HeckeOperator(B,p)) has repeat factors:
        p:=NextPrime(p);

    M:=HeckeOperator(B,p);
    f<x>:=Factor(CharPoly(M));
    Ev:=EigenvalsOverQ(M);

    for lambda in Ev do:
        E:=Eigenspace(M,lambda);
        S:=Append(S,Basis(E));

        zerocounter+=Count(phi,0);
        if Count(phi,0) == 0 then:
            zerofreeforms+=1;

    for factor in f do:
        if degree(factor) > 1 then:
```

```
        lambda:=Eigenvalue(factor);
        K:=NumberField(lambda);
        E:=Eigenspace(Matrix(K,M),lambda);
        S:=Append(S,Basis(E));

        zerocounter+=Count(phi,0);
        if Count(phi,0) == 0 then:
            zerofreeforms+=1;

    return S, zerocounter, zerofreeforms;
```

This gives us a method for computing quaternionic modular forms for $N \in Sq^*$. For example, if $N = 23$, we have the following:

N=23	x_1	x_2	x_3	Min poly. of α	Global root number
φ_1	1	1	1	$x - 3$	$+1$
φ_2	2	$\alpha - 1$	-3α	$x^2 + x - 1$	$+1$

Also note that the global root number $w_f = (-1)^k \prod_{p|N} w_p(f)$, where the w_p are the Atkin-Lehner eigenvalues. In the weight 2 case, we have $w_f = \prod_{p|N} w_p(f)$, where each $w_p(f) = -a_p(f)$ for $p \mid N$ for a_p the Hecke eigenvalues.

It is advantageous to see the values of our forms in terms of α because we can more easily see the action of the involution σ_N on φ. For example, for $N = 67$, we have the following data:

N=67	x_1	x_2	x_3	x_4	x_5	x_6	Min poly. of α_i
φ_1	1	1	1	1	1	1	$x-3$
φ_2	2	1	-1	-1	0	0	$x-2$
φ_3	4	$2\alpha_2-2$	α_2+1	α_2+1	$-2\alpha_2-1$	$-2\alpha_2-1$	x^2+x-1
φ_4	0	0	1	-1	α_3+2	$-\alpha_3-2$	x^2+3x+1

Recall that if $f \in S_k^{\text{new}}(N)$ is a newform, the sign of the functional equation w_f of the L-series $L(s,f)$ is $(-1)^{k/2} \cdot \lambda$, where λ is the eigenvalue of W_N, the Nth Atkin-Lehner operator. We decompose the newspace into $S_k^{\text{new},\pm}(N)$, the subspaces generated by newforms with $w_f = \pm 1$. We can see from the above data that x_1 and x_2 are fixed by σ_N, and x_3 and x_4 are interchanged, as are x_5 and x_6. This allows us to deduce the plus and minus spaces of $S_2^{\text{new}}(67)$, with φ_1 forming the Eisenstein subspace, φ_3 forming the plus space with dimension 2 (since φ_3 has a single conjugate because the minimal polynomial of α is degree 2), and φ_2 and φ_4 forming the minus space with dimension 3 (since φ_4 has a conjugate because its minimal polynomial is degree 2).

Note that due to the construction of our quaternionic modular forms, their values will in fact lie in $\mathbb{R}$, a fact we can use to calculate approximate values for our forms when needed. In particular, the zeros of the φ_i will be of particular interest, which we detect with reasonable accuracy using approximate eigenvector calculations in Sage.

3.4. Zeros of quaternionic modular forms with prime level

Consider the dimension of the plus and minus space observed in the above case when $N = 67$. It is possible to manually examine a given quaternionic modular form of level N and determine which φ_i are in the plus space and which are in the minus space, and indeed one can obtain a significant amount of information from such observations. However, when we wish to expedite such calculations, it is sufficient to calculate the dimension of $S_k^{\text{new},\pm}(N)$ for prime N. Observe that such calculations tell us how many (but not which) forms belong in the $\pm$ spaces. Such formulas have been developed in [22], [9], and [5]. Explicit formulas for N prime and N squarefree are given by Martin in [14], which we reiterate here.

From Theorem 2.2 of [14], we know that for $N > 3$ squarefree,

$$\dim S_k^{\text{new},\pm}(N) = \frac{1}{2}\dim S_k^{\text{new}}(N) \pm \frac{1}{2}\left(\frac{1}{2}h(\Delta_N)b(N,1) - \delta_{k,2}\right), \tag{3.1}$$

where Δ_N is the discriminant of $\mathbb{Q}(\sqrt{-N})$, $h(\Delta_N)$ is the class number of an order of discriminant Δ_N, and $b(N,1) = 1, 2$, or 4 according to whether $N \not\equiv 3 \bmod 4$, $N \equiv 7 \bmod 8$, or $N \equiv 3 \bmod 8$ (respectively).

Using the above formula along with the involution on σ_N, we can calculate the number of zeros (which we call trivial zeros) we expect to occur in the eigenforms of $M(\mathcal{O})$ for $\mathcal{O}$ a quaternion order of prime level N using the formula

$$E(N) = r_N \cdot \dim(S_2^{\text{new},-}(N)),$$

where $r_N = h(\mathcal{O}) - 2\dim(S_2^{\text{new},-}(N))$ for $h(\mathcal{O})$ the class number of a quaternion order of level N. Here r_N is the number of fixed points of σ_N, which acts on the eigenforms $\{\phi_k\}$. Since the action of σ_N on $\phi \in M^{\pm}(\mathcal{O})$ is given by $\phi(\sigma_N(x)) = \pm\phi(x)$ for all $x \in \mathrm{Cl}(\mathcal{O})$, then for the minus space $\phi(\sigma_N(x)) = -\phi(x)$. Moreover, if σ_N fixes x, then we have $\phi(\sigma_N(x)) = \phi(x) = -\phi(x)$, so it must be that $\phi(x) = 0$. So r_N represents the number of trivial zeros of a quaternionic modular form of level N, and $E(N)$ gives the total number of such trivial zeros across all quaternionic modular forms of prime level N. Note that for general $N \in Sq^*$, predicting the number of trivial zeros is more challenging.

Outside of the values of a given quaternionic modular form which must be zero as counted by r_N on an individual basis, and by $E(N)$ for all level N forms, we expect values of a given form to be zero with a zero percent probability in the distribution of levels $N \to \infty$. Indeed, we expect that almost all zeros of quaternionic modular forms are in fact trivial zeros. Our first conjecture describes this:

Conjecture 20. *Let $A(N)$ denote the number of zeros which occur in the eigenforms of $M(\mathcal{O})$ for $\mathcal{O}$ of prime level N. Then*

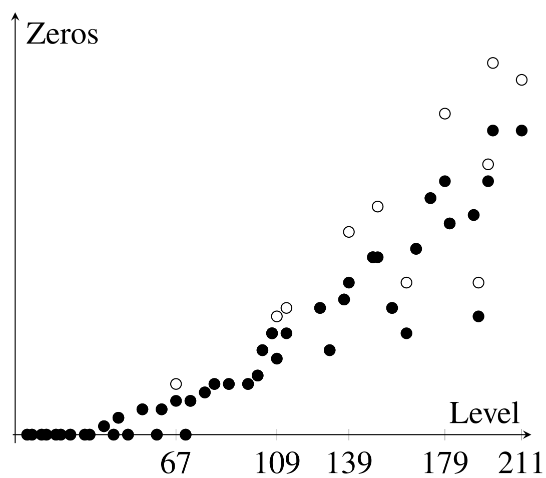
$$\lim_{N\to\infty} \frac{\displaystyle\sum_{\text{prime levels } L \le N} E(L)}{\displaystyle\sum_{\text{prime levels } L \le N} A(L)} = 1.$$

In fact, examining quaternionic modular forms of prime level N using the algorithm in the previous section — along with our formula for $E(N)$ — allows us to compare the number of trivial zeros (zeros which come from the minus space $S_2^{\mathrm{new},-}(N)$ where σ_N fixes x_i) to the actual number of zeros $A(N)$ to determine how many nontrivial zeros occur for a given level. For instance, consider again the example of $N = 67$:

N=67	x_1	x_2	x_3	x_4	x_5	x_6	w_f
φ_1	1	1	1	1	1	1	$+1$
φ_2	2	1	-1	-1	0	0	-1
φ_3	4	$2\alpha_2 - 2$	$\alpha_2 + 1$	$\alpha_2 + 1$	$-2\alpha_2 - 1$	$-2\alpha_2 - 1$	$+1$
φ_4	0	0	1	-1	$\alpha_3 + 2$	$-\alpha_3 - 2$	-1

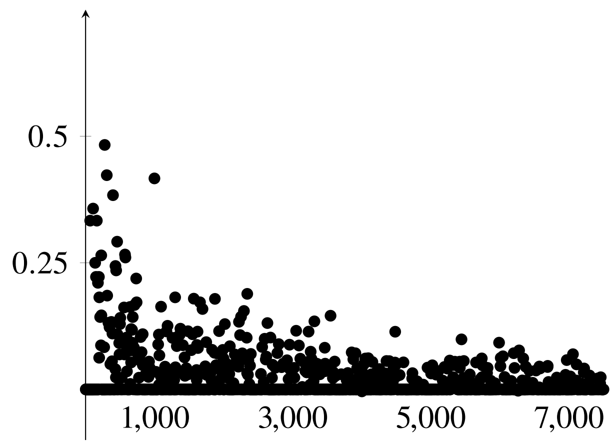
We know that φ_3 (along with its conjugate) span the plus space, and φ_2 and φ_4 and its conjugate span the minus space. Furthermore, the zeros of φ_2 and φ_4 are our trivial zeros, so along with multiplicity we have $E(67) = 6$. We now examine this trend for prime level:

Figure 3.1: Number of trivial zeros $E(N)$ (black) vs actual zeros $A(N)$ (white) (N - prime)



As we can see, there are occasional levels N for which the number of nontrivial zeros is particularly high, and we illustrate this by computing the ratio of nontrivial zeros in proportion to the total number of zeros:

Figure 3.2: nontrivial zeros / actual zeros (N - prime)



Notice that this ratio appears to converge to 0, meaning that as $N \to \infty$, almost all zeros of a given quaternionic modular form φ are trivial zeros. This data provides further justification for Conjecture 20.

For prime levels, we can directly compute the number of zeros we expect, but for general level this is not possible without significant computations using ideal classes. This leads us to a connected problem: can we predict how many quaternionic modular forms of level N are zerofree? The following theorem helps to answer this question:

Theorem 21. *Let N be prime. Then the number of quaternionic cusp forms of level N which have no trivial zeros is equal to* $\dim(S_2^{new,+}(N)) - 1$.

Proof. Suppose that φ is a quaternionic cusp form of prime level N which has no trivial zeros. Then there is no x_i for which $\varphi(\sigma_N(x)) = -\varphi(x)$ and $\sigma_N(x) = x$. So either σ_N has no fixed points, or φ is not in the minus space $S_2^{\text{new},-}(N)$. But for prime N, σ_N always has fixed points (see Lemma 4.3 of [13]). So it must be that $\varphi \in S_2^{\text{new},+}(N)$. The number of cusp forms in $S_2^{+}(N)$ is exactly $\dim(S_2^{\text{new},+}(N)) - 1$. $\square$

Thus we present a second conjecture on the number of forms with no trivial zeros which we can predict using the dimension formula 3.1. This will provide a common feature by which to compare the behavior of prime and nonprime levels in Sq^*.

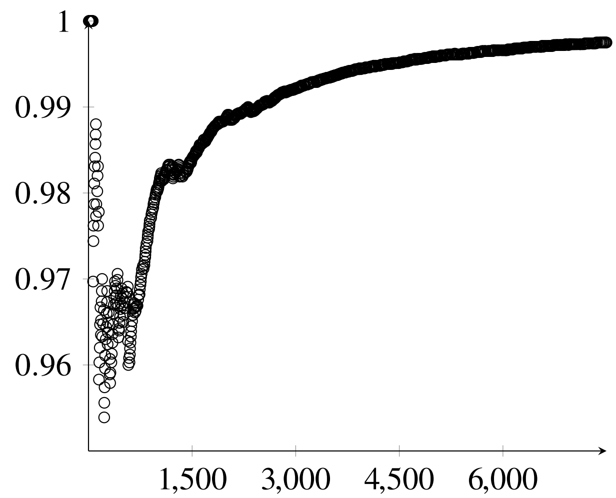
Conjecture 22. *Let $Z(N)$ denote the number of zerofree eigenforms of $M(O)$ of level N. Then*

$$\lim_{N\to\infty} \frac{\sum_{L\leq N} Z(L)}{\sum_{L\leq N} \dim(S_2^{new,+}(L))} = 1,$$

where the levels L in both sums are prime. In other words, we expect that a given quaternionic modular form with no trivial zeros will in fact have no zeros. The above ratio is computing the average of the forms of prime level $\leq N$ since we also expect particular levels to be significant outliers (meaning that the number of forms with nontrivial zeros is a significantly larger proportion). Denote by $R(N)$ the above (average) ratio.

For prime levels, we can compute the average ratio $R(N)$ conjectured above, and obtain the following data:

Figure 3.3: Average ratio $R(N)$ for prime level up to N



Here we see the behavior of the ratio in question for the conjecture seeming to illustrate that the limit is moving towards 1 for prime levels, with 150,298 total zerofree forms (excluding the Eisenstein series) of prime level $N \leq 7500$ and 149,923 total forms with no trivial zeros (again excluding the Eisenstein series) of prime level $N \leq 7500$. This gives us an average ratio of 149,923/150,298 = 0.9975. Also note this tells us that for prime level $N \leq 7500$, there are 375 cusp forms with nontrivial zeros.

The above data shows a number of levels of granularity when analyzing the zeros for eigenforms of prime level. For nonprime level in Sq^*, we have less information about the action of the σ_p, so our methods for predicting zeros will be more sophisticated.

3.5. Expanding to Sq^*

For general level $N \in Sq^*$, we must use more complex dimension formulas to predict the number of forms which we expect to be zerofree. Moreover, when our level is nonprime, there are multiple σ_p which act on $\mathrm{Cl}(\mathcal{O})$. Recall that in the previous section we predicted when we would obtain zeros of a quaternionic modular form of prime level by observing the behavior of σ_N, the only involution on the set of $\mathcal{O}$-ideal classes. When $N \in Sq^*$, notice that there is an involution σ_p for each $p \mid N$, and while it is true that each σ_p may have fixed points yielding trivial zeros — as was the case when N was prime — we must also consider cycles of the σ_p which yield trivial zeros. In particular, we may have σ_p with fixed points, and in the minus space, if σ_N fixes x, then we have $\phi(\sigma_p(x)) = \phi(x) = -\phi(x)$, so it must be that $\phi(x) = 0$. This is a one-cycle. There may also be longer cycles, where $\sigma_{p_1} \circ \sigma_{p_2} \circ \cdots \circ \sigma_{p_k}$ fixes some x. Cases such as this will yield additional trivial zeros for levels in Sq^*, and we wish to count the number of zeros we can predict via the σ_p. In order to calculate the dimension of the spaces where the σ_p have no fixed points, we must refine our dimension formulas using sign patterns ϵ_M.

Now consider a sign pattern ϵ_M as defined in [14], meaning a multiplicative function $d \mapsto \epsilon_M(d)$ on the divisors of M such that $\epsilon_M(1) = 1$ and $\epsilon_M(p) \in \{\pm 1\}$ for $p \mid M$. Then define $S_k^{\mathrm{new},\epsilon_M}(N)$ to be the subspace of $S_k^{\mathrm{new}}(N)$ generated by newforms which have Atkin-Lehner eigenvalues equal to $\epsilon_M(p)$ for each $p \mid M$. We will use the notation $-_M$ to indicate the sign pattern which has $\epsilon_M(p) = -1$ for all primes $p \mid M$.

From Proposition 3.2 of [14], we have the following: for N squarefree, $M > 1$

dividing N, and ϵ_M a sign pattern for M,

$$\dim(S_2^{\mathrm{new},\epsilon_M}(N)) = 2^{-\omega(M)} \cdot \sum_{d|M} \epsilon_M(d)\mathrm{tr}_{S_2^{\mathrm{new}}(N)} W_d.$$

Moreover, from Proposition 1.2 of [14] we have

$$\begin{aligned}\mathrm{tr}_{S_2^{\mathrm{new}}(N)} W_d = -\frac{1}{2}h'(\Delta_M)b(M, M') \cdot \prod_{M'_{\mathrm{odd}}} \left(\left(\frac{\Delta_M}{p}\right) - 1\right) + (-1)^{\omega(M')} \\ - \delta_{M,2} \cdot \frac{1}{2} \cdot \prod_{p|M'} \left(\left(\frac{-4}{p}\right) - 1\right) - \delta_{M,3} \cdot \frac{1}{3} \cdot \prod_{p|M'} \left(\left(\frac{-3}{p}\right) - 1\right) \quad (3.2)\end{aligned}$$

Lastly, when $d = 1$, the trace of W_1 is the dimension of the full new space $S_2^{\mathrm{new}}(N)$, which we recall for convenience from [10]:

$$\dim(S_2^{\mathrm{new}}(N)) = \frac{\varphi(N)}{12} - \frac{1}{4} \cdot \prod_{p|N} \left(\left(\frac{-4}{p}\right) - 1\right) - \frac{1}{3} \cdot \prod_{p|N} \left(\left(\frac{p}{3}\right) - 1\right) + \mu(N),$$

where $\varphi(N)$ is the Euler phi function, and $\mu(N)$ is the Möbius function.

We will use the above dimension formula to compute the number of forms with no trivial zeros for $N \in Sq^*$, based on the dimensions of subspaces along with the number of fixed points of σ_p. In particular, consider the $p \mid N$ for which σ_p has fixed points. The minus eigenspaces of the W_p correspond exactly to quaternionic cusp forms with no trivial zeros. We can determine the σ_p which have no fixed points using Lemma 4.3 of [13]. In particular, if $p \mid N$, then

- For $p > 2$, σ_p acts without fixed points if and only if $\left(\frac{-p}{q}\right) = 1$ for some odd prime $q \mid N$ or if N is even and $p \equiv 7 \bmod 8$.

- For $p = 2$, σ_p acts without fixed points if and only if N is divisible by a prime which is $1 \bmod 4$ and $\left(\frac{-2}{q}\right) = 1$ for some prime $q \mid N$.

Notice that in general we need to detect when a cycle $\sigma_{p_1} \circ \cdots \circ \sigma_{p_k}$ has fixed points. Observe that $\dim(S_2^{\text{new},-M}(N))$ equals the number of orbits of the σ_p if and only if there are no trivial zeros in $S_2^{\text{new},-M}(N)$. This yields the following theorem:

Theorem 23. *Let ϵ_M be a sign pattern for N and $M^{-\epsilon_M}(\mathcal{O}) = \{\varphi \in M(\mathcal{O}) : T_p(\varphi) = \epsilon_M(p) \cdot \varphi \text{ for } p \mid N\}$ the associated eigenspace. Then any nonzero form $\varphi \in M^{-\epsilon_M}(\mathcal{O})$ has no trivial zeros if and only if $\dim(M^{-\epsilon_M}(\mathcal{O})) = \dim(M^{+_N}(\mathcal{O}))$ (which is maximal among the subspaces of $S_2^{new}(N)$). Moreover, from [14] we know that $\dim(M^{-\epsilon_M}(\mathcal{O})) = \dim(S_2^{new,\epsilon_M}(N)$ and $\dim(M^{+_N}(\mathcal{O})) = 1+\dim(S_2^{new,-_N}(N))$ from the Jacquet-Langlands correspondence. So the number of cusp forms of level $N \in Sq^*$ with no trivial zeros is*

$$m \cdot (1 + \dim(S_2^{new,-_N}(N))) - 1,$$

where m is the number of sign patterns ϵ_M for which $\dim(S_2^{new,\epsilon_M}(N)) = 1 + \dim(S_2^{new,-_N}(N))$.

Proof. Consider a form $\varphi \in M^{-\epsilon_M}(\mathcal{O})$. Then φ has no trivial zeros if and only if there are no cycles $\sigma_{p_1} \circ \cdots \circ \sigma_{p_k}$ producing fixed points among the x_i in the subpsace $M^{-\epsilon_M}(\mathcal{O})$. Note that fixed points occur in such a cycle if and only if the parity of the cycle (the product of the signs associated to each orbit $\{x_i, \sigma_p(x_i)\}$) is -1. So if there are no cycles with parity -1 occurring in our subspace $M^{-\epsilon_M}(\mathcal{O})$, then we have no trivial zeros. Now observe that

$$\dim(M^{+_N}(\mathcal{O})) = 1 + \dim(S_2^{\text{new},-_N}(N))$$

is the number of orbits of $\text{Cl}(\mathcal{O})$ under the action of the σ_p, and this dimension is maximal among the subspaces of $S_2^{\mathrm{new}}(N)$. Moreover, note that all cycles of $M^{+_N}(\mathcal{O})$ have parity $+1$. So there are no cycles among the σ_p producing trivial zeros if and only if $\dim(M^{-\epsilon_M}(\mathcal{O})) = \dim(M^{+_N}(\mathcal{O}))$. We may calculate the number m of sign patterns which attain this maximum, and compute the dimension of this space of forms with no trivial zeros to be

$$m \cdot (1 + \dim(S_2^{\mathrm{new},-_N}(N))) - 1$$

as desired. □

Now that we have the dimension formula above and Theorem 23 to count the number of cusp forms with no trivial zeros, we can expand our conjecture on the distribution of zeros:

Conjecture 24. *Let $N \in Sq^*$ be a nonprime squarefree integer and let $S(N)$ denote the number of cusp forms with no trivial zeros, obtained via Theorem 23. As before, let $Z(N)$ denote the number of zerofree forms of level N. Then*

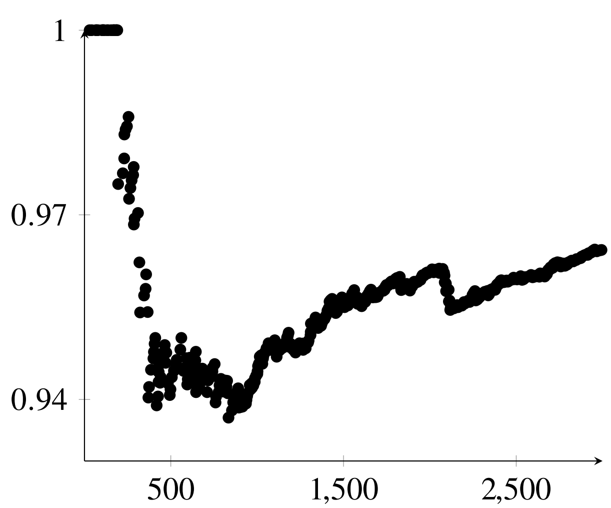
$$\lim_{N\to\infty} \frac{\sum_{L\leq N} Z(L)}{\sum_{L\leq N} S(L)} = 1,$$

where the levels in both sums are nonprime squarefree integers $L \in Sq^*$. Call the above average ratio $R(N)$ as before.

Notice that here we are averaging the number of zerofree forms of level $\leq N$ (obtained via our quaternionic modular forms calculations exhibited in the previous section), as well as the number of forms with no trivial zeros for level $\leq N$. A small sampling of data is helpful here to observe certain behavior in the average, specifically that particular levels contribute significantly to the average, after which the average moves up towards 1. This behavior of jumping and increasing is of interest and will be examined further.

In particular, we will be interested in levels N for which the number of forms with no trivial zeros of level N is significantly lower than the number of zerofree forms given by Theorem 23. Such forms will have a significant number of nontrivial zeros, and we will examine whether such zeros occur more frequently when a quaternionic modular form corresponds to a factor of low degree, or if there are significant instances of forms corresponding to high-degree factors with nontrivial zeros. This will be explored more fully at the end of this section, as well as in Section 3.8.

Figure 3.4: Average ratio $R(N)$ for nonprime level $N \in Sq^* \leq 3000$



We observe here that the ratio of zerofree forms to the number of forms with no trivial zeros is generally lower for nonprime level than for prime level, and there are more significant outliers for nonprime squarefree level; that is, there are more nonprime squarefree levels N where the ratio is unusually low, indicated by the jumps observed in the figure above. We can also observe that while the values of the ratio jump periodically due to the outliers, there is also a clustering occuring which moves towards 1 as $N \to \infty$, which occurs much more quickly for prime levels compared to general nonprime squarefree levels. This raises an important question: can we identify where such outliers occur among the nonprime squarefree levels in Sq^*?

Let's examine $N = 2110$, which has ratio $14/23$: excluding the quaternionic modular form corresponding to the Eisenstein series, we have 69 eigenforms, of which eight correspond to degree one factors, six of degree two, three of degree three, six of degree six, 16 of degree eight, 18 of degree nine, and 12 of degree twelve (counting conjugates). All of the forms except the 12 of degree twelve have zeros. Many of these zeros are ones that we expect, given that we only expect to have 23 zerofree forms. So there are 9 forms with nontrivial zeros.

Notice that the nontrivial zeros for nonprime squarefree levels in Sq^* require more computation to detect, as illustrated by $N = 195$:

N=195	x_1	x_2	x_3	x_4	x_5
φ_1	1	1	1	1	1
φ_2	0	0	1	-1	-1
φ_3	3	3	-1	-1	-1
φ_4	0	0	1	1	1
φ_5	0	0	1	1	-1
φ_6	8	-8	$\alpha^2 - 4\alpha - 8$	$-\alpha^2 + 4\alpha + 8$	$\alpha^2 - 4\alpha - 8$

x_6	x_7	x_8	Min poly. of α	w_f
1	1	1	$x-8$	$+1$
1	0	0	$x+1$	$+1$
-1	-1	-1	x	$+1$
1	-2	-2	$x+3$	$+1$
-1	0	0	$x-3$	$+1$
$-\alpha^2+4\alpha+8$	$2\alpha^2-4\alpha-24$	$-2\alpha^2+4\alpha+24$	$x^3-x^2-16x-16$	$+1$

Here all forms have global root number $+1$, and $\dim(S_2^{\text{new},-_195}(195)) = 2$, so the maximum dimension from Theorem 23 we are looking for is 3, which only occurs in $S_2^{\text{new},-_13}(195)$ and (trivially) in $S_2^{\text{new},-_195}(195)$. This gives our five forms with no trivial zeros. Notice that three zerofree forms come from φ_6 and its two conjugates, and φ_3 is the other zerofree form. So one of φ_2, φ_4, or φ_5 has nontrivial zeros. Using Lemma 4.3 of [14] we can calculate that σ_{13} acts without fixed points, while both σ_3 and σ_5 have fixed points. So we conclude that φ_4 has nontrivial zeros.

Now consider the average ratio $R(N)$ for general squarefree level $N \in Sq^*$. Given our previous two conjectures, along with the data presented above, it is natural to merge our conjectures together:

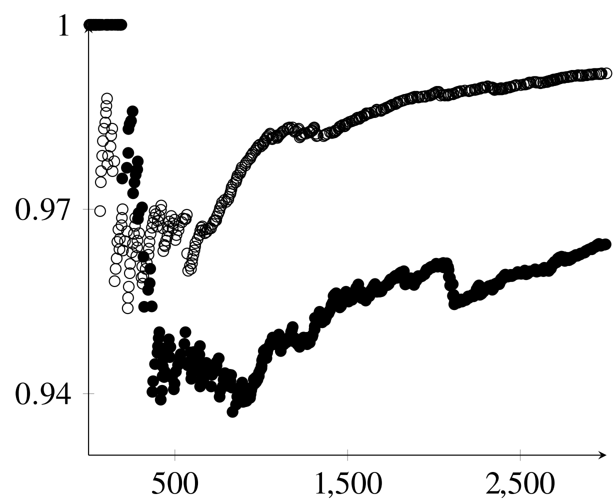
Conjecture 25. *Let $N \in Sq^*$ be a squarefree integer and $S(N)$ denote the number of cusp forms with no trivial zeros, obtained via Theorem 23 in nonprime levels, and via $\dim(S_2^{new,+}(N))$ in prime levels. As before, let $Z(N)$ denote the number of zerofree eigenforms of level N. Then*

$$\lim_{N\to\infty} \frac{\sum_{L\leq N} Z(L)}{\sum_{L\leq N} S(L)} = 1,$$

where the levels in both sums are squarefree integers $L \in Sq^*$. Call the above average ratio $R(N)$ as before.

Notice that the behaviors of prime levels and nonprime levels differ in that for prime level our average ratio converges more rapidly than for nonprime level, but both appear to be converging to one in the limit, as predicted by our conjectures:

Figure 3.5: $R(N)$ for prime level (white, above) vs $R(N)$ for nonprime squarefree level in Sq^* (black, below)



From this data we can see that the majority of nontrivial zeros occur for nonprime levels. Notice that the combined average ratio $R(3000) = \frac{36411}{36943}$, where there are 8346 zerofree cusp forms of nonprime squarefree level and 28,065 zerofree cusp forms of prime level. There are 8655 cusp forms of nonprime squarefree level with no trivial zeros, and 28,288 cusp forms of prime level with no trivial zeros. We can see that the majority of cusp forms of level ≤ 3000 come from prime level, but 309 of the 532 cusp forms with nontrivial zeros come from nonprime squarefree levels.

For nonprime N, computations of quaternionic modular forms become increasingly large, and as a result we have opted to sample a range of large N, calculating the number of zerofree forms using approximation methods in Sage:

N	**Forms with no trivial zeros**	**Actual zerofree forms**	$Z(N)/S(N)$
3585	56	29	29/56
3586	21	20	20/21
3590	21	19	19/21
3593	159	159	1
3594	19	19	1
3597	49	49	1
3598	35	28	28/35
3605	67	67	1
3606	17	17	1
3607	159	159	1
3613	156	156	1
3614	45	45	1
3615	55	54	1
3617	165	165	1
3619	127	124	124/127
3621	61	61	1
3623	173	172	172/173
3631	172	172	1
3633	55	52	52/55
3634	22	22	1

Observe that while there are outliers with relatively low ratios $Z(N)/S(N)$ —

where we have forms with nontrivial zeros — this data confirms our conjectures that $R(N) \to 1$ as $N \to \infty$.

3.6. General level

Consider the orders constructed in Chapter 3 of general level N. We examine here the quaternionic modular forms of level N in the most general setting.

We begin by describing the construction of quaternionic modular forms of general level: let B be a quaternion algebra with discriminant Δ and $\mathcal{O}$ be an order of level N given by 13. We can calculate the Hecke operators as before in Magma, and proceed with our construction of the quaternionic modular forms of level N. Of note for general N is that we may obtain a eigenspace of higher dimension corresponding to nonprimitive elliptic modular forms of level p^n. For instance, consider $N = 49$ and the order constructed in Example 2.6:

$$\mathcal{O} = \mathbb{Z}\left\langle 1, \frac{1+i}{2}, \frac{7(j-5k)}{22}, k \right\rangle,$$

where $a = -7$ and $b = -11$. Computing the eigenspaces of the Hecke operator T_2 gives us

N=49	x_1	x_2	x_3	x_4	Min poly. of α
φ_1	1	1	1	1	$x-3$
φ_2	1	1	1	-1	$x+3$
φ_3	1	0	-1	0	x
φ_4	0	1	-1	0	x

Note that both φ_3 and φ_4 have minimal polynomial x, which occurs because there is no p for which the Hecke operator T_p has distinct eigenvalues if our level is not squarefree. So φ_3 and φ_4 form a 2-dimensional eigenspace. For calculations of quaternionic modular forms of general level N, we will experience this problem for primes with $v_p(N) > 1$. Choosing a method by which to obtain eigenforms from the $v_p(N)$-dimensional eigenspaces is a nontrivial task, which we will not address here.

Based on the data presented above for both prime and nonprime squarefree level in Sq^*, we have shown evidence that for squarefree level in Sq^*, almost all forms with no trivial zeros (caused by the action of the σ_p on the subspaces of $S_2^{\text{new}}(N)$) in fact have no zeros.

Note that the occurrence of quaternionic modular forms with no zeros, as well as forms with nontrivial zeros, has ramifications in the vanishing of central L-values. In particular, for $\mathcal{O}$ a maximal order and $\varphi \in S(\mathcal{O})$ a zerofree quaternionic eigenform of level N and $f \in S_2^{\text{new},-N}(N)$ the newform associated to φ, if φ is zerofree then one can show that there is nonvanishing result for the central L-value associated to f. We will explore this connection in more detail in a joint paper with Kimball Martin in the future.

3.7. Asymptotics

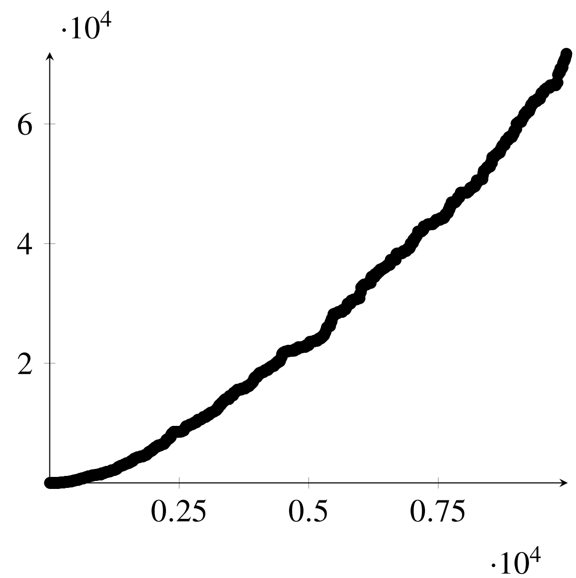
In this section, we wish to analyze the growth rates of the quantities examined above; in particular, we will examine the growth rate of the number of nontrivial zeros of quaternionic modular forms of prime level, as well as the growth rate of the number of quaternionic modular forms with no trivial zeros.

So consider the number of trivial zeros of quaternionic modular forms of prime level N given by

$$E(N) = r_N \cdot \dim(S_2^{\text{new},-}(N)) = (h(\mathcal{O}) - 2\dim(S_2^{\text{new},-}(N))) \cdot \dim(S_2^{\text{new},-}(N))$$

as before. If we denote by $A(N)$ the total number of zeros for forms of prime level N, and subtract the trivial zeros $E(N)$, we obtain the number of nontrivial zeros of level N. Consider the total number of nontrivial zeros $T(N)$ of quaternionic modular forms of prime level $\leq N$, given below:

Figure 3.6: $T(N)$ for prime level



Note that the above data tells us, for instance, that there are 71,733 nontrivial zeros among the quaternionic modular forms of prime level $\leq$ 10,000.

We wish to compare the rate of growth of this function to determine its asymptotic behavior, so we will graph $T(N)/f(N)$ for various continuous functions. We are looking for an upper bound which goes to zero in the limit. Clearly N is insufficient, but N^2 appears to be an asymptotic upper bound:

Figure 3.7: $T(N)/N$

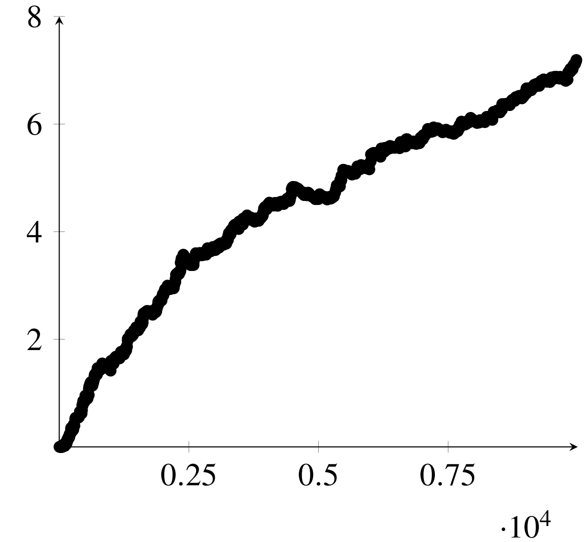
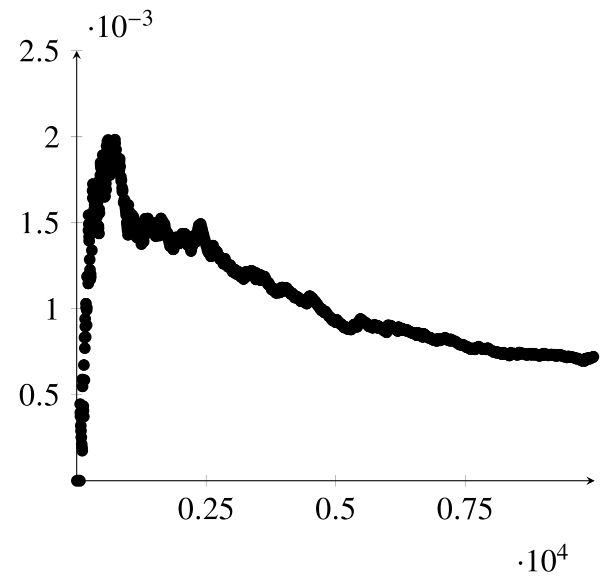
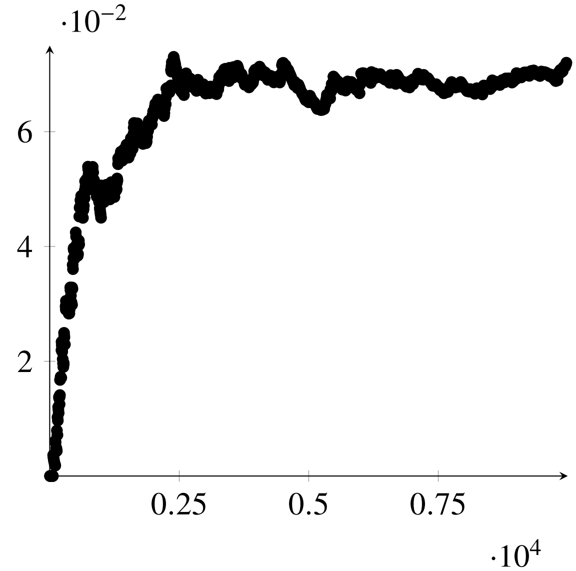


Figure 3.8: $T(N)/N^2$



It appears that $N^{3/2}$ is asymptotically equivalent to $T(N)$:

Figure 3.9: $T(N)/N^{3/2}$



While our data appears to asymptotically grow with $N^{3/2}$, accurately conjecturing this growth rate requires more data on the number of quaternionic modular forms, a problem which we will address separately in the future.

We would also like to examine the growth rate of the number of forms with nontrivial zeros. In order to calculate the number of forms with nontrivial zeros, we must use caution, as forms in the (global) minus space may have both trivial and nontrivial zeros. In order to find the forms with nontrivial zeros, we must separate the forms calculated in Sage and Magma into the (global) plus and minus spaces. To determine whether a given quaternionic modular form is in the minus space $S_2^{\text{new},-}(N)$, we begin by checking to see if it has at least r_N zeros (the number of trivial zeros for each form in the minus space). If it does, we can further check that $\varphi(x_i) = -\varphi(x_j)$ for each value of our form (this behavior occurs as a result of the action of σ_N). Once we have filtered the space of forms down using these techniques, we check to see if we have exactly $\dim(S_2^{\text{new},-}(N))$ such forms. If we have more forms, we proceed to check for each i the number of φ_j for which $\varphi_j(x_i) = 0$. In particular, for cusp forms in the minus space, the zeros occur for all such forms at the same x_i. We can use this property to detect whether we have the correct set of forms $\{\varphi_j\}$ spanning $S_2^{\text{new},-}(N)$. Forms in the (global) minus space $S_2^{\text{new},-}(N)$ with more than r_N zeros, in addition to any forms in the (global) plus space $S_2^{\text{new},+}(N)$ with zeros, give us all cusp forms with nontrivial zeros. Denote by $F(N)$ the number of cusp forms with nontrivial zeros.

Such calculations limit our dataset slightly, but we can still use the data to observe some asymptotic results:

Figure 3.10: $F(N)$ for prime level

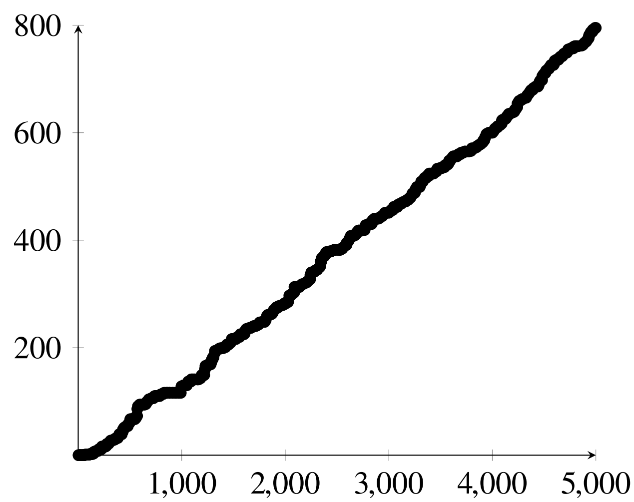
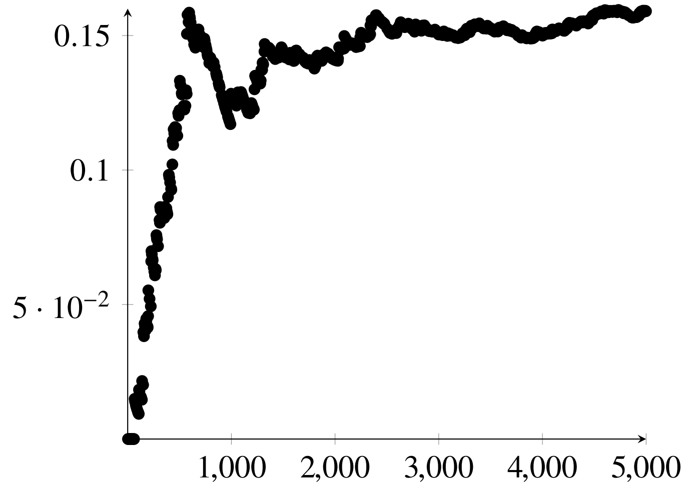


Figure 3.11: $F(N)/N$



It appears that the number of forms with nontrivial zeros of prime level asymptotically grows with N, but again note that accurately conjecturing an asymptotic here requires more exact data from Magma, a problem which we will address separately in the future.

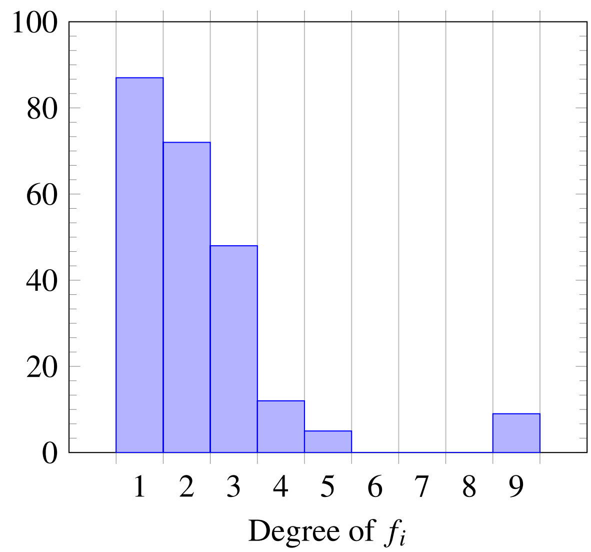
Note that some levels have significantly more forms with nontrivial zeros than others. For example, when $N = 571$, we have 19 forms in the minus space, with three forms (a degree 3 form and its conjugates) in the minus space having nontrivial zeros. In the plus space, there are two degree 1 forms, 4 degree two forms, and 4 degree 4 forms with (nontrivial) zeros. So there are 13 forms of level 571 with nontrivial zeros.

3.8. Degree histogram

In this section we will explore the degrees associated to forms with nontrivial zeros, and investigate the conjecture that almost all nontrivial zeros occur for quaternionic modular forms whose associated factors have low degree.

In order to determine when a form has nontrivial zeros, we use the same technique as in Section 3.7. Note that to obtain this data we eschew the use of approximations in favor of exact value calculations in Magma in order to obtain the degrees of the factors f_i associated to each quaternionic modular form φ_i.

Figure 3.12: Number of cusp forms with nontrivial zeros of prime level $N \leq 2000$ with nontrivial zeros of degree d



From the above histogram, you can see that the large majority of cusp forms with nontrivial zeros come from small degree factors. In fact, nearly 90% of the forms with nontrivial zeros of prime level $N \leq 2000$ come from factors of degrees 1, 2, or 3. This supports the conjecture that almost all nontrivial zeros occur in quaternionic modular forms whose factors have low degree. We will investigate this conjecture further in future work.

Appendix A

Tables of quaternionic modular forms of squarefree level $L \in Sq^*$

The following pages contain tables of the quaternionic modular forms of level $N \in Sq^*$. Note that the forms $\{\varphi_i\}$ are fixed up to scalar multiplication, which in particular indicates that the zeros listed for these forms are fixed. We will list the Eisenstein subspace $\mathrm{Eis}(\mathcal{O}) = \langle \varphi_1 \rangle$ and the cusp space $S(\mathcal{O}) = \langle \varphi_2, \ldots, \varphi_d \rangle$ for d the dimension of $M(\mathcal{O})$. We also list the global root number w_f of each form, which is the sign of the functional equation of its associated L-function. Note that the global root number $w_f = \prod_{p|N} w_p(f)$ for $w_p(f)$ the pth Atkin-Lehner eigenvalue. Furthermore, $w_p(f) = -a_p(f)$ for a_p the pth Hecke eigenvalue.

The forms are presented with their exact values using α_i an algebraic integer, along with the minimal polynomial of α_i.

N=3	x_1	Min poly. of α_i	w_f
φ_1	1	$x-3$	+1

N=5	x_1	Min poly. of α_i	w_f
φ_1	1	$x-3$	+1

N=7	x_1	Min poly. of α_i	w_f
φ_1	1	$x-3$	+1

N=11	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-3$	+1
φ_2	2	-3	$x+2$	+1

N=13	x_1	Min poly. of α_i	w_f
φ_1	1	$x-3$	+1

N=17	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-3$	+1
φ_2	3	-1	$x+1$	+1

N=19	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-3$	+1
φ_2	2	-1	x	+1

N=23	x_1	x_2	x_3	Min poly. of α_i	w_f
φ_1	1	1	1	$x-3$	+1
φ_2	2	α_2-1	$-3\alpha_2$	x^2+x-1	+1

N=29	x_1	x_2	x_3	Min poly. of α_i	w_f
φ_1	1	1	1	$x-3$	+1
φ_2	3	α_2	$-\alpha_2-1$	x^2+2x-1	+1

N=30	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-1$	+1
φ_2	1	−1	$x+1$	+1

N=31	x_1	x_2	x_3	Min poly. of α_i	w_f
φ_1	1	1	1	$x-3$	+1
φ_2	2	α_2-1	$-\alpha_2$	x^2-x-1	+1

N=37	x_1	x_2	x_3	Min poly. of α_i	w_f
φ_1	1	1	1	$x-3$	+1
φ_2	2	−1	−1	x	+1
φ_3	0	1	−1	$x+2$	−1

N=41	x_1	x_2	x_3	x_4	Min poly. of α_i	w_f
φ_1	1	1	1	1	$x-3$	+1
φ_2	6	$2\alpha_2$	$-\alpha_2^2-2\alpha_2+1$	α_2^2-3	x^3+x^2-5x-1	+1

N=42	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-1$	+1
φ_2	1	−1	$x+1$	+1

N=43	x_1	x_2	x_3	x_4	Min poly. of α_i	w_f
φ_1	1	1	1	1	$x-3$	+1
φ_2	4	$2\alpha_2-2$	$-\alpha_2$	$-\alpha_2$	x^2-2	+1
φ_3	0	0	1	−1	$x+2$	−1

N=47	x_1	x_2	x_3	x_4	x_5	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	$x-3$	$+1$
φ_2	2	α_2-1	$-2\alpha_2^3+\alpha_2^2+10\alpha_2-6$	$3\alpha_2^3-2\alpha_2^2-16\alpha_2+10$	$-3\alpha_2^3+3\alpha_2^2+15\alpha_2-12$	$x^4-x^3-5x^2+5x-1$	$+1$

N=53	x_1	x_2	x_3	x_4	x_5	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	$x-3$	$+1$
φ_2	6	$2\alpha_2$	$-2\alpha_2^2-2\alpha_2+4$	α_2^2-3	α_2^2-3	x^3+x^2-3x-1	$+1$
φ_3	0	0	0	1	-1	$x+1$	-1

N=59	x_1	x_2	x_3	x_4	x_5	x_6	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	1	$x-3$	$+1$
φ_2	8	$4\alpha_2-4$	$-\alpha_2^4-2\alpha_2^3+7\alpha_2^2+10\alpha_2-8$	$2\alpha_2^3-2\alpha_2^2-12\alpha_2+8$	$3\alpha_2^4-21\alpha_2^2+12$	$2\alpha_2^2-2\alpha_2-4$	$x^5-9x^3+2x^2+16x-8$	$+1$

N=61	x_1	x_2	x_3	x_4	x_5	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	$x-3$	+1
φ_2	2	$2\alpha_2-4$	$-2\alpha_2^2+2\alpha_2+4$	$\alpha_2^2-2\alpha_2-1$	$\alpha_2^2-2\alpha_2-1$	x^3-x^2-3x+1	+1
φ_3	0	0	0	1	−1	$x+1$	−1

N=66	x_1	x_2	x_3	x_4	Min poly. of α_i	w_f
φ_1	1	1	1	1	$x-6$	+1
φ_2	2	2	−3	−3	$x+4$	+1
φ_3	1	−1	0	0	$x-2$	+1
φ_4	0	0	1	−1	x	+1

N=67	x_1	x_2	x_3	x_4	x_5	x_6	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	1	$x-3$	+1
φ_2	2	1	−1	−1	0	0	$x-2$	+1
φ_3	4	$2\alpha_3-2$	α_3+1	α_3+1	$-2\alpha_3-1$	$-2\alpha_3-1$	x^2+x-1	+1
φ_4	0	0	1	−1	α_4+2	$-\alpha_4-2$	x^2+3x+1	−1

N=70	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-4$	+1
φ_2	1	−1	x	+1

N=71	x_1	x_2	x_3	x_4	x_5	x_6	x_7	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	1	1	$x-3$	+1
φ_2	2	α_2-1	$-\alpha_2^2-\alpha_2+4$	α_2-1	-3	$-\alpha_2$	α_2^2-2	x^3-5x+3	+1
φ_3	2	α_3-1	$-\alpha_3^2+\alpha_3+1$	$\alpha_3^2-2\alpha_3-1$	$-3\alpha_3^2+3\alpha_3+6$	$2\alpha_3^2-2\alpha_3-3$	$-\alpha_3^2+\alpha_3+1$	x^3+x^2-4x-3	+1

N=73	x_1	x_2	x_3	x_4	x_5	x_6	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	1	$x-3$	+1
φ_2	1	-1	-1	-1	1	1	$x-1$	+1
φ_3	2	$2\alpha_3-4$	$-\alpha_3+2$	$-\alpha_3+2$	-1	-1	x^2-x-3	+1
φ_4	0	0	1	-1	$-\alpha_4-1$	α_4+1	x^2+3x+1	-1

N=78	x_1	x_2	Min poly. of α_i	w_f
φ_1	1	1	$x-1$	+1
φ_2	1	-1	$x+1$	+1

N=79	x_1	x_2	x_3	x_4	x_5	x_6	x_7	Min poly. of α_i	w_f
φ_1	1	1	1	1	1	1	1	$x-3$	$+1$
φ_2	4	$2\alpha_2-2$	$-\alpha_2^4+\alpha_2^3+3\alpha_2^2-3\alpha_2+1$	$-\alpha_2^4+\alpha_2^3+3\alpha_2^2-3\alpha_2+1$	$2\alpha_2^3-8\alpha_2$	$2\alpha_2^4-2\alpha_2^3-8\alpha_2^2+6\alpha_2+2$	$-2\alpha_2^3+2\alpha_2^2+6\alpha_2-4$	x^5-6x^3+8x-1	$+1$
φ_3	0	0	1	-1	0	0	0	$x+1$	-1

N=83	x_1	x_2	x_3	x_4
φ_1	1	1	1	1
φ_2	8	$4\alpha_2-4$	$2\alpha_2^3-4\alpha_2^2-6\alpha_2+8$	$2\alpha_2^4-4\alpha_2^3-10\alpha_2^2+12\alpha_2+8$
φ_3	0	0	0	0

x_5	x_6
1	1
$-\alpha_2^5 - \alpha_2^4 + 9\alpha_2^3 + 7\alpha_2^2 - 16\alpha_2 - 8$	$3\alpha_2^5 - 3\alpha_2^4 - 21\alpha_2^3 + 9\alpha_2^2 + 30\alpha_2$
0	0

x_7	x_8	Min poly. of α_i	w_f
1	1	$x - 3$	$+1$
$2\alpha_2^2 - 2\alpha_2 - 4$	$2\alpha_2^2 - 2\alpha_2 - 4$	$x^6 - x^5 - 9x^4 + 7x^3 + 20x^2 - 12x - 8$	$+1$
1	-1	$x + 1$	-1

N=89	x_1	x_2	x_3	x_4	x_5	x_6
φ_1	1	1	1	1	1	1
φ_2	3	1	1	-1	-1	1
φ_3	6	$2\alpha_3$	$-\alpha_3^4 + \alpha_3^3 + 7\alpha_3^2 - 5\alpha_3 - 10$	$\alpha_3^3 - \alpha_3^2 - 5\alpha_3 + 3$	$-\alpha_3^3 - \alpha_3^2 + 5\alpha_3 + 5$	$\alpha_3^4 - \alpha_3^3 - 7\alpha_3^2 + 3\alpha_3 + 6$
φ_4	0	0	0	0	0	0

x_7	x_8	Min poly. of α_i	w_f
1	1	$x-3$	$+1$
-1	-1	$x-1$	$+1$
α_3^2-3	α_3^2-3	$x^5+x^4-10x^3-10x^2+21x+17$	$+1$
1	-1	$x+1$	-1

N=97	x_1	x_2	x_3	x_4	x_5	x_6
φ_1	1	1	1	1	1	1
φ_2	2	$2\alpha_2-4$	$\alpha_2^3-3\alpha_2^2-\alpha_2+5$	$\alpha_2^3-3\alpha_2^2-\alpha_2+5$	$-\alpha_2^3+2\alpha_2^2+2\alpha_2-3$	$-\alpha_2^3+2\alpha_2^2+2\alpha_2-3$
φ_3	0	0	1	-1	$\alpha_3^2+2\alpha_3-1$	$-\alpha_3^2-2\alpha_3+1$

x_7	x_8	Min poly. of α_i	w_f
1	1	$x-3$	$+1$
$\alpha_2^2-2\alpha_2-1$	$\alpha_2^2-2\alpha_2-1$	$x^4-3x^3-x^2+6x-1$	$+1$
$-\alpha_3^2-3\alpha_3$	$\alpha_3^2+3\alpha_3$	x^3+4x^2+3x-1	-1

References

[1] Albert, A. A. (1934). Integral domains of rational generalized quaternion algebras. *Bull. Amer. Math. Soc.*, 40(2):164–176.

[2] Atkin, A. O. L. and Lehner, J. (1970). Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160.

[3] Dembélé, L. (2014). On the computation of algebraic modular forms on compact inner forms of GSp_4. *Math. Comp.*, 83(288):1931–1950.

[4] Eichler, M. (1955). Über die Darstellbarkeit von Modulformen durch Thetareihen. *J. Reine Angew. Math.*, 195:156–171 (1956).

[5] Hasegawa, Y. and Hashimoto, K.-i. (1995). On type numbers of split orders of definite quaternion algebras. *Manuscripta Math.*, 88(4):525–534.

[6] Hijikata, H., Pizer, A., and Shemanske, T. (1989a). Orders in quaternion algebras. *J. Reine Angew. Math.*, 394:59–106.

[7] Hijikata, H., Pizer, A. K., and Shemanske, T. R. (1989b). The basis problem for modular forms on $\Gamma_0(N)$. *Mem. Amer. Math. Soc.*, 82(418):vi+159.

[8] Ibukiyama, T. (1982). On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. *Nagoya Math. J.*, 88:181–195.

[9] Iwaniec, H., Luo, W., and Sarnak, P. (2000). Low lying zeros of families of L-functions. *Inst. Hautes Études Sci. Publ. Math.*, (91):55–131 (2001).

[10] Martin, G. (2005). Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. *J. Number Theory*, 112(2):298–331.

[11] Martin, K. (2017). The Jacquet-Langlands correspondence, Eisenstein congruences, and integral L-values in weight 2. *Math. Res. Lett.*, 24(6):1775–1795.

[12] Martin, K. (2018a). The basis problem revisited. Preprint. arXiv:1804.04234.

[13] Martin, K. (2018b). Congruences for modular forms mod 2 and quaternionic S-ideal classes. *Canad. J. Math.*, 70(5):1076–1095.

[14] Martin, K. (2018c). Refined dimensions of cusp forms, and equidistribution and bias of signs. *J. Number Theory*, 188:1–17.

[15] Pacetti, A. and Rodriguez Villegas, F. (2005). Computing weight 2 modular forms of level p^2. *Math. Comp.*, 74(251):1545–1557. With an appendix by B. Gross.

[16] Pacetti, A. and Sirolli, N. (2014). Computing ideal classes representatives in quaternion algebras. *Math. Comp.*, 83(289):2479–2507.

[17] Pizer, A. (1976). On the arithmetic of quaternion algebras. *Acta Arith.*, 31(1):61–89.

[18] Pizer, A. (1980). An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390.

[19] Vignéras, M.-F. (1980). *Arithmétique des algébres de quaternions*, volume 800. Springer, Berlin.

[20] Voight, J. The arithmetic of quaternion algebras. To appear. Draft available at `http://math.dartmouth.edu/~jvoight/`.

[21] Voight, J. (2013). Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. 31:255–298.

[22] Wakatsuki, S. (2014). Congruences modulo 2 for dimensions of spaces of cusp forms. *J. Number Theory*, 140:169–180.