Quaternion Algebras and the Graph Method for Elliptic Curves

by
Isabelle Déchène

Supervised by
Henri Darmon

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Master of Science

Department of Mathematics and Statistics
McGill University, Montreal

December 1998

0-612-50750-5

Abstract

La méthode des graphes fait appel autant à la théorie des algèbres de quaternions qu'aux courbes elliptiques ou aux formes modulaires pour en arriver à déterminer tous les points supersinguliers en une charactéristique donnée et ainsi d'obtenir une base de $S_2(N)$.

La présente thèse vise donc à exposer le principe de la méthode des graphes: elle se divise en deux grandes parties. Dans un premier temps, on introduit les bases essentielles de l'arithmétique des quaternions. Cette partie est conçue pour répondre à la fois aux besoins des néophytes (en présentant une introduction relativement complète) et des initiés, en devenant une référence courte et rapide. La seconde partie porte plus spécifiquement sur la méthode des graphes en elle-même: après divers rappels, notamment au niveau des formes modulaires et des courbes elliptiques, le troisième chapitre se penche sur la méthode proprement dite. Une dernière section montrera pour sa part une application concrète de la théorie.

The graph method simultaneously uses the theory of quaternion algebras, elliptic curves and modular forms in order to determine all supersingular points in a given characteristic and hence to obtain a basis of $S_2(N)$. The goal of this thesis is to expose the principles of the graph method: it is therefore divided into two main parts: First, we introduce the essentials of the arithmetic of quaternions. This part is made to fit two needs: on one hand, a good introduction for novices; on the other hand, a fast and quick reference for those who are already familiar with the subject. The second part focusses on the graph method itself: after some recalls, namely about modular forms and elliptic curves, the third chapter is more specifically oriented toward the method as the last section gives a practical application of it.

Preface

Doing mathematics is something I always enjoyed. Back to Elementary school, I loved to rack my brain, trying to figure out how could work the mathematical trick allowing my uncle to guess my age simply by playing with numbers which could not be choosen randomly... Throughout the years, I became more and more familiar with maths. I even thought it could be a simple amusement: how fun it was to search for Fibonacci sequence in a pine cone...

So I decided to pursue studies in maths. It then became a serious matter, as subjects became harder and harder, as years go by. Being engaged in a Master's thesis didn't ease my task: like everyone else, I had my ups and downs, even during the last two years...

That is why I would like to thank all of you of the small community of students in number theory from the four Montreal universities. Special thanks to Dr. Andreas Schweizer for his precious help in my general studies on quaternion algebras (of which you will only see a small part in those pages). Good thoughts also to my supervisor, Henri Darmon, for his trust, his respect and the simplicity of our relationship. Et enfin, merci à toi Daniel, pour tes encouragements constants, ta patience et ton écoute.

That work is dedicated to all of them: after all, it is for people like them that I still love to do maths: because beyond the computer, there are men and women...

Contents

Introduction

A lot of people use the introduction of their manuals to justify the need of writing *'yet-another-book-on-the-subject...'*. This part will be easy for us, as the graph method touches on two strong topics of algebraic number theory: elliptic curves, which are fairly well treated (especially since Wiles proved Fermat's last theorem), and the arithmetic of quaternion algebras, somehow more neglected. In that case, the researcher is confronted with a choice: either work with original articles and therefore face the difficulty of various notations and languages, or use one of the main references such as the book of Marie-France Vignéras [Vig80], written in French.

We therefore saw a good occasion to prepare a thesis which would present an up-to-date synthesis on that particular matter. The first chapter may serve either as a quick introduction guide, providing important results for the beginners, or as a concise reference for those who are already familiar with the subject. Therefore, the emphasis will not be made on how the theorical results themselves are obtained, but rather on how to use them in practice.

After presenting elliptic curves and modular forms, we get to the heart of the matter: the graph method developped in the mid 1980's by J.-F. Mestre and J. Oesterlé. It can sometimes be used to obtain explicit equations of strong modular elliptic curves, which are fundamentals in number theory, but mainly for computing spaces of modular forms of a given level, their Fourier expansion, and the action of Hecke operators on them.

Chapter 1

Quaternion Algebras

The study of quaternion algebras from an arithmetic point of view gained its prominence around the 1930's, thanks to the important work of Eichler. Today, the subject has become an important part of modern number theory.

In this chapter, we use a minimalist approach to introduce quaternion algebras: our goal is to exploit them in regard to the graph method.

One will therefore find only few justifications, as well as few comments between definitions, lemmas or examples: this is done on purpose in order to ease the reading.

Those less familiar with the subject or wanting to learn more about a particular aspect will always find complete reference for each specific result not thoroughly explained.

1.1 Basic Concepts

Let K be a field.

Definition 1.1 :

A K-algebra A is said to be *central* if its center equals $K \cdot 1_A$ $(:= \{k \cdot 1_A | k \in K\})$

Definition 1.2 :

A K-algebra is said to be *simple* if it has no two-sided ideal except $\{0\}$ and itself.

Definition 1.3 :

A quaternion algebra H over K is a central simple K-algebra of degree 4 over K.

Remark : One can show that the following statement is indeed equivalent to the definition of a quaternion algebra just given:

H is a central K-algebra of degree 4 over K such that there is a separable K-algebra L of degree 2 over K for which there exists $\theta \in K \backslash \{0\}$ and $u \in H$

such that

$$\begin{cases} \bullet\ H = L + Lu \\ \bullet\ u^2 = \theta \\ \bullet\ um = \bar{m}u, \forall m \in L \end{cases}$$

where $m \mapsto \bar{m}$ is the nontrivial K-automorphism of L.

In this case, we write $H = \{L, \theta\}$.

Remark : One may write $L = K(i)$, where $i^2 = a \in K \backslash \{0\}$ if $Char(K) \neq 2$, and $i^2 + i = a \in K \backslash \{0\}$ if $Char(K) = 2$ (this follows from Kummer theory and Artin-Schreier theory respectively).

Setting $u = j$, one has $H = K + Ki + Kj + Kij$, where

$$i^2 + i = a, j^2 = u^2 = \theta, ij = j(1 + i), \text{ if } Char(K) = 2$$

and

$$i^2 = a, j^2 = u^2 = \theta, ij = -ji \text{ if } Char(K) \neq 2$$

Reference: For details, see [Vig80, I.1, p.1-5]

Example 1.4 : $M_2(K)$

$M_2(K)$, the K-algebra of 2×2 matrices over a field K is a quaternion algebra.

Example 1.5 : Hamilton's quaternions

Take $K := \mathbb{R}$ as the base field. The ring $\mathcal{H} := \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$ defined by the relations $i^2 = -1, j^2 = -1$ and $ij = -ji$ is a quaternion algebra over $\mathbb{R}$. Note that it is not isomorphic to $M_2(\mathbb{R})$ (since $\mathcal{H}$ is a division ring).

Definition 1.6 :

The *conjugation* ‘ $\bar{\cdot}$ ’ is the K-anti-automorphism $h \mapsto \bar{h}$ of H extending the nontrivial K-automorphism ‘ $\bar{\cdot}$ ’ of L determined by $\bar{u} = -u$.

Lemma 1.7 : Basic properties of conjugation

$\forall a, b \in K, \forall l, m \in L, \forall g, h \in H,$

- $\overline{ag + bh} = a\bar{g} + b\bar{h}$ (Linearity)
- $\bar{\bar{h}} = h$ (Involution)
- $\overline{gh} = \bar{h}\bar{g}$ (Anti-isomorphism)
- $\overline{l + mu} = \bar{l} - mu$

Definition 1.8 :

The *(reduced) Trace* $Tr(\cdot)$ is defined by:

$$\begin{array}{rccl} Tr: & H & \rightarrow & K \\ & h & \mapsto & Tr(h) := h + \bar{h} \end{array}$$

Definition 1.9 :

The *(reduced) norm* $N(\cdot)$ is defined by:

$$\begin{array}{rccl} N: & H & \rightarrow & K \\ & h & \mapsto & N(h) := h \cdot \bar{h} \end{array}$$

Remark : The trace and norm are well-defined since for all $h \in H$,

$Tr(h) \overset{def}{=} h + \bar{h} = \bar{\bar{h}} + \bar{h} = \overline{\bar{h} + h} = \overline{h + \bar{h}} \overset{def}{=} \overline{Tr(h)}$.
So, $Tr(h) = \overline{Tr(h)}$ and hence $Tr(h) \in K$.

$N(h) \overset{def}{=} h \cdot \bar{h} = \bar{\bar{h}} \cdot \bar{h} = \overline{h \cdot \bar{h}} \overset{def}{=} \overline{N(h)}$.
So, as above, $N(h) = \overline{N(h)}$ and therefore, $N(h) \in K$.

Lemma 1.10 : Basic properties of the Trace and Norm

$\forall a, b \in K, \forall g, h \in H$,

- $N(gh) = N(g)N(h)$
- $N(h) \neq 0$ if and only if $h \in H^{\times}$.
  In this case, we then have $h^{-1} = \bar{h} \cdot N(h)^{-1}$
- $Tr(ag + bh) = a \cdot Tr(g) + b \cdot Tr(h)$

Remark : For an element $h = w + xi + yj + zij$, we get $\bar{h} = w - xi - yj - zij$,

$Tr(h) = 2w$, $N(h) = w^2 - ax^2 - by^2 + abz^2$.

Example 1.11 :

With the matrices in $M_2(K)$, we have, if $h := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$,

$$\bar{h} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}, Tr(h) = a + d \,, N(h) = ad - bc$$

1.2 Internal structures

At first sight, the notions of this section may inevitably sound familiar. One will read the same words he is used to read, in a context that seems to be the same... But what if experience could sometimes betray us?

What if, all of a sudden, *'the set of integers would no longer form a ring'* or if *'ideals would not always be subrings'*?

Indeed, all the above occurs with quaternion algebras. That is why we suggest to the reader to keep his/her mind wide open, even if it means to pretend a temporary amnesia, for he will meet many 'homophones' in the next few pages.

That little warning completed, let us now introduce the actors we will play with throughout this section: let R be a Dedekind ring, K be its field of fractions and H be a quaternion algebra over K.

Definition 1.12 :
Let V be a vector space over K. A R-module L of V is said to be an *R-lattice* if $L \subseteq V$ and L is finitely generated.

Definition 1.13 :

Let V be a vector space over K. An R-lattice L of V is said to be *complete* if $K \otimes_R L \cong V$.

Definition 1.14 :

An *ideal* of H is a complete R-lattice.

Definition 1.15 :

An element $h \in H$ is said to be an *integer* over R if $R[h]$ is an R-lattice of H.

Lemma 1.16 : Let $h \in H$ be given. Then,

h is an integer over R if and only if $Tr(h) \in R$ and $N(h)$ belong to R.

Remark : In practice, one uses the above lemma instead of the definition in order to identify integers.

Warning : The sum and product of two integers is not necessary an integer! For example, take $R := \mathbb{Z}$, $K := \mathbb{Q}$, $H := M_2(\mathbb{Q})$,

$$a = \begin{bmatrix} 0 & 2 \\ 1/2 & 0 \end{bmatrix} \quad \& \quad b = \begin{bmatrix} 1/2 & 3/4 \\ -1 & 1/2 \end{bmatrix}$$

Here, a and b are integers, but neither $(a + b)$ or $(a \cdot b)$ is.

Hence, the set of integers does not form a ring. For this reason, we will focus on specific subsets (called orders) having a ring structure.

Definition 1.17 :

An ideal $\mathcal{O}$ of H is said to be an *order* if $\mathcal{O}$ is itself a ring.

Remark : The concept of order is fundamental in the study of the arithmetical properties of quaternion algebras. In our case, we will be ultimately interested in working with quaternion algebras over the rationals. So, if we set $R := \mathbb{Z}$, $K := \mathbb{Q}$ and H to be a quaternion algebra over $\mathbb{Q}$, it might be a good idea to explicitely rewrite the definition of an order in this case.

$$\mathcal{O} \text{ is an order of } H \Longleftrightarrow \begin{cases} \bullet\, \mathcal{O} \subseteq H \\ \bullet\, \mathcal{O} \text{ is a ring} \\ \bullet\, \mathcal{O} \text{ is finitely generated as a } \mathbb{Z}\text{-module} \\ \bullet\, \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} \cong H \end{cases}$$

Lemma 1.18 : Let $\mathcal{O} \subseteq H$ be given. Then,

$$\mathcal{O} \text{ is an order} \Longleftrightarrow \begin{cases} \bullet\, R \subseteq \mathcal{O} \\ \bullet \forall\, h \in \mathcal{O}, h \text{ is an integer} \\ \bullet\, \mathcal{O} \text{ is a ring} \\ \bullet\, K\mathcal{O} = H \end{cases}$$

Reference: [Vig80, proposition 4.2, p. 20]

Example 1.19 :

$M_2(\mathbb{Z})$ is an order of $M_2(\mathbb{Q})$.

Example 1.20 :

For the Hamilton's quaternion $\mathcal{H}$, the ring $\mathbb{Z}\left[i, j, \frac{1+i+j+ij}{2}\right]$ is an order.

Definition 1.21 :

Let $\mathcal{O}$ be an order of H. The *units* of $\mathcal{O}$ are the elements of $\mathcal{O}$ which have an inverse in $\mathcal{O}$. This group is denoted $\mathcal{O}^{\times}$.

Lemma 1.22 : Let $\mathcal{O}$ be an order of H. Then, an element $h \in \mathcal{O}$ belongs to $\mathcal{O}^{\times}$ if and only if $N(h) \in R^{\times}$.

Proof Simply remark that $h^{-1} = \overline{h} \cdot N(h)^{-1}$.

□

Definition 1.23 :

An order $\mathcal{O}$ is said to be *maximal* if it is not properly contained in any other order.

Definition 1.24 :

An order E is said to be an *Eichler order* if it is the intersection of two maximal orders.

Definition 1.25 :

Let I be an ideal. Let $\mathcal{O}_l := \mathcal{O}_l(I) := \{h \in H | hI \subseteq I\}$ and

$\mathcal{O}_r := \mathcal{O}_r(I) := \{h \in H | Ih \subseteq I\}$. Then, $\mathcal{O}_l$ and $\mathcal{O}_r$ are called respectively the *left and right order* of I. We also say that I is *'on the left of'* $\mathcal{O}_l$ and *'on the right of'* $\mathcal{O}_r$.

Definition 1.26 :

Let I be an ideal. The *reduced norm* $N(I)$ is the fractional ideal of R generated by the set $\{N(h)|\ h \in I\}$.

Definition 1.27 :

Let I be an ideal. Then, I is said to be:

- *two-sided* *if* $\mathcal{O}_l = \mathcal{O}_r$
- *normal* *if* $\mathcal{O}_l$ and $\mathcal{O}_r$ are maximal
- *integral* *if* $I \subseteq \mathcal{O}_l$ and $I \subseteq \mathcal{O}_r$
- *principal* *if* $\exists\ h \in H$ such that $I = \mathcal{O}_l h = h\mathcal{O}_r$

Definition 1.28 :

Let I be an ideal of H. Its *inverse* is defined by

$$I^{-1} = \{h \in H | Ih \in \mathcal{O}_l(I)\} = \{h \in H | hI \subseteq \mathcal{O}_r(I)\} = \{h \in H | IhI \subseteq I\}$$

Lemma 1.29 : Let I be an ideal of H. Then,

(i) I^{-1} is also an ideal of H

$$(ii) \begin{cases} \bullet\ \mathcal{O}_r(I) \subseteq \mathcal{O}_l(I^{-1}) \\ \bullet\ \mathcal{O}_l(I) \subseteq \mathcal{O}_r(I^{-1}) \end{cases}$$

$$(iii) \begin{cases} \bullet\ I \cdot I^{-1} \subseteq \mathcal{O}_l(I) \\ \bullet\ I^{-1} \cdot I \subseteq \mathcal{O}_r(I) \end{cases}$$

Reference: See [Vig80, Lemme 4.3(3), p.21] for details.

1.3 Quaternion algebras over local fields

The goal of this section is to characterize all the quaternion algebras over a given local field. We first reduce the problem to quaternion division rings. Then, we treat the cases where the base fields are respectively $\mathbb{R}$ and $\mathbb{C}$. Then, after some recalls from valuation theory, we expose the main result.

Let $\mathbb{R}_+$ denote the nonnegative real numbers and let K be a field.

Lemma 1.30 : Let H be a quaternion algebra over K. Then, either $H \cong M_2(K)$ or H is a division ring.

Proof By Wedderburn's structure of simple rings theorem [1], there exists a unique $n \in \mathbb{N}^*$ and a unique (up to isomorphism) division algebra D over K such that $H \cong M_n(D)$. But since H is of degree 4 over K, the only possibilities for n are 1 and 2:

[1] See, for example, [Wei73, theorem IX.1, p. 164]

- If $n = 1$, then $H \cong M_1(D) \cong D$. So, $H \cong D$ with D being a division algebra. Hence, H is also a division algebra.
- If $n = 2$, then $H \cong M_2(D)$. Hence, their center are isomorphic: K =Center(H) $\cong$Center($M_2(D)$) $\cong D$. We get that $K \cong D$ and so $H \cong M_2(K)$, as wanted.

□

Corollary 1.31 : For a quaternion algebra H over K, the following are equivalent:

(i) $\exists h \in H \backslash \{0\}$ such that $N(h) = 0$
(ii) $H \cong M_2(K)$
(iii) $\exists h \in H \backslash \{0\}$ such that $Tr(h) = N(h) = 0$

Proof

(i) ⇒ (ii) By hypothesis, $0 = N(h) \overset{def}{=} h \cdot \bar{h}$.
So, h is a zero divisor and hence H cannot be a division ring.
Therefore, by the above lemma, $H \cong M_2(K)$.

(ii) ⇒ (iii) Set $h := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then, clearly, $Tr(h) = N(h) = 0$.

(iii) ⇒ (i) Trivial.

□

We are now ready to classify the quaternion algebras over any algebraically closed field:

Theorem 1.32 :

Let K be an algebraically closed field and H be a quaternion algebra over K. Then $H \cong M_2(K)$.

Proof Say $H = \{L, \theta\}$. Then, since K is algebraically closed, L cannot be a field. So, $L \backslash \{0\}$ contains a non invertible element m. Therefore, $N(m) = 0$ (otherwise, $m \cdot (\overline{m} \cdot N(m)^{-1}) = 1$ with $\overline{m} \cdot N(m)^{-1} \in L$, so m would be invertible). Finally, $H \cong M_2(K)$ by above corollary.

□

Remark : $M_2(\mathbb{C})$ is the only quaternion algebra over $\mathbb{C}$.

We already know that $\mathcal{H}$ (section 1.1 on page 5) is a quaternion division algebra over $\mathbb{R}$. Indeed, much more is true...

Theorem 1.33 (Frobenius):

Any division quaternion algebra over $\mathbb{R}$ is isomorphic to the Hamilton's quaternion $\mathcal{H}$.

Reference: See [Vig80, corollary 2.5, p. 7] or [Hun74, corollary IX.6.8, p. 461] for details.

Definition 1.34 :

A map $\begin{array}{cccc} |\cdot| : & K & \rightarrow & \mathbb{R}_+ \\ & a & \mapsto & |a| \end{array}$ is said to be an *absolute value* on K if, for all

$a, b \in K$:

(*i*) $|a| = 0$ if and only if $a = 0$
(*ii*) $|a \cdot b| = |a| \cdot |b|$
(*iii*) $|a + b| \leq |a| + |b|$ (Triangle inequality)

Definition 1.35 :

An absolute value $|\cdot|$ on K is said to be *non-archimedean* if, for all $a, b \in K$:

$$(iii') \quad |a + b| \leq \max(|a|, |b|) \text{ (Strong triangle inequality)}$$

Definition 1.36 :

The absolute value

$$|\cdot|_T : \quad K \to \mathbb{R}_+$$
$$a \mapsto |a|_T := \begin{cases} 0 \text{ if } a = 0 \\ 1 \text{ if } a \neq 0 \end{cases}$$

is called the *trivial absolute value* of K.

Definition 1.37 :

An absolute value $|\cdot|$ on K is said to be *discrete* if the image of $K \backslash \{0\}$ under $|\cdot|$ is a cyclic group.

Definition 1.38 :

A *discrete valuation ring* is a principal ideal ring that has exactly one nonzero prime ideal.

Definition 1.39 :

Let R be a commutative discrete valuation ring with identity and let $\wp$ be its only nonzero prime ideal. Then, $R/\wp$ is called the *residue field* of R.

Definition 1.40 :

A field K with an absolute value $|\cdot\cdot|$ is called a *local field* if it satisfies the following conditions:

(*i*) $|\cdot|$ is non-archimedean, discrete and non-trivial.
(*ii*) K is complete relative to $|\cdot\cdot|$.
(*iii*) The residue field of $|\cdot\cdot|$ is finite

Example 1.41 :

For every prime number p, the field of p-adic numbers $\mathbb{Q}_p$ is a local field.

Example 1.42 :

$\mathbb{F}_n[[x]]$, the field of formal Laurent series in one indeterminate over the finite field $\mathbb{F}_n$, is a local field.

Theorem 1.43 :

Any local field is (isomorphic to) either $\mathbb{F}_n[[x]]$ for a finite field $\mathbb{F}_n$, or to a finite algebraic extension of $\mathbb{Q}_p$, for some p.

We are now ready to state the **classification theorem of quaternion algebras over local fields**

Theorem 1.44 :

Let K be a local field. Then, there is a unique (up to isomorphism) quaternion division algebra over K.

Reference: See [Vig80, theorems 1.1 and 1.3, p. 31-36] for details.

1.4 Quaternion algebras over global fields

Definition 1.45 :

A *global field* is a finite dimensional extension of one of the following fields:

- $\mathbb{Q}$, the field of rational numbers
- $\mathbb{F}_p(x)$, the field of rational fractions in one indeterminate with coefficients in the finite field $\mathbb{F}_p$, where p is a prime number.

Definition 1.46 :

Let K be a global field.

Let $\mathcal{E} := \{\ i | \text{for some local field } L, i : K \longrightarrow L, i \text{ embedding}\ \}$. Two embeddings $i, i' \in \mathcal{E}$, say $i : K \longrightarrow L$ and $i' : K \longrightarrow L'$ are said to be *equivalent* if $\exists f : L \longrightarrow L'$, f isomorphism such that $i' = f \circ i$ and we write $i \sim i'$. An equivalence class under ' $\sim$ ' is called a *place* of K. Let v be any place of K. We denote by $i_v : K \longrightarrow K_v$ a dense embedding of K in a local field K_v representing the place v. If K_v contains a field isomorphic to $\mathbb{R}$, then v is said to be an *infinite* (or *archimedean*) place of K. Otherwise, v is said to be a *finite* place of K.

Example 1.47 : Places of $\mathbb{Q}$

- Only one infinite place '∞' represented by the natural embedding of $\mathbb{Q}$ into $\mathbb{R}$
- The finite places are represented by the natural embeddings of $\mathbb{Q}$ into $\mathbb{Q}_p$, the field of p-adic numbers, for every prime number p.

For more details, see [Vig80, section III.1, p.58].

Definition 1.48 :

Let K be a global field and H be a quaternion algebra over K. Let v be a place of K and $i_v : K \longrightarrow K_v$ be a representative of v. If $H \otimes_K K_v$ is a division ring, then v is said to be *ramified* in H.

Definition 1.49 :

Let K be a global field and H be a quaternion algebra over K.

Let $Ram(H)$:= $\{ v|v$ is a place of K ramified in $H \}$

Definition 1.50 :

Let K be a global field and H be a quaternion algebra over K. The *reduced discriminant d* of H is defined by

$$d := \prod_{\substack{v \in Ram(H) \\ v \text{ finite}}} v$$

Lemma 1.51 : Let K be a global field and H be a quaternion algebra over K. Then,$|Ram(H)| < \infty$ (i.e. the number of places of K ramified in H is finite).

Reference: See [Vig80], lemma III.1, p. 58

Theorem 1.52 :

Classification of Quaternion Algebras over Global Fields

Let K be a global field. Then,

- If H is a quaternion algebra over K, then $|\mathrm{Ram}(H)|$ is even (i.e. the number of places of K ramified in H is even).
- Let S be a finite set of places of K such that $|S|$ is even. Then there is a unique H (up to isomorphism), H quaternion algebra over K such that S=Ram(H).

Reference: See [Vig80] , theorem 3.1, p. 74

Definition 1.53 :

Let H be a quaternion algebra over $\mathbb{Q}$. H is said to be *definite* if H is ramified at ∞. Otherwise, we say that H is *indefinite.*

Definition 1.54 :

Let p be a prime number. Let $H_{p,\infty}$ be *the* definite quaternion algebra over $\mathbb{Q}$ such that $Ram(H_{p,\infty}) = \{p, \infty\}$.

Remark : By the classification theorem over global fields (section 1.4, on page 20) since $|Ram(H_{p,\infty})| = 2$ is even, $H_{p,\infty}$ exists and is uniquely determined (up to isomorphism).

Remark : We have that $H_{2,\infty} = \mathcal{H}$, the Hamilton's quaternions (See section 1.1 on page 5).

Until now, our exposition of quaternion algebras has been very general, first because we wanted to give a true self-contained introduction and also because it wasn't more tedious to treat the whole theory. But for the definition of the next concept, we will restrict ourself to quaternion algebras over $\mathbb{Q}$ in order to simplify the exposition. It is indeed this particular case that we will be interrested in later on.

Notation: Let $\mathbb{Q}_\infty := \mathbb{R}$

Definition 1.55 :
Let H be a quaternion algebra over $\mathbb{Q}$ and L be a lattice of H. The quaternion algebra $H \otimes_\mathbb{Q} \mathbb{Q}_p$ over $\mathbb{Q}_p$ -is denoted by H_p and the lattice $L \otimes_\mathbb{Z} \mathbb{Z}_p$ of H_p is denoted by L_p.

Until the end of the section, let p be a fixed prime.

Definition 1.56 :
Let $r \in \mathbb{N}$ be given, $M \in \mathbb{N}^*$ be such that $p \not| M$ and let $N := p^{2r+1} \cdot M$. Also, let L be the unique unramified quadratic field extension of $\mathbb{Q}_p$ and R be the set of integers in L.

Definition 1.57 :

An order $\mathcal{O}$ of $H_{p,\infty}$ is said to have *level* N if, for every q, we have the following isomorphism over $\mathbb{Z}_q$:

$$\mathcal{O}_q \cong \begin{cases} \begin{bmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ N\mathbb{Z}_q & \mathbb{Z}_q \end{bmatrix} & \text{if } q \neq p \\ \left\{ \begin{bmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{bmatrix} \middle| \alpha, \beta \in R \right\} & \text{if } q = p \end{cases}$$

At first sight, this definition is not very intuitive. However, one can 'think' about the level as follows:

Let K be a field, H a quaternion algebra over K and E be an Eichler order of H. Then, by definition, there are maximal orders $\mathcal{O}$ and $\mathcal{O}'$ of H such that $E = \mathcal{O} \cap \mathcal{O}'$. Then, the *level* of E is somehow a **measure of the 'distance' between $\mathcal{O}$ and $\mathcal{O}$'.**

Later on, what we will want to do is to *pick* an Eichler order of a given level. Hence, we better make sure of its existence, and this is exactly what the following result shows in the case we will be treating:

Theorem 1.58 :

Let p be a prime number and N_1 be a positive integer such that $p \not| N_1$. Then, $H_{p,\infty}$ contains an Eichler order of level pN_1.

Reference: See [Vig80, p.39 and p. 84] as well as [BD96, p.417] for the details. Also, a method to obtain explicitely the Eichler orders of a given level N is explained in [Piz80, section 5, p. 368-371].

1.5 Class number

Definition 1.59 :

Two ideals I and J are said to be *left equivalent* (respectively *right equivalent*) if $\exists\ h \in H^\times$ such that $I = hJ$ (respectively $I = Jh$). In this case, we write $I \sim_l J$ (respectively $I \sim_r J$).

Remark : Of course, '$\sim_l$' and '$\sim_r$' are equivalence relations on any set S of ideals of H. We can therefore form left and right classes of ideals on S.

Definition 1.60 :

Let $\mathcal{O}$ be an order, $S_l := \{I | I$ ideal of H and $\mathcal{O}_l = \mathcal{O}\}$ and $S_r := \{I | I$ ideal of H and $\mathcal{O}_r = \mathcal{O}\}$. The *left classes* (respectively *right classes*) of $\mathcal{O}$ are the ideal classes of S_l (respectively S_r).

Lemma 1.61 : Let K be a field, H be a quaternion algebra over K and $\mathcal{O}$ be an order of H. Then, there is the same number of left and right classes of $\mathcal{O}$.

Reference: See [Vig80, lemme 4.9(1), p. 25].

Convention: The above lemma allows us to get rid of the specification 'left' or 'right' when talking about the 'number of classes of $\mathcal{O}$'.

Lemma 1.62 : Let K be a field and H be a quaternion algebra over K. Then, the class number of all **maximal** orders of H coincide.

Reference: See [Vig80, lemme 4.9(2), p. 25-26]

Definition 1.63 :
The *class number* h of H is the number of ideal classes of some **maximal** order.

Theorem 1.64 : Finiteness of the class number
Let K be a global field and H be a quaternion algebra over K. Then, the class number h of H is finite.

Reference: See [Vig80], theorem 5.4, p. 87.

Theorem 1.65 : Eichler's class number formula for indefinite quaternions
Let H be an indefinite quaternion algebra over $\mathbb{Q}$ and h be its class number. Then, $h = 1$.

Reference: The result follows from the 'strong approximation theorem' (See [Vig80, theorem 4.3, p. 81] for details).

Theorem 1.66 : Eichler's class number formula for $H_{p,\infty}$

Let p be a prime number and h be the class number of $H_{p,\infty}$. Then,

$$h = \begin{cases} 1 & if \quad p = 2 \\ \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{p-1}{12} & if \quad p \neq 2 \end{cases}$$

where $\left(\frac{a}{b}\right)$ is the Legendre symbol.

Reference: See [Eic38] for the original proof (in German) or [Vig80, proposition 3.2, p. 146] for a more general case.

Remark : Using the well-known properties of the Legendre's symbol [2] , one can rewrite the above formula for h in a case-by-case format that makes calculations by hand quicker.

$$h = \begin{cases} \lfloor \frac{p}{12} \rfloor & \text{if} \quad p \equiv 1(\text{mod } 12) \\ \lfloor \frac{p}{12} \rfloor \quad +1 & \text{if} \quad p \equiv 2,3 \text{ or } p \equiv 5,7(\text{mod } 12) \\ \lfloor \frac{p}{12} \rfloor \quad +2 & \text{if} \quad p \equiv 11(\text{mod } 12) \end{cases}$$

where $\lfloor \frac{a}{b} \rfloor$ is the 'floor function' (that is, $\lfloor \frac{a}{b} \rfloor$ is the unique integer such that $\lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} < \lfloor \frac{a}{b} \rfloor + 1$).

Table 1.1 : Value of some class number h of $H_{p,\infty}$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	$\cdots$
h	1	1	1	1	2	1	2	2	3	3	3	3	4	4	5	$\cdots$

Note : As we can see in the above table, the lowest value of p for which the class number is higher than one is when $p = 11$. This first nontrivial case will

[2] That can found, for example, in [ST87, p.242-250] or into your favorite book on basic number theory.

often be used in order to illustrate some parts of the theory: calculations by hand will then be less tedious and therefore make our exposition less laborious. Sometimes, we will even use various ways to compute the same quantities: this will give us a flavour of the difference of complexity between methods, which could not be done if we would use new examples each time. Moreover, we believe that keeping p to be 11 will make us appreciate how all the small steps we do will soon transform into parts of a **global procedure**. At the end, it might be a good idea to reread without interruption all the examples where $p = 11$ in order to see a full concrete application of the method. As we just saw, Eichler's class formula for $H_{p,\infty}$ (see 1.5 on page 24) gives us a simple expression for the class number of a given **maximal** order. In fact, it can be extended as follows to treat the case of any order.

Theorem 1.67 :

Let p be a prime number, $N_1 \in \mathbb{N}^*$ be such that $p \not| N_1$ and let $r \in \mathbb{N}$ be given. Let $N := p^{2r+1}N_1$ and $\mathcal{O}$ be an order of level N in $H_{p,\infty}$. Then, the class number $h(N)$ of $\mathcal{O}$ is given by:

$$\begin{aligned} h(N) = {} & \tfrac{N}{12}\left(1-\tfrac{1}{p}\right) \prod_{\substack{q|N_1 \\ q \text{ prime}}} \left(1+\tfrac{1}{q}\right) \\ & + \begin{cases} \frac{1}{4}\left(1-\left(\frac{-4}{p}\right)\right) \displaystyle\prod_{\substack{q|N_1 \\ q \text{ prime}}} \left(1+\left(\frac{-4}{q}\right)\right) & \text{if } 4 \not| N \\ 0 & \text{if } 4|N \end{cases} \\ & + \begin{cases} \frac{1}{3}\left(1-\left(\frac{-3}{p}\right)\right) \displaystyle\prod_{\substack{q|N_1 \\ q \text{ prime}}} \left(1+\left(\frac{-3}{q}\right)\right) & \text{if } 9 \not| N \\ 0 & \text{if } 9|N \end{cases} \end{aligned}$$

where $(\frac{a}{b})$ is the Legendre symbol.

In particular, the class number of any order of a **fixed** level N is independent of the particular order of level N.

Reference: See [Piz80, theorem 1.12, p. 346] for details.

1.6 Brandt matrices

Let p be a prime number and $N_1 \in \mathbb{N}$ be such that $p \nmid N_1$. We let $N := pN_1$. Throughout this section, we will restrict our study to the quaternion algebra $H_{p,\infty}$. As above, let $h(N)$ be the class number of level N. For each $n \in \mathbb{N}$, we will build from $H_{p,\infty}$ a matrix $B(n) = \left(b_{ij}{}^{(n)}\right) \in M_{h(N)}(\mathbb{Q})$ called the n^{th} Brandt matrix[3]. These matrices are of primordial importance for our later study of Hecke operators $\mathcal{T}_n$, but as in the best movie previews, let's keep the suspense on for the moment...

We fix our guest star to be an Eichler order $\mathcal{O}$ of $H_{p,\infty}$ of level N. Hence, $\mathcal{O}$ has $h(N)$ left classes of ideals. Let $I_1 \dots I_{h(N)}$ be representatives for each of these classes (so, by definition, $\mathcal{O}_l(I_i) = \mathcal{O}$ for $1 \leq i \leq h(N)$). To ease the notation, let, for $1 \leq i \leq h(N)$, $\mathcal{O}_i := \mathcal{O}_r(I_i)$ and $e_i := |\mathcal{O}_i^\times|$. Lastly, let, for $1 \leq i, j \leq h(N)$, $A_{ij}^{(n)} := \left\{\alpha \in I_j^{-1} I_i \,\middle|\, N(\alpha) \cdot \frac{N(I_j)}{N(I_i)} = n\right\}$.

[3] In the litterature, they are sometimes called Eichler-Brandt matrices.

Definition 1.68 :

With the above notations, the general term $b_{ij}^{(n)}$ of the n^{th} *Brandt matrix* $B(n)_{h(N)\times h(N)}$ is defined by

$$b_{ij}^{(n)} := \frac{|A_{ij}(n)|}{e_j}$$

Remark : For a generalization of the Brandt matrices to arbitrary quaternion algebras, see [Vig80, p.100].

Example 1.69 : N=11

Below are the first Brandt matrices when $N = 11$:

$$B(0) = \begin{bmatrix} 1/4 & 1/4 \\ 1/6 & 1/6 \end{bmatrix} \quad B(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad B(2) = \begin{bmatrix} 1 & 3 \\ 2 & 0 \end{bmatrix}$$

$$B(3) = \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} \quad B(4) = \begin{bmatrix} 5 & 3 \\ 2 & 4 \end{bmatrix} \quad B(5) = \begin{bmatrix} 4 & 3 \\ 2 & 3 \end{bmatrix}$$

From here, it's child's play to compute the eigenvalues a_n as well as other important quantities related to each $B(n)$. The following table reassemble some of them.

Properties of $B(n)$ for $N = 11$

n	$Tr(B(n))$	$c(n)$	a_n	
0	5/12	5/12	0	5/12
1	2	1	1	1
2	1	3	-2	3
3	3	4	-1	4
4	9	7	2	7
5	7	6	1	6

Chapter 2

Elliptic Curves and Modular Forms

As we did earlier, we will not be very general in this chapter: elliptic curves and modular forms being quite familiar for many mathematicians, we will assume that the basics of the subject are mastered by the reader. Those who would want more information before beginning this new chapter could find a good starting point in the article [Mur91] or on the web, at these two URL adresses http://www.best.com/˜cgd/home/flt/flt03.htm or http://www.best.com/˜cgd/home/flt/flt05.htm. For more complete references, one can find good help in [Sil86], [Kna92] or [Kob93].

We will therefore present elliptic curves and modular forms in a very precise manner, concentrating specifically on results regarding the graph method. However, some classical elements will be mentionned, as we do in our first section.

2.1 General recalls on elliptic curves

As usual, let K be a field.

Definition 2.1 :

Let $m \in \mathbb{Z}$ and let E be an elliptic curve over K. The *multiplication by m map* $[m]$ is defined by:

$$\begin{array}{rcl} [m]: E & \to & E \\ P & \mapsto & [m]P := \begin{cases} \underbrace{P + \ldots + P}_{m \quad terms} & if \quad m > 0 \\ 0 & if \quad m = 0 \\ \underbrace{(-P) + \ldots + (-P)}_{(-m) \quad terms} & if \quad m < 0 \end{cases} \end{array}$$

Definition 2.2 :

Let $m \in \mathbb{Z}^*$, E be an elliptic curve and $m \in \mathbb{Z}^*$.

$E[m] := \{P \in E | \ [m] \ P = 0\}$, the set of points of order m in E, is called the *m-torsion subgroup of E*.

Lemma 2.3 : Structure of the torsion subgroup

Let $m \in \mathbb{Z}^*$, K be a field and E be an elliptic curve over K. Then,

(*i*) $deg([m]) = m^2$

(*ii*) If $Char(K) = 0$ or $(m, Char(K)) = 1$, then $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$

(*iii*) If $Char(K) = p$, then $\forall\, n \in \mathbb{N}^*, E[p^n] \cong \{0\}$ or $\forall\, n \in \mathbb{N}^*, E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$.

Reference: See [Sil86, corollary 6.4, p. 89] for details.

Theorem 2.4 : On the value of $|Aut(E)|$

Let E be an elliptic curve over K and $Aut(E)$ be the automorphism group of E. Then,

$$|Aut(E)| = \begin{cases} 2 & \text{if} \quad j(E) \neq 0, 1728 & \\ 4 & \text{if} \quad j(E) = 1728 & \text{and } Char(K) \neq 2, 3 \\ 6 & \text{if} \quad j(E) = 0 & \text{and } Char(K) \neq 2, 3 \\ 12 & \text{if} \quad j(E) = 0 = 1728 & \text{and } Char(K) = 3 \\ 24 & \text{if} \quad j(E) = 0 = 1728 & \text{and } Char(K) = 2 \end{cases}$$

So, in all cases, $Aut(E)$ is a **finite** group such that $|Aut(E)| \,\Big|\, 24$.

Reference: See [Sil86, theorem 10.1, p. 103]

Definition 2.5 :

Let $N \in \mathbb{N}^*$, be given. The *Hecke subgroup* $\Gamma_o(N)$ is defined by:

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \mod N \right\}$$

Note : $\Gamma_0(N) \subseteq SL_2(\mathbb{Z})$

Theorem 2.6 :

Let $p \in \mathbb{N}$ be a prime number, K be a (perfect) field such that $Char(K) = p$ and E be an elliptic curve over K. For each $r \in \mathbb{N}^*$, let $\phi_r : E \longrightarrow E^{(p^r)}$ and $\hat{\phi}_r : E^{(p^r)} \longrightarrow E$ be the p^r-power Frobenius map and its dual. Then, the following are equivalent:

(i) $E[p^r] = 0$ for one (all) $r \geq 1$.

(ii) $\hat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$.

(iii) The multiplication by p map $[p] : E \longrightarrow E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

(iv) $End_K(E)$ is (isomorphic to) a **maximal** order in the quaternion algebra $H_{p,\infty}$.

Reference: See [Sil86, theorem 3.1(a), p. 137] and [Gro87, p.124] for details.

Definition 2.7 :

An elliptic curve satisfying the above equivalent conditions (i)-(iv) is said to be *supersingular*, or to have *Hasse invariant* 0. Otherwise, we say that E is *ordinary*, or that E has *Hasse invariant* 1.

Theorem 2.8 : Characterization of supersingular elliptic curves over finite fields

(i) Let K be a finite field such that $Char(K) = 2$. Then, the only supersingular elliptic curve over K is $y^2 + y = x^3$.

(ii) Let $p \in \mathbb{N}\backslash\{2\}$ be a prime number, K be a finite field such that $Char(K) = p$ and E be an elliptic curve over K with Weierstrass equation $E : y^2 = f(x)$, for some cubic polynomial $f(x) \in K[x]$ having distinct roots in $\bar{K}$. Then,

$$E \text{ is supersingular } \iff \text{ the coefficient of } x^{p-1} \text{ in } f(x)^{(p-1)/2} \text{ equals } 0$$

Reference: See [Sii86, theorem 4.1(2), p. 140] for all details.

Corollary 2.9 : Supersingular curves in Legendre form

Let $p \in \mathbb{N}\backslash\{2\}$ be a prime number, $m := (p-1)/2, H_p(t) := \sum_{i=0}^{m} \binom{m}{i}^2 t^i$, K be a finite field such that $Char(K) = p, \lambda \in \bar{K}\backslash\{0, 1\}$ and
$E : y^2 = x(x-1)(x-\lambda)$, an elliptic curve in the Legendre form over K. Then,

$$E \text{ is supersingular} \iff H_p(\lambda) = 0$$

Proof By part (ii) of above theorem,

$$\begin{aligned} E \text{ is supersingular } &\iff \text{ the coefficient of } x^{p-1} \text{ in } (x(x-1)(x-\lambda))^{(p-1)/2} \\ &\ \text{ equals zero} \\ &\iff \text{ the coefficient of } x^{2m} \text{ in } (x(x-1)(x-\lambda))^{m} \end{aligned}$$

equals zero

$\iff$ the coefficient of x^m in $(x-1)^m(x-\lambda)^m$

equals zero

$\iff$ the coefficient of x^m in

$\left(\sum_{j=0}^m \binom{m}{j} x^{m-j}(-1)^j\right)\left(\sum_{k=0}^m \binom{m}{k} x^{m-k}(-\lambda)^k\right)$

equals zero

$\iff \sum_{i=0}^m \binom{m}{m-i}(-1)^{m-i}\binom{m}{i}(-\lambda)^i = 0$

$\iff (-1)^m \cdot\cdot \sum_{i-0}^m \binom{m}{i}^2 \lambda^i = 0$

$\iff (-1)^m \cdot\cdot H_p(\lambda) = 0$

$\iff H_p(\lambda) = 0$

□

Example 2.10 : $N = p = 11$

Hence, $m = 5$ and

$$\begin{aligned} H_{11}(t) &= t^5 + 25t^4 + 100t^3 + 100t^2 + 25t + 1 \\ &\equiv t^5 + 3t^4 + t^3 + t^2 + 3t + 1 \pmod{11} \\ &\equiv (t^2 - t + 1)(t+1)(t-2)(t+5) \pmod{11} \end{aligned}$$

Hence, the only supersingular j-invariants in characteristic 11 are $j = 0$ and $j = 1 = 1728$.

2.2 Number of supersingular elliptic curves in characteristic p

Theorem 2.11 (Igusa):

Number of supersingular elliptic curves in characteristic p

Let $p \in \mathbb{N}$ be a prime number and h be the number (up to isomorphism) of supersingular elliptic curves in characteristic p. Then,

$$h = \begin{cases} \lfloor \frac{p}{12} \rfloor & \text{if } p \equiv 1 (\text{mod } 12) \\ \lfloor \frac{p}{12} \rfloor \; +1 & \text{if } p = 2,3 \text{ or } p \equiv 5,7 (\text{mod } 12) \\ \lfloor \frac{p}{12} \rfloor \; +2 & \text{if } p \equiv 11 (\text{mod } 12) \end{cases}$$

Reference: Oddly enough, when Deuring first conjectured this result, he thought that a direct computation of the number of supersingular invariant of characteristic p was *nicht leicht* [1]. In 1958, Jun-Ichi Igusa took up the challenge: the key was indeed to notice that the Hasse invariant satisfies a differential equation of the Gauss-Legendre type. The result? The whole article containing the proof [Igu58] is only two pages long! It is still the same proof that one can read in today's litterature, for example in [Sil86, theorem 4.1(c), p. 140-141].

Example 2.12 : $p = 11$

There are, up to isomorphism, two supersingular elliptic curves in characteristic p.

[1] Not easy at all!

Remark : It is on purpose that we used the letter 'h' in the above proposition just as we used it for the class number of a quaternion algebra. It is not ambiguous, since a quick glance at the **Eichler's class number formula for $H_{p,\infty}$** (page 24) reveals that they are equal! We thus obtain the following very important corollary:

Corollary 2.13 (Deuring): Quaternion algebras vs elliptic curves (Part II)
Let $p \in \mathbb{N}$ be a prime number, h_E be the number (up to isomorphism) of supersingular elliptic curves in characteristic p and h_Q be the class number of $H_{p,\infty}$. Then, $h_E = h_Q$.

Remark : This is the second time that we establish a connection between the seemingly unrelated quaternion algebras and elliptic curves. We recall that the first occurence was when we gave the equivalent definitions of a supersingular elliptic curve E on page 32: we then had that "$End(E)$ is a maximal order in $H_{p,\infty}$". This time, however, the affirmation is as strong as it is surprising. For the matter of being impressed, let's hold our breath a little more as there is still more (thrill) to come...

The main consequence of this is of course to be able to use quaternion algebras to derive properties of elliptic curves, just as we are used to do with modular forms. We must therefore always keep those relations in mind as they will be a true helping hand later on.

2.3 Supersingular points

Throughout the section, let $p \in \mathbb{N}$ be a prime number, $N_1 \in \mathbb{N}^*$ be such that $p \not| N_1$ and $N := pN_1$.

Definition 2.14 :

Let E (respectively E') be an elliptic curve over $\overline{\mathbb{F}}_p$ containing a cyclic subgroup C (respectively C') of order N_1. The two couples (E, C) and (E', C') are said to be *equivalent* if $\exists \phi : E \longrightarrow E', \phi$ $\overline{\mathbb{F}}_p$-isomorphism such that $\phi(C) = C'$.

Definition 2.15 :

Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and C be a fixed a cyclic subgroup of order N_1. Let S denote the equivalence class $(\bar{E}, \bar{C})$ of (E, C) under the above equivalence relation. Then, S is said to be a *supersingular point of $X_0(N_1)$ in characteristic p.*

Definition 2.16 :

Let $\mathcal{S} := \{S |\ S$ is a supersingular point of $X_0(N_1)$ in characteristic $p\}$.

Definition 2.17 :

Let $M_N := \bigoplus_{S \in \mathcal{S}} \mathbb{Z}[S]$.

The set $\mathcal{S}$ just defined will play a crucial role throughout our study. Let's first draw our attention to $|\mathcal{S}|$, the cardinality of $\mathcal{S}$. In order to count its elements, we first need to know the number of (non isomorphic) supersingular elliptic curves over $\overline{\mathbb{F}}_p$: this is indeed Igusa's theorem (section 2.2 on page 35). Then, for each of these curves, we must know all of its cyclic subgroups of order N_1 (recall that we already know their number by the 'structure of the torsion subgroup' lemma (section 2.1 on page 30)). Finally, it only remains to identify among all couples (E,C) found the ones that are not equivalent (in the sense defined above). One then gets the rather surprising result:

Lemma 2.18 : Cardinality of $\mathcal{S}$

Let $h(N)$ be the class number of an order $\mathcal{O}$ of level N in $H_{p,\infty}$.

Then, $|\mathcal{S}| = h(N)$.

Example 2.19 : $N = p = 11$

In this case, $N_1 = 1$ (so our cyclic subgroups have order one). Therefore, $|\mathcal{S}|$ is in this particular case equal to the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. So, by a previous example (section 2.2 on page 35), we get $|\mathcal{S}| = 2$.

Definition 2.20 :

Let $S \in \mathcal{S}$ be given. Then, the group of $\overline{\mathbb{F}}_p$-endomorphisms (respectively $\overline{\mathbb{F}}_p$ -automorphisms) of S is denoted by $End(S)$ (respectively $Aut(S)$).

Definition 2.21 :

For $S \in \mathcal{S}$, we let $\alpha_S := \frac{|Aut(S)|}{2}$.

Lemma 2.22 : Let $S = (\bar{E}, \bar{C}) \in \mathcal{S}$ be given. Then, in all cases, $\alpha_S \in \mathbb{N}^*$ and $\alpha_S \leq 12$. Moreover, if $p \neq 2, 3$, we have $\alpha_S \leq 3$.

Proof We surely have: $Aut(S) \subseteq Aut(E) \Rightarrow |Aut(S)| \leq |Aut(E)| \Rightarrow \alpha_S \leq \frac{|Aut(E)|}{2}$. But by the theorem on the value of $|Aut(E)|$ (section 2.1 on page 31), we have that $|Aut(E)|$ is always even, that $2 \leq |Aut(E)| \leq 24$ in all cases and that $|Aut(E)| \leq 6$ if $Char(\mathbb{F}_p) \neq 2, 3$.

Hence, $\alpha_S \in \mathbb{N}^*$, $\alpha_S \leq 12$ in all cases and $\alpha_S \leq 3$ if $p \neq 2, 3$, as wanted.

□

This lemma allows us to define the following inner product on M_N:

Definition 2.23 :

Let $\sum_{S \in \mathcal{S}} x_S[S] \in M_N$ and $\sum_{S \in \mathcal{S}} y_S[S] \in M_N$ be given. We define the following *inner product on M_N*:

$$\left\langle \sum_{S \in \mathcal{S}} x_S[S], \sum_{S \in \mathcal{S}} y_S[S]) \right\rangle := \sum_{S \in \mathcal{S}} (\alpha_S \cdot x_S \cdot y_S)$$

Definition 2.24 :

Let $S \in \mathcal{S}$ be given. Define $E_{is} := \sum\limits_{S \in \mathcal{S}} \frac{1}{\alpha_s}[S]$ and $M_N^0 := E_{is}{}^{\perp}$ (That is, M_N^0 is the orthogonal complement of E_{is} with respect to the inner product $< \cdot, \cdot >$ on M_N).

Remark : A straight computation yields that

$$M_N^0 = \left\{ \sum_{S \in \mathcal{S}} x_S[S] \in M_N \,\middle|\, \sum_{S \in \mathcal{S}} x_S = 0 \right\}$$

2.4 Hecke and Atkin-Lehner operators

Definition 2.25 :

Let $n \in \mathbb{N}^*$ be such that $p \not| n$. For each $S := (\bar{E}, \bar{C}) \in \mathcal{S}$,

let $\mathcal{C} := \left\{ C_n \leq E \middle| \; |C_n| = n \text{ and } C_n \cap C = \{0\} \right\}$ and

$$\begin{array}{rccl} T_n : & \mathcal{S} & \longrightarrow & M_N \\ & S := (\bar{E}, \bar{C}) & \longmapsto & T_n(S) := \sum\limits_{C_n \in \mathcal{C}} \left(\overline{E/C_n}, \overline{(C + C_n)/C_n} \right) \end{array}$$

Definition 2.26 :

Let

$$\begin{array}{rccl} \mathcal{W}_p : & \mathcal{S} & \longrightarrow & \mathcal{S} \\ & S := (\bar{E}, \bar{C}) & \longmapsto & W_p(S) := \left(\overline{-E^p}, \overline{-C^p} \right) \end{array}$$

Then, we define the *Atkin-Lehner involution* $\mathcal{W}_p$ on M_N by:

$$\begin{array}{rccl} \mathcal{W}_p : & M_N & \longrightarrow & M_N \\ & \sum\limits_{S\in\mathcal{S}} x_S[S] & \longmapsto & \mathcal{W}_p\left(\sum\limits_{S\in\mathcal{S}} x_S[S]\right) := \sum\limits_{S\in\mathcal{S}} x_S\,[W_p(S)] \end{array}$$

Definition 2.27 :

Let $q \in \mathbb{N}^*$ be such that $q|N_1$ and $(q, N_1/q) = 1$ and let $q' := N_1/q$. We then define W_q by:

$$\begin{array}{rccl} \mathcal{W}_q : & \mathcal{S} & \longrightarrow & \mathcal{S} \\ & S := (\bar{E},\bar{C}) & \longmapsto & W_q(S) := \left(\overline{E/q'C}, \overline{(E[q]+C)/q'C}\right) \end{array}$$

Then, we define the *Atkin-Lehner involution* $\mathcal{W}_q$ on M_N by:

$$\begin{array}{rccl} \mathcal{W}_q : & M_N & \longrightarrow & M_N \\ & \sum\limits_{S\in\mathcal{S}} x_S[S] & \longmapsto & \mathcal{W}_q\left(\sum\limits_{S\in\mathcal{S}} x_S[S]\right) := \sum\limits_{S\in\mathcal{S}} x_S[W_q(S)] \end{array}$$

The operators $\mathcal{T}_n$'s, $\mathcal{W}_q$'s and $\mathcal{W}_p$ possess many useful properties that are easy consequences of their definitions.

Lemma 2.28 : Basic properties of Hecke and Atkin-Lehner operators

(i) $\mathcal{W}_p$ is an involution

(ii) Every $\mathcal{W}_q$ is an involution

(iii) The set of $\mathcal{T}_n$'s for which $(n, N) = 1$ together with the $\mathcal{W}_q$'s generates a commutative semigroup of hermitian operators (with respect to the inner product $< \cdot, \cdot >$).

(iv) $\forall n, m \in \mathbb{N}^*$ such that $p \not| n$ and $p \not| m, \mathcal{T}_n \circ \mathcal{T}_m = \mathcal{T}_m \circ \mathcal{T}_n$

(v) $\forall n, m \in \mathbb{N}^*$ such that $p \not| n, p \not| m$ and $(n, m) = 1, \mathcal{T}_{mn} = \mathcal{T}_m \circ \mathcal{T}_n$

(vi) $\forall q, r \in \mathbb{N}^*$ such that $q | N_1, r | N_1$ and $(q, N_1/q) = (r, N_1/r) = (q, r) = 1, \mathcal{W}_{qr} = \mathcal{W}_q \circ \mathcal{W}_r$

(vii) $\forall d \in \mathbb{N}^*$ such that $d | N_1, \exists\ \phi_d : M_N \longrightarrow M_{N/d}$, ϕ_d morphism such that $\phi_d\Big((\bar{E}, \bar{C})\Big) = (\bar{E}, \overline{dC})$.

(viii) ϕ satisfies the following properties:
- $\forall n \in \mathbb{N}^*$ such that $(n, N) = 1,\ \phi_d$ commutes with the $\mathcal{T}_n$'s.
- $\forall q \in \mathbb{N}^*$ such that $q | N_1,\ q \Big| \frac{N}{d}$ and $(q, N_1/q) = 1, \phi_d$ commutes with the $\mathcal{W}_q$'s.
- $\forall d \in \mathbb{N}^*$ such that $d | N_1$ and $(d, N_1/d) = 1, \mathcal{T}_d \phi_d = \phi_d(\mathcal{T}_d + \mathcal{W}_d)$

2.5 Oldforms and newforms

We will now briefly introduce the notions of 'oldforms' ans 'newforms' due to Atkin and Lehner. A complete exposition on the subject can be found in [AL70] or in [Kna92, chapter IX, section 7, p. 283]. We will then relate the Hecke spaces M_N and $S_2(\Gamma_0(N))$, which will turn out to be a key result for the graph method.

Definition 2.29 :

We let $R := \Big\{ z \in \mathbb{H} \Big| \ |Re(z)| \leq 1/2 \text{ and } |z| \geq 1 \Big\}$.

Lemma 2.30 : Fundamental domain in $\mathbb{H}$ for $SL_2(\mathbb{Z})$

R is a fundamental domain for the action of $SL_2(\mathbb{Z})$ in $\mathbb{H}$.

Reference: [Kna92, theorem 8.5, p. 230].

Definition 2.31 :

Let $k \in \mathbb{N}^*$ and $f, g \in S_k$ be given. Then, we define the *Petersson inner product* $< \cdot, \cdot >_P$ by:

$$< f, g >_P := \int_R f(z)\overline{g(z)}\, y^k \frac{dxdy}{y^2}$$

Definition 2.32 :

Let $r_1, r_2 \in \mathbb{N}^*$, $N \in \mathbb{N}^*$ be such that $r_1 r_2 | N$ and let $f(z)$ be an eigenform for $\Gamma_0(\frac{N}{r_1 r_2})$. Then, it is known that $f(r_2 z)$ is an eigenform for $\Gamma_0(N)$ **with the same eigenvalues**. For this reason, we call $f(r_2 z)$ an *oldform*. Let $S_k^{old}(\Gamma_0(N))$ denote the linear span of the oldform and $S_k^{new}(\Gamma_0(N)) := \left(S_k^{old}(\Gamma_0(N))\right)^{\perp}$ (That is, $S_k^{new}(\Gamma_0(N))$ is the orthogonal complement of $S_k^{old}(\Gamma_0(N))$ with respect to the Petersson inner product $< \cdot, \cdot >_P$). The eigenform belonging to $S_k^{new}(\Gamma_0(N))$ are said to be *newforms*.

We now state an important and deep result that establishes a strong connexion between M_N^0 and $S_2(\Gamma_0(N))$.

Theorem 2.33 : An isomorphism with $S_2(\Gamma_0(N))$

Let $R_2(N) \subseteq S_2(\Gamma_0(N))$ be the subspace generated by the newforms of level

N and the oldforms arising from cusp forms of weight 2 and level pd, for $d|N_1$. Then $\exists\ \psi : M_N^0 \otimes \mathbb{C} \longrightarrow R_2(N), \psi$ isomorphism such that ψ is compatible with the action of Hecke operators.

Reference: See [AL70] for details.

2.6 Brandt matrices and Hecke operators

The goal of this section, as the title indicates, is to establish a link between Brandt matrices and Hecke operators. For this purpose, we first need the following settings:

As usual, let $p \in \mathbb{N}$ be a prime number, $N_1 \in \mathbb{N}^*$ be such that $p \not| N_1$ and $N := pN_1$. Also, let $n \in \mathbb{N}^*$, $h(N) := |\mathcal{S}|, \{S_1, S_2, \ldots, S_{h(N)}\} := \mathcal{S}$ and $S := S_1$. Choose a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$ containing a cyclic subgroup C of order N_1 such that $S = (\bar{E}, \bar{C})$.

One of the equivalent conditions for E to be said supersingular (see section 2.1 on page 32, statement (iv)) is that $End_{\overline{\mathbb{F}}_p}(E)$ is (isomorphic to) a maximal order in the quaternion algebra $H_{p,\infty}$. Then, the ring of endomorphisms $End(S)$ of S is an Eichler order $\mathcal{O}$ of level N in $H_{p,\infty}$.

Now, in order to construct the n^{th} Brandt matrix $B(n)$, we have to find representatives of each of the left ideal classes of $\mathcal{O}$. So, for $1 \leq i \leq h(N)$, let $I_i := Hom(S_i, S)$, $J_i := Hom(S, S_i)$ and $\mathcal{O}_i := End(S_i)$.

Theorem 2.34 : Quaternion Algebras vs Elliptic Curve (Part III)
Let $p \in \mathbb{N}$ be a prime number, $N_1 \in \mathbb{N}^*$ be such that $p \not| N_1$ and $N := pN_1$. Then, with above notation,

$$\forall\, n \in \mathbb{N}^*, \mathcal{T}_n = B(n)^T$$

(where the n^{th} Hecke operator $\mathcal{T}_n$ is here viewed as a matrix acting on M_N).

Proof

We have:

$$\begin{aligned}
\mathcal{O}_l(I_i) &\overset{def}{=} \left\{\eta \in H \middle| \eta I_i \subseteq I_i\right\} \\
&\overset{def}{=} \left\{\eta \in H \middle| \eta \circ \phi \in Hom(S_i, S), \forall \phi \in Hom(S_i, S)\right\} \\
&= \left\{\eta \in H \middle| \eta : S \longrightarrow S, \eta \text{ homomorphism}\right\} \\
&\overset{def}{=} End(S) \\
&\overset{def}{=} \mathcal{O}
\end{aligned}$$

Hence, we have that $I_1, \ldots I_h$ are the desired representatives of the left ideal classes of $\mathcal{O}$. Similarly,

$$\mathcal{O}_r(I_i) \overset{def}{=} \left\{\eta \in H \middle| I_i \eta \subseteq I_i\right\}$$

$$\begin{aligned}
&\overset{def}{=} \left\{\eta \in H \middle| \phi \circ \eta \in Hom(S_i, S), \forall \phi \in \ Hom(S_i, S)\right\} \\
&= \left\{\eta \in H \middle| \eta : S_i \longrightarrow S_i, \eta \text{ homomorphism}\right\} \\
&\overset{def}{=} End(S_i) \\
&\overset{def}{=} \mathcal{O}_i
\end{aligned}$$

We also have:

$$\begin{aligned}
I_i^{-1} &\overset{def}{=} \left\{\eta \in H \middle| I_i \eta I_i \subseteq I_i\right\} \\
&= \left\{\eta \in H \middle| \eta : S \longrightarrow S_i, \eta \text{ homomorphism}\right\} \\
&\overset{def}{=} Hom(S, S_i) \\
&\overset{def}{=} J_i
\end{aligned}$$

Collecting all the above informations yields that the general term ${b_{ij}}^{(n)}$ of the n^{th} Brandt matrix is indeed the number of isogenies from S_i to S_j such that no two of them differs only by an automorphism of S_j. Finally, we have recovered the matrix of the n^{th} Hecke operator, as wanted.

□

Example 2.35 : $N = 11$

We recall that we already have computed the first few Brandt matrices when $N = p = 11$ (see section 1.6 on page 28).

Hence, in the light of the above theorem, we also know the corresponding matrices of Hecke operators:

$$\mathcal{T}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathcal{T}_2 = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}, \mathcal{T}_3 = \begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix}, \mathcal{T}_4 = \begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix}, \mathcal{T}_5 = \begin{bmatrix} 4 & 2 \\ 3 & 3 \end{bmatrix}$$

Chapter 3

Graph Method

In this chapter, we finally arrive to the heart of our subject: all the various results which seemed unrelated until now will be put together with a few more specific complements in order to give a global perspective on our puzzle.

3.1 A procedure to compute the first a_n's

First, we need to recall the following result which will be of main importance for the method we are about to explain.

Theorem 3.1 : Properties of $j(\tau)$

The j-function $j(\tau)$ has the following properties:

- $j(\tau)$ is holomorphic on $\mathbb{H}$.
- $j(\tau)$ is a modular fonction of weight 0.
- The Fourier series of $j(\tau)$ has the form:

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n, \text{ where } c_n \in \mathbb{Z} \text{ for all } n \in \mathbb{N}^*.$$

Reference: See [Kna92, corollary 8.2, p. 226-227] for the proof.

We first reduce to the case when $N_1 = 1$. That is, $N = p$, a prime number. Let $f(q) := \sum a_n q^n$ (where $q := e^{2\pi i\tau}$) be a normalized newform of weight 2 and level N, $j = j(\tau)$ be the corresponding j-function and $K \subseteq \mathbb{C}$ be the extension of $\mathbb{Q}$ generated by the a_n's.

We now explain a procedure to compute the first coefficients a_n's of $f(q)$. By the 'isomorphism with $S_2(\Gamma_0(N))$' theorem (section 2.5 on page 43) , there is an element $\sum\limits_{S \in \mathcal{S}} x_S[S] \in M_N^0 \otimes K$ such that $\sum\limits_{S \in \mathcal{S}} x_S[S]$ is mapped to $f(q)$.

On the other hand, we know by above theorem that for each supersingular point $S = (\overline{E}, \overline{C}) \in \mathcal{S}$, the associated j-function $j_S = j_S(\tau)$ has the form:

$$j_S(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n, \text{ where } c_n \in \mathbb{Z} \text{ for all } n \in \mathbb{N}^*.$$

Then, the following congruence of Laurent series holds:

$$\boxed{\begin{array}{c} \left(\sum\limits_{S\in\mathcal{S}} x_S j_S\right) f(q)\frac{dq}{q} \equiv \sum\limits_{S\in\mathcal{S}} x_S \frac{dj}{j-j_S} \bmod \wp \\ \\ \text{for some prime ideal } \wp \text{ of } K \text{ lying over } p. \end{array}}$$

This congruence really is the **key point** that sometimes allows us to find the first few coefficients a_n of $f(q)$. For instance, suppose that $f(q)$ corresponds to a modular curve of prime conductor N. Then, all coefficients a_n of $f(q)$ lies in $\mathbb{Z}$. Therefore, $K = \mathbb{Q}, \wp = p$ and so $\sum\limits_{S\in\mathcal{S}} x_S[S] \in M_N^0 \otimes \mathbb{Q}$ and all x_S are in $\mathbb{Z}$. In this case, we always have that $\sum\limits_{S\in\mathcal{S}} x_S j_S \not\equiv 0$. This implies that we know **all** the a_n's mod p.

But, for every prime r such that $r < p^2/16$, we have that $2\sqrt{r} < p/2$ and so by virtue of the classical Hasse's inequality [1] , we have that $|a_r| < 2\sqrt{r} < p/2$. Hence, we simultaneously know the value of a_r mod p and that $|a_r| < p/2$. So, **the exact value of a_r is known for every prime r such that $r < p^2/16$.**

3.2 Construction of $\mathcal{S}$

The procedure explained in this section will fully justify the appellation "graph method". We will indeed construct a tree (in the sense of the graph

[1] See for example [Kna92, theorem 10.5, p. 296].

theory): the vertices of our graph being the supersingular points $S \in \mathcal{S}$ and the edges, the 2-isogenies between them.

As in botanics, the first step in order for a tree to grow is to find a seed: in our case, a supersingular point S_1. Then, we search for the (at most three) vertices S_i directly connected to S_1. Next, we take back each S_i found and again compute the supersingular points connected to S_i by a 2-isogeny. We repeat this step with each new vertex found until we have all the points in $\mathcal{S}$. We recall that we have seen (in section 2.3 on page 38) that $|\mathcal{S}|$ equals the class number $h(N)$ of some order $\mathcal{O}$ of level N in $H_{p,\infty}$, for which we already have an explicit formula (See section 1.5 on page 26).

Therefore, we know right from the start how many vertices our tree must have. So, the above procedure contains a finite number of steps and terminates as soon as the $h(N)$ vertices are found.

Let us first recall a useful special case of the class number formula that will be of great help later on.

Theorem 3.2 (Baker, Heegner and Stark):
Imaginary quadratic fields having class number one
Let $d \in \mathbb{N}^*$ be squarefree and h be the class number of $\mathbb{Q}(\sqrt{-d})$. Then,

$$h = 1 \Longleftrightarrow d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$$

Reference: Consult [ST87, theorem 10.5, p. 194] for a complete proof (as well as for interesting related results and remarks).

We will also need the following result from basic algebraic number theory:

Theorem 3.3 : Inert primes in quadratic fields
Let $p \in \mathbb{N}$ be prime and $d \in \mathbb{Z}$ be squarefree. Then,

$$\text{(i)} \qquad \begin{array}{c} 2 \text{ is inert in } \mathbb{Q}(\sqrt{-d}) \\ \Longleftrightarrow \\ d \equiv 3 \ (\text{mod} 8) \end{array}$$

$$\text{(ii)} \quad \text{if } p \neq 2, \quad \begin{array}{c} p \text{ is inert in } \mathbb{Q}(\sqrt{-d}) \\ \Longleftrightarrow \\ p \not| d \ \& \left(\frac{-d}{p}\right) = -1 \end{array}$$

where $\left(\frac{a}{b}\right)$ is the Legendre symbol.

Reference: This is a special case of [Mar77, theorem 25, p. 74].

Now, to simplify the exposition of the method, we will here suppose that N is odd, that an explicit model of the curve $X_0(N_1)$ is known as well as the action of the Hecke operator $\mathcal{T}_2$ on that specific model.

Step I: The seed, S_1

Our goal here is to find any supersingular point S_1 in $\mathcal{S}$. By the equivalent definition (iii) of a supersingular elliptic curve, we know that there are all defined over $\mathbb{F}_{p^2}$. Moreover, there is always at least one lying in $\mathbb{F}_p$: so one always has the possibility of enumerating all the elements of $\mathbb{F}_p$ until one hits a supersingular value. However, this way is obviously time consuming since there are few (aroud $\sqrt{p}$) such points. Therefore, one better consider the special case he is working on in order to find shortcuts.

For instance, suppose that $N_1 = 1$. That is, $N = p$ is prime.

If: $\exists\, d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ such that p is is inert in $\mathbb{Q}(\sqrt{-d})$.

Then: In this situation, we take as basepoint the j-invariant of the elliptic curve with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-d})$.

Else: Instead of working with quadratic imaginary fields having class number one, the second best thing to do is to consider those who have a small number of classes. For them, we again consider the elliptic curves with complex multiplication by their ring of integers as well as the minimal polynomials of the associated j-invariant. Then, after having solved the polynomial equation in $\mathbb{F}_{p^2}$, we are back to the above 'then' case.

Finally, in one way or the other, one can always find a supersingular point S_1 to start with.

Step II: The first branches

Since we assumed at the very beginning that the action of $\mathcal{T}_2$ on $X_0(N_1)$ was known, it suffices to solve a cubic polynomial over $\mathbb{F}_{p^2}$ in order to know the supersingular points *linked* to S_1 by a 2-isogeny. There are, of course, at most three of them.

Remark : It sometimes happens that we don't even have to do that. For example, suppose again that $N_1 = 1$ and that $N = p \equiv -1 (\text{mod } 6)$. In this case, p is always inert in $\mathbb{Q}(\sqrt{-3})$, so that $j = 0$ can be taken as our basepoint. In that case, we know that all three 2-isogenies map S_1 to the curve S_2 with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$, for which $j = 2^4 3^3 5^3 = 54000$.

Step III: Ramifications

For each new S_i found in the previous step, we repeat Step II. Except that this time, we know that one of the three 2-isogenies is the dual of the 2-isogeny from S_1 to S_i that we already have encountered in the last step. Hence, in the worst case, we don't have to solve a cubic, but rather a quadratic polynomial over $\mathbb{F}_{p^2}$.

Again, apply Step II each time a new vertex is computed, until we end up having all points.

Remark : Now that the method is explained, it only remains to convince ourselves that all supersingular points are indeed reached by this process. To do so, it is enough to show that the graph of $\mathcal{T}_2$ (and more generally $\mathcal{T}_n$) is connex. But Jean-Pierre Serre noticed that the number of connex components of the graph of $\mathcal{T}_2$ is smaller or equal to the multiplicity of the eigenvalue $a_2 = 3$ of $\mathcal{T}_2$.

Indeed, for each connex component $\Omega \subseteq \mathcal{S}$ of the graph of $\mathcal{T}_2$, let $v_\Omega := \sum_{S\in\Omega}[S] \in M_N$.

Then, we apply $\mathcal{T}_2$ to v_Ω and get $\mathcal{T}_2(v_\Omega) = \sum_{S\in\Omega} \lambda_S[S]$, for some $\lambda_S \in \mathbb{Z}$. Remark that the sum stays over Ω (and not over $\mathcal{S}$), since Ω is connex. We then compute the value of a given λ_S:

$$\lambda_S \overset{def}{=} |\{S' \in \mathcal{S}| \text{ there is a 2-isogeny } \varphi : S' \longrightarrow S\}|$$

But by the existence of the dual isogeny, we get:

$$\lambda_S = |\{S' \in \mathcal{S}| \text{ there is a 2-isogeny } \psi : S \longrightarrow S'\}|$$

But we already know that this last quantity equals 3 for each S. Hence, we get that

$$\mathcal{T}_2(v_\Omega) \overset{def}{=} \sum_{S\in\Omega} \lambda_S[S] = \sum_{S\in\Omega} 3[S] = 3\sum_{S\in\Omega}[S] \overset{def}{=} 3 \cdot v_\Omega$$

That is, $\mathcal{T}_2(v_\Omega) = 3 \cdot v_\Omega$. So, v_Ω is an eigenvector of $\mathcal{T}_2$ belonging to the eigenvalue $a_2 = 3$.

Moreover, all the v_Ω's (corresponding to each connex component Ω) are obviously independent eigenvectors. Hence, the number of connex components of $\mathcal{T}_2$ is smaller or equal to the multiplicity of $a_2 = 3$, as wanted.

So we only have to show that the multiplicity of $a_2 = 3$ is one. But the subspace M_N^0 of M_N has codimension 1, so if $a_2 = 3$ would have a multiplicity greater than 1, we would have $3 = |a_2| < 2\sqrt{2} < 3$, which is a contradiction. Finally, we have shown that $\mathcal{T}_2$ is connex.

Example 3.4 : $N = 11$

We first notice that since $11 \nmid 3$ and $\left(\frac{-3}{11}\right) = \left(\frac{-1}{11}\right) \cdot \left(\frac{3}{11}\right) = (-1)^5 \cdot 1 = -1$, it follows by the theorem on primes inert in quadratic fields that 11 is inert in $\mathbb{Q}(\sqrt{-3})$. Hence, we can take our first vertex to be $S_1 := (\bar{E}_1, \bar{C}_1)$, where E_1 is the supersingular curve with j-invariant zero (e.g. $E_1 : y^2 = x^3 + 1$).

Next, we need to find a second supersingular point. But as we noticed earlier, the three 2-isogenies from S_1 are mapped to $S_2 := (\bar{E}_2, \bar{C}_2)$, where $\bar{E}_2$ is the class of supersingular elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$ (e.g. $E_2 : y^2 = x^3 + x$), for which the j-invariant is 1.

Since we already know by previous examples that $|\mathcal{S}| = 2$ when $N = 11$, we are already done.

Hence, the only supersingular j-invariants in characteristic 11 are 0 and 1.

We recall that we obtained this same result with another method using the Legendre form (in section 2.1 in page 34).

Remark : Finally, let's mention that the tree we have built not only gives us all the supersingular points, but also informations on the second Hecke operator $\mathcal{T}_2$. Indeed, since the vertices were the supersingular points and the edges, the 2-isogenies, given any $S \in \mathcal{S}$, we can explicitely count the number of 2-isogenies from S to S'. This way, we obtain all the entries of $\mathcal{T}_2$ and hence, $\mathcal{T}_2$ itself.

Chapter 4

Application to Strong Modular Curves

Our general goal in this chapter is to use the graph method to obtain an explicite equation of an elliptic curve arising from a newform of weight 2 and prime level.

So, we are given a newform $f(q) := \sum_{n=1}^{\infty} a_n q^n$, where $\forall n \in \mathbb{N}^*, a_n \in \mathbb{Z}$, having weight 2 and **prime** level N. Hence, $f(q)$ corresponds to a strong modular curve $\mathcal{E}$ of conductor N.

The task of determining explicitely the coefficients of $\mathcal{E}$, even if all a_n's are given, is not in general a simple matter. However, the following step-by-step method should ease, in most cases, our task.

The procedure that we are about to explain will rely on quite a few results and hence, in order to keep the exposition as fluent as possible, no recall to the theory has been made here [1].

4.1 Construction of r_f

We already know by the theorem 'An isomorphism with $S_2(\Gamma_0(N)))$' (in section 2.5 on page 43) that $f(q)$ corresponds to an eigenvector $v_f := \sum_{s \in \mathcal{S}} x_S[S]$ (where $\forall S \in \mathcal{S}, x_S \in \mathbb{Z}$) of Hecke operators.

Since we already have described a procedure to compute in this case the first a_n's (see section 3 on page 49), we can take for granted that they are known.

Moreover, the construction of $\mathcal{S}$ we made (in section 3.1 on page 51) by building a certain tree gave us simultaneously all the supersingular points and the matrix of $\mathcal{T}_2$ acting on M_N. Therefore, we can compute the eigenspace V_2 associated to the eigenvalue a_2.

- If $dim(V_2) = 1$, then we stop the procedure right away and set $V := V_2$.
- If $dim(V_2) > 1$, we apply the Hecke operator $\mathcal{T}_3$ on V_2 to obtain V_3:
- If $dim(V_3) = 1$, we are done. Set $V := V_3$
- If $dim(V_3) > 1$, apply successively $\mathcal{T}_4, \mathcal{T}_5, \mathcal{T}_6, \ldots$, one at a time, until a space of dimension one is found. Then, let V be that space.

[1] But as usual, references are given.

Remark : Although the search of V might theorically require a large number of steps, in practice, however, we know that $dim(V_2) \leq 6$, for all $N \leq 80\ 000$.

Since $dim(V) = 1$, by construction, the basis of V consists of a single vector, say b. So, V is simply all the scalar multiples of b. Among them, there is clearly a unique (up to sign) vector $r_f := \sum_{s \in \mathcal{S}} \kappa_s[S] \in V$ such that $\kappa_s \in \mathbb{Z}$, for all $S \in \mathcal{S}$ and such that the κ_s's are relatively prime.

4.2 Geometric interpretation of the κ_s's

Since $\mathcal{E}$ is defined over $\mathbb{Q}$ and that $\mathbb{Q}$ has class number 1, it follows (c.f. [Sil86, corollary 8.3, p. 226]) that $\mathcal{E}$ possesses a minimal Weierstrass equation $\mathcal{E}_W$. Moreover, since $\mathcal{E}$ is a strong modular curve, there is a minimal modular parametrization $\varphi : X_0(N) \longrightarrow \mathcal{E}$ (c.f. [Kna92, p. 392]). Then, let $\Delta := \Delta_{\mathcal{E}_W} = \pm N^\delta$ be the discriminant of $\mathcal{E}_W$ and $n := deg(\varphi)$.

Now, P. Deligne and M. Rapoport in [DR73] showed the following deep result:

> *"There is a model $X_0(N)_{/\mathbb{Z}}$ of $X_0(N)$ defined over $\mathbb{Z}$ such that $\tilde{X}_0(N)_{/\mathbb{Z}}$, its reduction modulo N, is the union of two projective lines C_0 and C_∞ such that:*

- *C_0 classifies the elliptic curves in characteristic N having the "verschiebung"*
- *C_∞ classifies the elliptic curves in characteristic N corresponding to inseparable isogenies.*

Then, the intersection of C_0 and C_∞ are the supersingular points."

So, let $\mathcal{E}_N$ be the Néron model of $\mathcal{E}$ (c.f. [Sil86, appendix C.15, p. 357-360]), $\tilde{\mathcal{E}}_N$ be its reduction modulo N and $\tilde{\mathcal{E}}^0_{/\mathbb{F}_N}$ be the identity component of $\tilde{\mathcal{E}}_N$. Then, $\tilde{\mathcal{E}}^0_{/\mathbb{F}_N}$ is isomorphic (over $\mathbb{F}_{N^2}$) to the multiplicative group G_m. It can be shown that there is an extension Φ of φ to $X_0(N)_{/\mathbf{Z}}\backslash\mathcal{S}$, such that Φ induces (by specialization and restriction) a regular application from $C_\infty\backslash\mathcal{S}$ to $\tilde{\mathcal{E}}^0_{/\mathbb{F}_N}$, and hence a rational function $\phi : C_\infty \longrightarrow C_\infty$ such that its poles and zeros belong to E. Let $\Lambda := \sum\limits_{S\in S} \lambda_S[S] \in M_N^0$ be the divisor of ϕ (it is defined up to sign).

Until now, we have pointed out two special elements of M_N^0, r_f and Λ. In the next section, we will see that they are far from independant.

4.3 An explicit equation for $\mathcal{E}$

Together, the following two results due to J.-F. Mestre ([Mes86]) will make us achieve our main goal: compute the value of the coefficients of $\mathcal{E}$.

Lemma 4.1 (Mestre):

$$\Lambda = \pm r_f$$

Reference: The proof can be found in [Mes86, p.228-229]. It uses the famous result (see [Rib90]) conjectured by J.-P. Serre in 1985 and shown by K. Ribet in 1986 that implied that *"Fermat's last theorem would follow from the Shimura-Taniyama-Weil conjecture"*.

Theorem 4.2 (Mestre):

Let $\mathcal{E}$ be a strong modular elliptic curve with prime conductor N and $\Lambda := \sum_{S \in \mathcal{S}} \lambda_S[S] \in M_N^0$ be as in the above construction. Then, $\exists\ c_4, c_6 \in \mathbb{Z}$ such that:

$$E : y^2 = x^3 - \frac{c_4}{48} \cdot x - \frac{c_6}{864}$$

(i) $H \leq \frac{8n}{\sqrt{N-2}} \cdot \left(log \left(\frac{H^6}{1728} \right) + b \right)$,
where $H := sup \left(\sqrt{|c_4|}, \sqrt[3]{|c_6|} \right)$
and $b := \left(\frac{\Gamma(1/3)}{\Gamma(2/3)} \right)^3 \approx 7.74316962$

(ii) Let $\Delta' := \frac{c_4{}^3 - c_6{}^2}{1728}$. Then,

$$\Delta' = \begin{cases} \Delta & \text{if } \mathcal{E} \text{ is supersingular at 2} \\ \Delta \text{ or } 2^{12}\cdot\Delta & \text{otherwise} \end{cases}$$

(iii) $c_4 \equiv \left(\sum_{S\in\mathcal{S}} \lambda_S j_S\right)^4 \pmod{N}$

(iv) $c_6 \equiv -\left(\sum_{s\in\mathcal{S}} \lambda_S j_S\right)^6 \pmod{N}$

(v) $n\cdot\delta = \sum_{S\in\mathcal{S}} \lambda_S^2 \cdot |Aut(S)|$

To efficiently use the above theorem, we use the following steps:

- First compute V, and hence r_f by the method explained in section 4 on page 60. Then, use the fact that $\Lambda = \pm r_f$.
- Next, obtain n (the degree of φ) by (v).
- Obtain by (i) an upper bound for c_4 and c_6.
- Finally, deduce the value of c_4 and c_6 by (ii).

Remark : The congruences (iii) in above theorem can be used to reduce the computations.

So, as wanted, we found an explicit equation of the strong modular curve $\mathcal{E}$ given the corresponding newform $f(q)$.

Conclusion

- "Les bonnes idées n'ont pas d'âge:
elles n'ont que de l'avenir"

"Good ideas are ageless: they only a have future". This statement certainly applies to many mathematical topics, including, as we will see, the graph method.

We already saw that this method is very useful to find explicit equations of strong modular curves associated to newforms of weight 2 and prime level N. We must say that this application is only the first of many more...

Conversely, we are sometimes able to show with this method that a given elliptic curve is modular. For instance, J.-F. Mestre, in [Mes85], was able to demonstrate that the curve

$$y^2 + y = x^3 - 7x + 6$$

of conductor 5 077 was indeed modular. Although this curve seems quite ordinary, it is now known, from the work of J. E. Cremona ([Cre97]), to be the least modular curve[2] to have a Mordell-Weil group of rank strictly greater than 2.

The classification of quadratic imaginary fields having class number one (3.2 on page 52) has been really useful in developping the graph method. In return, the classification of quadratic imaginary fields having class number three follows from that same method:

Theorem 4.3 (Mestre):
Imaginary quadratic fields having class number three
Let $d \in \mathbb{N}^*$ be squarefree and h be the class number of $\mathbb{Q}(\sqrt{-d})$. Then,

$$h = 3$$

$$\Longleftrightarrow$$

$$d \in \{23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907\}$$

Reference: [Mes86, theorem 4, p. 232]

Another utility of this method exposed in [Mes86, Section 4, p.232-237] is to test Serre's conjecture. Although it is known to imply Shimura-Taniyama-Weil, no one has yet been able to prove or disprove it.

[2] when ordering elliptic curves by increasing conductors

Finally, even if this list of examples is not exhaustive, we certainly see that applications to this method are as numerous as diversified.

There is however a last one that we honestly *have* to mention: the recent method developped by M. Bertolini and H. Darmon to find rational points on modular curves gave yet a new life to the graph method...

List of Notation

p	Prime number	
$\mathbb{N}$	Natural numbers: $\{0, 1, 2, \ldots\}$	
$\mathbb{Z}$	Rationals integers	
$\mathbb{Q}$	Rationals numbers	
$\mathbb{R}$	Real numbers	
$\mathbb{R}_+$	Nonnegative real numbers	
$\mathbb{C}$	Complex numbers	
$\mathbb{F}_{p^n}$	Field of p^n elements	
$\mathbb{Q}_p$	Field of p-adic numbers	
$\mathbf{T}$	Hecke algebra	
$\vert S\vert$	Number of elements in the set S	
$Hom(A, B)$	$\{\phi : A \longrightarrow B \vert\ \phi$ homomorphism$\}$	
$End(A)$	$\{\phi : A \longrightarrow A \vert\ \phi$ endomorphism$\}$	
$Aut(A)$	$\{\phi : A \longrightarrow A \vert\ \phi$ automorphism$\}$	
K	Field	
$\bar{K}$	A fixed algebraic closure of K	
$Char(K)$	Characteristic of K	
$M_n(R)$	Ring of $n \times n$ matrices over the ring R	
$SL_n(R)$	$\{A \in M_n(R) \vert det(A) = 1\}$	
M_k	Vector space of modular forms or weight k	
S_k	Subspace of cusp forms of weight k	
$M_k(\Gamma_0(N))$	Space of modular forms of weight k and level N	
$S_k(\Gamma_0(N))$	Space of cusp forms of weight k and level N	
H	Quaternion algebra over K	4
$\mathcal{H}$	Hamilton's Quaternions	5

$Tr(h)$	(Reduced) Trace of h	6
$N(h)$	(Reduced) norm of h	6
I	Ideal of H	9
$\mathcal{O}$	Order of H	10
E	Eichler order of H	11
h	Class number of H	24
$H_{p,\infty}$	The quaternion algebra over $\mathbb{Q}$ such that $Ram(H_{p,\infty}) = \{p, \infty\}$	20
$\left(\frac{a}{b}\right)$	Legendre symbol	
$\mathbb{H}$	Upper half plane	
$\mathbb{H}^*$	Extended upper half plane	
$H(\Omega)$	Class of holomorphic functions in Ω	
$\lfloor\frac{a}{b}\rfloor$	Floor function	25
$\bar{h}$	Conjugate h	6
E	Elliptic curve over K	
S	Supersingular point of $X_0(N_1)$ in characteristic p	37
M_N	$\bigoplus_{S\in\mathcal{S}} \mathbb{Z}[S]$	37
R	Fundamental domain in $\mathbb{H}$ for $SL_2(\mathbb{Z})$	42
$< \cdot, \cdot >_P$	Petersson inner product	43

Bibliography

[AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematiche Annalen*, 185:134–160, 1970.

[BD96] Massimo Bertolini and Henri Darmon. Heegner points on Mumford-Tates curves. *Inventiones mathematicae*, 126:413–456, 1996.

[BD98] Massimo Bertolini and Henri Darmon. Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization. *Inventiones mathematicae*, 131:453–491, 1998.

[Cre97] J.E. Cremona. *Algorithms for Modular Elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.

[Deu41] M. Deuring. Die typen des multiplikatorenringe elliptischer funktionenkörper. *Abhandl. Math. Sem. Hans. Univ.*, 14:197–272, 1941.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. *Springer Lecture Notes*, 349:143–316, 1973.

[Eic38] M. Eichler. Ueber die ideal klassenzahl total definiter quternionenalgebren. *Math.Z*, 43:102–109, 1938.

[Gro87] Benedict H. Gross. Heights and the special values of L-series. In *Canadian Mathematical Society Conference Proceedings*, volume 7, pages 115–187, 1987.

[Hun74] Thomas W. Hungerford. *Algebra.* Springer, New York, 1974.

[Igu58] Jun-Ichi Igusa. Class number of a definite quaternion with prime discriminant. In *Proceedings of the National Academy of Sciences of the United States of America*, volume 44, pages 312–314, 1958.

[Jac89] Nathan Jacobson. *Basic Algebra II.* W.H.Freeman and Company, New York, 1989.

[Kna92] Anthony W. Knapp. *Elliptic curves.* Princeton University Press, Princeton, New Jersey, 1992.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, New York, second edition, 1993.

[Lat48] Claiborne G. Latimer. Quaternion algebra. *Duke Mathematical Journal*, 15:357–366, 1948.

[Mar77] Daniel A. Marcus. *Number Fields.* Springer-Verlag, New York, 1977.

[Mes85] J.-F. Mestre. Courbes de Weil de conducteur 5077. In *C.R. Acad. Sc. Paris*, volume 300, pages 509–512, 1985.

[Mes86] J.-F. Mestre. La méthode des graphes: exemples et applications. In *Proceedings of the International Conference on Class Numbers and Fundamental Units of algebraic number fields*, pages 217–242, 1986.

[MM97] Henry McKean and Victor Moll. *Elliptic curves: function theory, geometry, arithmetic.* Cambridge University Press, New York, 1997.

[Mur91] M. Ram Murty. Elliptic curves and modular forms. *Canadian Mathematical Bulletin/Bulletin canadien de mathématiques*, 34(3):375–384, 1991.

[Piz80] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *Journal of Algebra*, 64:340–390, 1980.

[Rib90] K. Ribet. On modular representations of Gal($\bar{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms. *Invent. Math.*, 100:431–476, 1990.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[ST87] Ian Stewart and David Tall. *Algebraic Number Theory.* Chapman and Hall, New York, 1987.

[Vig80] Marie-France Vignéras. *Arithmétique des Algèbres de quaternions.* Springer-Verlag, New-York, 1980.

[Wei73] André Weil. *Basic Number Theory.* Springer-Verlag, New York Berlin Heidelberg, 1973.