Modular Arithmetic of Quaternion Norms

Rietveld, Robbe

Modular Arithmetic of Quaternion Norms

Robbe Rietveld

r.a.rietveld@umail.leidenuniv.nl

Bachelor's Thesis

Date: June 30, 2025

Thesis supervisor: dr. Jonathan Love

Leiden University
Mathematical Institute

Contents

1 Introduction

Quaternions were originally described by Hamilton in 1843. We briefly discuss how this description came about, with reference to Section 1.1 of Voight [Voi21]. Hamilton knew that the complex numbers $\mathbb{C}$ could be interpreted as points on a plane such that addition and multiplication correspond to translations, scaling and rotations. Hamilton was looking for a number system that could model three-dimensional space in a similar way. He was looking for numbers that are similar to complex numbers, but with a "two-dimensional" imaginary part. He did not succeed in finding such numbers. Instead, he had to add a fourth dimension, and came up with the ring we now denote with $\mathbb{H}$: the Hamilton quaternions. It is given as $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, induced by the multiplication rules

$$i^2 = j^2 = k^2 = ijk = -1.$$

The group $\mathbb{H}^1 := \{t + xi + yj + zk \in \mathbb{H} : t^2 + x^2 + y^2 + z^2 = 1\}$ acts by rotation on $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ via conjugation [Voi21, Proposition 2.4.18]. This result shows that the quaternions in $\mathbb{H}$ do indeed "model" three-dimensional space in some way.

The notion of a quaternion algebra can be generalized far beyond just the Hamilton quaternions (see Definition 2.1). Abstracting from the geometric interpretation, quaternion algebras have applications in other branches of mathematics as well. For instance, every quaternion algebra has a multiplicative norm defined on it, which can be expressed as a quadratic form (Lemma 2.1.4). This can be used to prove number theoretic results such as Lagrange's four-square theorem [Voi21, Theorem 11.4.3].

In recent years, another application of quaternion algebras has arisen. There is a remarkable connection between elliptic curves and quaternion algebras. Some elliptic curves E over $\mathbb{F}_{p^2}$ have an endomorphism ring that is actually a quaternion algebra over $\mathbb{Q}$ [Voi21, Theorem 42.1.9]. This connection is exploited in cryptography. In Section 5, we will look at SQIsign2D-East [Cas+24], [Nak+24]. This is a contender for a post-quantum signature scheme, meaning that it is believed to be secure against attacks by quantum computers [GL24, p. 2]. In SQIsign2D-East, the goal is to establish a method that provides the sender of a message with an unforgeable signature. When such a signature is sent along with a message, the receiver of the message knows for sure that the message originated from the right person.

The main idea behind the procedure of signature creation is as follows. Given is a hard problem in terms of elliptic curves that is almost impossible to solve without further information. No one has any further information, except for the sender of the message. The sender has additional private information that can be used to convert the hard problem of elliptic curves into a (much easier) problem in terms of quaternion algebras. Once the quaternion problem is solved, a corresponding signature is created and the receiver of the message can then verify that the signature was indeed a solution to the problem.

In [Cas+24, Section 2], it is found that repeatedly generating signatures leaks information that can be used to determine private information of the sender. A fix that avoids this leakage is then proposed [Cas+24, Section 3]. In the fix, elements in integral ideals (Definition 2.2.10) are sampled repeatedly at random. In order for the fix to work, an element that satisfies a specific congruence relations on its norm must be found. So the efficacy of the fix relies on the probabilities that a randomly sampled element satisfies a certain congruence relation on its norm.

Inspired by the question of what these probabilities are, we try to answer the question as general as possible (Problem 2.3.1). In this thesis, we go through the properties of quaternion algebras, lattices, orders and their completions in Sections 2 and 3. Then we will find the desired probabilities in Section 4. The main results of this thesis are the formulas for the probabilities that the norm of a sampled element in a certain integral ideal satisfies any congruence relation. These formulas are given in Theorem 4.5.1 and apply to every locally principal integral ideal of any Eichler order in any quaternion algebra that is ramified at ∞. Finally, we apply the found results in the context of SQIsign2D-East in Section 5.

2 Quaternion algebras

We begin by building up the required theoretical framework around quaternion algebras. Throughout this section, we use Voight as our main reference [Voi21]. In this section, let F be a field with $\mathrm{char}(F) \neq 2$.

Definition 2.1. Let B be a ring equipped with a homomorphism $F \to B$ such that the image of F lies in the center $Z(B)$ of B. The ring B is a *quaternion algebra* over F if there exist $i, j \in B$ such that $1, i, j, ij$ is an F-basis for B and

$$i^2 = a, \quad j^2 = b, \quad ij = -ji,$$

for some $a, b \in F^\times$.

The multiplication rules in B are entirely determined by the values of a and b. So, for $a, b \in F^\times$, we define $\left(\frac{a,b}{F}\right)$ as the quaternion algebra over F with basis $1, i, j, ij$ such that $i^2 = a, j^2 = b$ and $ij = -ji$. For the purpose of formatting, we also write $(a, b \mid F)$.

Remark 2.2. Note that a homomorphism $F \to B$ is necessarily injective. Therefore, we may think of B as containing a copy of F, such that every element in F commutes with every element in B.

Remark 2.3. In a quaternion algebra B over F with basis $1, i, j, ij$, we can scale i by $x \in F^\times$ and j by $y \in F^\times$ to obtain a new basis $1, xi, yj, xyij$ with

$$(xi)^2 = x^2 a, \quad (yj)^2 = y^2 b.$$

It follows that

$$\left(\frac{a, b}{F}\right) \cong \left(\frac{ax^2, by^2}{F}\right).$$

So, the elements a and b induce the same quaternion algebra when they are scaled by squares in $F^\times$. In particular, if $F = \mathbb{Q}$, then any quaternion algebra is isomorphic to some quaternion algebra $(a, b \mid \mathbb{Q})$ for some $a, b \in \mathbb{Z} \setminus \{0\}$.

Remark 2.4. There is a more general characterization of quaternion algebras that also includes quaternion algebras over fields of characteristic 2 [Voi21, Chapter 6]. However, for our purpose it suffices to only consider quaternion algebras over fields of $\mathrm{char}(F) \neq 2$.

There also exist quaternion algebras where it is more convenient to have a basis independent description. Consider the following example.

Example 2.5. For a field F, the ring $M_2(F)$ of 2×2 matrices with entries in F is a quaternion algebra. We have a homomorphism $F \to M_2(F)$

$$x \mapsto \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}.$$

It can be checked that $(1, 1 \mid F) \cong M_2(F)$ via

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2.1 Standard involutions

In this subsection, let B denote the quaternion algebra $(a, b \mid F)$. We have the explicit basis $1, i, j, ij$ for B. With respect to this basis, we can define some useful maps on B.

Definition 2.1.1. An *involution* $B \to B$ is an F-linear map denoted by $\alpha \mapsto \overline{\alpha}$, such that for all $\alpha, \beta \in B$, it satisfies

(i) $\overline{1} = 1$;

(ii) $\overline{\overline{\alpha}} = \alpha$;

(iii) $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$.

If $\alpha\overline{\alpha} \in F$ for all $\alpha \in B$, the involution is called *standard*.

With respect to the basis $1, i, j, ij$, we can define the map $B \to B$

$$t + xi + yj + zij \mapsto \overline{t + xi + yj + zij} = t - xi - yj - zij. \tag{2.1.2}$$

And it can be verified that this map is a standard involution on B.

Definition 2.1.3. Let the map $B \to B$ with $\alpha \mapsto \overline{\alpha}$ be a standard involution. We define the *trace* on B as a map $B \to F$ given as

$$\alpha \mapsto \mathrm{tr}(\alpha) = \alpha + \overline{\alpha}.$$

We also define the *norm* on B as a map $B \to F$ given as

$$\alpha \mapsto \mathrm{N}(\alpha) = \alpha\overline{\alpha}.$$

Note that the trace is well defined as a map $B \to F$, since we have that

$$(\alpha + 1)\overline{(\alpha + 1)} = \alpha\overline{\alpha} + \alpha + \overline{\alpha} + 1 \in F.$$

We know that 1 and $\alpha\overline{\alpha}$ are in F, so $\alpha + \overline{\alpha}$ is in F as well.

Lemma 2.1.4. *Let $N : B \to F$ be the norm map induced by a standard involution on B. The norm is multiplicative, that is, $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in B$.*

Proof. We use that F is in the center of B and the third property of Definition 2.1.1. We compute

$$\mathrm{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha\mathrm{N}(\beta)\overline{\alpha} = \alpha\overline{\alpha}\mathrm{N}(\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

□

With respect to the basis $1, i, j, ij$ and the standard involution from 2.1.2, we can write the trace and norm of elements in B as

$$\mathrm{tr}(t + xi + yj + zij) = 2t; \tag{2.1.5}$$

$$\mathrm{N}(t + xi + yj + zij) = t^2 - x^2a - y^2b + z^2ab. \tag{2.1.6}$$

We also find that

$$\alpha^2 = (\alpha + \overline{\alpha})\alpha - \overline{\alpha}\alpha. \tag{2.1.7}$$

And note that $\alpha\overline{\alpha} - \overline{\alpha}\alpha \in F$ with trace 0. By 2.1.5, we find that an element $\alpha \in F$ has trace zero if and only if $\alpha = 0$. As a result, $\alpha\overline{\alpha} = \overline{\alpha}\alpha$, so the polynomial $x^2 - \mathrm{tr}(\alpha)x + \mathrm{N}(\alpha) \in F[x]$ annihilates α. It follows that every element in B is contained in a quadratic extension of F.

Lemma 2.1.8. *A quaternion algebra B over F has a unique standard involution.*

Proof. Let $\gamma \in B$ such that $F(\gamma) \neq F$. The extension $F(\gamma)$ is quadratic with basis $1, \gamma$. We define a standard involution on $F(\gamma)$ as a map that satisfies all properties of Definition 2.1.1 for all $\alpha, \beta \in F(\gamma)$. The standard involution then induces a trace and norm on $F(\gamma)$ analogous to the trace and norm on B.

Equality $\gamma^2 = t\gamma - n$ must hold for uniquely determined $t, n \in F$. But we know that $t = \gamma + \overline{\gamma}$ and $n = \gamma\overline{\gamma}$ hold as well. We find that the standard involution is uniquely determined as $\gamma \mapsto t - \gamma$. We also know there exists a standard involution on B such that $\overline{\gamma} = t - \gamma$.

Any standard involution on B restricts to a standard involution on $F(\gamma)$, and by the unicity of standard involutions on $F(\gamma)$, this uniquely determines the standard involution on B for all elements $\gamma \in B$ such that $F(\gamma) \neq F$. On elements in F, the standard involution is determined by the linearity and the condition $\overline{1} = 1$. We find that a standard involution on B is unique. □

When we consider matrix rings, it can be more convenient to consider the properties of their standard involution without reference to a basis.

Example 2.1.9. Let $B = M_2(F)$. The assignment $B \to B$ with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

is the unique standard involution. So in $M_2(F)$, the trace and norm correspond, respectively, to the maps

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix}; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}.$$

Note that the trace corresponds to the usual trace of a matrix, while the norm corresponds to the determinant.

2.2 Lattices

In this subsection, let R be a principal ideal domain and F its field of fractions, still with $\mathrm{char}(F) \neq 2$.

Definition 2.2.1. Let V be a finite-dimensional F-vector space. A finitely generated R-submodule $I \subset V$ is called an *R-lattice* if $IF = V$.

An equivalent condition to $IF = V$ is that I contains an F-basis for V. If $R = \mathbb{Z}$, we may omit the ring and just refer to a lattice.

Note that every quaternion algebra B over F is in particular a 4-dimensional vector space over F, so it makes sense to talk about lattices inside B.

First we give some convenient properties of modules and lattices.

Lemma 2.2.2 (Structure theorem)**.** *Let R be a principal ideal domain and let M be a nonzero finitely generated R-module. Then there exist cyclic R-modules $Rx_1, \ldots, Rx_n$ such that M is the direct sum $M \cong Rx_1 \oplus \cdots \oplus Rx_n$, and such that the annihilators $Ann(x_i)$ satisfy*

$$R \supsetneq Ann(x_1) \supset \cdots \supset Ann(x_n).$$

Proof. This is a well known result. See [Jac12, Theorem 3.8] for instance. □

By grouping together all terms with trivial and nontrivial annihilators, we may write the module M as $M \cong R^r \oplus T_M$ for some $r \in \mathbb{Z}_{\geq 0}$, where T_M is the torsion module of M.

Lemma 2.2.3. *Let V be a finite-dimensional F-vector space, let $I \subset V$ be an R-lattice and let $J \subset V$ be a finitely generated R-module. Then there exists a nonzero element $r \in R$ such that $rJ \subset I$.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a generating set for J. We know that I contains an F-basis $y_1, \ldots, y_m$ for V, so every x_i can be written as an F-linear combination of the y_i. We find that there exist $f_{ij} \in F$ such that any element in J is of the form

$$\sum_{i=1}^{n} r_i \sum_{j=1}^{m} f_{ij} y_j,$$

where $r_i \in R$. Since F is the field of fractions of R, there exists an $r \in R$ such that $r f_{ij} y_j \in R$ for every $f_{ij} y_j$. We find $rJ \subset I$. □

Lemma 2.2.4. *Let I be an R-lattice in an F-vector space V with $\dim V = n$. Then, I is free of rank n as an R-module.*

Proof. Note that I can be embedded into a vector space over F. Since $R \subset F$ holds, we find that I is torsion free. Then I is free by the structure theorem of finitely generated modules over a principal ideal domain (2.2.2).

Suppose I has rank m and has a submodule J. We have that $J \subset V$, so J is torsion free. Every element in J is a unique R-linear combination of an R-basis $x_1, \ldots, x_m$ for I. We find that J is finitely generated, hence free of rank $l \leq m$. Otherwise, there would necessarily be R-linear dependence within a basis of J.

Let $y_1, \ldots, y_n \in I$ be an F-basis for V, and let $N = \bigoplus_{i=1}^{n} R y_i \cong R^n$. We have $N \subset I$, so we find $n \leq m$. Now, by Lemma 2.2.3, we find that there is some nonzero $r \in R$ such that $rI \subset N$, so we conclude that $n = m$. □

Any quaternion algebra B over F is a 4-dimensional vector space over F, so every lattice in B is free over R of rank 4. In particular, if an R-lattice I has R-basis x_1, x_2, x_3, x_4, then this basis is automatically an F-basis for V.

Some lattices that are particularly in our interest, are the ones that also have a ring structure.

Definition 2.2.5. An R-lattice $O \subset B$ is an *order* if it is a subring of B. If O is not properly contained in another order, O is called *maximal*.

The following orders are a specific type of orders that will appear throughout this thesis.

Definition 2.2.6. Let $O, O' \subset B$ be two (not necessarily distinct) maximal orders. The intersection $O \cap O'$ is called an *Eichler order*.

Remark 2.2.7. Note that the intersection of two rings is again a ring. The intersection $O \cap O'$ is also a R-module that is free and finitely generated. By Lemma 2.2.3, there exists a nonzero $r \in R$, such that $rO' \subset O$. We find $rO' \subset O \cap O'$, so we find that $O \cap O'$ spans B. So indeed, as the name suggests, an Eichler order is an order.

For every R-lattice I, we can define its respective left and right order in the following way:

$$O_L(I) = \{\alpha \in B : \alpha I \subset I\}, \quad O_R(I) = \{\alpha \in B : I\alpha \subset I\}.$$

We will now show that these are indeed orders.

Lemma 2.2.8. *Let I be an R-lattice in B. Then, $O_L(I)$ and $O_R(I)$ are orders in B.*

Proof. By Lemma 2.2.3, there is a nonzero $r \in R$ such that $r \in I$. Then we find that I^2 is a lattice as well, since it is finitely generated by the products of generators of I and $rI \subset I^2$. Again, by Lemma 2.2.3, there is a nonzero $s \in R$ such that $sI^2 \subset I$. We find $(sI)I \subset I$, so $sI \subset O_L(I)$. It follows that $O_L(I)$ spans B.

By Lemma 2.2.3, there is a nonzero $t \in R$ such that $tO_L(I) \subset I$, hence $O_L(I) \subset t^{-1}I$. $O_L(I)$ is contained in a finitely generated free R-module, so $O_L(I)$ is torsion free, hence free. In the proof of Lemma 2.2.4, we have seen that this implies that $O_L(I)$ is finitely generated.

Now it is left to check that $O_L(I)$ is a ring. It contains 0 and 1, and for $\alpha, \beta \in O_L(I)$, we have

$$(\alpha + \beta)I \subset \alpha I + \beta I \subset I + I = I;$$
$$(\alpha\beta)I \subset \alpha(\beta I) \subset \alpha I \subset I.$$

The other requirements are easy to check, so we conclude that $O_L(I)$ is an order in B.

The proof for $O_R(I)$ is analogous. □

One important property of orders is that they are integral structures within quaternion algebras.

Proposition 2.2.9. *Any element in an order $O \subset B$ is integral. That is, every element in O is the root of some monic polynomial in $R[x]$.*

Proof. Let $\alpha \in O$. We have $R[\alpha] \subset O$. The R-module $R[\alpha]$ can be embedded in B, so it is torsion free. In the proof of Lemma 2.2.4, we saw that the rank of a torsion free submodule $I \subset J$ is bounded above by the rank of J if J is free as well. So $R[\alpha]$ is finitely generated, and free by the Structure theorem 2.2.2. Then, there exists a smallest $m \in \mathbb{Z}$ such that every element in $R[\alpha]$ is a polynomial in α of degree less than m. We find that $1, \alpha, \ldots, \alpha^{m-1}$ is an R-basis for $R[\alpha]$. Then, $\alpha^m = \sum_{i=0}^{m-1} x_i\alpha^i$ for some choice of $x_i \in R$. It follows that α is integral. □

Every element in B satisfies a monic quadratic polynomial in $F[x]$, where the coefficients are the trace and norm. If the trace and norm of some $\alpha \in B$ are not both in R, then α is not the root of any monic polynomial in $R[x]$. We observe that elements $\alpha \in B$ are integral if and only if $\mathrm{N}(\alpha), \mathrm{tr}(\alpha) \in R$.

Definition 2.2.10. Let I be an R-lattice in B. Then I is called *integral* if $I^2 \subset I$.

On first sight, the definition of an integral lattice has nothing to do with the integrality of its elements. There is, however, a connection between the two.

Lemma 2.2.11. *Let I be an R-lattice in B. The following are equivalent:*

(i) I is integral;

(ii) I is closed under multiplication;

(iii) I is a left ideal of $O_L(I)$;

(iv) I is a right ideal of $O_R(I)$;

(v) $I \subset O_L(I) \cap O_R(I)$.

Proof. (i) ⇔ (ii) is clear. If I is integral, then clearly $I \subset O_L(I)$, and $O_L(I)I = I$. If I is a left ideal of $O_L(I)$, it is clearly closed under multiplication. This gives (i) ⇔ (iii) and a similar argument for $O_R(I)$ gives (i) ⇔ (iv). Then, (i) ⇒ (v) is immediate from combining (iii) and (iv). If I is contained in both $O_L(I)$ and $O_R(I)$, it follows that $O_L(I)I = I$, so I is a left ideal of $O_L(I)$. The last implication (v) ⇒ (i) follows. □

We see that every integral lattice I is an ideal of its left and right order. So by 2.2.9, every element in an integral lattice is integral. Because every integral lattice is an ideal of some order, we will also refer to integral lattices as *integral ideals*. Note that not every ideal of an order is an integral ideal (the zero ideal for instance), despite its elements being integral.

For integral ideals, the following definition makes sense because all its elements are integral.

Definition 2.2.12. The *norm* $\mathrm{N}(I)$ of an integral R-lattice I is defined as $\gcd(\{\mathrm{N}(\alpha) : \alpha \in I\})$.

An order O is an integral lattice, and its norm is 1. For an R-basis β_i, $i = 1, 2, 3, 4$ of O, note that the traces of the products $\mathrm{tr}(\beta_i\beta_j)$ are integers, since $\beta_i\beta_j \in O$.

Definition 2.2.13. Let O be an order in B with R-basis $\beta_1, \beta_2, \beta_3, \beta_4$. The *discriminant* of O with respect to the basis $\beta_1, \beta_2, \beta_3, \beta_4$ is the ideal

$$\mathrm{disc}(O) = (\det(\mathrm{tr}(\beta_i\beta_j))_{i,j=1,2,3,4}) \subset R.$$

Remark 2.2.14. The definition for the discriminant we gave does not depend on the choice for a basis of O [Voi21, Corollary 15.2.7], so we may as well omit "with respect to a basis" and refer to the discriminant of O instead.

We will use discriminants of orders to study how orders sit inside one another. To formalize this, we first introduce the R-index.

Definition 2.2.15. Let I, J be two R-lattices of rank n in an n-dimensional vector space V over F. The *R-index* $[J : I]_R$ is the ideal in R generated by $\{\det f : f \in \mathrm{End}_F(V), f(J) \subset I\}$.

Lemma 2.2.16. *Let $I \subset J$ be two R-lattices of rank n in an n-dimensional vector space V over F. Then $[J : I]_R = R$ if and only if $J = I$.*

Proof. If $J = I$, then we have $\det(\mathrm{id}) = 1 \in [J : I]_R$. Now suppose $[J : I]_R = R$. Then there is an $f : V \to V$ that restricts to $f|_J : J \to J \in \mathrm{End}_R(J)$, such that $\det f \in R^\times$. But then f is also invertible in $\mathrm{End}_R(J)$. In particular f is surjective, so from the inclusions $f(J) \subset I \subset J$, we find that $I = J$. □

We can use R-indices to show that every order is contained in a maximal order. This is a consequence of the following lemma.

Lemma 2.2.17. *Let $O \subset O' \subset B$ be two orders in a quaternion algebra B over F. Then $\mathrm{disc}(O) = [O' : O]_R^2 \mathrm{disc}(O')$. Moreover, $O = O'$ if and only if $\mathrm{disc}(O) = \mathrm{disc}(O')$.*

Proof. Let M a basis transformation matrix from an R-basis of O to an R-basis of O'. By [Voi21, Lemma 9.6.4], $\det(M)$ generates $[O' : O]_R$. And by [Voi21, Lemma 15.2.5], $\mathrm{Disc}(O) = \det(M)^2\mathrm{disc}(O')$. We find that $\mathrm{Disc}(O) = [O' : O]^2\mathrm{Disc}(O')$. By Lemma 2.2.16, we have that $\mathrm{Disc}(O) = \mathrm{Disc}(O')$ if and only if $O = O'$. □

Corollary 2.2.18. *Every order O is contained in a maximal order.*

Proof. Suppose we have a chain of orders

$$O \subsetneq O_1 \subsetneq O_2 \subsetneq \dots.$$

Then by 2.2.17, we have a chain

$$\mathrm{disc}(O) \subsetneq \mathrm{disc}(O_1) \subsetneq \mathrm{disc}(O_2) \subsetneq \dots.$$

And since R is a principal ideal domain, it is in particular noetherian, so this chain must terminate. As a consequence, the chain of orders must also terminate, hence O is contained in a maximal order. □

2.3 Statement of the problem

Now that the basic definitions and properties of quaternion algebras and lattices have been established, we are ready to state the central problem of this paper.

Problem 2.3.1. Let $B = (a, b \mid \mathbb{Q})$ be a quaternion algebra for some $a, b \in \mathbb{Z}_{<0}$, let J be an integral lattice in B and let $r \in \mathbb{Z}$, $n \in \mathbb{Z}_{>1}$.

What is

$$\lim_{X\to\infty} \frac{\#\{\alpha \in J : \mathrm{N}(\alpha) \leq X, \mathrm{N}(\alpha) \equiv r \pmod n\}}{\#\{\alpha \in J : \mathrm{N}(\alpha) \leq X\}}? \tag{2.3.2}$$

This problem is inspired by Castryck [Cas+24, Conjecture 6], and has applications in cryptography (see section 5).

Remark 2.3.3. The following diagram commutes.

$$\begin{array}{ccc} J & \xrightarrow{\mathrm{N}} & \mathbb{Z} \\ \downarrow & & \downarrow \\ J/nJ & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array} \tag{2.3.4}$$

The vertical maps are reduction maps and the lower horizontal map is $\alpha \pmod{nJ} \mapsto N(\alpha) \pmod n$. We show this map is well defined. Note that with respect to some $\mathbb{Z}$-basis β_i, $i = 1, 2, 3, 4$ for J, the norm $\mathrm{N}(x_1\beta_1 + x_2\beta_2 + x_3\beta_3 + x_4\beta_4)$ is a homogeneous quadratic polynomial in x_1, x_2, x_3, x_4. The coefficient of x_ix_j is given as $\beta_i\overline{\beta_j} + \beta_j\overline{\beta_i} = \mathrm{N}(\beta_i + \beta_j) - \mathrm{N}(\beta_i) - \mathrm{N}(\beta_j)$ if $i \neq j$ and the coefficient of x_i^2 is $\mathrm{N}(\beta_i)$. All coefficients are integers, so the quadratic form associated to N with respect to the basis β_i reduces to a well defined map modulo n. We will also refer to the map norm map $J/nJ \to \mathbb{Z}/n\mathbb{Z}$ as N.

Lemma 2.3.5. *Limit 2.3.2 exists and is equal to* $\#\{\alpha \in J/nJ : N(\alpha) \equiv r \ (mod\ n)\}/\#(J/nJ)$.

Proof. Let $M(X) = \{\alpha \in J : \sqrt{\mathrm{N}(\alpha)} \leq X\}$, $S_{r,n} = \{\alpha \in J/nJ : \mathrm{N}(\alpha) \equiv r \pmod n\}$ and let $A_{r,n}(X) = \{\alpha \in J : \sqrt{\mathrm{N}(\alpha)} \leq X, \mathrm{N}(\alpha) \equiv r \pmod n\}$.

We first show that $M(X)$ is finite for every X. We have chosen $a, b \in \mathbb{Z}_{<0}$, and the norm of elements in B is given as

$$N(t + xi + yj + zij) = t^2 - ax^2 - by^2 + abz^2.$$

It follows that every element has nonnegative norm. This actually induces a metric on B if we define the distance between α and β as $\sqrt{\mathrm{N}(\alpha - \beta)}$. We embed B into $\mathbb{R}^4$ via $t+xi+yj+zij \mapsto (t, x, y, z)$, and the metric on B extends to a metric on $\mathbb{R}^4$ via $(t, x, y, z) \mapsto \sqrt{t^2 - ax^2 - by^2 + abz^2}$. This metric on $\mathbb{R}^4$ induces the Euclidean topology on $\mathbb{R}^4$, but note that the metric is not the standard metric. It is obtained by scaling coordinates by a nonzero factor. The reason we embed B into $\mathbb{R}^4$ is so we can talk about volumes.

Let β_i, $i = 1, 2, 3, 4$ be a $\mathbb{Z}$-basis for J. This basis spans a parallelepiped P with side lengths $\sqrt{\mathrm{N}(\beta_i)}$ and finite volume V. We can translate P along the basis vectors to identify each point $x = \sum_{i=1}^4 x_i\beta_i \in J$ with the parallelepiped P_x obtained from $P \mapsto P + x$. Then all these P_x cover $\mathbb{R}^4$ in such a way that $P_x \cup \{x\} = \{x\}$ and $\mathrm{Vol}(P_x \cap P_y) = 0$ whenever $x \neq y$. So the points in J can be identified with parallelepipeds P_x.

Let $D_r(\alpha) \subset \mathbb{R}^4$ be the closed ball of radius r around α. The set $M(X)$ is contained in $D_r(0)$ for some $r > 0$. Therefore, $M(X)$ is contained in a set with finite volume. But then it follows that $M(X)$ can only contain finitely many parallelepipeds P_x, hence $M(X)$ is finite.

Now let $Q(X) = \bigcup_{x\in M(X)} P_x$. Then there is a fixed constant d such that for every sufficiently large X, we have $D_{X-d}(0) \subset Q(X) \subset D_{X+d}(0)$. We have $\mathrm{Vol}(Q(X)) = \#M(X)V$, and since the volume $D_r(0)$ is proportional to r^4, there is a constant $c > 0$ such that

$$\mathrm{Vol}(D_{X-d}(0)) = c(X - d)^4 \leq \#M(X)V \leq c(X + d)^4 = \mathrm{Vol}(D_{X+d}(0)).$$

Now let

$$R_x = \bigcup_{x_1,x_2,x_3,x_4 \in \{0,\dots,n-1\}} P_{x+x_1\beta_1+x_2\beta+x_3\beta_3+x_4\beta_4}.$$

Then $\bigcup_{x\in J} R_{nx}$ covers $\mathbb{R}^4$ in such a way that $\mathrm{Vol}(R_{nx} \cap R_{ny}) = 0$ whenever $x \neq y$, and for every $\alpha \in J/nJ$, there is a $\beta \in R_{nx}$ that reduces to α. And since $\mathrm{Vol}(R_{nx}) = n^4V = \#(J/nJ)V$, we may even identify R_{nx} with a set of unique representatives for each class in J/nJ. From Remark 2.3.3, we find that for sufficiently large X, we have $\#(A_{r,n}(X) \cap R_{nx}) = \#S_{r,n}$. Using a similar argument for imposing bounds, we find that there is a fixed e such that for sufficiently large X, we have

$$\mathrm{Vol}(D_{X-e}(0)) = c(X-e)^4 \leq \#A_{r,n}(X)V\frac{n^4}{\#S_{r,n}} \leq c(X+e)^4 \leq \mathrm{Vol}(D_{X-e}(0)).$$

We can combine the two bounds into

$$\frac{c(X-e)^4}{c(X+d)^4}\frac{\#S_{r,n}}{n^4} \leq \frac{\#A_{r,n}(X)V}{\#M(X)V} \leq \frac{c(X+e)^4}{c(X-d)^4}\frac{\#S_{r,n}}{n^4}$$

As we let $X \to \infty$, we find by the squeeze theorem that the limit of 2.3.2 exists and is equal to $\#S_{r,n}/n^4 = \#S_{r,n}/\#(J/nJ)$. □

So not only did we find that the limit 2.3.2 exists, but we can determine the limit 2.3.2 from studying the norm map $J/nJ \to \mathbb{Z}/n\mathbb{Z}$ between finite sets.

We may think of the limit in 2.3.2 as the probability that a randomly sampled element in an integral ideal J has a norm congruent to $r \pmod n$. For that reason, we will refer to the value of this limit as $\mathbb{P}_{r,n}$. Note that the choice of J is not clear from the notation $\mathbb{P}_{r,n}$, so we have to keep in mind that we first have to choose an integral ideal before we can talk about probabilities $\mathbb{P}_{r,n}$.

Lemma 2.3.6. *Let p and q be coprime integers and let $n = pq$. The probabilities satisfy $\mathbb{P}_{r,p}\mathbb{P}_{r,q} = \mathbb{P}_{r,n}$ for all $r \in \mathbb{Z}$.*

Proof. By the Chinese remainder theorem and Remark 2.3.3, we have

$$\begin{aligned}
\mathbb{P}_{r,n} &= \frac{\#\{\alpha \in J/nJ : \mathrm{N}(\alpha) \equiv r \pmod n\}}{\#(J/nJ)}; \\
&= \frac{\#\{(\alpha,\alpha') \in (J/pJ) \oplus (J/qJ) : \mathrm{N}(\alpha) \equiv r \pmod p, \mathrm{N}(\alpha') \equiv r \pmod q\}}{\#((J/pJ) \oplus (J/qJ))}; \\
&= \frac{\#\{\alpha \in J/pJ : \mathrm{N}(\alpha) \equiv r \pmod p\} \cdot \#\{\alpha \in J/qJ : \mathrm{N}(\alpha) \equiv r \pmod q\}}{\#(J/pJ) \cdot \#(J/qJ)}; \\
&= \mathbb{P}_{r,p}\mathbb{P}_{r,q}.
\end{aligned}$$

□

It follows from the prime factorization that problem 2.3.2 can easily be solved once the probabilities $\mathbb{P}_{r,p^k}$ are known for primes p and positive integers k. Our main focus will therefore be to solve problem 2.3.2 whenever n is a prime power.

3 Completions

In this section, we look at completions of $\mathbb{Q}$. We use Voight as our main reference [Voi21].

3.1 Construction

Completions can be constructed with respect to an absolute value.

Definition 3.1.1. Let F be a field. An *absolute value* is a map $|\ |: F \to \mathbb{R}_{\geq 0}$ such that

(i) $|x| = 0$ if and only if $x = 0$;

(ii) $|xy| = |x||y|$ for all $x, y \in F$;

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

For $F = \mathbb{Q}$, we have the well known absolute value that multiplies each element by its sign. We will denote this absolute value as $|\ |_\infty$. Apart from this absolute value, there exist other absolute values on $\mathbb{Q}$.

Note that every $x \in \mathbb{Q}^\times$ can be uniquely written as $x = p^k \frac{a}{b}$, where p is a prime and $k, a, b \in \mathbb{Z}$ such that a and b are coprime with each other and with p.

Definition 3.1.2. Let p be a prime number. The *p-adic valution* on $\mathbb{Q}$ is the map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined as

$$p^k \frac{a}{b} \mapsto k; \quad 0 \mapsto \infty$$

where a and b are coprime with each other and with p.

We can now define the *p-adic absolute value* $|\ |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as $|x|_p = p^{-v_p(x)}$, with the convention $p^{-\infty} = 0$, such that $|0|_p = 0$.

Lemma 3.1.3. *The p-adic absolute value is an absolute value.*

Proof. We check the conditions of 3.1.2. For any $x \in \mathbb{Q}^\times$, $p^{-v_p(x)} > 0$ and $|0|_p = 0$ by definition, so (i) holds.

Let $x = p^k \frac{a}{b}, y = p^l \frac{c}{d} \in \mathbb{Q}^\times$ be the unique representations of x and y. We have that $|xy|_p = |p^{k+l} \frac{ac}{bd}|_p = p^{-k-l} = |x||y|$, and condition (ii) clearly holds if x or y is zero.

Let $k \geq l$ without loss of generality. Then $|x + y|_p = |p^k(\frac{a}{b} + p^{l-k} \frac{c}{d})|_p \leq p^{-k} = |x|_p$. It follows that $|x + y|_p \leq \sup\{|x|_p, |y|_p\}$, so in particular, $|x + y|_p \leq |x|_p + |y|_p$. □

An absolute value that satisfies the stronger inequality $|x + y|_p \leq \sup\{|x|_p, |y|_p\}$ is called *nonarchimedean*. So for every prime p, the absolute value $|\ |_p$ is nonarchimedean, while $|\ |_\infty$ is archimedean (that is, not nonarchimedean).

The sets $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are the respective completions of $\mathbb{Q}$ and $\mathbb{Z}$ with respect to $|\ |_p$. That is, $\mathbb{Q}_p$ ($\mathbb{Z}_p$ respectively) is the smallest set such that every Cauchy sequence of elements in $\mathbb{Q}$ ($\mathbb{Z}$ respectively) converges in $\mathbb{Q}_p$ ($\mathbb{Z}_p$ respectively). The completions of $\mathbb{Q}$ and $\mathbb{Z}$ with respect to $|\ |_\infty$ are $\mathbb{R}$ and $\mathbb{Z}$, respectively.

We list a few properties of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ that are proven in [Neu13, Chapter II]. Elements in $\mathbb{Q}_p$ can be uniquely represented as Laurent series in p with coefficients in $\{0, \ldots, p-1\}$, so we have

$$\mathbb{Q}_p = \left\{ \sum_{i \geq k} a_i p^i : k \in \mathbb{Z}, a_i \in \{0, 1, \ldots, p-1\} \right\}.$$

The usual addition and multiplication rules of Laurent series make $\mathbb{Q}_p$ into a field of characteristic 0. The valuation v_p extends to $\mathbb{Q}_p$ as follows:

$$v_p\left(\sum_{i\geq k} a_i p^i\right) = \min\{i \in \mathbb{Z}_{\geq k} : a_i \neq 0\}.$$

With this new valuation, $|\ |_p$ extends to an absolute value on $\mathbb{Q}_p$. The completion of $\mathbb{Z}$ is then a ring

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\} = \left\{\sum_{i\geq 0} a_i p^i : a_i \in \{0, 1, \ldots, p-1\}\right\}.$$

Furthermore, $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. From these properties, we will show that $\mathbb{Z}_p$ is a *local ring*, meaning that it has a unique maximal ideal.

Lemma 3.1.4. *The ring $\mathbb{Z}_p$ has a unique maximal ideal (p), and every ideal is either 0 or of the form (p^k) for some $k \in \mathbb{Z}_{\geq 0}$.*

Proof. Note that an element in $\mathbb{Z}_p$ is invertible if and only if its p-adic absolute value is equal to 1 by the multiplicativity of $|\ |_p$. Every nonzero $\alpha \in \mathbb{Z}_p$ can then be written as $\alpha = p^k\alpha'$ for some $\alpha' \in \mathbb{Z}_p^\times$ and some $k \in \mathbb{Z}_{\geq 0}$. It follows that $(\alpha) = p^k\alpha'\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p \leq |\alpha|_p\} = (p^k)$. In particular, $(p) = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$, so that is the unique maximal ideal of $\mathbb{Z}_p$.

Note that if $I \subset \mathbb{Z}_p$ is a nonzero ideal with $m = \min\{v_p(\alpha) : \alpha \in I\}$, we find the expression $I = \{x \in \mathbb{Z}_p : |x|_p \leq p^{-m}\} = (p^m)$, which proves the statement. □

In particular, we find that $\mathbb{Z}_p$ is a principal ideal domain.

Note that the quotients $\mathbb{Z}_p/p^k\mathbb{Z}_p$ are isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. This is clear from the representation of $\mathbb{Z}_p$ as series in p. This observation allows us to talk about reduction maps in another way. Instead of directly reducing integers modulo p^k, we can first embed them into $\mathbb{Z}_p$ and then reduce modulo p^k. This turns out to be a useful observation in the context of integral structures in quaternion algebras.

Another useful property of the p-adic integers becomes clear when we consider the following Lemma.

Lemma 3.1.5 (Hensel)**.** *Let $f \in \mathbb{Z}_p[x]$ be a polynomial and let $a \in \mathbb{Z}_p$ be a p-adic integer such that $f(a) \equiv 0 \pmod p$ and $f'(a) \not\equiv 0 \pmod p$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \pmod p$ and $f(\alpha) = 0$.*

Proof. Let $a, b \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \pmod{p^k}$, $f'(a) \not\equiv 0 \pmod p$ and $a \equiv b \pmod{p^k}$. The Taylor expansion of f around a is $f(x) = f(a) + (x-a)f'(a) + (x-a)^2 g(x)$, for some $g \in \mathbb{Z}_p[x]$. We have $f(b) \equiv tp^k + t'p^k f'(a) + t''p^{2k} \pmod{p^{k+1}}$ for some integers t, t', t''. Note that t is fixed by a up to multiple of p^k, while t' is determined by b. We find that $f(b) \equiv 0 \pmod{p^{k+1}}$ if and only if $t + t'f'(a) \equiv 0 \pmod p$. There is a unique solution for t' modulo p, namely $t' \equiv -t \cdot f'(a)^{-1} \pmod p$. We find that there exist elements $b \in \mathbb{Z}_p$ such that $f(b) \equiv 0 \pmod{p^{k+1}}$, $f'(b) \not\equiv 0 \pmod p$ and $b \equiv a \pmod{p^k}$, such that every b with these properties reduces to the same element modulo p^{k+1}.

We have somehow "lifted" a solution a in $\mathbb{Z}/p^k\mathbb{Z}$ to a unique solution b in $\mathbb{Z}/p^{k+1}\mathbb{Z}$. We can inductively repeat this "lifting" argument to find that there exists a unique root $\alpha \in \mathbb{Z}_p$ of f, such that $\alpha \equiv a \pmod p$. □

The p-adic integers contain the integers $\mathbb{Z}$, so we can apply Hensel's Lemma for polynomials in $\mathbb{Z}[x]$ as well. This gives us a tool to find whether polynomials with integer coefficients have p-adic solutions.

3.2 Local quaternion algebras

In this subsection, we explore properties of quaternion algebras over fields $\mathbb{Q}_p$.

We will call quaternion algebras B over $\mathbb{Q}_p$ and the lattices and orders inside B local. The lattices and orders in quaternion algebras over $\mathbb{Q}$ global.

Lemma 3.2.1. *Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion algebra with $a, b \in \mathbb{Q}^\times$. Then, $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a quaternion algebra over $\mathbb{Q}_p$ and $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}$ is a quaternion algebra over $\mathbb{R}$.*

Proof. The elements $1 \otimes 1$, $i \otimes 1$, $j \otimes 1$, $ij \otimes 1$ form a basis for B_p as a $\mathbb{Q}_p$-vector space, and B_p contains a copy of $\mathbb{Q}_p$ via the embedding $x \mapsto 1 \otimes x$. With multiplication $(a \otimes b)(c \otimes d) = ac \otimes bd$, B_p becomes a ring. We have

$$(i \otimes 1)^2 = a \otimes 1, \quad (j \otimes 1)^2 = b \otimes 1, \quad (i \otimes 1)(j \otimes 1) = ij \otimes 1 = -ji \otimes 1 = -(j \otimes 1)(i \otimes 1),$$

so B_p is a quaternion algebra. The proof for B_∞ is analogous. □

The norm on B_p is induced by $\alpha \otimes m \mapsto \mathrm{N}(\alpha)m^2$, where N is the norm on B.

It turns out that quaternion algebras can be classified into two kinds. A quaternion is either a matrix ring or a division algebra.

Proposition 3.2.2. *Let $B = (a, b \mid F)$ be a quaternion algebra with char$(F) \neq 2$. The following are equivalent:*

(i) $B \cong M_2(F)$;

(ii) B is not a division ring;

(iii) There is a nonzero $\alpha \in B$ such that $N(\alpha) = 0$;

(iv) There exist $x, y \in F$ such that $1 = ax^2 + by^2$.

Proof. The proof uses properties of quadratic forms. For the full proof, see Voight [Voi21, Main Theorem 5.4.4]. □

When B satisfies one of the equivalent criteria of Proposition 3.2.2, we call B *split*. It becomes immediately clear that the quaternion algebras $B = (a, b \mid \mathbb{Q})$ with $a, b \in \mathbb{Z}_{<0}$ and the corresponding B_∞ are division algebras, since $ax^2 + by^2 = 1$ has no solutions over $\mathbb{Q}$ or $\mathbb{R}$.

Definition 3.2.3. Let B be a quaternion algebra over $\mathbb{Q}$. We call B *ramified* at p if B_p is a division algebra.

By Proposition 3.2.2, a quaternion algebra B_p is either split or ramified.

Lemma 3.2.4. *Let $B = (a, b \mid \mathbb{Q})$ be a quaternion algebra. There are only finitely many primes p where B is ramified.*

Proof. Consider the equation $ax^2 + by^2 = 1$. We will show that this equation has solutions over $\mathbb{Q}_p$ for all but finitely many primes p. Let $p \nmid 2ab$. Then a, b are units in $\mathbb{F}_p$. The equation reduces to $ax^2 \equiv 1 - by^2 \pmod{p}$. As we let x and y run over all elements in $\mathbb{F}_p$, ax^2 takes on $(p+1)/2$ values and so does $1 - by^2$. If both sides of the equation would not agree on at least one value, there would have to be at least $p + 1$ elements in $\mathbb{F}_p$; a contradiction. We conclude that $ax^2 + by^2 \equiv 1 \pmod{p}$ has solutions when $p \nmid 2ab$.

Note that any solution $(x, y) \in \mathbb{F}_p^2$ is not $(0, 0)$. It follows that at least one of $2ax, 2by$ is a unit in $\mathbb{F}_p$. Let (x', y') be a solution. We can apply Hensel's Lemma to either $f(x) = ax^2 + by'^2 - 1$ evaluated at x' or to $g(y) = ax'^2 + by^2 - 1$ evaluated at y'. We find that there exists a p-adic solution to $ax^2 + by^2 = 1$. Since the constraint $p \nmid 2ab$ only excludes finitely many primes p, the result follows. □

As a result of this Lemma, the following definition is well defined.

Definition 3.2.5. Let B be a quaternion algebra over $\mathbb{Q}$, and let $\mathrm{ram}(B)$ be the set of primes where B ramifies. The *discriminant* of B is

$$\mathrm{disc}(B) = \prod_{p \in \mathrm{ram}(B)} p.$$

Remark 3.2.6. The set $\mathrm{ram}(B)$ is never empty if B_∞ is a division algebra. This is a consequence of Hilbert reciprocity [Voi21, Proposition 14.2.1]. For the quaternion algebras we consider for Problem 2.3.2, we have $\mathrm{disc}(B) > 1$.

When B_p is split, we have an explicit isomorphism $B_p \cong M_2(\mathbb{Q}_p)$. The norm map on $M_2(\mathbb{Q}_p)$ is the determinant map by Example 2.1.9. We would like another explicit isomorphism for B_p when B is ramified at p.

Definition 3.2.7. Let α be a root of a monic irreducible polynomial in $\mathbb{Z}_p[x]$. We call the extension $\mathbb{Q}_p(\alpha) \supset \mathbb{Q}_p$ *unramified* if $p\mathbb{Z}_p[\alpha]$ is the unique maximal ideal in $\mathbb{Z}_p[\alpha]$.

Voight gives a more general definition of unramified extensions [Voi21, 13.2.3], but the definition above is sufficient for our purpose. We only need to find an explicit separable quadratic unramified extension of $\mathbb{Q}_p$.

If $L \supset K$ is a Galois extension, we define the *field norm* as

$$\mathrm{N}_{L/K}(\alpha) := \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Lemma 3.2.8. *For p odd, let $u \in \mathbb{Z}_p$ such that $u \in \mathbb{F}_p$ is a (nonzero) quadratic nonresidue. Then $\mathbb{Q}_p(\sqrt{u})$ is a separable unramified extension. Furthermore, if α is a root of $x^2 + x + 1 \in \mathbb{Z}_2[x]$, then $\mathbb{Q}_2(\alpha)$ is a separable unramified extension.*

Proof. Let $p \neq 2$ and u as described. Since the equation $x^2 - u$ has no solutions in $\mathbb{F}_p$, it has no solutions in $\mathbb{Q}_p$ either. The extension is clearly separable and normal, hence Galois, so every element $a + b\sqrt{u} \in \mathbb{Q}_p(\sqrt{u})$ has field norm

$$\mathrm{N}_{\mathbb{Q}_p(\sqrt{u})/\mathbb{Q}_p}(a + b\sqrt{u}) = a^2 - ub^2,$$

and field norms are multiplicative. If we have $a, b \in \mathbb{Z}_p$, then

$$|\mathrm{N}_{\mathbb{Q}_p(\sqrt{u})/\mathbb{Q}_p}(a + b\sqrt{u})|_p \leq \max\{|a^2|_p, |b^2|_p\} \leq 1.$$

By the multiplicativity of $|\ |_p$ and the field norm, for units in $\mathbb{Z}[\sqrt{u}]$, we must have equalities in the equations above. On the other hand, if $|a^2 - ub^2|_p = 1$, the element $a + b\sqrt{u}$ has inverse

$$(a + b\sqrt{u})^{-1} = (a - b\sqrt{u}) \cdot (a^2 - ub^2)^{-1}.$$

We find

$$\mathbb{Z}_p[\sqrt{u}]^\times = \{a + b\sqrt{u} \in \mathbb{Z}_p[\sqrt{u}] : |\mathrm{N}_{\mathbb{Q}_p(\sqrt{u})/\mathbb{Q}_p}(a + b\sqrt{u})|_p = 1\}.$$

Every element $a + b\sqrt{u} \in \mathbb{Z}_p[\sqrt{u}]$ with $|a^2 - ub^2|_p < 1$ satisfies $a^2 \equiv ub^2 \pmod{p}$. Since u is a quadratic nonresidue, equality only holds if $a \equiv b \equiv 0 \pmod{p}$, and then $a + b\sqrt{u}$ is a multiple of p. We find $\mathbb{Z}_p[\sqrt{u}] \setminus \mathbb{Z}_p[\sqrt{u}]^\times = (p)$, so (p) is the unique maximal ideal.

For $\mathbb{Q}_2(\alpha)$, note that $x^2 + x + 1$ has no solutions over $\mathbb{F}_2$, and therefore no solutions in $\mathbb{Q}_2$ either. Note that if α is a root, then so is $-(\alpha+1)$. The extension is thus separable and normal, so we have field norm

$$N_{\mathbb{Q}_2(\alpha)/\mathbb{Q}_2}(a + b\alpha) = a^2 + ab(\alpha - (\alpha + 1)) - b^2\alpha(\alpha + 1) = a^2 - ab + b^2.$$

The rest of the proof is analogous to the case of $\mathbb{Q}_p(\sqrt{u})$, only with inverse

$$(a+b\alpha)^{-1} = (a-b\alpha-b)\cdot(a^2-ab+b^2)^{-1}.$$

Direct verification yields that $a^2-ab+b^2 \equiv 0 \pmod 2$ if and only if a and b are both multiples of 2. The result follows. □

An important result is the following.

Theorem 3.2.9. *Let B be a quaternion algebra over $\mathbb{Q}$ that is ramified at p. There is a unique quadratic unramified separable extension of $\mathbb{Q}_p$ up to isomorphism, which we will denote as $\mathbb{Q}_q$. Furthermore, we have that*

$$B_p \cong \left(\frac{\mathbb{Q}_q, p}{\mathbb{Q}_p}\right),$$

is a division algebra. The notation $(\mathbb{Q}_q, p \mid \mathbb{Q}_p)$ refers to a quaternion algebra that contains $\mathbb{Q}_q$ and has an element j such that $j^2 = p$.

Proof. For the proof, we refer to Voight. The proof uses a classification of division algebras via extensions of valuations [Voi21, Theorem 13.3.11(a)]. □

We can find explicit quaternion algebras over $\mathbb{Q}_p$ that contain $\mathbb{Q}_q$. For $p=2$, let α be a root of $x^2+x+1 \in \mathbb{Z}_2[x]$, and for p odd, let α be a root of $x^2-u \in \mathbb{Z}_p[x]$ for a quadratic nonresidue $u \in \mathbb{F}_p$. Let $\overline{\alpha} = -\alpha$ for p odd and $\overline{\alpha} = -\alpha - 1$ for $p = 2$. Then, it can be checked that

$$\left\{ \begin{pmatrix} a+b\alpha & p(c+d\alpha) \\ c+d\overline{\alpha} & a+b\overline{\alpha} \end{pmatrix} : a,b,c,d \in \mathbb{Q}_p \right\} \subset M_2(\mathbb{Q}_2(\alpha)) \tag{3.2.10}$$

is a quaternion algebra over $\mathbb{Q}_p$ that satisfies the criteria. The traces and norms of elements in this quaternion algebra correspond to the traces and determinants of the matrices.

As a consequence, we now have an explicit way of computing norms in division algebras $(\mathbb{Q}_q, p \mid \mathbb{Q}_p)$. We have

$$\mathrm{N}\left(\begin{pmatrix} a+b\alpha & p(c+d\alpha) \\ c+d\overline{\alpha} & a+b\overline{\alpha} \end{pmatrix}\right) = \mathrm{N}_{\mathbb{Q}_q|\mathbb{Q}_p}(a+b\alpha) - p\mathrm{N}_{\mathbb{Q}_q|\mathbb{Q}_p}(c+d\alpha). \tag{3.2.11}$$

3.3 Local orders

Now that we have a basic understanding of the quaternion algebras B_p, we can look at lattices inside B_p. First, we consider the case where B_p is split.

Proposition 3.3.1. *Let $B_p \cong M_2(\mathbb{Q}_p)$. Every maximal order $O \subset B_p$ is conjugate to $M_2(\mathbb{Z}_p)$. In particular, $O \cong M_2(\mathbb{Z}_p)$ as $\mathbb{Z}_p$-modules.*

Proof. Let A_{ij} denote the matrix in $M_2(\mathbb{Z}_p)$ with a 1 on the entry in row i and column j, with zeroes everywhere else. The ring $M_2(\mathbb{Z}_p)$ is clearly an order, since it is generated as a $\mathbb{Z}_p$-module by the matrices A_{ij}, and B_p is generated by A_{ij} as a vector space over $\mathbb{Q}_p$.

We will now show that $M_2(\mathbb{Z}_p)$ is a maximal order. Suppose that $M_2(\mathbb{Z}_p)$ is contained in another order O'. Orders can only contain integral elements by Lemma 2.2.9. Let A be a matrix with entries $a,b,c,d \in \mathbb{Q}_p$, then the traces of the matrices $A_{ij}A \in O'$ are precisely a,b,c,d, so we find that $a,b,c,d \in \mathbb{Z}_p$. We conclude $M_2(\mathbb{Z}_p) = O'$, so $M_2(\mathbb{Z}_p)$ is maximal.

Let N be a lattice in $\mathbb{Q}_p^2$ and let O be a maximal order in $M_2(\mathbb{Q}_p)$. Then the set $M = \{n \in N : On \subset N\}$ is a finitely generated $\mathbb{Z}_p$-submodule of N. By Lemma 2.2.3, there is a nonzero $r \in \mathbb{Z}_p$ such that $rON \subset N$, since ON is finitely generated. We find that $rON \subset M$, so $rN \subset M$ holds as well. We find that M is a lattice in $\mathbb{Q}_p^2$.

Let $L \subset \mathbb{Q}_p^2$ be the lattice with basis $(1,0),(0,1)$. Note that $M_2(\mathbb{Z}_p) = \mathrm{End}_{\mathbb{Z}_p}(L)$. Then $\mathrm{End}_{\mathbb{Z}_p}(M) = gM_2(\mathbb{Z}_p)g^{-1}$, for some $g \in M_2(\mathbb{Q}_p)^\times$, as we can obtain $\mathrm{End}_{\mathbb{Z}_p}(M)$ from $\mathrm{End}_{\mathbb{Z}_p}(L) = M_2(\mathbb{Z}_p)$ via a basis transformation of $\mathbb{Q}_p^2$. We find that $\mathrm{End}_{\mathbb{Z}_p}(M)$ is an order that contains O. And by the maximality of O, we have an equality. Now, we find that $O = \mathrm{End}_{\mathbb{Z}_p}(M) = gM_2(\mathbb{Z}_p)g^{-1}$. A change of basis does not change the $\mathbb{Z}_p$-module structure, so $O \cong M_2(\mathbb{Z}_p)$. □

The fact that every maximal order in $M_2(\mathbb{Q}_p)$ is conjugate to $M_2(\mathbb{Z}_p)$ also enables us to find explicit isomorphisms for intersections of maximal orders.

Proposition 3.3.2. *Every Eichler order $O \subset M_2(\mathbb{Q}_p)$ is conjugate to*

$$E_m := \left\{ \begin{pmatrix} a & b \\ cp^m & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}_p \right\},$$

for some $m \in \mathbb{Z}_{\geq 0}$. In particular, $O \cong E_m$ as $\mathbb{Z}_p$-modules.

Proof. Let $O = A \cap B$, for A, B maximal orders. And since conjugation of $M_2(\mathbb{Z}_p)$ only corresponds to a change of basis, we may assume without loss of generality that $A = M_2(\mathbb{Z}_p)$ and $B = gM_2(\mathbb{Z}_p)g^{-1}$ for some invertible $g \in M_2(\mathbb{Q}_p)$. We know that $g = p^k\alpha$ for some $\alpha \in M_2(\mathbb{Z}_p) \setminus pM_2(\mathbb{Z}_p)$ and some $k \in \mathbb{Z}$. We find $B = \alpha p^k M_2(\mathbb{Z}_p) p^{-k}\alpha^{-1} = \alpha M_2(\mathbb{Z}_p)\alpha^{-1}$. There exist $\beta, \gamma \in M_2(\mathbb{Z}_p)^\times$ such that

$$\beta\alpha\gamma = \begin{pmatrix} p^n & 0 \\ 0 & p^{n+m} \end{pmatrix},$$

for some $n, m \in \mathbb{Z}_{\geq 0}$. This follows from the fact that α is invertible in $M_2(\mathbb{Q}_p)$, along with the existence of the Smith normal form [Jac12, Theorem 3.8]. Now we have

$$\beta O\beta^{-1} = \beta M_2(\mathbb{Z}_p)\beta^{-1} \cap \beta\alpha M_2(\mathbb{Z}_p)\alpha^{-1}\beta^{-1} = M_2(\mathbb{Z}_p) \cap \beta\alpha(\gamma M_2(\mathbb{Z}_p)\gamma^{-1})\alpha^{-1}\beta^{-1}.$$

And

$$\begin{aligned} \beta\alpha(\gamma M_2(\mathbb{Z}_p)\gamma^{-1})\alpha^{-1}\beta^{-1} &= \begin{pmatrix} p^n & 0 \\ 0 & p^{n+m} \end{pmatrix} \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \begin{pmatrix} p^{-n} & 0 \\ 0 & p^{-n-m} \end{pmatrix}; \\ &= \begin{pmatrix} \mathbb{Z}_p & p^{-m}\mathbb{Z}_p \\ p^m\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}. \end{aligned}$$

We find $\beta O\beta^{-1} = E_m$, so O and E_m are conjugated. And since a change of basis does not change the $\mathbb{Z}_p$-module structure, we find that they are isomorphic as $\mathbb{Z}_p$-modules. □

Let A_{ij} denote the matrices with a 1 on row i, column j and zeroes everywhere. Then $A_{11}, A_{12}, p^m A_{21}, A_{22}$ forms a $\mathbb{Z}_p$-basis for E_m. An explicit computation gives $\mathrm{disc}(E_m) = (p^{2m})$. Let $O = gE_m g^{-1}$, then by the identity $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for traces of matrices A, B, we find that $\mathrm{disc}(O) = \mathrm{disc}(E_m)$. So if $O = gE_m g^{-1} = hE_n h^{-1}$, then $m = n$. An Eichler order can thus be associated with a unique standard Eichler order E_m.

The integer p^m that shows up in the bottom left entry in E_m is called the *level* of an Eichler order in $M_2(\mathbb{Q}_p)$. An order $O \subset M_2(\mathbb{Q}_p)$ is then maximal if and only if the level of O is 1, since O is conjugate to $M_2(\mathbb{Z}_p) = E_0$.

Now, let B_p be a quaternion division algebra over $\mathbb{Q}_p$. By Theorem 3.2.9, $B_p \cong (\mathbb{Q}_q, p \mid \mathbb{Q}_p)$. Again, we will classify all Eichler orders in B_p.

Proposition 3.3.3. *Let B_p be a division quaternion algebra over $\mathbb{Q}_p$. The set of all integral elements in B_p is an order.*

Proof. Let $\alpha \in \mathbb{Q}_q$ and $a, b, c, d \in \mathbb{Q}_p$ as in 3.2.10 and 3.2.11. Let A be the matrix of the form in 3.2.10 induced by a, b, c, d. If we choose $a, b, c, d \in \mathbb{Z}_p$, then we find $\mathrm{N}(A) \in \mathbb{Z}_p$ and $\mathrm{tr}(A) \in \mathbb{Z}_p$.

Let $a, b \in \mathbb{Q}_p^\times$ with $v_p(a) = m$, $v_p(b) = n$ and assume without loss of generality that $m \geq n$. We find $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha) = p^{2n}\mathrm{N}_{\mathbb{Q}_p/\mathbb{Q}_p}(p^{-n}a + p^{-n}b\alpha)$. If $m > n$ holds, then $v_p(p^{-n}a) > 0$, $v_p(p^{-n}b) = 0$, so we find $v_p(\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha)) = 2n$. If equality $m = n$ holds, we have $v_p(p^{-n}a) = v_p(p^{-n}b) = 0$, so $p^{-n}a, p^{-n}b \in \mathbb{Z}_p^\times$. As we have seen in the proof of Lemma 3.2.8, the field norm on $a+b\alpha$ with $a, b \in \mathbb{Z}_p$ is a multiple of p if and only if a and b are. We find $v_p(\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha)) = 2\min\{v_p(a), v_p(b)\}$.

Now, let $\mathrm{N}(A), \mathrm{tr}(A) \in \mathbb{Z}_p$. Then, $\mathrm{N}(A) = \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha) - p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha) \in \mathbb{Z}_p$. Suppose one of a, b, c, d is in $\mathbb{Q}_p \setminus \mathbb{Z}_p$. Then $\min\{v_p(\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha)), v_p(p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha))\} < 0$. Also note that $v_p(\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha)) \neq v_p(p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha))$, since one is always odd, the other even. It follows that $v_p(\mathrm{N}(A)) < 0$, so we conclude that an element $A \in B_p$ is integral if and only if its corresponding a, b, c, d are in $\mathbb{Z}_p$.

The set of integral elements is then clearly a ring. It also clearly spans B_p and is finitely generated, so it follows that the set of integral elements in B_p is an order. □

This Proposition has a consequence that simplifies the classification of Eichler orders significantly.

Corollary 3.3.4. *Let B_p be a division quaternion algebra over $\mathbb{Q}_p$. The set of all integral elements $O \subset B_p$ is the unique maximal order in B_p. Furthermore, if $O' \subset B_p$ is an Eichler order, then $O = O'$.*

Proof. From Proposition 3.3.3, we know that O is an order. By Proposition 2.2.9, an order can only contain integral elements, so O cannot be contained properly in another order. We find that O is maximal, and since every order is contained in a maximal order **REF**, O is the unique maximal order. If $O' \subset B_p$ is an Eichler order, it is an intersection of maximal orders. The only intersection of maximal orders is $O \cap O = O$, so we find $O = O'$. □

3.4 Local-global connection

Up to this point, our main focus has been to describe the structures of quaternion algebras over $\mathbb{Q}_p$ and orders in those quaternion algebras. Now we will focus on the connection between these local results and the global structures. In the light of solving problem 2.3.2, we want to know what the properties of lattices and orders in B_p tell us about the properties of lattices and orders in B.

Let $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\} \subset \mathbb{Q}$ for a prime p. We call this the *localization* of $\mathbb{Z}$ at p. For a more detailed introduction of localizations, see [Voi21, Section 9.4]. We will list some properties of $\mathbb{Z}_{(p)}$:

(i) $\mathbb{Z}_{(p)}$ is a local ring, and every ideal is of the form (p^k) for some $k \in \mathbb{Z}_{\geq 0}$;

(ii) $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$;

(iii) $\bigcap_{p \text{ prime}} \mathbb{Z}_{(p)} = \mathbb{Z}$.

In particular, $\mathbb{Z}_{(p)}$ is a principal ideal, so it makes sense to talk about $\mathbb{Z}_{(p)}$-lattice inside vector spaces over its field of fractions $\mathbb{Q}$.

Lemma 3.4.1. *Let $I \subset B$ be a lattice in a quaternion algebra B over $\mathbb{Q}$. Then we have that $I_p := I \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a $\mathbb{Z}_p$-lattice in B_p, and $I_{(p)} := I\mathbb{Z}_{(p)}$ is a $\mathbb{Z}_{(p)}$-lattice in B. If I is an order, then I_p and $I_{(p)}$ are orders as well.*

Proof. Any lattice I is free as a $\mathbb{Z}$-module and thus has a basis $\beta_1, \beta_2, \beta_3, \beta_4$. The elements $\beta_i \otimes 1 \in B_p$ with $i = 1, 2, 3, 4$ generate I_p as a $\mathbb{Z}_p$-module and they generate B_p as a $\mathbb{Q}_p$-vector space. The elements $\beta_i \in B$ also generate $I_{(p)}$ as a $\mathbb{Z}_{(p)}$-module and B as $\mathbb{Q}$-vector space. It follows that I_p and $I_{(p)}$ are lattices. If I is an order, it is clear that $I_{(p)} \subset B$ inherits a ring structure. The $\mathbb{Z}_p$-module I_p becomes a ring via the multiplication $(\alpha \otimes n)(\beta \otimes m) = \alpha\beta \otimes nm$. □

The reason why we bring up localizations is because of the following connection.

Lemma 3.4.2 (Local-global dictionary for lattices)**.** *Let $\mathbb{Z}$ a finite-dimensional $\mathbb{Q}$-vector space and let $M, N \subset V$ be lattices. The map $N \mapsto (N_{(p)})_{p \text{ prime}}$ with inverse $(N_{(p)})_p \mapsto \bigcap_p N_{(p)} = N$ is a bijection from lattices $N \subset V$ to collections $(N_{(p)})_p$ of localizations indexed by primes p for which $M_{(p)} = N_{(p)}$ for all but finitely many primes. Furthermore, the map $N_{(p)} \mapsto N_p = N_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p$ is a bijection from $\mathbb{Z}_{(p)}$-lattices in V to $\mathbb{Z}_p$-lattices in $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ with inverse $M_p \mapsto M_p \cap V$.*

Proof. We refer to Voight [Voi21, Theorem 9.4.9, Lemma 9.5.3]. □

We will now use the results of the Local-global dictionary to explore the connections between global lattices, their localizations and their completions.

Lemma 3.4.3. *Let $O \subset B$ be an order in a quaternion algebra B over $\mathbb{Q}$. Maximality and being Eichler are local properties, that is, O is maximal (Eichler respectively) if and only if O_p is maximal (Eichler respectively) for all primes p.*

Proof. If O is not maximal, then suppose $O \subsetneq O'$. It follows that $O_{(p)} \subsetneq O'_{(p)}$ for at least one prime p by the Local-global dictionary. And for such a prime p, we have $O_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p \subsetneq O'_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p$ as well. We find that O_p is not maximal for at least one prime p.

If O_p is not maximal, let $O_p \subsetneq O'_p$. Then $O_{(p)} = B \cap O_p \subsetneq B \cap O'_p = O'_{(p)}$. Then every global lattice O with localization $O_{(p)}$ is not maximal.

Now, let O', O'' be maximal global orders and let $O = O' \cap O''$. We have just shown that O'_p and O''_p are maximal for all primes p. Then $O'_{(p)}$ and $O''_{(p)}$ are also maximal. We then find that $O_{(p)} = (O' \cap O'')\mathbb{Z}_{(p)} = O'\mathbb{Z}_{(p)} \cap O''\mathbb{Z}_{(p)}$. It follows that

$$O_p = (O'_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p) \cap (O''_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p) = O'_p \cap O''_p,$$

which proves the statement. □

We similarly find that discriminants are local properties of orders. If O has basis β_i for $i = 1, 2, 3, 4$, then we have an explicit basis for $O_{(p)}$ and O_p as well. A direct verification yields

$$\operatorname{disc}(O) = \bigcap_{p \text{ prime}} \operatorname{disc}(O_{(p)}) = \Big(\bigcap_{p \text{ prime}} \operatorname{disc}(O_p) \Big) \cap \mathbb{Z} \tag{3.4.4}$$

We will now find some properties that are determined by discriminants.

Lemma 3.4.5. *Let $O \subset B_p$ be an order in a split quaternion algebra $B_p \cong M_2(\mathbb{Q}_p)$. Then, O is maximal if and only if $\operatorname{disc}(O) = \mathbb{Z}_p$.*

Proof. If O is maximal, then by Proposition 3.3.2 we have $O \cong M_2(\mathbb{Z}_p)$. Since O is conjugated to $M_2(\mathbb{Z}_p)$ in $M_2(\mathbb{Q}_p)$, we find that $O = \operatorname{End}(N)$ for some lattice $N \subset \mathbb{Q}_p^2$. With respect to the standard basis of N, let A_{ij} be the matrix with a 1 on row i and column j and zeroes everywhere else. With respect to the $\mathbb{Z}_p$-basis A_{ij} of O, an explicit computation gives $\operatorname{disc}(O) = \mathbb{Z}_p$. For the other direction, if O' is an order that contains O, it follows from Lemma 2.2.17 that $[O' : O]_{\mathbb{Z}_p} = \mathbb{Z}_p$, so $O = O'$ by 2.2.16. □

Lemma 3.4.6. *Let $O \subset B_p$ be an order in a division quaternion algebra B_p over $\mathbb{Q}_p$. Then, O is maximal if and only if $\operatorname{disc}(O) = p^2\mathbb{Z}_p$.*

Proof. If O is maximal, then by Corollary 3.3.4, O is the ring of all integral elements in B_p. The ring with integral elements consists of the elements in of the form as in 3.2.10. The matrices are induced

by a, b, c, d. Let A_a be the matrix induced by $a = 1, b = c = d = 0$, and similarly for A_b, A_c, A_d. Then, A_a, A_b, A_c, A_d form a basis for O. We find

$$\det \begin{pmatrix} 2 & \alpha+\overline{\alpha} & 0 & 0 \\ \alpha+\overline{\alpha} & \alpha^2+\overline{\alpha}^2 & 0 & 0 \\ 0 & 0 & 2p & p\overline{\alpha}+p\alpha \\ 0 & 0 & p\overline{\alpha}+p\alpha & 2p\alpha\overline{\alpha} \end{pmatrix} = -p^2(\alpha-\overline{\alpha})^4$$

We find $\mathrm{disc}(O) = p^2\mathbb{Z}_p$. The other direction follows from Lemmas 2.2.16 and 2.2.17. □

Theorem 3.4.7. *Let $O \subset B$ be an order in a quaternion algebra B over $\mathbb{Q}$. Then, O is maximal, if and only if $disc(O) = (disc(B)^2)$.*

Proof. Let $\mathrm{ram}(B)$ be the set of primes where B is ramified. The order O is maximal if and only if O_p is maximal for every prime p by Lemma 3.4.3. If we combine Lemmas 3.4.5, 3.4.6 and the expression for the discriminant in 3.4.4, O is maximal if and only if

$$\mathrm{disc}(O) = \mathbb{Z} \cap \bigcap_{p \in \mathrm{Ram}(B)} p^2\mathbb{Z}_p = (\mathrm{disc}(B)^2).$$

This proves the statement. □

Corollary 3.4.8. *Let O be an order in a quaternion algebra B over $\mathbb{Q}$. Then O_p is maximal for all but finitely many primes p.*

Proof. This is a consequence of Theorem 3.4.7, together with Lemma 2.2.17. □

We end this section by exploring the connection between the global norm map $O \to \mathbb{Z}$ and the norm maps of reductions $O/p^kO \to \mathbb{Z}/p^k\mathbb{Z}$. If we know what O_p looks like, we can deduce the structure of O/p^kO. If J is a $\mathbb{Z}$-lattice, we have the following isomorphisms:

$$J \otimes_{\mathbb{Z}} \mathbb{Z}/p^k\mathbb{Z} \cong J \otimes_{\mathbb{Z}} \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^k\mathbb{Z} \cong J_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^k\mathbb{Z}_p \cong J_p/p^kJ_p.$$

So we find $O/p^kO \cong O_p/p^kO_p$.

Suppose that O_p is isomorphic to an order A with known norm map $A \to \mathbb{Z}_p$. Then for each $k \in \mathbb{Z}_{>0}$ we have the following diagram:

$$\begin{array}{ccccc} O & & \longrightarrow & & \mathbb{Z} \\ \downarrow & & & & \downarrow \\ O_p & \xrightarrow{\sim} & A & \longrightarrow & \mathbb{Z}_p \\ \downarrow & & \downarrow & & \downarrow \\ O/p^kO & \xrightarrow{\sim} & A/p^kA & \longrightarrow & \mathbb{Z}/p^k\mathbb{Z} \end{array} \tag{3.4.9}$$

The vertical maps are the natural embeddings and reductions. The horizontal maps that are not isomorphisms are the norm maps.

Lemma 3.4.10. *Let $\#S_{r,p^k} = \#\{\alpha \in O/p^kO : N(\alpha) \equiv r \ (mod\ p^k)\}$. Then, using the notation of diagram 3.4.9, equality $\#S_{r,p^k} = \#\{\alpha \in A/p^kA : N(\alpha) \equiv r \ (mod\ p^k)\}$ holds.*

Proof. Let $\varphi : O_p \to A$ denote the isomorphism in Diagram 3.4.9. If we define a mapping $A \to A$ as $\overline{\varphi(\alpha)} = \varphi(\overline{\alpha})$, then this defines a standard involution on A. By the unicity of standard involutions (Lemma 2.1.8), this is also the only standard involution on A. We find

$$\mathrm{N}(\varphi(\alpha)) = \varphi(\alpha)\overline{\varphi(\alpha)} = \varphi(\alpha)\varphi(\overline{\alpha}) = \varphi(\alpha\overline{\alpha}) = \varphi(\mathrm{N}(\alpha)) = \mathrm{N}(\alpha).$$

Using a similar argument as in Remark 2.3.4, the bottom right square in Diagram 3.4.9 is commutative. But since norms are preserved under φ, we also find that

$$\mathrm{N}(\alpha \pmod{p^k O}) = \mathrm{N}(\varphi(\alpha) \pmod{p^k A}).$$

We find that $\#S_{r,p^k} = \#\{\alpha \in A/p^k A : \mathrm{N}(\alpha) \equiv r \pmod{p^k}\}$. □

It can also be checked that Diagram 3.4.9 is commutative as a whole.

If B is ramified at p and if O_p is an Eichler order in B_p, then O_p is the unique maximal order in B_p. With the notation of 3.2.10, we have

$$O_p/p^k O_p = \left\{ \begin{pmatrix} a + b\alpha & p(c + d\alpha) \\ c + d\overline{\alpha} & a + b\overline{\alpha} \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p^k\mathbb{Z} \right\}.$$

And if C is the matrix induced by a, b, c, d, we have norm map

$$\mathrm{N}(C) \equiv \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha) - p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha) \pmod{p^k}. \tag{3.4.11}$$

Now, let p be a prime such that B is not ramified at p, and let O be an order such that O_p is Eichler order of level p^m for some $m \in \mathbb{Z}_{\geq 0}$. Then $O_p \cong E_m$, so we have

$$O_p/p^k O_p = \left\{ \begin{pmatrix} a & b \\ cp^m & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p^k\mathbb{Z} \right\}.$$

And if C is the matrix induced by a, b, c, d, we have norm map

$$\mathrm{N}(C) \equiv ad - p^m bc \pmod{p^k}. \tag{3.4.12}$$

4 Results

In this section, let B be a quaternion algebra over $\mathbb{Q}$ such that B_∞ is a division algebra, let $O \subset B$ be an order and let $J \subset O$ be an integral lattice in O. We let $S^J_{r,p^k} = \{\alpha \in J/p^k J : \mathrm{N}(\alpha) \equiv r \pmod{p^k}\}$, and recall that for an integral ideal J, its associated probabilities are $\mathbb{P}_{r,p^k} = \#S^J_{r,p^k}/p^{4k}$. If the lattice J is clear from the context, we omit the J and refer instead to S_{r,p^k}. We denote J_p, O_p and B_p as the respective completions of J, O and B at the prime p. Our aim in this chapter is to solve Problem 2.3.1 for *locally principal ideals* J in Eichler orders $O \subset B$. We call an integral ideal $J \subset O$ a locally principal ideal if J_p is a principal ideal of O_p for every prime p.

4.1 Counting solutions

We will first solve problem 2.3.1 for orders O. So whenever we refer to S_{r,p^k}, we mean S^O_{r,p^k}.

Lemma 4.1.1. *Let p be a prime number and r and s be two integers such that $r, s \not\equiv 0 \pmod{p}$. Then, equality $\#S_{r,p} = \#S_{s,p}$ holds whenever $S_{r,p}$ and $S_{s,p}$ are nonempty. In particular, if we have $\#S_{1,p} = 0$, then $\#S_{r,p} = 0$ for every $r \not\equiv 0 \pmod{p}$.*

Proof. Suppose that $S_{r,p}$ and $S_{s,p}$ are not empty. For any $\alpha \in S_{r,p}$, we have an inverse element $\alpha^{-1} = \overline{\alpha} \cdot N(\alpha)^{-1} \in S_{r^{-1},p}$. Here, $N(\alpha)^{-1}$ denotes the inverse of $N(\alpha)$ in $\mathbb{F}_p$. Note that $\overline{\alpha} \in O$, since $\alpha + \overline{\alpha} \in \mathbb{Z} \subset O$. We find that $S_{1,p}$ is nonempty, since $\alpha\alpha^{-1} \in S_{1,p}$. By the multiplicativity of the norm, we find that $\bigcup_{i=1}^{p-1} S_{i,p}$ is a group under multiplication.

The norm map is a multiplicative group homomorphism $\bigcup_{i=1}^{p-1} S_{i,p} \to \mathbb{F}_p^\times$ with kernel $S_{1,p}$, so in particular, $S_{1,p}$ is a normal subgroup. Then $S_{r,p}$ and $S_{s,p}$ are cosets $\alpha S_{1,p}$ and $\beta S_{1,p}$ respectively, for $\alpha \in S_{r,p}$ and $\beta \in S_{s,p}$. We find $\#S_{r,p} = \#S_{s,p}$. □

In particular, this Lemma shows that if $\mathrm{N} : J/pJ \to \mathbb{Z}/p\mathbb{Z}$ is surjective, then $\#S_{r,p} = \#S_{s,p} \neq 0$ for every $r, s \not\equiv 0 \pmod{p}$.

Another tool we will use for finding the values $\#S_{r,p^k}$ is an application of Hensel's Lemma. For the rest of this section, whenever we use "Hensel's lifting", we will be referring to the following result.

Lemma 4.1.2 (Hensel's lifting)**.** *Let $f(t,x,y,z) \in \mathbb{Z}_p[t,x,y,z]$ be a polynomial in four variables. If $(a,b,c,d) \in \mathbb{Z}_p^4$ is a root of $f \pmod{p}$ such that the partial derivatives of f do not all vanish at (a,b,c,d) modulo p, then there are $p^{3(k-1)}$ roots of $f \pmod{p^k}$ that reduce to $(a,b,c,d) \in \mathbb{F}_p^4$.*

Proof. Since the partial derivatives of $f(t,x,y,z)$ are not all multiples of p, we may assume without loss of generality that $\frac{\partial f}{\partial t}(a,b,c,d) \not\equiv 0 \pmod{p}$. Let $g_{m_1,m_2,m_3}(t) = f(t, b+m_1p, c+m_1p, d+m_1p)$. Note that $g'_{m_1,m_2,m_3}(t) \not\equiv 0 \pmod{p}$.

When applying Hensel's Lemma to g_{m_1,m_2,m_3}, we find a unique root $a' \in \mathbb{Z}/p^k\mathbb{Z}$ of $g_{m_1,m_2,m_3} \pmod{p^k}$ such that $a' \equiv a \pmod{p}$. For each choice of (m_1,m_2,m_3) with $m_i \in 0, \ldots, p^{k-1}-1$, we get a different root in $\mathbb{Z}/p^k\mathbb{Z}$, but they all reduce to $(a,b,c,d) \in \mathbb{F}_p^4$. We find that there are $p^{3(k-1)}$ roots of $f \pmod{p^k}$ that reduce to $(a,b,c,d) \in \mathbb{F}_p^4$. □

In order to find the values $\#S_{r,p^k}$ for arbitrary k, we have to deal with cases where we cannot directly apply Hensel's lifting, because all partial derivatives vanish. The following observation, which we will refer to as the "division trick", can help with that.

Lemma 4.1.3 (division trick)**.** *Let $f(x_1,x_2,x_3,x_4) \in \mathbb{Z}_p[x_1,x_2,x_3,x_4]$ be a polynomial in four variables and let $r \in p\mathbb{Z}/p^k\mathbb{Z}$. For $i = 1,2,3,4$, let d_i be either 1 or p, and suppose that the polynomial $f(d_1x_1, d_2x_2, d_3x_3, d_4x_4)$ is a multiple of p. Let $I \subset \{1,2,3,4\}$ denote the set of indices i*

such that $d_i = p$. Let S be the set of solutions $(x_1, x_2, x_3, x_4) \in (\mathbb{Z}/p^k\mathbb{Z})^4$ such that $f(x_1, x_2, x_3, x_4) \equiv r \ (mod\ p^k)$ and $x_i \equiv 0 \ (mod\ p)$. Then $\#S$ is equal to

$$p^{4-\#I} \cdot \# \left\{ (x_1, x_2, x_3, x_4) \in (\mathbb{Z}/p^{k-1}\mathbb{Z})^4 : \frac{1}{p} f(d_1x_1, d_2x_2, d_3x_3, d_4x_4) \equiv \frac{r}{p} \ (mod\ p^{k-1}) \right\}.$$

Proof. In the equation $f(d_1x_1, d_2x_2, d_3x_3, d_4x_4) \equiv r \pmod{p^k}$, both sides are multiples of p. We may then divide everything by p to get the equation

$$\frac{1}{p} f(d_1x_1, d_2x_2, d_3x_3, d_4x_4) \equiv \frac{r}{p} \pmod{p^{k-1}}.$$

If d_i is p, then a solution in $x_i \pmod{p^{k-1}}$ corresponds to a uniquely determined solution in $x_i \pmod{p^k}$. However, if d_i is 1, then a solution in $x_i \pmod{p^{k-1}}$ corresponds to p different solutions in $x_i \pmod{p^k}$, since there are p different elements in $\mathbb{Z}/p^k\mathbb{Z}$ that reduce to the same element in $\mathbb{Z}/p^{k-1}\mathbb{Z}$. We observe that for each solution of the equation modulo p^{k-1}, there are $p^{4-\#I}$ solutions modulo p^k. □

4.2 Unramified case

Let p be a prime such that B is unramified at p. In this subsection, we will find the values of $\#S_{r,p^k}$ for orders O such that $O_p \subset B_p \cong M_2(\mathbb{Q}_p)$ is Eichler.

Let O_p be an Eichler order of level p^m. In this subsection, we let $\#S_{r,p^k,m}$ be the value of $\#S_{r,p^k}$ associated to the order O_p. If O_p is Eichler of level 1 (that is, O_p is maximal), we omit $m = 0$, so $\#S_{r,p^k,0} = \#S_{r,p^k}$

By 3.4.12, the value $\#S_{r,p^k,m}$ is the number of solutions $(a, b, c, d) \in (\mathbb{Z}/p^k\mathbb{Z})^4$ to the equation

$$ad - p^m bc \equiv r \pmod{p^k}. \tag{4.2.1}$$

Note that this equation has solutions for each r, so by Lemma 4.1.1, $\#S_{1,p,m} = \#S_{r,p,m}$ holds whenever $r \not\equiv 0 \pmod{p}$.

Our approach to counting these solutions in the most general case is to solve for $k = 1$ first, then use Hensel's lifting and the division trick to find the other values $\#S_{r,p^k,m}$. The division trick is, in the general case, only useful when p^m, p^k and r have sufficiently large p-adic valuation. Keeping that in mind, we first solve for some base cases, and then we use an inductive argument to find the general result.

First we find the values $\#S_{r,p}$.

Lemma 4.2.2. *Let O_p be an Eichler order of level 1 in $B \cong M_2(\mathbb{Q}_p)$. We have*

$$\#S_{r,p} = \begin{cases} p^3 + p^2 - p, & \text{If } r \equiv 0 \ (mod\ p); \\ p^3 - p, & \text{If } r \not\equiv 0 \ (mod\ p). \end{cases}$$

Proof. Equation 4.2.1 is in this case just the determinant equation for matrices in $M_2(\mathbb{F}_p)$. A matrix has a nonzero determinant if and only if its rows are linearly independent. We can choose any nonzero vector for the first row. For the second row, we can choose any vector that is not a scalar multiple of the first row. We find $\#S_{0,p} = p^4 - (p^2 - 1)(p^2 - p) = p^3 + p^2 - p$. If $r \not\equiv 0 \pmod{p}$, Lemma 4.1.1 yields $\#S_{r,p} = (p^2 - 1)(p^2 - p)/(p - 1) = p^3 - p$. □

Now, we find the values $\#S_{r,p,m}$ with $m > 0$.

Lemma 4.2.3. *Let O_p be an Eichler order of level p^m in $B \cong M_2(\mathbb{Q}_p)$. Let $m > 0$. We have*

$$\#S_{r,p,m} = \begin{cases} 2p^3 - p^2, & \text{If } r \equiv 0 \ (mod\ p); \\ p^3 - p^2, & \text{If } r \not\equiv 0 \ (mod\ p). \end{cases}$$

Proof. Equation 4.2.1 reduces to $ad \equiv r \pmod{p}$. This is nonzero if and only if a and d are nonzero. We find that $\#S_{0,p,m} = p^4 - p^2(p-1)^2 = 2p^3 - p^2$. And, by Lemma 4.1.1, $\#S_{r,p,m} = p^2(p-1)^2/(p-1) = p^3 - p^2$ if $r \not\equiv 0 \pmod{p}$. □

Note that the function $f(a,b,c,d) = ad - p^m bc - r \in \mathbb{Z}_p[a,b,c,d]$ can have partial derivatives that vanish modulo p. If $m = 0$, this happens if and only if $(a,b,c,d) = (0,0,0,0) \in \mathbb{F}_p^4$. If $m > 0$, this happens if and only if $(a,d) = (0,0) \in \mathbb{F}_p^2$. Note that in both cases, the criteria are met for applying the division trick. This is a nice result. We can either use Hensel's lifting directly, or we can use the division trick.

In the $m = 0$ case, we introduce new variables a_1, b_1, c_1, d_1 after applying the division trick and in the $m > 0$ case, we introduce a_1, d_1 as new variables. These are linked to the original variables via $pa_1 \equiv a \pmod{p^k}$ and similarly for b_1, c_1, d_1. Then, for each solution modulo p^{k-1} in a variable with index 1, there is a unique solution modulo p^k. And for each solution modulo p^{k-1} in a variable without index 1, there are p different solutions modulo p^k. These indices help us to keep track of how many solutions we have to count.

We now solve for the general case $m = 0$.

Lemma 4.2.4. *Let O_p be an Eichler order of level 1 in $B \cong M_2(\mathbb{Q}_p)$. We have*

$$\#S_{r,p^k} = \begin{cases} p^{3k} + p^{3k-1} - p^{2k-1}, & \text{If } r \equiv 0 \ (mod\ p^k); \\ p^{3k} + p^{3k-1} - (p+1)p^{3k-v_p(r)-2}, & \text{If } r \not\equiv 0 \ (mod\ p^k). \end{cases}$$

Proof. We count solutions to Equation 4.2.1 with induction on k. We set $\#S_{1,1} = 1$, so that the result holds for $k = 0$. For $k = 1$, these results coincide with Lemma 4.2.2. So let $k > 1$. If $v_p(r) = 0$, by Hensel's lifting we have $\#S_{r,p^k} = p^{3(k-1)}\#S_{1,p} = p^{3k} - p^{3k-2}$.

If $v_p(r) > 0$, we cannot apply Hensel's lifting when a, b, c, d are all multiples of 0. In that case, we use the division trick and count the solutions to

$$p(a_1 d_1 - b_1 c_1) \equiv r/p \pmod{p^{k-1}}.$$

If $v_p(r) = 1$, there are no solutions. We get

$$\#S_{r,p^k} = p^{3(k-1)}(\#S_{0,p} - 1) = p^{3k} + p^{3k-1} - p^{3k-2} - p^{3k-3}.$$

Let $v_p(r) > 1$. If we apply the division trick again, we get the equation

$$a_1 d_1 - b_1 c_1 \equiv r/p^2 \pmod{p^{k-2}}.$$

We use the induction hypothesis and Hensel's lifting to find

$$\begin{aligned} \#S_{0,p^k} &= p^{3(k-1)}(\#S_{0,p} - 1) + p^4 \#S_{0,p^{k-2}}. \\ &= p^{3k} + p^{3k-1} - p^{3k-2} - p^{3k-3} + p^4(p^{3k-6} + p^{3k-7} - p^{2k-5}); \\ &= p^{3k} + p^{3k-1} - p^{2k-1}. \end{aligned}$$

If $r \not\equiv 0 \pmod{p^k}$, we find

$$\begin{aligned} \#S_{r,p^k} &= p^{3(k-1)}(\#S_{0,p} - 1) + p^4 \#S_{r/p^2,p^{k-2}}; \\ &= p^{3k} + p^{3k-1} - p^{3k-2} - p^{3k-3} + p^4(p^{3k-6} + p^{3k-7} - (p+1)p^{3k-(v_p(r)-2)-8}); \\ &= p^{3k} + p^{3k-1} - (p+1)p^{3k-v_p(r)-2}. \end{aligned}$$

□

Now we solve for $m = 1$.

Lemma 4.2.5. *Let O_p be an Eichler order of level p in $B \cong M_2(\mathbb{Q}_p)$. We have*

$$\#S_{r,p^k,1} = \begin{cases} 2p^{3k} - p^{2k}, & \text{If } r \equiv 0 \ (mod\ p^k); \\ 2p^{3k} - (p+1)p^{3k-v_p(r)-1}, & \text{If } r \not\equiv 0 \ (mod\ p^k). \end{cases}$$

Proof. We count solutions to Equation 4.2.1 by induction to k. If $k = 0, 1$, the results coincide with Lemma 4.2.3 if we let $\#S_{1,1,m} = 1$. So let $k > 1$. If $v_p(r) = 0$, we use Hensel's lifting and we find $\#S_{r,p^k,1} = p^{3(k-1)}\#S_{1,p,1} = p^{3k} - p^{3k-1}$.

If $v_p(r) > 0$, we cannot use Hensel's lifting whenever both a and d are multiples of p. With the division trick, we get the equation

$$pa_1d_1 - bc \equiv r/p \ (\text{mod } p^{k-1}).$$

We combine the induction hypothesis with Hensel's lifting to find that

$$\begin{aligned} \#S_{0,p^k,1} &= p^{3(k-1)}(\#S_{0,p,1} - p^2) + p^2\#S_{0,p^{k-1},1}; \\ &= 2p^{3k} - 2p^{3k-1} + 2p^{3k-1} - p^{2k}; \\ &= 2p^{3k} - p^{2k}. \end{aligned}$$

And if $r \not\equiv 0 \ (\text{mod } p)$:

$$\begin{aligned} \#S_{r,p^k,1} &= p^{3(k-1)}(\#S_{0,p,1} - p^2) + p^2\#S_{r/p,p^{k-1},1}; \\ &= 2p^{3k} - 2p^{3k-1} + 2p^{3k-1} - (p+1)p^{3k-(v_p(r)-1)-2}; \\ &= 2p^{3k} - (p+1)p^{3k-v_p(r)-1}. \end{aligned}$$

□

The cases $m = 0, 1$ enable us to compute the general case for $m > 1$.

Theorem 4.2.6. *Let O_p be an Eichler order of level p^m in $B \cong M_2(\mathbb{Q}_p)$. We have*

$$\#S_{r,p^k,m} = \begin{cases} (k+1)p^{3k} - kp^{3k-1}, & \text{If } p^k | r \text{ and } m \geq k; \\ (m+1)p^{3k} - (m-1)p^{3k-1} - p^{2k+m-1}, & \text{If } p^k | r \text{ and } m < k; \\ (v_p(r)+1)(p^{3k} - p^{3k-1}), & \text{If } p^k \nmid r \text{ and } m > v_p(r); \\ (m+1)p^{3k} - (m-1)p^{3k-1} - (p+1)p^{3k-v_p(r)+m-2}, & \text{If } p^k \nmid r \text{ and } m \leq v_p(r). \end{cases}$$

Proof. We count solutions to Equation 4.2.1 by induction to k. The formulas coincide with Lemmas 4.2.4 and 4.2.5 Let $k, m > 1$. If $v_p(r) = 0$, we use Hensel's lifting to find $\#S_{r,p^k,m} = p^{3(k-1)}\#S_{1,p,m} = p^{3k} - p^{3k-1}$.

If $v_p(r) > 0$, we cannot use Hensel's lifting when both a and d are multiples of p. The division trick gives equation

$$p(a_1d_1 - p^{m-2}bc) \equiv r/p \ (\text{mod } p^{k-1}),$$

which has no solutions if $v_p(r) = 1$. In that case, we find

$$\#S_{r,p^k,m} = p^{3(k-1)}(\#S_{0,p,m} - p^2) = 2p^{3k} - 2p^{3k-1}.$$

Now, let $v_p(r) > 1$. We can use the division trick again, to get the equation

$$a_1d_1 - p^{m-2}bc \equiv r/p^2 \ (\text{mod } p^{k-2}).$$

We can combine Hensel's lifting with the induction hypothesis to find

$$\begin{aligned}\#S_{r,p^k,m} &= p^{3(k-1)}(\#S_{0,p,m} - p^2) + p^6 \#S_{r/p^2,p^{k-2},m-2};\\ &= 2(p^{3k} - p^{3k-1}) + p^6 \#S_{r/p^2,p^{k-2},m-2}.\end{aligned}$$

Note that the four formulas in the statement of this theorem have some common aspects. Each formula has two terms of the form $x_1 p^{3k} - x_2 p^{3k-1}$, where x_1 and x_2 are either k, m or $v_p(r)$ added with $-1, 0$ or 1. Then there are two coefficients $x_3, x_4 \in \{0, 1\}$ of p^{2k+m-1} and $(p+1)p^{3k-v_p(r)+m-2}$. All different formulas can then be written as

$$x_1 p^{3k} - x_2 p^{3k-1} - x_3 p^{2k+m-1} - x_4(p+1)p^{3k-v_p(r)+m-2}.$$

And if we have a combination of x_1, x_2, x_3, x_4 in the expression for $\#S_{r,p^k,m}$, then we have the combination $x_1 - 2, x_2 - 2, x_3, x_4$ in the expression for $\#S_{r/p^2,p^{k-2},m-2}$. Indeed, note that if m, r and k are chosen such that they satisfy one of the four conditions in the statement of this theorem, then $m-2, r/p^2$ and $k-2$ satisfy the same condition. We find

$$\begin{aligned}\#S_{r,p^k,m} &= p^6((x_1-2)p^{3k-6} - (x_2-2)p^{3k-7} - x_3 p^{2k+m-7} - x_4(p+1)p^{3k-v_p(r)+m-8})\\ &\quad + 2(p^{3k} - p^{3k-1});\\ &= x_1 p^{3k} - x_2 p^{3k-1} - x_3 p^{2k+m-1} - x_4(p+1)p^{3k-v_p(r)+m-2}.\end{aligned}$$

This proves the theorem. □

4.3 Ramified case

Let p be a prime such that B is ramified at p. In this subsection, we will find the values of $\#S_{r,p^k}$ for orders O such that O_p is Eichler in the division algebra B_p.

By 3.3.4, there is only one maximal order in B_p, so every intersection of two maximal orders is the maximal order itself. We find that there is only one maximal order in B_p; the unique maximal order.

By 3.4.11, the value $\#S_{r,p^k}$ is the number of solutions $(a, b, c, d) \in (\mathbb{Z}/p^k\mathbb{Z})^4$ to the equation

$$\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha) - p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha) \equiv r \pmod{p^k}. \tag{4.3.1}$$

Note that this equation has solutions for every $r \pmod p$. The field norm is either of the form $a^2 - ub^2$ or $a^2 - ab + b^2$. In the first case, $a^2 - ub^2 \equiv r \pmod p$ has solutions for every r, as we have seen in the proof of Lemma 3.2.4. For $p = 2$, the result is immediate. By Lemma 4.1.1, $\#S_{1,p} = \#S_{r,p}$ holds whenever $r \not\equiv 0 \pmod p$.

In the proof of Lemma 3.2.8, we have seen that $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a + b\alpha) \equiv 0 \pmod p$ if and only if $a, b \equiv 0 \pmod p$.

Our approach to counting the solutions is similar to the approach in subsection 4.2. We use Hensel's lifting and the division trick to find the values $\#S_{r,p^k}$ using an inductive argument. It turns out that in the ramified case, there are far fewer base cases to consider, so we compute the general result directly.

Theorem 4.3.2. *Let O_p be an Eichler order in the division algebra B_p. We have*

$$\#S_{r,p^k} = \begin{cases} p^{2k}, & \text{If } r \equiv 0 \ (mod\ p^k);\\ (p+1)p^{3k-v_p(r)-1}, & \text{If } r \not\equiv 0 \ (mod\ p^k).\end{cases}$$

Proof. We count solutions to Equation 4.3.1 with induction to k. For $k = 1, r = 0$, there is a solution if and only if a and b are 0 modulo p. We find $\#S_{0,p} = p^2$ and by Lemma 4.1.1, the other values are $\#S_{r,p} = (p^4 - p^2)/(p-1) = p^3 + p^2$ if $r \not\equiv 0 \pmod p$.

Let $k > 1$. If $v_p(r) = 0$, we use Hensel's lifting to find that $\#S_{r,p^k} = p^{3(k-1)}\#S_{1,p} = p^{3k} + p^{3k-1}$.

If $v_p(r) > 1$, we can use Hensel's lifting whenever a and b are not both multiples of p. If they are, we use the division trick to get the equation

$$\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c + d\alpha) - p\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a_1 + b_1\alpha) \equiv -r_1 \pmod{p^{k-1}}.$$

Since -1 is a unit in $\mathbb{F}_p$, we have $v_p(-r_1) = v_p(r_1) = v_p(r) - 1$. A combination of Hensel's lifting and the induction hypothesis yields

$$\#S_{0,p^k} = p^{3(k-1)}(\#S_{0,p} - p^2) + p^2(\#S_{0,p^{k-1}}) = p^{2k}.$$

And if $r \not\equiv 0 \pmod{p^k}$:

$$\begin{aligned}\#S_{r,p^k} &= p^{3(k-1)}(\#S_{0,p} - p^2) + p^2(\#S_{r/p,p^{k-1}});\\ &= p^2(p+1)p^{3k-(v_p(r)-1)-4};\\ &= (p+1)p^{3k-v_p(r)-1}.\end{aligned}$$

This proves the theorem. □

4.4 Ideals

In this subsection, let J denote an ideal of an order O in a quaternion algebra B over $\mathbb{Q}$. We will find the values of $\#S^J_{r,p^k}$ for integral ideals J such that J_p is a principal integral ideal of O_p, in terms of the values $\#S^O_{r,p^k}$.

Theorem 4.4.1. *Let $J \subset O$ be an integral ideal such that J_p is a principal integral ideal of O_p and let $n = v_p(N(J))$ We have:*

$$\#S^J_{r,p^k} = \begin{cases} p^{4k}, & \text{If } r \equiv 0 \ (mod\ p^k) \text{ and } n \geq k;\\ 0, & \text{If } r \not\equiv 0 \ (mod\ p^k) \text{ and } n > v_p(r);\\ p^{4n}\#S^O_{r/p^n,p^{k-n}}, & \text{Otherwise.}\end{cases}$$

Proof. We will prove the statement for left integral ideals $J \subset O$, but the proof for right integral ideals is analogous. Let $J_p = O_p\alpha$ be an integral ideal of O_p for some $\alpha \in O_p$. Then $x \mapsto x\alpha$ is a $\mathbb{Z}$-module isomorphism $O_p \to J_p$. Note that the following diagram commutes by the multiplicativity of the norm:

$$\begin{array}{ccc} O_p & \xrightarrow{\mathrm{N}} & \mathbb{Z}_p \\ \downarrow{\scriptstyle \cdot\alpha} & & \downarrow{\scriptstyle \cdot\mathrm{N}(\alpha)} \\ J_p & \xrightarrow{\mathrm{N}} & \mathbb{Z}_p \end{array}$$

Reduction maps commute with $\cdot\alpha$ and $\cdot\mathrm{N}(\alpha)$, and by Diagram 3.4.9, reduction maps also commute with taking norms. The following diagram is then commutative as well.

$$\begin{array}{ccc} O/p^kO & \xrightarrow{\mathrm{N}} & \mathbb{Z}/p^k\mathbb{Z} \\ \downarrow{\scriptstyle \cdot\alpha} & & \downarrow{\scriptstyle \cdot\mathrm{N}(\alpha)} \\ J/p^kJ & \xrightarrow{\mathrm{N}} & \mathbb{Z}/p^k\mathbb{Z} \end{array}$$

And in particular, since $J/p^kJ \cong J_p/p^kJ_p$, we find that for every $x \in J/p^kJ$, there exists a $y \in O$ such that $x \equiv y\alpha \pmod{p^kJ}$. We find that $x \in J/p^kJ$ has norm $\mathrm{N}(x) \equiv r \pmod{p^k}$ if and only if $\mathrm{N}(y)\mathrm{N}(\alpha) \equiv r \pmod{p^k}$.

Note that $v_p(N(J)) = v_p(N(\alpha))$. This follows from the fact that $N(J)$ is the smallest integer such that every element's norm is a multiple of $N(J)$. On the other hand, the norm map on J modulo p^k is obtained from the norm map on O modulo p^k via multiplication by $N(\alpha)$, so the connection between the two follows.

All three formulas then follow directly. □

4.5 Overview

We give a summary of the results in this chapter and we specify to what extent we have solved Problem 2.3.1. Let J be an integral lattice inside an order $O \subset B$, where B is a quaternion algebra over $\mathbb{Q}$ that is ramified at ∞ and finitely many primes. Let $\mathbb{P}_{r,p^k}$ be the limit 2.3.2 with respect to J. Recall that $\mathbb{P}_{r,p^k} = \#S_{r,p^k}/p^{4k}$.

We introduce new notation in order to formulate the results in a more compact way. For an integral lattice J, let $n = v_p(\mathrm{N}(J))$ and let $\mathbb{P}'_{r,p^k} := \mathbb{P}_{rp^n,p^{k+n}}$.

Furthermore, let O be a global Eichler order. We define the level of O as the product of the levels of O_p, where p runs over all primes. Note that this is well defined by Corollary 3.4.8.

Theorem 4.5.1. *Let $D := disc(B)$, let O be a global Eichler order of level M such that $v_p(M) = m$, and let $J \subset O$ be an integral ideal that is locally principal. Then*

$$\mathbb{P}'_{r,p^k} = \begin{cases} p^{-2k}, & \text{If } p^k|r \text{ and } p|D; \\ \dfrac{p+1}{p^{k+v_p(r)+1}}, & \text{If } p^k \nmid r \text{ and } p|D; \\ \dfrac{(k+1)p-k}{p^{k+1}}, & \text{If } p^k|r,\ m \geq k \text{ and } p \nmid D; \\ \dfrac{(m+1)p^{k-m+1}-(m-1)p^{k-m}-1}{p^{2k-m+1}}, & \text{If } p^k|r,\ m < k \text{ and } p \nmid D; \\ \dfrac{(v_p(r)+1)(p-1)}{p^{k+1}}, & \text{If } p^k \nmid r,\ m > v_p(r) \text{ and } p \nmid D; \\ \dfrac{(m+1)p^{v_p(r)-m+2}-(m-1)p^{v_p(r)-m+1}-(p+1)}{p^{k+v_p(r)-m+2}}, & \text{If } p^k \nmid r,\ m \leq v_p(r) \text{ and } p \nmid D. \end{cases}$$

Proof. If $v_p(\mathrm{N}(J)) = 0$, we have $\mathbb{P}'_{r,p^k} = \mathbb{P}_{r,p^k}$. The results follows directly from the combination of Theorems 4.2.6 and 4.3.2.

If $n = v_p(\mathrm{N}(J)) > 0$, every $x \in J/p^{k+n}J$ can be written as $x = y\alpha$ for some $y \in O/p^{k+n}O$ and an element α with $v_p(\mathrm{N}(\alpha)) = n$. Then by the division trick, the number of solutions to $\mathrm{N}(x) \equiv rp^n \pmod{p^{k+n}}$ is equal to the number of solutions to $\mathrm{N}(y) \equiv r \pmod{p^k}$, multiplied by p^{4n}. We find that $\mathbb{P}'_{r,p^k}$ is equal to the probability $\mathbb{P}_{r,p^k}$ corresponding to the order $O \supset J$. □

If $n = v_p(\mathrm{N}(J)) > 0$, we can recover the original probabilities from $\mathbb{P}'_{r,p^k}$ using Theorem 4.4.1. Then, for an arbitrary integer with prime factorization $p_1^{e_1} \cdot \cdots \cdot p_l^{e_l}$, we can use Lemma 2.3.6 to compute the probabilities

$$\mathbb{P}_{r,p_1^{e_1}\cdot\cdots\cdot p_l^{e_l}} = \prod_{i=1}^{l} \mathbb{P}_{r,p_i^{e_i}}.$$

By Corollary 3.4.8, every global order O has maximal completions O_p for all but finitely many primes p. And since the results of Theorem 4.5.1 were derived locally, the probabilities $\mathbb{P}_{r,p^k}$ associated to O still correspond to the values in Theorem 4.5.1 for all but finitely many primes p.

In the derivation of the results in 4.5.1, we did use the condition that an integral ideal $J \subset O$ is locally principal. So a natural question that arises is: when are integral ideals locally principal? Principal ideals are in particular locally principal, so every order O has at least some integral ideals J that are locally principal. But we can say something stronger.

Lemma 4.5.2. *Let O be a global order. Every integral ideal (both left and right) of O is locally principal if and only if O is an Eichler order of level M, with M squarefree. That is, for every prime p we have $p^2 \nmid M$.*

Proof. We combine [Voi21, Main theorem 16.1.3, Main theorem 20.3.9, Corollary 21.1.5] to find that a local order has the property that every integral ideal is principal if and only if it is an Eichler order of level 1 or p. For global orders O we find that all its integral ideals J are locally principal if and only if $\mathrm{disc}(O)$ is cubefree. For the standard Eichler order E_m of level m, its discriminant is (p^{2m}), so the result follows. □

The property that all integral ideals of a global order are locally principal, is again a local property. So even if O not an Eichler order of squarefree level, its completion O_p still is for all but finitely many primes. So for all but finitely many primes p is it the case that every integral ideal of O_p is principal.

We end this section by turning our attention to Conjecture 6 in [Cas+24]. First of all, note that their conjecture is stated in terms of $\mathbb{P}'_{r,n}$. We see that the values for the probabilities $\mathbb{P}'_{r,n}$ correspond to the formulas in 4.5.1 if we take $m = 0$ and look at the unramified case. For $m = 0$, we also do not have to worry about possible integral ideals that are not locally principal, so Conjecture 6 is true for maximal orders. However, for $m > 0$ the values no longer correspond to the conjectured ones. So if there exists a global Eichler order of level $M > 1$, we have shown that Conjecture 6 is not true in general. And since being Eichler is a local property, by the Local-global dictionary, there exist global Eichler orders of level $M > 1$.

So Conjecture 6 is not true in general, but with the extra condition that we only consider integral ideals J in maximal orders O, the results are true. However, as we will find out in Section 5, the results of Conjecture 6 are only applied to integral ideals of maximal orders. So for their specific application, the results of Conjecture 6 may be used.

5 Applications

In this chapter, we explore the connection between Problem 2.3.2 and its applications in cryptography. Specifically, we look at the connection with SQIsign2D-East as discussed in [Nak+24] and [Cas+24]. Our goal is mainly to illustrate the connection, so we will not go into details of proofs.

5.1 Isogenies

The scheme SQIsign2D-East is isogeny-based, so before we can explore its content, we need some definitions.

Definition 5.1.1. An *elliptic curve* E over a field F is a smooth projective curve of genus 1, equipped with a point 0_E, called the *origin*, or the *point at infinity*.

Every elliptic curve E is isomorphic over F to some projective curve associated to the affine equation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

with all $a_i \in F$.

For a field extension $K \supset F$, we denote $E(K) = \{(x,y) \in K^2 : f(x,y) = 0\} \cup \{0_E\}$ as the set of K-rational points of E. For any such field extension, $E(K)$ has an abelian group structure [Hus87, Chapter 3, Theorem 1.2], and can therefore be regarded as a $\mathbb{Z}$-module.

For each elliptic curve E, let $F(E)$ denote the field of fractions of $F[x,y]/(f)$.

Definition 5.1.2. Let E and E' be two elliptic curves over F. An *isogeny* $\phi : E \to E'$ is a nonconstant regular rational function such that $\phi(0_E) = 0_{E'}$.

For the definition of a regular rational function, we refer to Silverman [Sil09, I.3].

An isogeny is automatically surjective by [Har13, II.6.8], and a group homomorphism [Sil09, Theorem III.4.8]. An isogeny $\phi : E \to E'$ also induces an embedding $\phi^* : F(E') \to F(E)$, and we define the *degree* $\deg\phi := [F(E) : \phi^*F(E')]$. Every isogeny also has a dual $\phi^\vee : E' \to E$ such that $\phi^\vee \circ \phi$ and $\phi \circ \phi^\vee$ are the multiplication maps by $\deg\phi = \deg\phi^\vee$ [Voi21, 42.1.3]. Let $\mathrm{Hom}(E,E')$ be the collection of isogenies $E \to E'$ and $\mathrm{End}(E) := \mathrm{Hom}(E,E)$.

Definition 5.1.3. Let E be an elliptic curve over F and let $E_{\overline{F}}$ be the elliptic curve that is associated to the same equation as E, only as an equation over an algebraic closure $\overline{F}$. The curve E is called *supersingular* if $\mathrm{End}(E_{\overline{F}})_{\mathbb{Q}} := \mathrm{End}(E_{\overline{F}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$.

Lemma 5.1.4. *Let E be a supersingular elliptic curve over F. Then the following hold:*

(i) F is a field with $char(F) = p > 0$;

(ii) If E is an elliptic curve over $\overline{F}$, then $B = End(E)_{\mathbb{Q}}$ is a quaternion algebra over $\mathbb{Q}$ that is ramified at p and ∞;

(iii) If E is an elliptic curve over $\overline{F}$, then $End(E)$ is a maximal order in B.

Proof. See [Voi21, Proposition 42.1.7, 42.1.9]. □

Note that by [Voi21, 42.1.8], statements (ii) and (iii) still hold for supersingular elliptic curves over $\mathbb{F}_{p^2}$.

By [Voi21, Lemma 42.1.11], if E and E' are two supersingular elliptic curves over the same field, then there exists an isogeny $E \to E'$. The converse also holds, so if there exists an isogeny $E \to E'$ with E a supersingular elliptic curve, then E' is a supersingular elliptic curve as well.

By [GL24, Definition 3.1, 3.2.6], there exist connected supersingular isogeny graphs $\mathcal{G}(p,l)$ for every $l \neq p$ prime. We will not go into details of what these graphs are, but the important thing is that paths in supersingular isogeny graphs correspond to compositions of isogenies, and the degree of a

composition is the product of the degrees. This gives us a way of constructing isogenies of certain degree. More precisely, let E be a supersingular elliptic curve, then for every $D \in \mathbb{Z}_{>0}$ such that $p \nmid D$, there exists a curve E' and an isogeny $E \to E'$ of degree D.

We let E_0 denote a supersingular elliptic curve. We let $O_0 := \mathrm{End}(E_0)$ be the corresponding maximal order in the quaternion algebra $B_0 := O_0 \otimes_{\mathbb{Q}} \mathbb{Q}$.

Theorem 5.1.5 (Deuring correspondence)**.** *The association $E \mapsto Hom(E, E_0)$ is functorial and defines an equivalence of categories of*

supersingular elliptic curves over F, under isogenies

and

invertible left O_0-modules, under nonzero left O_0-module homomorphisms.

Moreover, The mapping $E \mapsto [I]$ from isomorphism classes of supersingular elliptic curves to O_0-isomorphism classes of invertible left O_0-ideals $I \subset O_0$ is a bijection. We also have $End(E) \cong O_R(I)$ and $Aut(E) \cong O_R(I)^\times$.

Proof. See Voight [Voi21, Theorem 42.3.2, Corollary 42.3.7]. □

Up to O_0-isomorphism, every invertible left O_0-module I is contained in O_0. This means that I is a lattice in O_0, hence it is an integral lattice. We may therefore regard the invertible left O_0-modules as integral left ideals of O_0.

By [Voi21, Remark 42.3.3], the functor $\mathrm{Hom}(-, E_0)$ is contravariant. However, there is a similar categorical equivalence if instead of left O_0-modules, we take right invertible O_0-modules and the covariant functor $\mathrm{Hom}(E_0, -)$.

The Deuring correspondence allows us to describe problems regarding isogenies of supersingular elliptic curves in terms of ideals in orders of quaternion algebras. In the next subsection we explore how this connection finds its applications in cryptography.

5.2 SQIsign2D-East

We use [GL24, 4.3], [Cas+24] and [Nak+24] as our main references. SQIsign2D-East is a cryptographic protocol. Its name is an abbreviation of "short quaternion and isogeny signature", the "2D" stands for 2-dimensional. The "East" part is to distinct the protocol from SQIsign2D-West, which is another protocol. We describe the main idea behind SQIsign2D-East in this subsection.

SQIsign2D-East is a *digital signature scheme*. Consider three persons: the sender, the receiver and the forger. The sender wants to send a message to the receiver, while the forger wants to send a message to the receiver that seems to originate from the sender. The goal of a digital signature scheme is to give the sender a signature along with his message that the forger could never reproduce. If there is a reliable way to make such signatures, the receiver can know for sure that the message he receives actually originates from the sender, rather than the forger.

The general idea for such a signature is as follows. Let M be a message that the sender wants to send to the receiver. There is some publicly available method that converts a message M into a challenge $C(M)$ and there is a publicly available method $V(x)$ for verifying whether a given input x is a solution to $C(M)$. The sender then publishes $C(M)$ based on his message. The sender is the only one with the private information necessary to solve $C(M)$, so the sender solves $C(M)$ and publishes some information X, his signature, that can be used as input for the verification process. The receiver uses X as input for the verification process and computes $V(X)$. When it is confirmed that X was indeed a solution to $C(M)$, the receiver knows that the message M originated from the sender.

In SQIsign2D-East, the setup is as follows.

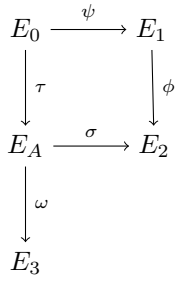
(i) p is a very large prime of the form $p = 2^{a+b}f - 1$ with $a \approx b$ and $p \approx 2^{a+b}$;

(ii) E_0 is the supersingular elliptic curve defined by $y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$;

(iii) O_0 is the maximal order with $\mathbb{Z}$-basis $1, i, \frac{i+j}{2}, \frac{1+ij}{2}$ in the quaternion algebra $\mathrm{End}(E_0)_{\mathbb{Q}}$ over $\mathbb{Q}$ that is ramified at p and ∞.

The information (p, a, b, E_0, O_0) is then published. Note that [Cas+24] also publishes two points P_0, Q_0. These points are necessary for the functioning of certain algorithms that are being used in SQIsign2D-East, but we will not go into the role of these points. So for the sake of simplicity, we will ignore these points.

First, the sender generates an isogeny $\tau : E_0 \to E_A$ of prime degree $N_\tau < \sqrt[4]{p}$. The curve E_A is published and τ is kept private. The sender then computes an isogeny $\psi : E_0 \to E_1$ of odd degree $N_\psi < 2^{a+b}$ and again publishes E_1, while keeping ψ secret. The sender then uses some publicly available method to convert his message into an isogeny $\phi : E_1 \to E_2$ of degree $N_\phi = 2^b$. The challenge, then, is for the sender to find isogenies $\sigma : E_A \to E_2$ and $\omega : E_A \to E_3$ with very specific properties. For the exact properties, see [Cas+24, 1.2] Using the private information τ, the sender privately computes such σ, ω and publishes them. The receiver can then verify that these isogenies indeed satisfy the specific criteria. This can be visualized in the following diagram:



Everything in this diagram is public, except for τ and ψ.

The security of SQIsign2D-East relies on the assumption that the challenge to find ω, σ with the right properties is very hard without knowledge of τ. If someone like the forger wants to impersonate the sender and does not know τ, the forger is stuck in the hard formulation of the problem in terms of isogenies. However, the curve E_0 and its endomorphism ring $\mathrm{End}(E_0) = O_0$ are known, so with a known isogeny $\tau : E_0 \to E_A$, the sender can use the Deuring correspondence to rephrase the problem in terms of ideals of orders in quaternion algebras.

This is also why ψ is kept secret. If it would be public, then after publishing σ, the forger could compute $\sigma^\vee \circ \phi \circ \psi$, which is an isogeny $E_0 \to E_A$. The Deuring correspondence can then be used as well to state the problem in terms of ideals. This can be used to generate new σ', ω' that also pass the verification without being rejected. But then the signature is forged!

5.3 Sampling ideals

In this subsection, we zoom in on how isogenies correspond to ideals in SQIsign2D-East. We use [Cas+24, 4.2] as our main reference.

For an isogeny s, let I_s be its corresponding ideal under the Deuring correspondence. In SQIsign2D-East, the sender finds an isogeny σ by computing its corresponding ideal I_σ. First, the isogeny $\phi \circ \psi \circ \tau^\vee : E_A \to E_2$ is computed. Its corresponding ideal is $J := \overline{I}_\tau I_\psi I_\phi$. The assignment $I \mapsto \overline{I}$ is the standard involution. Then an element $\alpha \in J$ is sampled in order to find an ideal $I_\sigma = J\frac{\overline{\alpha}}{N_\tau N_\psi 2^b}$. The sampled α must, however, have some properties.

Definition 5.3.1. Let q be a positive integer, let N_τ prime and let $M(q) := q(2^a - q)(2^{a+b} - q(2^a - q)$. Then, q is $(2^a, 2^b, N_\tau)$-nice if q satisfies:

(i) $q \equiv 1 \pmod 2$;

(ii) $q < 2^a$;

(iii) $q(2^a - q) < 2^{a+b}$;

(iv) $\left(\frac{M(q)}{N_\tau}\right) = \left(\frac{-1}{N_\tau}\right)$.

The symbols $\left(\frac{\cdot}{\cdot}\right)$ denote Legendre symbols.

The element α must be generated such that the resulting ideal I_σ has norm $\mathrm{N}(I_\sigma)$ that is $(2^a, 2^b, N_\tau)$-nice. As shown in [Cas+24, 2], when $N_\tau \approx 2^e$ holds, then after approximately e signatures, the value of N_τ can be uniquely determined by the forger due to a leakage of Legendre symbols. To avoid this, the $(2^a, 2^b, N_\tau)$-niceness requirement is replaced by another requirement.

Definition 5.3.2. Let q be a positive integer. Then, q is $(2^a, 2^b, f)_3$-*nice* if $q' := q/\gcd(q, f)$ satisfies:

(i) $q'(2^a - q')(2^{a+b} - q(2^a - q)) \equiv 0 \pmod 3$;

(ii) $q' \equiv 1 \pmod 2$;

(iii) $q' < 2^a$;

(iv) $q'(2^a - q') < 2^{a+b}$.

In the proposed fix for SQIsign2D-East in [Cas+24, 3], an element α is sampled with the property that $\mathrm{N}(\alpha) < f2^a\mathrm{N}(J)$ and such that $q := \mathrm{N}(\alpha)/\mathrm{N}(J)$ is $(2^a, 2^b, N_\tau)_3$-nice. We can then take $I_\sigma = J\frac{\overline{\alpha}}{\mathrm{N}(J)}$.

The approach for generating such elements $\alpha \in J$ is by sampling them at random 1000 times, and then hopefully a suitable α is found. Since we take $2^a \approx \sqrt{p}$, it is not guaranteed that we actually find a suitable α, as there are way more than 1000 elements in J that do not satisfy the $(2^a, 2^b, f)_3$-niceness criteria. So in order for the fix to be feasible, we must know something about the probabilities that a sampled α has an associated $q = \mathrm{N}(\alpha)/\mathrm{N}(J)$ that is $(2^a, 2^b, f)_3$-nice.

By conditions (iii) and (iv) of Definition 5.3.2, there are only finitely many elements α to consider sampling, since these criteria impose bounds on the norm of α. By conditions (i) and (ii), we need to know what the odds are that specific congruence relations are satisfied on the norm of α.

We let $\mathbb{P}_{r,n}$ denote the value of the limit of Problem 2.3.2, associated to the ideal J. The probability that q (associated to a sampled α) is $(2^a, 2^b, f)_3$-nice can be approximated as

$$\mathbb{P}(q \text{ is nice}) \approx \sum_{r=0}^{6f-1} c_{r,2}c_{r,3}\mathbb{P}_{r\mathrm{N}(J),6f\mathrm{N}(J)}\frac{\gcd(r,f)^2}{f^2}. \tag{5.3.3}$$

Here $c_{r,2}c_{r,3} \in \{0, 1\}$ with $c_{r,2} = 1$ if and only if $r/\gcd(r, f)$ is odd, and $c_{r,3} = 1$ if and only if $a \equiv b \pmod 2$ or $r/\gcd(r, f) \not\equiv 1 \pmod 3$.

The values of $\mathbb{P}(q \text{ is nice})$ can be found using Theorem 4.5.1, once we have verified that J is a lattice that satisfies the necessary criteria. The ideal J is a left ideal of the order O_0; the order that is obtained from $\mathrm{End}(E_0)$ via the Deuring correspondence. This order O_0 is maximal in a quaternion algebra B that is ramified at p and ∞, and isomorphic to $\mathrm{End}(E_0)$. By Lemma 4.5.2, we see that J satisfies the criteria, so we can apply the results. Furthermore, note that $6f$ is way less than p, so we are never dealing with the probabilities in the ramified case.

The results in [Cas+24] that are deduced from approaches using $\mathbb{P}(q \text{ is nice})$ rely on the truth of Conjecture 6 in [Cas+24]. As we have seen in Subsection 4.5, Conjecture 6 is not true in its greatest generality. However, for the purpose of sampling ideals I_σ with the right properties, the probabilities $\mathbb{P}_{r,n}$ do correspond to the conjectured values. In particular, the derived results that were reliant on Conjecture 6 do hold.

6 Future work

The central problem in this thesis has been to find the limits 2.3.2. We did manage to solve Problem 2.3.1 for all Eichler orders and all their locally principal lattices, but that is far from solving Problem 2.3.1 in its greatest generality. So it would be interesting to further study the probabilities $\mathbb{P}_{r,n}$ for arbitrary orders O and for integral lattices that are not locally principal.

We can generalize the problem even further by considering ideals I with integral elements, but where $I^2 \subset I$ does not hold. An example is the lattice I with $\mathbb{Z}$-basis $1, i, j, 2ij$ inside $(-1, -1 \mid \mathbb{Q})$. All its elements are integral, so the limit 2.3.2 does make sense for I, but $ij \notin I$, so we find $I^2 \not\subset I$.

We can also notice that the local approach we used for solving Problem 2.3.1 still works if the corresponding global quaternion algebra is split. So is there any way to make sense of the probabilities $\mathbb{P}_{r,n}$ for integral lattices in $M_2(\mathbb{Q})$?

Finally, we can regard Problem 2.3.1 as a problem stated in terms of a quaternary quadratic form. Every norm map of a quaternion algebra is a quadratic form after all. We can extend the problem to include arbitrary quadratic forms instead of just norm forms. We heavily made use of the multiplicative property of the norm, so It would be interesting to investigate the effect of this multiplicativity on the outcome of the probabilities.

References

[Cas+24] Wouter Castryck et al. *Breaking and Repairing SQIsign2D-East*. Cryptology ePrint Archive, Paper 2024/1453. 2024. URL: https://eprint.iacr.org/2024/1453.

[GL24] Eyal Z Goren and Jonathan R Love. "Supersingular elliptic curves, quaternion algebras and applications to cryptography". In: *arXiv preprint arXiv:2410.06123* (2024).

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[Hus87] Dale Husemöller. "Elliptic curves, volume 111 of". In: *Graduate Texts in Mathematics* 99 (1987).

[Jac12] Nathan Jacobson. *Basic algebra I*. Courier Corporation, 2012.

[Nak+24] Kohei Nakagawa et al. "SQIsign2D-East: A new signature scheme using 2-dimensional isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2024, pp. 272–303.

[Neu13] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[Voi21] John Voight. *Quaternion algebras*. Springer Nature, 2021.