Explicit connections between supersingular isogeny graphs and Bruhat–Tits trees

Laia Amorós,[1] Annamaria Iezzi,[2,3] Kristin Lauter,[4]
Chloe Martindale,[5] and Jana Sotáková[6,7]*

[1]Aalto University, [2]University of South Florida, [3]Université de la Polynésie Française,
[4]Microsoft Research, [5]University of Bristol, [6]QuSoft, [7]University of Amsterdam

laia.ac@protonmail.com, annamaria.iezzi@gmail.com, kristinelauter@gmail.com,
chloe.martindale@bristol.ac.uk, ja.sotakova@gmail.com

March 19, 2021

Abstract

We give an exposition of supersingular isogeny graphs, quaternion ideal graphs and Bruhat–Tits trees, and of their connections. Bruhat–Tits trees are combinatorial objects whose vertices and edges have a very simple representation as two-by-two matrices, which, as we show, is useful for understanding certain aspects of the corresponding elliptic curves and isogenies. Moreover Bruhat–Tits trees can be given an orientation and a notion of depth that we translate into the setting of supersingular isogeny graphs. We give some suggestions towards using Bruhat–Tits trees as a tool for cryptanalysis of certain cryptosystems based on supersingular isogeny graphs.

1 Introduction

Post-Quantum Cryptography (PQC) is a subfield of cryptography that focuses on cryptosystems designed to withstand an attacker who has access to a quantum computer. An emerging field in post-quantum cryptography is isogeny-based cryptography, which is based on the hardness of computing a large-degree isogeny between two given elliptic curves. Most practical proposals in the area restrict to isogenies of supersingular elliptic curves, which were introduced into cryptography by Charles, Goren and Lauter [CGL09a] (first published in 2006 [CGL06]) for constructing cryptographic hash functions. Later, Jao and De Feo [JF11] proposed a Diffie–Hellman style key exchange based on supersingular isogenies called SIDH, or *Supersingular Isogeny Diffie–Hellman*. Post-quantum cryptography has enjoyed an increase in interest since the advent of the NIST international 'competition' [NIST], initiated in 2016, to find a post-quantum cryptographic standard. The only isogeny-based submission in the NIST competition is the key encapsulation mechanism SIKE [SIKE], or *Supersingular Isogeny Key Encapsulation*, which is based on SIDH. To assure the long-term security of schemes for future use in widely deployed cryptosystems, we need more research on the hardness of computing isogenies in supersingular

[*] Authors in alphabetical order; `https://www.ams.org/profession/leaders/culture/CultureStatement04.pdf`.

isogeny graphs. There are other competitive schemes [CLMPR18; CD20; BKV19] based on different assumptions (inspired by ordinary elliptic curves following [Cou06; RS06; DKS18]) that emerged since NIST submissions closed, but in this article we focus on the setting of SIDH.

Both the CGL hash function and SIKE are based on the *supersingular ℓ-isogeny graph*, consisting of vertices which are isomorphism classes of supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$, where p is a prime of cryptographic size. Each isomorphism class has a representative defined over $\mathbb{F}_{p^2}$, and vertices are labelled with the j-invariant of the curve, all of which are in $\mathbb{F}_{p^2}$. The edges are degree-ℓ isogenies, where $\ell \neq p$ is prime; in SIKE $\ell = 2$ or 3. We denote the supersingular ℓ-isogeny graph by $\mathcal{G}_\ell$; it has about $p/12$ vertices, is connected, and is undirected and $(\ell+1)$-regular at every vertex except for those vertices that represent elliptic curves with non-trivial automorphisms. If $p \equiv 1 \pmod{12}$ then the supersingular isogeny graph is *Ramanujan* [CGL09b; Piz90]. Ramanujan graphs are optimal expander graphs: they have good mixing properties and short walks end at an approximately uniformly distributed vertex, where the approximation depends on the expansion constant.

It is important for security that the inherent algebraic properties of the supersingular isogeny graph do not give rise to non-trivial attacks. For instance, there should be no special paths that can be constructed with non-negligible probability, and starting at the vertex specified in SIKE should not give skewed data. Experimental verification is of course out of the question for cryptographic-size examples. Recently [ACLLNSS19] studied the special properties of the $\mathbb{F}_p$-subgraph, and [KMPPS20] showed that there are exponentially many weak starting curves for the SIKE protocol. These two papers show that the graph does have some inherent structure that may be exploited in cryptanalysis, which motived our attempt in this work to gain a better understanding of the algebraic structures associated to the isogeny graph.

The 'algebraic structures associated to the isogeny graphs' that are typically studied are quaternion algebras: indeed the Deuring correspondence [Deu41] maps a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ to its endomorphism ring, which is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞. This map gives a correspondence[1] between the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves and maximal orders in $B_{p,\infty}$ (up to conjugation), and maps isogenies of degree ℓ to left-ideals of norm ℓ. The hard problem of path-finding on the supersingular isogeny graph can be solved in heuristic polynomial time on the corresponding graph of quaternion orders [KLPT14], but it is a fundamental hard problem to make the correspondence between the two graphs explicit [EHLMP18].

In this paper we propose that we take one step further, from quaternion algebras to *Bruhat–Tits trees*. Bruhat–Tits trees are combinatorial objects whose vertices and edges have a very simple representation as two-by-two matrices: for a prime ℓ, the Bruhat–Tits tree for $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, denoted by $\mathcal{T}_\ell$, is a $(\ell+1)$-regular infinite tree, for which one can choose the root as the vertex with label $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, representing a $\mathbb{Z}_\ell$-basis of a maximal order in $M_2(\mathbb{Q}_\ell)$. Starting from the root one can build the rest of the tree, knowing that from each vertex there are $\ell+1$ outgoing edges labelled either with the matrices

$$\begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix}, \quad i = 0, \dots, \ell-1, \qquad \text{or} \qquad \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} \ell & i \\ 0 & 1 \end{pmatrix}, \quad i = 0 \dots \ell-1 \qquad \text{or} \qquad \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix},$$

depending on where in the tree you are;[2] these labels can be thought of as 'directions'. Every edge gives the basis change from a vertex to an adjacent one. So, in particular, a vertex can be

[1] Pizer [Piz90] used this description to prove the Ramanujan property for $p \equiv 1 \pmod{12}$.

[2] This choice is to some extent arbitrary, we could equivalently have chosen the same direction labels for every vertex. Determining which labels to use is easy; see Section 2.3.

labelled with the sequence of the edges leading to it from the root. Translating this sequence into the product of the corresponding matrices returns a matrix that represents the $\mathbb{Z}_\ell$-basis of a maximal order in $M_2(\mathbb{Q}_\ell)$.

The connection between Bruhat–Tits trees, quaternion algebras, and supersingular ℓ-isogeny graphs was explained in [CGL09b] and [CFLMP18]. The bijection between the class set of maximal orders in a quaternion algebra and the double quotient of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is given in [CGL09b, Section 5.3.1, Equation (1)]. This series of bijections was used to show the Ramanujan property of supersingular ℓ-isogeny graphs. This is further explained in [CFLMP18, Proposition 7.2], and the definition and generators for the Bruhat–Tits tree are given in [CFLMP18, Section 6.2, Equation (8)]. However, these expositions were not aimed at a cryptographic audience and they did not cover the details of the corresponding graph structure.

The main goal of this paper is to provide an expository resource about these connections, as well as highlighting their potential applications in the cryptanalysis of isogeny-based protocols that make use of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, such as the CGL hash function and SIKE.

1.1 Contributions

Bruhat–Tits trees are standard tools when studying Shimura curves, and their applications in number theory are plentiful. However, they are usually described in language inaccessible to anyone without a working knowledge of algebraic geometry. We give a thorough expository treatment in Section 3 that will hopefully help to remedy this gap.

Section 4 explicitly connects the different viewpoints on supersingular isogeny graphs: quaternion ideal graphs and Bruhat–Tits trees. We show how to translate, via the ℓ-adic Tate module of a given elliptic curve, the notions of 'directions' and 'distance from the root' of the Bruhat–Tits tree $\mathcal{T}_\ell$ into the setting of the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$. This allows us to interpret non-backtracking walks in $\mathcal{G}_\ell$ as 'distance-increasing' (or *level-increasing*) walks in $\mathcal{T}_\ell$. We also review the classical Deuring correspondence between quaternion orders and supersingular elliptic curves and the classical correspondence due to Ribet [Rib90] between the quotient of the Bruhat–Tits tree $\mathcal{T}_\ell$ by a well-chosen matrix group and the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$. Finally we outline the explicit correspondence between quaternion orders and vertices of the Bruhat–Tits trees following [Mil15].

In Section 5 we move away from expository material and give some tentative suggestions for using Bruhat–Tits trees in cryptanalysis, since two-by-two matrices are very easy to work with. In Section 5.1 we explain how truncating the Bruhat–Tits tree at a certain level gives a close approximation of the subgraph of the supersingular isogeny graph relevant for SIKE. In Section 5.2 we give an algorithm to compute the isogeny corresponding to a given path in the Bruhat–Tits tree. We have also implemented this algorithm and include an explicit example. In Section 5.3 we explore the BTQuotient module by [FM14] for general quotients of Bruhat–Tits trees. We show how the functions already written there can be used to compute with cryptographic-size isogeny graphs, the case of interest to us, which was not covered by their code. In particular, we use the code in [FM14] to study the norm equations in specific directions of the Bruhat–Tits tree. In Section 5.4, we give an example of how the algorithms adapted from BTQuotient may be used to study SIKE: we exhibit a path in the Bruhat–Tits tree for which we can completely parameterize the norm equations of the corresponding orders on the quaternion graph.

1.2 Acknowledgement

We want to thank the organisers of the Women in Numbers Europe 3 conference for giving us the opportunity to work on this project. We also wish to thank the anonymous reviewers for their helpful comments.

Jana Sotáková, as well as a follow up visit of Laia Amorós, Annamaria Iezzi, and Chloe Martindale at the CWI in Amsterdam, were supported by the Dutch Research Council (NWO) through Gravitation-grant Quantum Software Consortium - 024.003.037. Laia Amorós was supported by Academy of Finland grant #282938 and by Helsinki Institute for Information Technology HIIT. Chloe Martindale was partially supported by CHIST-ERA USEIT (NWO project 651.002.004).

2 Background

In this section we give a brief expository overview of the necessary background of elliptic curves, quaternion algebras and Bruhat–Tits trees. We use the notation p for a prime $p > 3$ (which we assume throughout) and $q = p^n$ for a prime power. We reserve ℓ for a prime $\ell \neq p$.

2.1 Elliptic curves over finite fields

We summarise the basic arithmetic of elliptic curves over finite fields. The interested reader can look at [Sil09, Ch. III&V] for more details.

Let E be an elliptic curve defined over $\mathbb{F}_q$ (which we will write as $E/\mathbb{F}_q$). The set of points $E(\overline{\mathbb{F}}_q)$ equipped with an operation of addition forms an abelian group. As $p = \mathrm{char}(\mathbb{F}_q) > 3$, we can assume without loss of generality that E is isomorphic to a curve given by a Weierstrass equation $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{F}_q$ and $4A^3 + 27B^2 \neq 0$. We associate to E an element $j(E) \in \mathbb{F}_q$, called the *j-invariant* of E and defined as $j(E) := 1728\frac{4A^3}{4A^3+27B^2}$. The j-invariant is an $\overline{\mathbb{F}}_q$-isomorphism invariant.

2.1.1 Isogenies and endomorphisms

Given two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$, an *isogeny* $\varphi : E_1 \to E_2$ defined over $\mathbb{F}_q$ (resp. $\overline{\mathbb{F}}_q$) is a non-constant rational map defined over $\mathbb{F}_q$ (resp. $\overline{\mathbb{F}}_q$) which is also a surjective group homomorphism; it follows that the kernel $\ker(\varphi)$ is always finite.

One example is, for $m \in \mathbb{Z}$, the mutiplication-by-m map on any elliptic curve E, sending any point $P \mapsto mP$ and denoted by $[m] : E \to E$. The degree of an isogeny φ is its degree as a rational map; we refer to an isogeny of degree ℓ as an *ℓ-isogeny*. In particular, when φ is separable (which is always the case when $p \nmid \deg(\varphi)$), we have $\deg(\varphi) = |\ker(\varphi)|$. Also, for every ℓ-isogeny $\varphi : E_1 \to E_2$, there exists a (canonical) dual ℓ-isogeny $\widehat{\varphi} : E_2 \to E_1$ such that $\varphi \circ \widehat{\varphi} = \widehat{\varphi} \circ \varphi = [\ell]$. Given generators of its kernel, the rational maps defining an isogeny can be computed in time linear in the degree via Vélu's formulas [Vél71].

An *endomorphism* of an elliptic curve E is either an isogeny $\varphi : E \to E$ or the zero morphism. One example is given by the multiplication-by-m map $[m]$ defined above. Note that $[m]$ is an isogeny of degree m^2 and is separable if and only if $p \nmid m$; in this case

$$E[m] := \ker([m]) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

We also refer to $E[m]$ as the *m-torsion subgroup* of E and to its elements as the *m-torsion points* of E (these points are defined over $\overline{\mathbb{F}}_q$).

An important endomorphism is the *Frobenius endomorphism* π_q, or π, defined as follows:

$$\begin{array}{cccc} \pi : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

The set of all endomorphisms of E defined over $\overline{\mathbb{F}}_q$, denoted $\mathrm{End}(E)$, form a ring with the operations of addition and composition, and we refer to it as the *endomorphism ring* of E.

For an elliptic curve $E/\mathbb{F}_q$, the endomorphism ring $\mathrm{End}(E)$ is either an order in an imaginary quadratic field (in which case we call E *ordinary*) or a maximal order in a quaternion algebra ramified only at $p = \mathrm{char}(\mathbb{F}_q)$ and ∞ (in which case we call E *supersingular*). Any supersingular elliptic curve E satisfies $j(E) \in \mathbb{F}_{p^2}$ and it follows that E can be defined over $\mathbb{F}_{p^2}$.

For an ordinary curve $E/\mathbb{F}_q$, the endomorphism ring $\mathrm{End}(E)$ can be any order $\mathcal{O}$ in the imaginary quadratic field $\mathbb{Q}(\pi)$ that satisfies $\mathcal{O} \supset \mathbb{Z}[\pi]$. For a supersingular elliptic curve $E/\mathbb{F}_q$, as the endomorphism ring is a maximal order in a quaternion algebra it has $\mathbb{Z}$-rank 4. If $q = p$ then not all endomorphisms of E can be defined over $\mathbb{F}_p$ but Frobenius does not act like a scalar so in particular is not in $\mathbb{Z}$; if $q = p^2$, the Frobenius endomorphism π does act like a scalar. If $j(E) \notin \mathbb{F}_p$ it is a hard problem in isogeny-based cryptography [Koh96; EHLMP18] to find non-scalar endomorphisms of E. This article will only consider supersingular elliptic curves.

2.1.2 Supersingular ℓ-isogeny graphs

Let ℓ and p be prime numbers with $\ell \neq p$. First we define the graph whose vertices are j-invariants of supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ and such that there is a (directed) edge from $j(E_1)$ to $j(E_2)$ for every ℓ-isogeny (defined over $\overline{\mathbb{F}}_p$) $\varphi : E_1 \to E_2$. The number of edges from $j(E_1)$ to $j(E_2)$ is independent of the choice of the curves E_1, E_2. Because there are $\ell + 1$ cyclic subgroups in $E[\ell]$ for any E, there are $\ell + 1$ outgoing edges from every j-invariant $j(E)$; loops and multi-edges are possible. For every ℓ-isogeny $\varphi : E_1 \to E_2$, there is a dual ℓ-isogeny $\hat{\varphi} : E_2 \to E_1$. We identify the edge corresponding to φ with the edge corresponding $\hat{\varphi}$; we call the resulting (undirected) graph the *supersingular ℓ-isogeny graph* $\mathcal{G}_\ell := \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

For $p \equiv 1 \bmod 12$, we obtain a $(\ell + 1)$-regular graph (at every vertex, there are $\ell + 1$ edges). However, for $p \not\equiv 1 \mod 12$, the j-invariants 0 and 1728 can be supersingular. Because of the extra automorphisms of curves E_j with j-invariant $j \in \{0, 1728\}$, multiple isogenies $\varphi_i : E_j \to E$ have the same dual isogeny $\hat{\varphi} : E \to E_j$ and so in this identification, we have fewer edges from $j = 0$ and $j = 1728$. For instance, for $j = 1728$ and $\ell = 2$, there is always a 2-isogeny $\phi : E_{1728} \to E_{1728}$ and a pair of isogenies $\varphi, \psi : E_{1728} \to E_{287496}$ which satisfy $\hat{\varphi} = \hat{\psi}$. Therefore, the edges from $j = 1728$ in $\mathcal{G}_2$ are $(1728, 1728)$ and $(1728, 287496)$.

In Figure 2.1, we have $p = 241$ and $\ell = 2$. Note that $241 \equiv 1 \bmod 12$ and so the graph $\mathcal{G}_2$ is 3-regular.

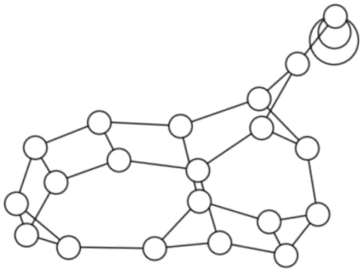

Figure 2.1: *Supersingular 2-isogeny graph for $p = 241$. Every vertex of the graph corresponds to a supersingular j-invariant in $\mathbb{F}_{431^2}$.*

2.2 Quaternion algebras over $\mathbb{Q}$

A *quaternion algebra* over $\mathbb{Q}$ is a central simple algebra that has dimension 4 over $\mathbb{Q}$. For $a, b \in \mathbb{Q} - \{0\}$ we denote by $\left(\frac{a,b}{\mathbb{Q}}\right)$ the $\mathbb{Q}$-algebra generated by a basis $\{1, i, j, k\}$ such that

$i^2 = a, j^2 = b$, and $ij = -ji = k$. Any quaternion algebra B over $\mathbb{Q}$ is isomorphic to $\left(\frac{a,b}{\mathbb{Q}}\right)$ for some $a, b \in \mathbb{Z}$. For every prime p we define

$$B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p,$$

and for the *infinite prime* ∞ we define

$$B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}.$$

A quaternion algebra B over $\mathbb{Q}$ is said to be *ramified* or *non split* at p (resp. at ∞) if B_p (resp. B_∞) is a division algebra. It is said to be *unramified* or *split* at p (resp. at ∞) if $B_p \cong M_2(\mathbb{Q}_p)$ (resp. $B_\infty \cong M_2(\mathbb{R})$). Moreover it is called *definite* (resp. *indefinite*) if it is ramified (resp. split) at ∞. The *discriminant* of B is the product of all ramified primes in B, so it is a square-free positive integer.

A quaternion algebra B over $\mathbb{Q}$ is endowed with a standard involution given by conjugation: the *conjugate* of an element $\alpha = x + yi + zj + tk \in B$ is $\overline{\alpha} = x - yi - zj - tk$, where $x, y, z, t \in \mathbb{Q}$. The *reduced trace* of α is $\mathrm{trd}(\alpha) = \alpha + \overline{\alpha}$, and the *reduced norm* of α is $\mathrm{nrd}(\alpha) = \alpha\overline{\alpha}$. We always have $\mathrm{trd}(\alpha),\ \mathrm{nrd}(\alpha) \in \mathbb{Q}$.

The endomorphism ring of any supersingular elliptic curve over $\mathbb{F}_q$, where q is a power of p, is a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞, denoted by $B_{p,\infty}$. Pizer [Piz80] gave an explicit description for all such possible quaternion algebras.

Theorem 2.1 *Let p be an odd prime. Then, up to isomorphism, the unique quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞ is given by:*

- $B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$, *if* $p \equiv 3 \pmod 4$*;*
- $B_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$, *if* $p \equiv 5 \pmod 8$*;*
- $B_{p,\infty} = \left(\frac{-r,-p}{\mathbb{Q}}\right)$, *if* $p \equiv 1 \pmod 8$*, where r is a prime such that* $r \equiv 3 \pmod 4$ *and* $\left(\frac{r}{p}\right) = -1$*.*

Moreover, we have $r = O(\log^2 p)$ under the generalized Riemann hypothesis [EHLMP18].

2.2.1 Arithmetic of quaternion algebras

Just like number fields, quaternion algebras are endowed with rich arithmetic, but the non-commutativity produces some interesting differences. We recall here the basic concepts for the convenience of the reader.

For a quaternion algebra B over $\mathbb{Q}$, an *ideal* of B is a $\mathbb{Z}$-lattice of B of rank 4. An *order* of B is an ideal which is also a subring. A *maximal order* is an order that is not properly contained in another order. Unlike in number fields, maximal orders in quaternion algebras are not necessarily unique - see Section 4.1.

Example 2.2 *We can always write down a maximal order in $B_{p,\infty}$ for any p [Piz80, Prop 5.2]. For example, if $p \equiv 3 \mod 4$ and $\{1, i, j, k\}$ is a basis of $B_{p,\infty}$ with $i^2 = -1$, $j^2 = -p$, and $k = ij$, we can take the maximal order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$.*

Let $\mathcal{O}$ be an order of B. An ideal I of B is said to be a *left-ideal* (resp. *right-ideal*) of $\mathcal{O}$ if $\mathcal{O}I := \{xI : x \in \mathcal{O}\} \subseteq I$ (resp. $I\mathcal{O} := \{Ix : x \in \mathcal{O}\} \subseteq I$). The *reduced norm* $\mathrm{nrd}(I)$ of an ideal I is $\gcd\{\mathrm{nrd}(\alpha) : \alpha \in I\}$. Two ideals I and J of B belong to the same *left-ideal class* (resp. *right-ideal class*) if there exists $\beta \in B^\times$ such that $I = J\beta$ (resp. $I = \beta J$). For a maximal order $\mathcal{O}$ we denote by $\mathrm{Cl}_l(\mathcal{O})$ the *set of left-ideal classes* (analogously, $\mathrm{Cl}_r(\mathcal{O})$ is the set of right-ideal classes), which is a finite set. To any ideal I of B we associate two orders:

- the *left-order* of I, i.e. the order $\mathcal{O}_l(I) := \{x \in B : xI \subseteq I\}$;
- the *right-order* of I, i.e. the order $\mathcal{O}_r(I) := \{x \in B : Ix \subseteq I\}$.

Any ideal $I \subset B$ is a left-ideal for its left-order and a right-ideal for its right-order. In particular, if $\mathcal{O}$ is maximal and I is a left-ideal of $\mathcal{O}$ then $\mathcal{O}_l(I) = \mathcal{O}$, as $\mathcal{O} \subseteq \mathcal{O}_l(I)$.

We say that two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are *linked* if there exists an ideal I in B such that $\mathcal{O}_l(I) = \mathcal{O}_1$ and $\mathcal{O}_r(I) = \mathcal{O}_2$. If two orders are linked then they have the same number of left- (or right-) ideal classes. In particular, since any two maximal orders of B are linked, maximal orders have all the same number of left- (or right-) ideal classes. Two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are said to be *conjugate* (or of the same *type*) if there exists $\alpha \in B^\times$ such that $\mathcal{O}_2 = \alpha^{-1}\mathcal{O}_1\alpha$. By the Skolem–Noether theorem for central simple algebras, two orders are conjugate if and only if they are isomorphic as rings.

2.2.2 ℓ-ideal graph of a quaternion algebra

Let $\mathrm{Brt}(B)$ denote the set of all the left-ideal classes of all maximal orders in B (up to conjugation). For ideal classes $[I], [J]$ in $\mathrm{Brt}(B)$ such that $\mathcal{O}_r(I) = \mathcal{O}_l(J)$ we denote the multiplication of $[I]$ and $[J]$ by $[I] * [J]$. $(\mathrm{Brt}(B), *)$ is clearly not a group, since the operation is not defined for all classes. However, the operation $*$ does equip $\mathrm{Brt}(B)$ with a *groupoid* structure [Voi, Chapter 19] and $(\mathrm{Brt}(B), *)$ is known as the *Brandt groupoid* of B [Bra43].

We can visualise the Brandt groupoid of B as a graph whose vertices are the maximal orders of B considered up conjugation, and an edge connects two vertices whenever the corresponding maximal orders are linked by an ideal. In Figure 2.2 we represent the Brandt groupoid for the quaternion algebra $B_{241,\infty}$. We omit half of the edges: if the inverse of an ideal was already represented, then its representation was not included.

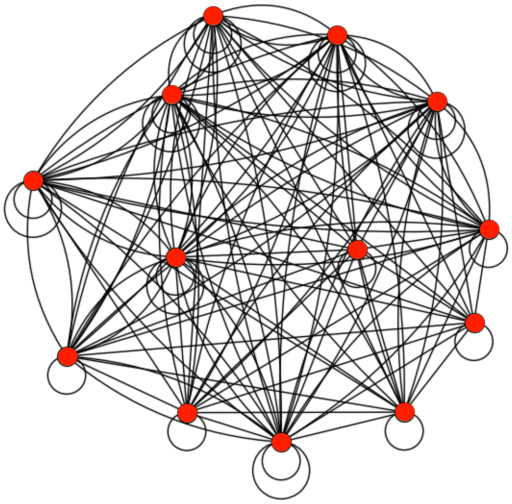

Figure 2.2: *Graph of the Brandt groupoid for the quaternion algebra $B_{241,\infty}$.*

Let us now consider only the ideal classes which admit representatives of a certain norm:

Definition 2.3 (ℓ-ideal graph) *Let B be a quaternion algebra over $\mathbb{Q}$ of discriminant D. For every prime $\ell \nmid D$ we define the ℓ-*ideal graph *of B as the undirected graph whose vertices are the maximal orders in B considered up to conjugation, and two vertices are connected by an edge if the corresponding maximal orders are linked by a left-ideal class admitting a representative of reduced norm ℓ.*

Note that the sets of vertices and edges of the ℓ-ideal graph do not depend on the choice of representatives of the vertices [Voi, Theorem 19.1.8].

Finally, we relate the ℓ-ideal graph and the ℓ-isogeny graph. For a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ denote by E^p any elliptic curve with j-invariant $j(E)^p$. Then $\operatorname{End}(E)$ and $\operatorname{End}(E^p)$ are isomorphic as rings, hence conjugate. Therefore, in the ℓ-ideal graph, vertices corresponding to $\operatorname{End}(E)$ and $\operatorname{End}(E^p)$ are identified. Since ℓ-isogenies correspond to ideals of norm ℓ (for more details, see Section 4.1), there is an edge between the isomorphism classes of $\operatorname{End}(E)$ and $\operatorname{End}(E')$ if and only if there is an ℓ-isogeny between E and E'.

Because of the above, the supersingular ℓ-isogeny graph is a 2-covering of the ℓ-ideal graph, except for the vertices defined over $\mathbb{F}_p$ (for which we have a 1-to-1 correspondence). As an example, for $\ell = 2$ and $p = 241$, we plot in Figure 2.3 the 2-ideal graph for the quaternion algebra $B_{241,\infty}$, which can be compared with the supersingular 2-isogeny graph for $p = 241$ in Figure 2.1.

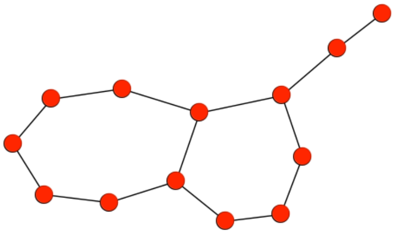

Figure 2.3: *2-ideal graph for $B_{241,\infty}$. Compare also with the supersingular 2-isogeny graph for $p = 241$ in Figure 2.1.*

2.2.3 Norm forms of maximal orders

Let B be the quaternion algebra $\left(\frac{-r,-p}{\mathbb{Q}}\right)$ with $r, p \in \mathbb{Z}_{>0}$ and a basis $\{1, i, j, k\}$ such that $i^2 = -r, j^2 = -p$ and $k^2 = -pr$. For $a, b, c, d \in \mathbb{Q}$, the reduced norm introduced in the previous section defines a quadratic form in 4 variables:

$$\operatorname{nrd}(a + bi + cj + dk) = a^2 + rb^2 + pc^2 + prd^2. \tag{1}$$

The structure of the quaternion algebra B is related to the properties of the quadratic form nrd. For instance, the property of being a definite quaternion algebra (which, over $\mathbb{Q}$ is the same as having $i^2 < 0, j^2 < 0$) is equivalent to the norm form being positive definite.

We can also associate an integral quadratic form to any order $\mathcal{O}$ in B. Once an integral basis $\{\beta_i\}_{i=1}^4$ of $\mathcal{O}$ is fixed, an element α in $\mathcal{O}$ can be written as $\alpha = a\beta_1 + b\beta_2 + c\beta_3 + d\beta_4$, with $a, b, c, d \in \mathbb{Z}$. If we compute the reduced norm of α in this basis, we obtain a quadratic form in 4 variables over $\mathbb{Z}$ which we refer to as the *norm form of* $\mathcal{O}$. The norm form of different orders can be used for attacks on SIDH-style cryptosystems [Pet17; KMPPS20] under special circumstances; this is discussed further in Section 5.4.

Example 2.4 *Let $p \equiv 3 \pmod 4$. We take the maximal order*

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2} \subseteq \left(\frac{-1,-p}{\mathbb{Q}}\right),$$

where $i^2 = -1$, $j^2 = -p$ and $k = ij$. Write an element $\alpha \in \mathcal{O}$ as $\alpha = a + bi + c\left(\frac{i+j}{2}\right) + d\left(\frac{1+k}{2}\right)$ with $a, b, c, d \in \mathbb{Z}$. Then we can compute the norm form associated to the order $\mathcal{O}$ using the *reduced norm form (1):*

$$\begin{aligned}\mathrm{nrd}(\alpha) = \mathrm{nrd}\left(a + bi + c\left(\frac{i+j}{2}\right) + d\left(\frac{1+k}{2}\right)\right) = \mathrm{nrd}\left(a + \frac{d}{2} + \left(b + \frac{c}{2}\right)i + \frac{c}{2}j + \frac{d}{2}k\right) = \\ = a^2 + b^2 + bc + \left(\frac{p+1}{4}\right)c^2 + ad + \left(\frac{p+1}{4}\right)d^2.\end{aligned}$$

2.3 The Bruhat–Tits tree for $\mathrm{PGL}_2(\mathbb{Q}_\ell)$

There are several ways to define the Bruhat–Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. Its vertices can be described as:

- classes of homothetic $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$,
- classes of equivalent norms on these lattices,
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$, or
- maximal orders in the quaternion algebra $\mathrm{M}_2(\mathbb{Q}_\ell)$.

For more details on each case see [Mil15, Chapter 2]. We will give the definition of the Bruhat–Tits tree as a graph whose vertices are homothety classes of lattices, but we will still use the other interpretations in order to get an explicit description that we can work with.

We consider lattices in $\mathbb{Q}_\ell^2$. Two lattices $M, M' \subseteq \mathbb{Q}_\ell^2$ are said to be *homothetic* if there exists $\lambda \in \mathbb{Q}_\ell^\times$ such that $M' = \lambda M$. The homothety class of M will be denoted by $\{M\}$. Given two homothety classes $\{M\}$ and $\{M^{'}\}$ one can always choose their representatives such that, for some $n \in \mathbb{N}$, we have that $\ell^n M \subseteq M' \subseteq M$. For example, if $M = \langle m_1, m_2 \rangle$, then we can take $M' = \langle m_1, \ell^n m_2 \rangle$ [Ser77, Chapter 2, Section 1.1].

Two homothety classes $\{M\}$ and $\{M'\}$ are said to be *adjacent* if their representatives can be chosen so that $\ell M \subsetneq M' \subsetneq M$. Note that this is equivalent to M' being a cyclic sublattice of index ℓ in M.

Definition 2.5 (Bruhat–Tits tree) *The* Bruhat–Tits tree *associated to* $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ *is the infinite tree $\mathcal{T}_\ell$ with set of vertices* $\mathrm{Ver}(\mathcal{T}_\ell)$ *given by the set of homothety classes of lattices of* $\mathbb{Q}_\ell^2$*, and whose set of edges* $\mathrm{Ed}(\mathcal{T}_\ell)$ *is the set of pairs of adjacent homothety classes.*

The graph $\mathcal{T}_\ell$ is a $(\ell+1)$-regular tree [Ser77, Chapter II]. The group $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ acts on $\mathrm{Ver}(\mathcal{T}_\ell)$ by matrix multiplication: if $M = \langle m_1, m_2 \rangle \subseteq \mathbb{Q}_\ell^2$ and $\gamma \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ then $\gamma \cdot M := \langle \gamma m_1, \gamma m_2 \rangle$, and the induced action of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ on the classes of lattices is then well-defined. The action

$$\begin{array}{ccc} \mathrm{PGL}_2(\mathbb{Q}_\ell) \times \mathrm{Ver}(\mathcal{T}_\ell) & \to & \mathrm{Ver}(\mathcal{T}_\ell) \\ (\gamma, v) & \mapsto & \gamma \cdot v \end{array}$$

induces a homeomorphism

$$\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell) \simeq \mathcal{T}_\ell,$$

where $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is taken with its natural topology. This bijection gives a way to represent each vertex by a class of matrices: if $v = \{M\}$, then the vertex v can be also represented by the class $\{\alpha_M\} \in \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$ such that α_M is the matrix whose columns form a basis of the lattice M.

Any lattice $\langle u, v \rangle$ (notice that we are fixing a basis here) contains $\ell + 1$ cyclic sublattices of index ℓ which are given by $\langle u + iv, \ell v \rangle$, for $i = 0, \ldots, \ell - 1$, and $\langle \ell u, v \rangle$. In terms of matrices, this corresponds to multiplying the matrix $(u|v)$, which has u and v as its columns, on the right by one of the following matrices:

$$D_i = \begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix}, \text{ where } i = 0, \ldots, \ell - 1, \quad \text{or} \quad D_\infty = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}. \tag{2}$$

Therefore, starting from the vertex corresponding to the class of $\langle u, v\rangle$, we can label the $\ell + 1$ outgoing edges with the matrices in (2), and think of them as the 'directions' $0, \dots, \ell - 1$ and ∞ respectively.

In a similar way, for every sublattice of the form $\langle u + iv, \ell v\rangle$, $i = 0, \dots, \ell - 1$, we can use the matrices in (2) to describe the corresponding $\ell + 1$ sublattices of index ℓ. Note that ℓ of these new sublattices will define a new class, while one (the one which is obtained by taking the ∞ direction) will belong to the same class as $\langle u, v\rangle$. We treat the case of the sublattice $\langle \ell u, v\rangle$ separately because, for convenience, once we have taken the ∞ direction, we are going to redefine the direction matrices in the following way:

$$D'_i = \begin{pmatrix} \ell & i \\ 0 & 1 \end{pmatrix}, \text{ where } i = 0, \dots, \ell - 1, \quad \text{or} \quad D'_\infty = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}. \tag{3}$$

This allows us to have the directions defined in a way such that the ∞ direction always points to the root. By repeating this process, starting from a chosen root with representative $\langle u, v\rangle$, we can describe a representative of any vertex at distance k from the root by multiplying the matrix $(u|v)$ on the right by a product of k direction matrices:

$$D_{i_1} D_{i_2} \cdots D_{i_k}, \text{ with } i_j \in \{0, \dots, \ell - 1\}, \text{ for } 1 \le j \le k,$$

or

$$D_\infty D'_{i_2} \cdots D'_{i_k}, \text{ with } i_j \in \{0, \dots, \ell - 1\}, \text{ for } 2 \le j \le k.$$

Note that the representative which is obtained is a cyclic sublattice of index ℓ^k in $\langle u, v\rangle$. See below for an explicit description of the representatives that are obtained in this way.

Let $v^{(0)} = \{\alpha^{(0)}\}$ denote the vertex of $\mathcal{T}_\ell$ whose representative is the matrix $\alpha^{(0)} := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We will define again the vertices of $\mathcal{T}_\ell$ 'level by level': for $k \ge 0$, we say that a vertex v is *at level k* if the distance between v and the chosen root is equal to k. There is a unique vertex at level 0, the root of the tree.

- Level 1: for every $i_1 \in \{0, 1, \dots, \ell - 1, \infty\}$, let $v^{(1)}_{i_1} = \left\{\alpha^{(1)}_{i_1}\right\}$ denote the vertex represented by the matrix

  $$\alpha^{(1)}_{i_1} := \begin{cases} \begin{pmatrix} 1 & 0 \\ i_1 & \ell \end{pmatrix}, & \text{if } i_1 \ne \infty, \\ \\ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}, & \text{if } i_1 = \infty. \end{cases}$$

  These matrices define $\ell + 1$ different vertices $v^{(1)}_0, \dots, v^{(1)}_{\ell-1}, v^{(1)}_\infty$ adjacent to $v^{(0)}$.

- Level 2: for every vertex $v^{(1)}_{i_1}$ at level 1, we define ℓ new adjacent vertices $v^{(2)}_{i_1,i_2}$, with $i_2 \in \{0, 1, \dots, \ell - 1\}$, represented by the matrices

  $$\alpha^{(2)}_{i_1,i_2} := \begin{cases} \begin{pmatrix} 1 & 0 \\ i_1 + i_2\ell & \ell^2 \end{pmatrix}, & \text{if } i_1 \ne \infty, \\ \\ \begin{pmatrix} \ell^2 & i_2\ell \\ 0 & 1 \end{pmatrix}, & \text{if } i_1 = \infty. \end{cases}$$

- Level k: we denote a generic vertex at distance k from $v^{(0)}$ by $v^{(k)}_{i_1,\dots,i_k}$, where $i_1 \in \{0, 1, \dots, \ell - 1, \infty\}$, and $i_j \in \{0, 1, \dots, \ell - 1\}$ for $j = 2, \dots, k$. Note that the vertex $v^{(k)}_{i_1,\dots,i_k}$ at level k is connected to the vertex $v^{(k-1)}_{i_1,\dots,i_{k-1}}$ at level $k - 1$. We have $v^{(k)}_{i_1,\dots,i_k} = \{\alpha^{(k)}_{i_1,\dots,i_k}\}$, where

$$\alpha^{(k)}_{i_1,\dots,i_k} := \begin{cases} \begin{pmatrix} 1 & 0 \\ \sum_{j=1}^{k} i_j \ell^{j-1} & \ell^k \end{pmatrix}, & \text{if } i_1 \neq \infty \\ \\ \begin{pmatrix} \ell^k & \sum_{j=2}^{k} i_j \ell^{j-1} \\ 0 & 1 \end{pmatrix}, & \text{if } i_1 = \infty. \end{cases} \tag{4}$$

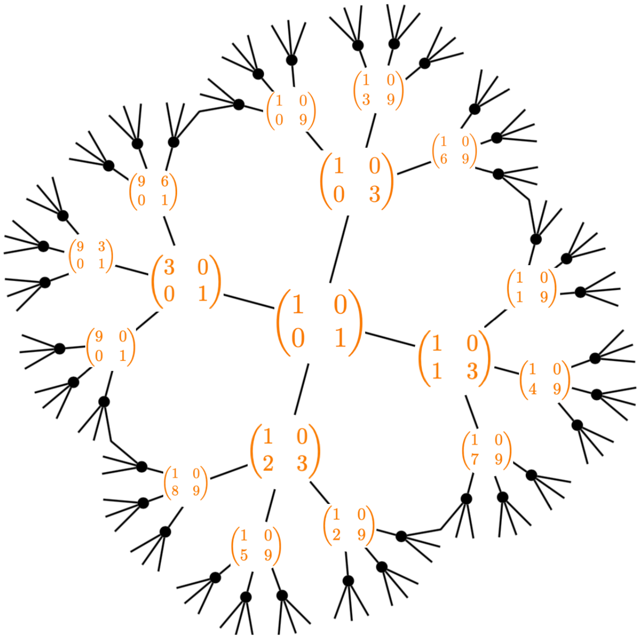
$\begin{pmatrix}1&0\\0&9\end{pmatrix}$
$\begin{pmatrix}1&0\\3&9\end{pmatrix}$
$\begin{pmatrix}1&0\\6&9\end{pmatrix}$
$\begin{pmatrix}9&6\\0&1\end{pmatrix}$
$\begin{pmatrix}1&0\\0&3\end{pmatrix}$
$\begin{pmatrix}9&3\\0&1\end{pmatrix}$
$\begin{pmatrix}3&0\\0&1\end{pmatrix}$
$\begin{pmatrix}1&0\\1&9\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$\begin{pmatrix}9&0\\0&1\end{pmatrix}$
$\begin{pmatrix}1&0\\1&3\end{pmatrix}$
$\begin{pmatrix}1&0\\4&9\end{pmatrix}$
$\begin{pmatrix}1&0\\2&3\end{pmatrix}$
$\begin{pmatrix}1&0\\7&9\end{pmatrix}$
$\begin{pmatrix}1&0\\8&9\end{pmatrix}$
$\begin{pmatrix}1&0\\2&9\end{pmatrix}$
$\begin{pmatrix}1&0\\5&9\end{pmatrix}$

Figure 2.4: *The Bruhat–Tits tree $\mathcal{T}_\ell$ for $\ell = 3$.*

Given the description of $\mathcal{T}_\ell$, it is easy to see that there are $(\ell+1)\ell^{k-1}$ vertices at level k. Moreover, we have the following ascending chain of subtrees of $\mathcal{T}_\ell$. For every $k \geq 0$, let $\mathcal{T}_\ell^{(k)}$ denote the subtree of $\mathcal{T}_\ell$ with set of vertices $\mathrm{Ver}(\mathcal{T}_\ell^{(k)}) = \{v = \{\alpha\} : \det(\alpha) = \ell^i \text{ for } i \leq k\}$. We call $\mathcal{T}_\ell^{(k)}$ the *truncated tree at level* k. Then we have

$$\mathrm{Ver}(\mathcal{T}_\ell^{(0)}) = \{v^{(0)}\}, \quad \mathrm{Ver}(\mathcal{T}_\ell^{(k)}) \subseteq \mathrm{Ver}(\mathcal{T}_\ell^{(k+1)}) \text{ for every } k \geq 0, \text{ and } \mathcal{T}_\ell = \bigcup_{k \geq 0} \mathcal{T}_\ell^{(k)}.$$

3 The graph of the bad reduction of Shimura curves

Shimura curves are compact Riemann surfaces defined using quaternion algebras that can be regarded as algebraic curves. They generalise modular curves: modular curves are constructed using congruence subgroups of the matrix algebra $M_2(\mathbb{Q})$, while Shimura curves are constructed using subgroups of any given quaternion algebra different from $M_2(\mathbb{Q})$.

There is a close connection between graphs of bad reductions of Shimura curves and supersingular isogeny graphs, which we will explore in more detail in Section 4.3. Graphs of bad reductions of Shimura curves can be computed as quotients of the Bruhat–Tits tree. Let $D > 1$ be an integer and let ℓ be a prime such that $\ell \nmid D$. After defining a group that we will denote by $\Gamma_{\ell,+}$, and which depends on ℓ and on the definite quaternion algebra ramified at primes dividing

D and at ∞, we will show how to compute the quotient graph of the Bruhat–Tits tree

$$\Gamma_{\ell,+}\backslash\mathcal{T}_\ell.$$

In Section 4.3 we will show that this graph is a double covering of the supersingular isogeny graph $\mathcal{G}_\ell$.

In order to properly define the group $\Gamma_{\ell,+}$, we need to introduce the theory of Shimura curves to the reader, both over $\mathbb{Q}$ and over $\mathbb{Q}_\ell$. We stress that this theory is very technical, with tools from different areas (schemes, uniformisation of algebraic curves, rigid analytic geometry,...). Definitions are usually complicated for a first-time approach, so we will try to explain the theory in a simplified way, prioritising helping the reader gain intuition and keeping the analogy with the complex case. [3]

Here is the outline of this section: in Section 3.1 we define Shimura curves over $\mathbb{Q}$. In Section 3.2 we introduce the ℓ-adic upper half plane and in Section 3.3 we define Shimura curves over $\mathbb{Q}_\ell$. Finally in Section 3.4 we are ready to compute the graph we are interested in: $\Gamma_{\ell,+}\backslash\mathcal{T}_\ell$.

3.1 Shimura curves from indefinite quaternion algebras

Let H be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D_H > 1$ and let $\mathcal{O} \subseteq H$ be a maximal order (which, since H is indefinite and over $\mathbb{Q}$, is unique up to isomorphism). Since H is indefinite, we have a canonical embedding $\Phi : H \hookrightarrow \mathrm{M}_2(\mathbb{R})$ of H into the algebra of the 2×2 matrices with coefficients in $\mathbb{R}$.

Let $\mathcal{O}^\times := \{\alpha \in \mathcal{O} \mid \mathrm{nrd}(\alpha) = \pm 1\}$ denote the unit group of $\mathcal{O}$. In order to look at this group as a matrix group, we consider its image under Φ and we define:

$$\Gamma_+ := \Phi(\mathcal{O}^\times)/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R}).$$

The group Γ_+ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, so one can consider its action on the complex upper half-plane $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$

$$\begin{array}{ccc} \Gamma_+ \times \mathcal{H} & \to & \mathcal{H} \\ \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\right) & \mapsto & \frac{az+b}{cz+d}, \end{array}$$

which is well-defined. The quotient $\Gamma_+\backslash\mathcal{H}$ is a Riemann surface that is compact if $D_H > 1$.

The case $D_H = 1$ gives a non-compact quotient which, after compactifying, can be regarded as an algebraic curve known as a *modular curve*. In this case, the algebra H is just the matrix algebra $M_2(\mathbb{Q})$ and Γ_+ is the modular group $\mathrm{PSL}_2(\mathbb{Z})$. For a positive integer N, let $\Gamma_0(N)$ denote the subgroup in $\mathrm{SL}_2(\mathbb{Z})$ of all matrices that reduce modulo N to an upper triangular matrix. It is well known (check for example [Sil09] for more details) that there exists a smooth projective curve $X_0(N)$ defined over $\mathbb{Q}$ and a complex analytic isomorphism

$$j_{N,0} : \Gamma_0(N) \setminus \mathcal{H} \to X_0(N)(\mathbb{C})$$

such that the elliptic curve E_τ associated to an element $\tau \in \Gamma_0(N)\backslash\mathcal{H}$ is defined over the number field $K = \mathbb{Q}(j_{N,0}(\tau))$.

Remark 3.1 *The notion of a modular curve of a given level also has its counterpart in the theory of Shimura curves: an* Eichler order *of a given level. An Eichler order is the intersection of two maximal orders, and its level is its index in either of the maximal orders. A maximal order is an Eichler order of level 1; for the sake of simplicity we will present the theory with maximal orders only.*

[3] See [Mil15; BC91] for a more rigorous introduction.

When $D_H > 1$, Shimura [Shi67] proved that there exists an algebraic curve $X(D_H)$ defined over $\mathbb{Q}$ and an isomorphism

$$J : \Gamma_+ \backslash \mathscr{H} \to X(D_H)(\mathbb{C}) \tag{5}$$

characterised by certain arithmetic properties related to complex multiplication theory. The curve $X(D_H)$ is known as the *(canonical model of the) Shimura curve* of discriminant D_H (and level $N = 1$). The isomorphism J is called the *complex* or *∞-adic uniformisation* of $X(D_H)$.

Since $X(D_H)$ is an algebraic curve over $\mathbb{Q}$, it makes sense to consider its reductions modulo a prime. For a prime $\ell \nmid D_H$, the reduction $X(D_H)_{\mathbb{F}_\ell}$ is smooth [Mor81]. A prime ℓ such that $\ell \mid D_H$ is called a *prime of bad reduction*; the reduction of a Shimura curve at a bad prime $X(D_H)_{\mathbb{F}_\ell}$ has totally degenerate semistable bad reduction: it is connected and isomorphic to several copies of projective lines $\mathbb{P}^1$, and its only singularities are ordinary double points [Kur79, Sect. 3]. In this case, we will call $X(D_H)_{\mathbb{F}_\ell}$ the *special fibre* or *bad reduction* at ℓ of the Shimura curve $X(D_H)$. This special fibre can be interpreted as a graph in the following way (see [Kur79] for more details).

Definition 3.2 (Graph of the special fibre) *Let $D > 1$ be an integer and ℓ be a prime such that $\ell \mid D$. The graph $\mathcal{G}$ of the special fibre at ℓ of $X(D)$ is defined as follows. The vertices of $\mathcal{G}$ correspond to the irreducible components of $X(D)_{\mathbb{F}_\ell}$ over $\overline{\mathbb{F}}_\ell$, which are isomorphic to the projective line $\mathbb{P}^1_{\mathbb{F}_\ell}$ over $\mathbb{F}_\ell$. The edges of $\mathcal{G}$ correspond to double points, i.e. two vertices of $\mathcal{G}$ are connected by an edge if the corresponding irreducible components intersect.*

To compute these graphs explicitly, we need to go to the ℓ-adic side of the theory of Shimura curves.

3.2 The ℓ-adic upper half-plane

We start by briefly introducing the *ℓ-adic upper half-plane*,[4] an ℓ-adic analogue to the complex upper half-plane, which is the starting point of the construction of ℓ-adic Shimura curves.

Let $\mathbb{Q}_\ell$ denote the field of ℓ-adic numbers and $\mathbb{C}_\ell$ the completion of a fixed algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$. Let $\mathbb{P}^1_{\mathbb{Q}_\ell}$ denote the algebraic projective line over $\mathbb{Q}_\ell$. The *ℓ-adic upper half-plane* is a ℓ-adic rigid analytic variety $\mathscr{H}_\ell$ over $\mathbb{Q}_\ell$ whose set of L-points, for every field extension $\mathbb{Q}_\ell \subseteq L \subseteq \mathbb{C}_\ell$, is

$$\mathscr{H}_\ell(L) := \mathbb{P}^1_{\mathbb{Q}_\ell}(L) - \mathbb{P}^1_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell),$$

that is, removing the $\mathbb{Q}_\ell$-points. One important property of the ℓ-adic upper half-plane is that it has a good "reduction" map that takes $\mathscr{H}_\ell$ to the Bruhat–Tits tree $\mathscr{T}_\ell$.

Proposition 3.3 ([Mil15], Thm. 2.2.31) *For every field extension $\mathbb{Q}_\ell \subseteq L \subseteq \mathbb{C}_\ell$, there is a map*

$$\mathrm{Red} : \mathscr{H}_\ell(L) \to \mathscr{T}_\ell$$

satisfying the following property: it is equivariant with respect to the action of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$*, that is, for every $z \in \mathscr{H}_\ell(L)$ and every $\gamma \in$* $\mathrm{PGL}_2(\mathbb{Q}_\ell)$*, we have that* $\mathrm{Red}(\gamma \cdot z) = \gamma \cdot \mathrm{Red}(z)$*.*

By taking the direct limit of this construction, we obtain the tree $\mathscr{T}_\ell$ as the graph of the reduction mod ℓ of $\mathscr{H}_\ell$. We can think of the Bruhat–Tits tree as the skeleton of the ℓ-adic upper half plane via this reduction map. This reduction map will be useful to describe the special fibres of a Shimura curve.

[4] We are using the prime ℓ to be consistent with the isogeny graphs to which we want to connect this theory. In the Shimura curves literature, p is widely used as the chosen prime, so *p-adic upper half-plane* is more standard.

3.3 ℓ-adic Shimura curves

Let H denote an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D_H = D\ell$, with $D > 1$ and $\ell \nmid D$. To highlight the importance of the prime ℓ in what follows, we will write $D\ell$ instead of D_H. We consider as before the embedding $\Phi : H \hookrightarrow \mathrm{M}_2(\mathbb{R})$. We are interested in the ℓ-adic analogue $\Gamma_{+,\ell}$ of the group Γ_+ defined in section 3.1.

We will first define an intermediate group Γ_ℓ. The group Γ_ℓ is defined, following Čerednik [Cer76, Theorem 2.1], by interchanging the prime ℓ for ∞ in the quaternion algebra H. That is, instead of the indefinite quaternion algebra H, we consider the definite quaternion algebra $B = B_{D,\infty}$ of discriminant D and ramified at ∞. Let $\mathcal{O}_B \subseteq B$ be a maximal order in B and define the localised order $\mathcal{O}_B[1/\ell] := \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell]$ over $\mathbb{Z}[1/\ell]$. Like in the complex case, there exists an ℓ-adic matrix immersion $\Phi_\ell : B \hookrightarrow \mathrm{M}_2(\mathbb{Q}_\ell)$. The unit group in $\mathcal{O}_B[1/\ell]$ is formed by the elements in $\mathcal{O}_B[1/\ell]$ whose reduced norm is a unit in $\mathbb{Z}[1/\ell]$:

$$\mathcal{O}_B[1/\ell]^\times := \{\alpha \in \mathcal{O}_B[1/\ell] : \mathrm{nrd}(\alpha) \in \mathbb{Z}[1/\ell]^\times\} = \{\alpha \in \mathcal{O}_B[1/\ell] : \mathrm{nrd}(\alpha) = \ell^k,\ k \in \mathbb{Z}\}.$$

We define the (discrete cocompact) subgroup Γ_ℓ of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ as

$$\Gamma_\ell := \Phi_\ell(\mathcal{O}_B[1/\ell]^\times)/\mathbb{Z}[1/\ell]^\times.$$

Because scaling by powers of ℓ does not change anything, we can in fact generate the group Γ_ℓ by images of elements in O_B with norm a power of ℓ.

Remark 3.4 *The maximal $\mathbb{Z}$-order $\mathcal{O}_B$ might not be unique up to conjugation, as the quaternion algebra B is definite. Nevertheless, the $\mathbb{Z}[1/\ell]$-order $\mathcal{O}_B[1/\ell]$ is unique up to conjugation, as it satisfies Eichler's condition* [Vig80, Corollaire 5.7].

In [Dri76], Drinfel'd constructed an ℓ-adic analogue of the isomorphism (5) called *Drinfel'd integral model* of the Shimura curve $X(D\ell)$, extending the modular interpretation of $X(D\ell)(\mathbb{C})$ over $\mathbb{Q}_\ell$. Jordan and Livne [JL84] give an important consequence of Čerednik and Drinfel'd's results that we will use.

We finally have all the ingredients to define the group $\Gamma_{\ell,+} \subset \mathrm{PGL}_2(\mathbb{Q}_\ell)$ mentioned in the beginning of Section 3:

$$\Gamma_{\ell,+} := \Phi_\ell(\{\alpha \in \mathcal{O}_B[1/\ell]^\times \mid \mathrm{nrd}(\alpha) = \ell^{2n}, \text{ for } n \in \mathbb{Z}\})/\mathbb{Z}[1/\ell]^\times \subseteq \Gamma_\ell.$$

Our interest in this group comes from Drinfel'd's theorem, which gives a bijection between the following sets of $\mathbb{Q}_{\ell^2}$-points:

$$\Gamma_{\ell,+}\backslash\mathcal{H}_\ell(\mathbb{Q}_{\ell^2}) \simeq X(D\ell)(\mathbb{Q}_{\ell^2}),$$

where $\mathbb{Q}_{\ell^2}$ denotes the quadratic unramified extension of $\mathbb{Q}_\ell$ contained in $\mathbb{C}_\ell$. Moreover, this theorem states that the graph of the special fibre $X(D\ell)_{\mathbb{F}_\ell}$ is the graph $\Gamma_{\ell,+}\backslash\mathcal{T}_\ell$. We will see in Section 4.3 that the graph $\Gamma_{\ell,+}\backslash\mathcal{T}_\ell$ is a 2-covering of the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$.

3.4 Computing the graph of the special fibre of a Shimura curve

Now we explain how to compute the graph $\mathcal{G}$ of the special fibre at ℓ of the Shimura curve $X(D\ell)$ of discriminant $D\ell$, with $\ell \nmid D$, using its interpretation as the quotient $\Gamma_{\ell,+}\backslash\mathcal{T}_\ell$ of the Bruhat–Tits tree $\mathcal{T}_\ell$.

In [FM14] the authors take a computational approach to this problem and provide an algorithm, which they implemented in Sage, to compute the graph $\mathcal{G}$ for every quaternion algebra. It is also possible to construct the graph $\mathcal{G}$ explicitly when the left-ideal class number of the quaternion algebra $B_{D,\infty}$ is 1, as was done in [AM19].

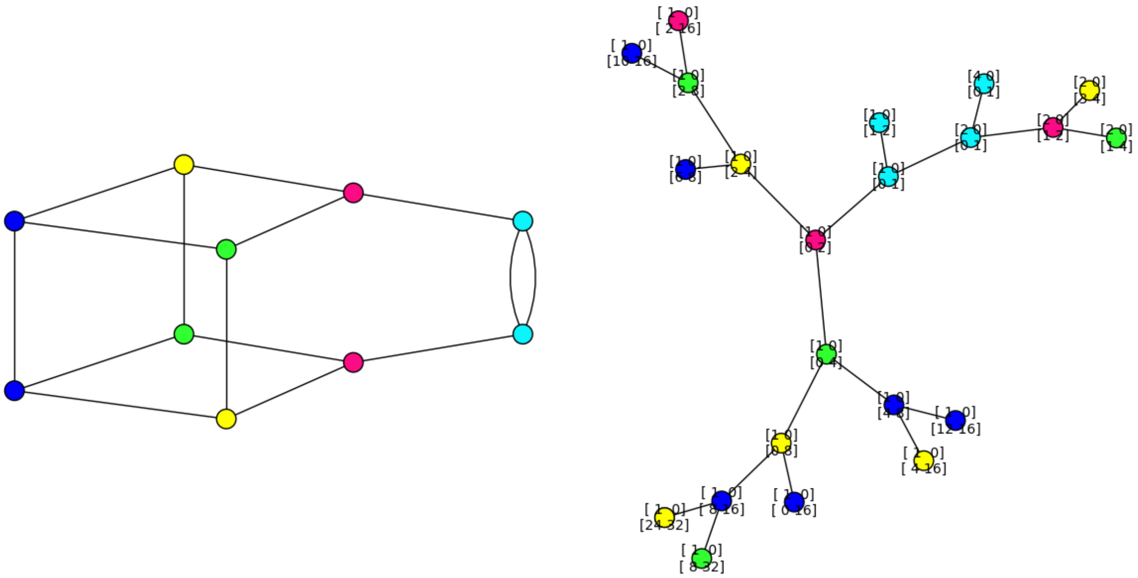

Figure 3.1: *Graph of the special fibre at* $\ell = 2$ *of the Shimura curve* $X(61\cdot 2)$ *(left) and fundamental domain of* $X(61 \cdot 2)$ *inside* $\mathcal{T}_2$ *(right), computed with the code provided in [FM14].) Vertices with the same colour correspond to (classes of) lattices* Λ *with the same endomorphism ring* $\mathrm{End}(\Lambda)$*, see also Section 4.4.*

The code in [FM14] allows us to compute the graph of special fibres of Shimura curves, such as in Figure 3.1. The result can be represented as a compact graph or as a fundamental domain inside $\mathcal{T}_\ell$ whose edges are labelled by representatives of the 2×2 matrices as described in Section 2.3.
In Section 4.3 we will see that the graph $\mathcal{G}$ is a double covering of the supersingular isogeny graph $\mathcal{G}_\ell$.

4 Different views on supersingular isogeny graphs

In this section, we explain the relations between the three main objects from the previous sections: supersingular isogeny graphs, quaternion ideal graphs, and (quotients of) Bruhat–Tits trees. In Section 4.1 we recap Deuring's correspondence, which shows the relationship between the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$ and the quaternion ℓ-ideal graph. In Section 4.2 we show how to explicitly identify vertices and edges of the Bruhat–Tits tree $\mathcal{T}_\ell$ with supersingular elliptic curves and ℓ-isogenies, via ℓ-adic Tate modules. This allows us to think of the Bruhat–Tits tree as an "unfolding" of the supersingular isogeny graph. In Section 4.3 we recap Ribet's correspondence, which shows that the quotient of the tree of Section 4.2 by the group $\Gamma_{+,\ell}$ of Section 3.3 gives a graph that is a double cover of the supersingular isogeny graph $\mathcal{G}_\ell$. Finally, in Section 4.4 we explain how to relate the vertices of the Bruhat–Tits tree $\mathcal{T}_\ell$ to maximal orders in the quaternion algebra $B_{p,\infty}$.

4.1 Supersingular elliptic curves and endomorphism rings: Deuring's correspondence

Deuring's correspondence [Deu41] between supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ and maximal orders in $B_{p,\infty}$ translates ℓ-isogenies into left-ideals of reduced norm ℓ. This correspondence establishes a natural connection between supersingular isogeny graphs and quaternionic ideal graphs. Here we give a construction of the correspondence.

Let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. Then $\mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, where $B_{p,\infty}$ is the definite quaternion algebra over $\mathbb{Q}$ of discriminant p, and $\mathrm{End}(E)$ is isomorphic to a maximal order $\mathcal{O}$ in $B_{p,\infty}$. To any left-ideal $I \subseteq \mathcal{O}$ we associate the subgroup of $E(\overline{\mathbb{F}}_p)$

$$E[I] = \bigcap_{\alpha \in I} \ker(\alpha).$$

This subgroup is necessarily finite, and if $p \nmid \mathrm{nrd}(I)$ we have $\mathrm{nrd}(I) = \#E[I]$. We define the associated isogeny $\varphi_I : E \to E/E[I]$ by its kernel $E[I]$. Then φ_I is an isogeny of degree $\deg(\varphi_I) = \mathrm{nrd}(I)$ and the right-order $\mathcal{O}_r(I)$ of I can be identified with $\mathrm{End}(E/E[I])$. Conversely, any isogeny $\varphi : E \to E'$ is of the form $\varphi = \rho \circ \varphi_I$ for some left-ideal $I \subseteq \mathcal{O}$ and some isomorphism $\rho : E/E[I] \to E'$ [Voi, Cor. 42.2.21].

Moreover, we have $E/E[I] \cong E/E[J]$ if and only if I and J are in the same left-ideal class of $\mathcal{O}$, that is, if $I = J\beta$ for some $\beta \in B_{p,\infty}^{\times}$. Therefore, starting from E, we can enumerate all the isomorphism classes of supersingular elliptic curves isogenous to E by taking isogenies φ_I for $[I]$ running over the left-ideal classes of $\mathcal{O}$. Moreover, left-ideals of reduced norm ℓ give isogenies of norm ℓ.

Note that there is no bijection between isomorphism classes of supersingular elliptic curves and isomorphism classes (or conjugacy classes, or types) of maximal orders in $B_{p,\infty}$: elliptic curves with conjugate supersingular j-invariants j and j^p will have endomorphism rings which are isomorphic as rings.

Example 4.1 *Let $p \equiv 3 \pmod 4$ and let $E : y^2 = x^3 + x$ be the supersingular elliptic curve defined over $\mathbb{F}_p$ with $j(E) = 1728$. If we identify i with the endomorphism $\varphi : (x, y) \mapsto (-x, \sqrt{-1}y)$, j with the endomorphism $\pi : (x, y) \mapsto (x^p, y^p)$, and set $k := ij$, then*

$$\mathrm{End}(E) = \mathbb{Z} \oplus i\mathbb{Z} \oplus \frac{i+j}{2}\mathbb{Z} \oplus \frac{1+k}{2}\mathbb{Z},$$

which is the maximal order in $B_{p,\infty}$ that we met already in Example 2.2.

4.2 The Bruhat–Tits tree viewed as an unfolding of the supersingular isogeny graph

There is a correspondence between vertices of the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$ and the Bruhat–Tits tree $\mathcal{T}_\ell$. This can be described explicitly once a specific elliptic curve E in $\mathcal{G}_\ell$ (or better, its Tate module) has been identified with the root $\langle (1,0), (0,1) \rangle$ of $\mathcal{T}_\ell$. Through this correspondence we can interpret non-backtracking paths starting from E in $\mathcal{G}_\ell$ as paths from the chosen root of $\mathcal{T}_\ell$ in the infinite tree $\mathcal{T}_\ell$ that increase the distance from the root at every step. We call this a "level-increasing" path on $\mathcal{T}_\ell$. The Bruhat–Tits tree $\mathcal{T}_\ell$ can then be seen as an "unfolding" of the supersingular isogeny graph $\mathcal{G}_\ell$, which may help in studying walks in $\mathcal{G}_\ell$, an idea we return to in Section 5.

4.2.1 The Tate module

For any elliptic curve E, there is a natural choice of a $\mathbb{Z}_\ell$-lattice: the Tate module $T_\ell(E)$. Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve and let $\ell \neq p$ be a prime. We have that $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ as abelian groups and we have connecting maps

$$\begin{array}{rccc} [\ell]: & E[\ell^{n+1}] & \to & E[\ell^n] \\ & P & \mapsto & \ell P. \end{array}$$

The *Tate module* is defined to be the inverse limit of $E[\ell^n]$ with respect to the connecting maps:

$$T_\ell(E) = \lim_{\leftarrow} E[\ell^n].$$

As $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$, it follows that there exists an isomorphism $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules. Therefore, any $T_\ell(E)$ admits a basis $\{(P_n)_{n=1}^\infty, (Q_n)_{n=1}^\infty\}$ where $\{P_n, Q_n\}_{n=1}^\infty$ is a system of *compatible bases* of $E[\ell^n]$: for all $n \geq 1$ we have that $\{P_n, Q_n\}$ is a basis of $E[\ell^n]$ and $\ell P_{n+1} = P_n$, $\ell Q_{n+1} = Q_n$. The connecting maps commute with isogenies: for any n and for any isogeny $\varphi : E \to E'$, we have $\varphi(E[\ell^n]) \subseteq E'[\ell^n]$. By taking inverse limits, we obtain a map on the Tate modules $\varphi_\ell : T_\ell(E) \to T_\ell(E')$.

Now we turn to endomorphisms. By [Sil09, Chap. III Thm 3.4] we have that

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_\ell(E)).$$

Moreover, both $\mathrm{End}(E)$ and $T_\ell(E)$ come with a Galois action. For a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$, we know that $j(E) \in \mathbb{F}_{p^2}$ and hence E is isomorphic to a curve that can be defined over $\mathbb{F}_{p^2}$. Moreover, we can assume that $\mathrm{tr}(\pi) = \pm 2p$ (remember we assume $p > 3$). Possibly replacing E by its quadratic twist, we can therefore assume that $\mathrm{tr}(\pi) = -2p$. In this case, the Frobenius endomorphism acts like the scalar $[-p]$ and so all endomorphisms of E and $T_\ell(E)$ are necessarily Galois equivariant, that is, commute with the Frobenius endomorphism. This allows us to specialise Tate's theorem (as stated in [Sil09, Chap. III Thm 3.7]) to the following:

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E)).$$

Recall that the endomorphism ring of any $\mathbb{Z}_\ell$-lattice of rank 2 is a maximal order in the local quaternion algebra $M_2(\mathbb{Q}_\ell)$ and, as such, it is conjugate to $M_2(\mathbb{Z}_\ell)$. In other words, any lattice $\Lambda \subseteq (\mathbb{Q}_\ell)^2$ of rank 2 admits a basis in which $\mathrm{End}(\Lambda) = M_2(\mathbb{Z}_\ell)$.

In conclusion, by choosing a basis of the Tate module $T_\ell(E)$, we can identify the elliptic curve E with the vertex $\langle (1,0), (0,1) \rangle$ in the Bruhat–Tits tree. Moreover, this lattice retains arithmetic information about E, since $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$. We will see in the next two subsections that any other vertex of the Bruhat–Tits tree built from $T_\ell(E)$ can also be interpreted as an elliptic curve.

4.2.2 Translating vertices of Bruhat–Tits trees into sublattices of the Tate module

The Tate module $T_\ell(E)$ is a $\mathbb{Z}_\ell$-lattice of rank 2, so its endomorphism ring is a maximal order in $M_2(\mathbb{Q}_\ell)$, thus is conjugate to $M_2(\mathbb{Z}_\ell)$. In particular, by choosing a basis of $T_\ell(E)$, we can identify $T_\ell(E)$ with the lattice $\langle (1,0), (0,1) \rangle = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ so that $\mathrm{End}(T_\ell(E)) = M_2(\mathbb{Z}_\ell)$. This is the same as identifying $T_\ell(E)$ with the root vertex of the Bruhat–Tits tree, which is given by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Starting from the root vertex, we can build the rest of the Bruhat–Tits tree by identifying each vertex at level k with a cyclic sublattice of index ℓ^k in $T_\ell(E)$. If $\{(P_n)_{n=1}^\infty, (Q_n)_{n=1}^\infty\}$ is a given basis of $T_\ell(E)$, we can use the description of vertices of the Bruhat–Tits tree in terms of matrices (given in Section 2.3) for obtaining explicit bases for the corresponding sublattices. For instance, given $i_1 \in \{0, 1, \ldots, \ell-1, \infty\}$ and $i_j \in \{0, 1, \ldots, \ell-1\}$ for $j \geq 2$, we associate to the matrix $\alpha^{(k)}_{i_1,\ldots,i_k}$ described in (4) the cyclic sublattice $L^{(k)}_{i_1,\ldots,i_k} \subseteq T_\ell(E)$ of index ℓ^k with basis:

$$L^{(k)}_{i_1,\dots,i_k}: \quad \begin{cases} \{(P_n + \sum_{j=1}^{k} i_j \ell^{j-1} Q_n)_{n=1}^{\infty}, (\ell^k Q_n)_{n=1}^{\infty}\}, & \text{if } i_1 \neq \infty \\ \\ \{(\ell^k P_n)_{n=1}^{\infty}, (\sum_{j=2}^{k} i_j \ell^{j-1} P_n + Q_n)_{n=1}^{\infty}\}, & \text{if } i_1 = \infty. \end{cases}$$

Remark 4.2 *The Bruhat–Tits tree associated to the Tate module $T_\ell(E)$ can be also found, in a less explicit form, in De Feo's Habilitation thesis [DeFeo18, Sec I.4].*

4.2.3 Translating sublattices of the Tate module into subgroups of elliptic curves

As the Tate module $T_\ell(E)$ is the inverse limit of the torsion subgroups, there is a canonical map $T_\ell(E) \to E[\ell^k]$ for every $k \geq 1$. In particular this map sends a cyclic sublattice of index ℓ^k in $T_\ell(E)$ into a cyclic subgroup of order ℓ^k in $E[\ell^k]$. Hence, the Bruhat–Tits tree coming from the Tate module can be translated into a tree where at each level k we find all the cyclic subgroups of order ℓ^k of $E[\ell^k]$. More explicitly, if O_E denotes the identity of E and $\{(P_n)_{n=1}^{\infty}, (Q_n)_{n=1}^{\infty}\}$ is a basis of $T_\ell(E)$, it follows that:

- $v^{(0)} = \langle O_E \rangle$ is the root vertex.
- Each vertex at level k corresponds to a cyclic subgroup of $E[\ell^k]$ of order ℓ^k.
- A vertex $v^{(k)} = \langle R^{(k)} \rangle$ at level k is connected to a vertex $v^{(k+1)} = \langle R^{(k+1)} \rangle$ at level $(k+1)$ if and only if $\langle \ell R^{(k+1)} \rangle = \langle R^{(k)} \rangle$.
- For $i_1 \in \{0, 1, \dots, \ell-1, \infty\}$ and $i_j \in \{0, 1, \dots, \ell-1\}$ for $j \geq 2$, the corresponding vertex at level k is $v^{(k)}_{i_1,\dots,i_k} = \langle R^{(k)}_{i_1,\dots,i_k} \rangle$, where

$$R^{(k)}_{i_1,\dots,i_k} := \begin{cases} P_k + (\sum_{j=1}^{k} i_j \ell^{j-1}) Q_k, & \text{if } i_1 \neq \infty, \\ (\sum_{j=2}^{k} i_j \ell^{j-1}) P_k + Q_k, & \text{if } i_1 = \infty. \end{cases}$$

Example 4.3 *The $\ell+1$ vertices at level 1, i.e. adjacent to the root $v^{(0)}$, are $v^{(1)}_0, \dots, v^{(1)}_{\ell-1}, v^{(1)}_\infty$. For every $i_1 \in \{0, \dots, \ell-1, \infty\}$, $v^{(1)}_{i_1} = \langle R^{(1)}_{i_1} \rangle$, where*

$$R^{(1)}_{i_1} := \begin{cases} P_1 + i_1 Q_1, & \textit{if } i_1 \neq \infty, \\ Q_1, & \textit{if } i_1 = \infty. \end{cases}$$

Each one of these $\ell+1$ vertices has ℓ adjacent vertices at level 2, and so on.

It is easy now to translate our vertices (i.e. subgroups) into elliptic curves. Indeed, for every $(i_1, \dots, i_k) \in \{0, \dots, \ell-1, \infty\} \times \{0, \dots, \ell-1\}^{k-1}$, if $G := \langle R^{(k)}_{i_1 \dots i_k} \rangle$, then E/G is isomorphic to an elliptic curve E' which isogenous via a cyclic ℓ^k-isogeny to E.

4.2.4 Non-backtracking walks in $\mathcal{G}_\ell$ as level-increasing paths from the root of $\mathcal{T}_\ell$

Starting from a supersingular elliptic curve E we can perform a finite or infinite walk in the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$. If the walk is finite of length k and non-backtracking, the landing curve E' is isomorphic to E/G where G is a subgroup of $E[\ell^k]$ of order ℓ^k. As seen in Section 4.2.3, given a basis $\{P_k, Q_k\}$ of $E[\ell^k]$ there exists

$$(i_1, \dots, i_k) \in \{0, \dots, \ell-1, \infty\} \times \{0, \dots, \ell-1\}^{k-1}$$

such that

$$G = \left\langle P_k + \left(\sum_{j=1}^{k} i_j \ell^{j-1} \right) Q_k \right\rangle \quad \text{or} \quad G = \left\langle \left(\sum_{j=2}^{k} i_j \ell^{j-1} \right) P_k + Q_k \right\rangle;$$

in the second case $i_1 = \infty$. In this way we can label our walk in $\mathcal{G}_\ell$ with the finite sequence $(i_1, i_2, \ldots, i_k)$. Now, from $\{P_k, Q_k\}$ we can build a basis $\{(P_n)_{n=1}^{\infty}, (Q_n)_{n=1}^{\infty}\}$ of $T_\ell(E)$ such that $P_j = \ell^{k-j} P_k$, $Q_j = \ell^{k-j} Q_k$ for every $j = 1, \ldots, k$, and we can consider the Bruhat–Tits tree $\mathcal{T}_\ell$ built with respect to this basis. We then interpret the non-backtracking walk $(i_1, i_2, \ldots, i_k)$ in $\mathcal{G}_\ell$ as the level-increasing walk from the root of $\mathcal{T}_\ell$ which takes the 'direction' i_{n+1} at each level n. Note that this reasoning could be easily extended to infinite non-backtracking walks and in this case the label would be an infinite sequence $(i_1, i_2, \ldots)$.

In conclusion, this explicit description of the Bruhat–Tits tree offers a way of orienting a supersingular isogeny graph, by fixing a supersingular curve together with a basis of its Tate module as the root of the tree.

4.3 Bruhat–Tits tree quotients and supersingular isogeny graphs: Ribet's correspondence

Fix a prime p and let $\mathcal{E}(p) = \{E_1, \ldots, E_h\}$ be a system of representatives of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. For $a, b \in \{1, \ldots, h\}$ and $n \in \mathbb{N}$, let

$$I_{ab}(n,p) = \{\varphi \,|\, \varphi : E_a \to E_b \text{ is an isogeny with } \deg(\varphi) = n\}.$$

Recall that $\mathrm{End}(E_1)$ is isomorphic to a maximal order $\mathcal{O}_1$ in $B_{p,\infty}$, the definite quaternion algebra over $\mathbb{Q}$ of discriminant p. Take a prime $\ell \neq p$ and define from the order $\mathcal{O}_1[1/\ell]$ the group $\Gamma_{\ell,+} \subseteq \mathrm{PGL}_2(\mathbb{Q}_\ell)$ as in Section 3.3.

As we have seen, when we quotient the Bruhat–Tits tree $\mathcal{T}_\ell$ by this group we obtain a graph $\mathcal{G} := \Gamma_{\ell,+} \setminus \mathcal{T}_\ell$ which can be interpreted as the graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ coming from an indefinite quaternion algebra of discriminant $p\ell$. Ribet [Rib90] showed that the graph $\mathcal{G}$ is a double covering of the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$. More precisely, Ribet [Rib90, Prop. 4.4.] proves the following graph relation:

$$\mathrm{Ver}(\mathcal{G}) = \mathcal{E}(p) \bigsqcup \mathcal{E}(p),$$

$$\mathrm{Ed}(\mathcal{G}) = \bigsqcup_{1 \le i,j \le h} I_{ab}(\ell,p)/\sim,$$

where an isogeny $\varphi \in I_{ab}(\ell,p)$ is considered as an edge $[E_a, E_b]$ and two edges given by $\varphi, \varphi' \in I_{ab}(\ell,p)$ are identified, i.e. $\varphi \sim \varphi'$, if and only if there is $\alpha \in \mathrm{Aut}(E_a)$ and $\beta \in \mathrm{Aut}(E_b)$ such that $\varphi' = \beta \circ \varphi \circ \alpha$.

Remark 4.4 *Note that Ribet's correspondence is a 2:1 covering from $\mathcal{G}$ to the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$, whereas Deuring's correspondence is only 2:1 onto the vertices defined over $\mathbb{F}_{p^2} - \mathbb{F}_p$, and 1:1 onto the vertices defined over $\mathbb{F}_p$. In particular, there cannot be a perfect 1:1 correspondence between the quaternion ideal graph and the Bruhat–Tits quotient $\mathcal{G}$.*

Remark 4.5 *The correspondence between supersingular isogeny graphs and the Bruhat–Tits tree is explained in [CGL09b] and [CFLMP18]. By Deuring's correspondence, isomorphism classes of supersingular elliptic curves are in bijection with the class set of maximal orders in a definite quaternion algebra. This class set is in bijection with a double coset of the adelic points of a quaternion algebra. Section 7 of [CFLMP18] is devoted to explaining strong approximation for the adelic quotient, which gives a bijection between the vertices of the supersingular isogeny graph and the double cosets $\mathcal{O}[\ell^{-1}]^\times \backslash GL_2(\mathbb{Q}_\ell)/GL_2(\mathbb{Z}_\ell)$, where $\mathcal{T}_\ell = GL_2(\mathbb{Q}_\ell)/GL_2(\mathbb{Z}_\ell)$ is the Bruhat–Tits tree.*

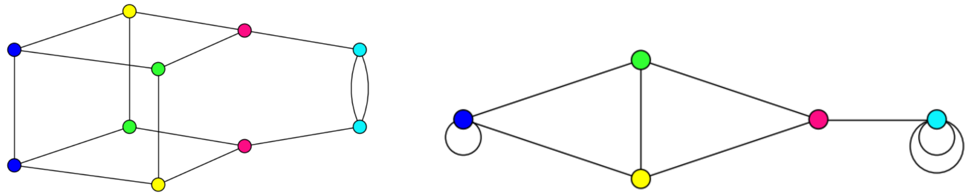

Figure 4.1: *Comparision of the graph of the special fibre at ℓ of the Shimura curve $X(p \cdot \ell)$ (left) and the supersingular ℓ-isogeny graph (right) for $\ell = 2$ and $p = 61$. Vertices with the same colour on the left map under Ribet's correspondence to the vertex of the same colour on the right. Compare also with the coloring of the vertices in Figure 3.1.*

4.4 The Bruhat–Tits tree and quaternion orders

Following [Mil15, Sec. 2.2.2.4], we outline how to relate the vertices of a Bruhat–Tits tree, viewed as classes of homothetic $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$, to maximal orders in $B := B_{p,\infty}$.

Let $\mathcal{O}$ be a maximal order of B. For a prime $\ell \neq p$, we consider the localisation $B_\ell := B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and write $\mathcal{O}_\ell$ for the localization of $\mathcal{O}$. Since B is split at ℓ, there is an isomorphism $B_\ell \cong M_2(\mathbb{Q}_\ell)$. Under this isomorphism, the maximal order $\mathcal{O}_\ell$ gets mapped to a maximal order in $M_2(\mathbb{Q}_\ell)$. But in $M_2(\mathbb{Q}_\ell)$, any maximal order is conjugate to the maximal order $M_2(\mathbb{Z}_\ell)$: as described in Section 3.3, we can choose an embedding

$$\Phi_\ell : B \hookrightarrow M_2(\mathbb{Q}_\ell)$$

such that $\Phi_\ell(\mathcal{O}) = M_2(\mathbb{Z}_\ell)$, and the embedding Φ_ℓ is the composition of the localization map and a conjugation in $M_2(\mathbb{Q}_\ell)$. Under Φ_ℓ, other maximal orders in B map to maximal orders in $M_2(\mathbb{Q}_\ell)$, and hence are endomorphism rings of lattices in $\mathbb{Q}_\ell^2$. The embedding Φ_ℓ factors as the localization map $B \to B_\ell$ and an isomorphism $\Psi_\ell : B_\ell \to M_2(\mathbb{Q}_\ell)$. Given a homothety class $\{M\}$ of $\mathbb{Z}_\ell$-lattices of rank 2, define $\mathcal{O}_{\{M\}} := \Psi_\ell^{-1}(\mathrm{End}(M))$. The order $\mathcal{O}_{\{M\}}$ is maximal in B_ℓ [Vig80, p. II.2.1]. In fact, the set of vertices of the Bruhat–Tits tree $\mathcal{T}_\ell$ is in bijection with the set of maximal orders of B_ℓ, and the bijection is given by

$$\{M\} \in \mathrm{Ver}(\mathcal{T}_\ell) \mapsto \mathcal{O}_{\{M\}} \subseteq B_\ell;$$

this bijection depends on the isomorphism Ψ_ℓ and the choice of basis for $\mathbb{Q}_\ell^2$ [Mil15, Sec. 2.2.2.4].

We emphasize that this construction depends on the choice of the embedding Φ_ℓ. Conversely, if we take any maximal order $\mathcal{O} \subseteq B_{p,\infty}$, we can choose Φ_ℓ such that $\Phi_\ell(\mathcal{O}) = M_2(\mathbb{Z}_\ell)$, which is the endomorphism ring of the lattice $\langle(1,0),(0,1)\rangle$, i.e., we can choose $\mathcal{O}$ as root of the Bruhat–Tits tree.

Remark 4.6 *The Bruhat–Tits tree $\mathcal{T}_\ell$ can also be interpreted in terms of global orders in B. For a fixed maximal order $\mathcal{O} \subseteq B$, consider the set of maximal orders $\mathcal{O}' \subseteq B$ defined locally by*

$$\begin{cases} \mathcal{O}'_{\tilde{\ell}} := \mathcal{O}_{\tilde{\ell}}, & \text{for } \tilde{\ell} \neq \ell, \\ \mathcal{O}'_\ell := x\mathcal{O}_\ell x^{-1}, & \text{for some } x \in B_\ell. \end{cases}$$

This set is in bijection with the set of local maximal orders in B_ℓ [Mil15]. Note that we can choose $\mathcal{O}$ to be such that $\mathcal{O}_\ell = \mathcal{O}_{\{M^0\}}$, with $M^0 = M_2(\mathbb{Z}_\ell) = \langle(1,0),(0,1)\rangle$.

5 Towards cryptographic applications

In this section we explore the possibility of using Bruhat–Tits trees for cryptanalysis of isogeny-based protocols that make use of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, which includes the CGL hash function [CGL09a] and any SIDH-based protocols (e.g. [SIKE]) but excludes commutative isogeny-based proposals like CSIDH [CLMPR18].

In Section 5.1 we argue why the Bruhat–Tits tree truncated at a certain level may actually be more instructive than the supersingular isogeny graph $\mathcal{G}_\ell$ for cryptanalysis of, for example, SIKE. We find this interesting for several reasons:

- Computing paths on the Bruhat–Tits tree $\mathcal{T}_\ell$ is much more simple and efficient than computing paths in isogeny graphs $\mathcal{G}_\ell$ or graphs of quaternion orders, since it just involves linear algebra with $M_2(\mathbb{Z}_\ell)$, see Section 5.3.
- Computing a path from a given vertex on the Bruhat–Tits tree to the root vertex (corresponding by our choices to $j = 1728$) is trivial.
- Computing the isogeny corresponding to a given path is simple and efficient, see Algorithm 1.
- Information about the quaternion order corresponding to a given vertex, such as its norm form, can be read off from the label of the vertex. A speculative cryptanalytic application of this is discussed in Section 5.4.

5.1 A truncated Bruhat–Tits tree from SIKE parameters

In this section, we argue that the truncation of the Bruhat–Tits tree, as defined at the end of Section 2.3, is a useful tool for the cryptanalysis of SIKE since it gives a convenient 'approximation' of the subgraph of $\mathcal{G}_\ell$ relevant for SIKE. The parameter setup in SIKE already specifies a basis of two torsion groups of the form $E[\ell^e]$ of a given supersingular elliptic curve E, and the truncated Bruhat–Tits tree can be built from this basis as described in Sections 4.2.1 and 4.2.4; this is not captured by the graph $\mathcal{G}_\ell$ because $\mathcal{G}_\ell$ only keeps track of which curves are ℓ-isogenous.

In SIKE, the prime p is chosen such that $p = 2^{e_A}3^{e_B}-1$, and the starting elliptic curve $E_0/\mathbb{F}_{p^2}$ is chosen such that the trace of the Frobenius endomorphism is $-2p$, so that $\#E_0(\mathbb{F}_{p^2}) = (p+1)^2$. Moreover, in the protocol we have as public parameters a basis $\{P_A, Q_A\}$ of $E_0[2^{e_A}] \subseteq E_0(\mathbb{F}_{p^2})$ and a basis $\{P_B, Q_B\}$ of $E_0[3^{e_B}] \subseteq E_0(\mathbb{F}_{p^2})$. Alice (resp. Bob) takes a pseudorandom walk in the supersingular isogeny graph $\mathcal{G}_2$ (resp. $\mathcal{G}_3$) of length e_A (resp. e_B) from E_0. This pseudorandomness is achieved by choosing an integer $0 \le n_A < 2^{e_A}$ (resp. $0 \le n_B < 3^{e_B}$) and by computing the isogeny $\varphi_A : E_0 \to E_A$ (resp. $\varphi_B : E_0 \to E_B$) with kernel $G_A = \langle P_A + n_A Q_A\rangle$ (resp. $G_B = \langle P_B + n_B Q_B\rangle$). Note that the isogeny φ_A (resp. φ_B) can be computed very efficiently as a sequence of $\mathbb{F}_{p^2}$-rational 2-isogenies (resp. 3-isogenies).

We revisit Alice's walk step by step. Notice that for every $1 \le k \le e_A$, the points $\{2^{e_A-k}P_A, 2^{e_A-k}Q_A\}$ form a system of compatible bases of $E_0[2^k]$, which allows us to consider the Bruhat–Tits tree $\mathcal{T}_2$ with root E_0 and truncated at level e_A. Following the notation introduced in Section 2.3, we will denote this truncated Bruhat–Tits tree by $\mathcal{T}_2^{(e_A)}$. Now, the first step of Alice's walk in $\mathcal{G}_2$ is given by the isogeny $E_0 \to E_0/\langle 2^{e_A-1}(P_A + n_A Q_A)\rangle$. Since $2^{e_A-1}(P_A+n_AQ_A) = 2^{e_A-1}P_A + i_1 2^{e_A-1}Q_A$ where $i_1 \equiv n_A \pmod 2$, and $\{2^{e_A-1}P_A, 2^{e_A-1}Q_A\}$ is a basis of $E_0[2]$, this step can be identified on $\mathcal{T}_2^{(e_A)}$ with the step from the root in the direction i_1, which is labelled by the matrix

$$\begin{pmatrix} 1 & 0 \\ i_1 & 2 \end{pmatrix}.$$

More in general, if we represent n_A with its 2-adic expansion, i.e.

$$n_A = \sum_{j=1}^{e_A} i_j 2^{j-1}, \quad i_j \in \{0,1\} \text{ for all } j = 1, \dots, e_A,$$

then it is easy to see that the kth step of Alice's walk on $\mathcal{G}_2$ corresponds to a level-increasing step on $\mathcal{T}_2^{(e_A)}$ in the direction i_k. Hence, we can label Alice's walk with the sequence of directions $(i_1, i_2, \dots, i_{e_A}) \in \{0,1\}^{e_A}$. In other words we can see all Alice's non-backtracking walks from E_0 on $\mathcal{G}_2$ as level-increasing walks from the root on $\mathcal{T}_2^{(e_A)}$ for which the first step also cannot be in direction ∞. This restriction on the first step is due to the choice in SIKE to write the generator of the kernel in the form $P_A + nQ_A$. As a consequence, we are walking on the subtree $\mathcal{T}_2' \subsetneq \mathcal{T}_2^{(e_A)}$ obtained from $\mathcal{T}_2^{(e_A)}$ by 'trimming' the direction ∞. To see directly that the leaves of the subtree $\mathcal{T}_2'$ give all the possible public keys E_A, note that this subtree has on its k^{th} level the elliptic curves given by, for $0 \le n < 2^{e_A} - 1$, the quotients

$$E_0/\langle 2^{e_A - k}\,(P_A + nQ_A)\rangle.$$

Mutatis mutandis, Bob's walk from E_0 to E_B in $\mathcal{G}_3$ can be considered as a level-increasing walk on the subtree $\mathcal{T}_3'$ of the Bruhat–Tits tree $\mathcal{T}_3$ truncated at level e_B and trimmed of the ∞ direction.

The vertices in $\mathcal{T}_\ell'$ for $\ell \in \{2,3\}$ do not necessarily correspond to curves with different j-invariants. We can map $\mathcal{T}_\ell' \subseteq \mathcal{T}_\ell \to \mathcal{G}_\ell$ by identifying vertices corresponding to curves with the same j-invariant and by identifying equivalent edges. However, in [OAT20], Onuki, Aikawa, and Takagi compute that the image of $\mathcal{T}_\ell'$ in $\mathcal{G}_\ell$ is 'almost a tree', and in cases of interest, it is indeed a tree: the image of $\mathcal{T}_\ell'$ in $\mathcal{G}_\ell$ is a tree for (the parameter sets in) SIKEp434 for $\ell = 2$ and for SIKEp504 for both $\ell = 2$ and $\ell = 3$; for SIKE p434 and $\ell = 3$ the mapping of $\mathcal{T}_3'$ into $\mathcal{G}_3$ glues two pairs of vertices together. A similar computation is in principle possible for larger parameter sets but seems computationally expensive.

Remark 5.1 *Recall that if we want a level-increasing walk on the Bruhat–Tits tree, we need to avoid the ∞ direction in all except for the first step and as explained above, in SIKE, the ∞ direction is avoided also in the first step by the explicit choice of kernel generators $P_A + nQ_A$. However, there is another design choice of SIKE for $\ell = 2$ that can be thought of as avoiding the ∞ direction: For $\ell_A = 2$, the j-invariant $j = 1728$ admits a self-loop and two 2-isogenies to the elliptic curve with j-invariant $j = 287496$. Therefore, SIKE chooses the starting curve $E_6 : y^2 = x^3 + 6x^2 + x$ and, for the 2-isogeny walks, chooses a basis $\{P_A, Q_A\} \subseteq E_6[2^{e_A}]$ such that none of the 2^{e_A}-isogenies pass through $j = 1728$. This is equivalent to ensuring that $[2^{e_A - 1}]P_A \ne (0,0)$.*

5.2 Isogenies from paths in the Bruhat–Tits tree

The root vertex of the Bruhat–Tits tree corresponds to an elliptic curve E_0 of known endomorphism ring and a choice of a 'suitable basis' $\{P_k, Q_k\} \subseteq E_0[\ell^k]$, defined below. Given a level-increasing path of length k from the root vertex $v^{(0)}$, we show that it is easy to translate the path into a sequence of isogenies starting at E_0.

Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Recall that the Bruhat–Tits tree can be constructed in two fashions. The first was described in Section 4.2.1: use a basis of the Tate module $T_\ell(E)$ to map E to the vertex $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$; project the basis of $T_\ell(E)$ to $E[\ell^k]$ to get a basis $\{P_k, Q_k\}$ of $E[\ell^k]$. The directions in the Bruhat–Tits tree exactly correspond to the choice of the kernel generators, as seen in Section 4.2.4. We call the basis $\{P_k, Q_k\}$ of $E[\ell^k]$ a 'suitable basis'. Alternatively, under any localization map $\Phi_\ell : B_{p,\infty} \to B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$, the endomorphism ring $\mathcal{O}$ maps to a maximal order in $M_2(\mathbb{Q}_\ell)$ and hence is the endomorphism ring of some lattice in $\mathbb{Q}_\ell^2$. This maps E to some vertex in the Bruhat–Tits tree $\mathcal{T}_\ell$; if desirable we can place E at the root of the tree by choosing the Φ_ℓ for which $\Phi_\ell(\mathrm{End}(E)) = M_2(\mathbb{Z}_\ell)$.

In some cases, having taken the second approach, it is still possible to recover a suitable basis. Specifically, if we know the endomorphism ring $\mathrm{End}(E) = \mathcal{O} \subseteq B_{p,\infty}$, then we can find a suitable basis: take any basis $\{P_k, Q_k\}$ of $E[\ell^k]$. Denote by $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ a basis of $\mathcal{O}$ and compute the images $\Phi_\ell(\alpha_i) \in M_2(\mathbb{Q}_\ell)$. We can interpret them as maps in $\mathrm{End}(T_\ell(E))$ and compute the action of $\Phi_\ell(\alpha_i)$ on $\{P_k, Q_k\}$. Provided that ℓ is small, it is not difficult to construct a basis $\{P_k, Q_k\}$ of $E[\ell^k]$ such that the action of α_i on $E[\ell^k]$ is given by the matrices $\Phi_\ell(\alpha_i)$.

Algorithm 1 Computing the isogeny corresponding to a non-backtracking path in the Bruhat–Tits quotient

```
Require: 1. A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with known endomorphism ring $\mathrm{End}(E) \cong \mathcal{O}$.
         2. An embedding $\Phi_\ell : \mathcal{O} \hookrightarrow M_2(\mathbb{Q}_\ell)$ such that $\Phi_\ell(\mathcal{O}) = M_2(\mathbb{Z}_\ell)$, and a suitable basis $\{P, Q\}$ of $E[\ell^k]$.
         3. A vertex $w$ in the truncated Bruhat–Tits tree $\mathcal{T}_\ell^{(k)}$ at distance $d \leq k$ from the vertex $v$.
Ensure: Sequence of $\ell$-isogenies $(\varphi_1, \dots, \varphi_d)$ such that $\varphi = \varphi_d \circ \cdots \circ \varphi_1 : E \to E_d$ is the isogeny corresponding
  to the path from $v$ to $w$.

1. Compute the shortest path from $v$ to $w$ in the Bruhat–Tits tree, as a sequence of directions $(i_1, \dots, i_d)$
  with $i_1 \in \{0, \dots, \ell-1, \infty\}$ and $i_j \in \{0, \dots, \ell-1\}$ for $j \geq 2$, as defined in Equation (2).
2. ($j = 1$ case) Set $E_0 = E$.
    1. If $i_1 \neq \infty$, set $S_1 = P + [i_1]Q$ and $T_1 = Q$. Otherwise, set $S_1 = Q$ and $T_1 = P$.
    2. Compute the $\ell$-isogeny $\varphi_1 : E_0 \to E_1$ with kernel $[\ell^{k-1}]S_1$.
    3. Replace $S_1 = \varphi_1(S_1)$ and $T_1 = \varphi_1(T_1)$ .
3.
  for $j = 2, \dots, d$ do
    3a.  Set $S_j = S_{j-1} + [i_j \cdot \ell^{j-1}]T_{j-1}$. (Note that the order of $S_j$ is $\ell^{k-j+1}$.)
    3b.  Compute the $\ell$-isogeny $\varphi_j : E_{j-1} \to E_j$ with kernel $[\ell^{k-j}]S_j$.
    3c.  Replace $S_j = \varphi_j(S_j)$ and $T_j = \varphi_j(T_j)$.
  end for
  return $(\varphi_1, \dots, \varphi_d)$ and $E_d$.
```

Remark 5.2 *In Algorithm* 1*, we assume that the vertex corresponding to E is at the root $v^{(0)}$ of the Bruhat–Tits tree. However, it is easy to extend the algorithm to compute paths between elliptic curves corresponding to any vertices $v, w \in \mathcal{T}_\ell^{(k)}$.*

Since $\mathcal{T}_\ell^{(k)}$ is a tree, we obtain the shortest path from v to w by walking towards the root vertex until they reach the same vertex u (and take the minimal choice of u). Then the shortest path from v to w is the path $v \to u \to w$. The isogeny corresponding to this path can be obtained by first computing the isogenies corresponding to the paths $v^{(0)} \to u \to v$ and $v^{(0)} \to u \to w$ and then composing the dual of the isogeny corresponding to the path $u \to v$ with the isogeny corresponding to the path $u \to w$.

Note also that identifying the direction towards the root from the vertex v on level k corresponding to a lattice Λ is easy: it is the matrix form M_i of the unique direction i such that $M_i\Lambda = \ell \cdot \Lambda'$ for some lattice $\Lambda' \subseteq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Then $\Lambda' = \frac{1}{\ell}(M_i\Lambda)$ can be taken as a representative of the unique class of lattices that gives the unique neighbour of v on level $k-1$.

Example 5.3 *In this example, we set $p = 2^{128} \cdot 3^{81} - 1$ and $E_0/\mathbb{F}_p : y^2 = x^3 - x$ to be the supersingular elliptic curve with j-invariant* 1728*. We want to compute the first* 4 *steps in the Bruhat–Tits $\mathcal{T}_3$ tree in direction 2. We choose $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$.*

We know that $\mathrm{End}(E_0) \cong \mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$*. Since we are only interested in the action of $\mathcal{O}$ on $E_0[3^4]$, we use the function* `_local_splitting_map_big` *with precision* = 4 *to* *compute the local embedding* $\mathcal{O} \hookrightarrow M_2(\mathbb{Z}_\ell)$ *sending*

$$i \mapsto \begin{pmatrix} 0 & 2+2\cdot 3+2\cdot 3^2+2\cdot 3^3+O(3^4) \\ 1+O(3^4) & 0 \end{pmatrix}, \tag{6}$$

$$j \mapsto \begin{pmatrix} 1+O(3^4) & 0 \\ 0 & 2+2\cdot 3+2\cdot 3^2+2\cdot 3^3+O(3^4) \end{pmatrix}. \tag{7}$$

We approximate the action of these matrices on $E[3^4]$ *by the matrices*

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad j \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{8}$$

From this we see that we can obtain a suitable basis $\{P, Q\} \subseteq E_0[3^4]$ *by choosing any* $P = (x_P, y_P) \in E[3^4]$ *with coefficients in* $\mathbb{F}_p$ *and then setting* $Q = i(P) = (-x_P, \sqrt{-1}y_P)$.

We choose the following:

$$\begin{aligned}
P &= (6909005812112653454355345091420247124314944411268723628219610395053698657567 4,\\
&\quad 1481491796909512517415432471402015746937971965247577239261155913482055765601 75)\\
\sqrt{-1} &= 1508902149747805841268574310872641836707583265569498552975198745954459435663 35 \cdot \alpha\\
&\quad +1508902149747805841268574310872641836709825959002068570142225655675856900587 51\\
Q = i(P) &= (8180015685365404958330398017306171242805742113077662244872915258918844997549 3,\\
&\quad 5784293758440959378532437388930619351059004471930126358572253974547021442032 7 \cdot \alpha\\
&\quad +1043665762795950889560909024882851885908984549813825611583238981425978254857 47)
\end{aligned}$$

Applying Algorithm 1 for the directions $(2, 2, 2, 2)$ *(that is, sidestepping Step 1.) we obtain the following sequence of isogenies:*

$$\begin{aligned}
&E_0 \to E_1 \to E_2 \to E_3 \to E_4\\
j(E_1) &= 1508902149747805841268574310872343577575343338187410134049362251097563287671 67,\\
j(E_2) &= 7547000210304043792970944750504583966240784144527277273032649279470104828914 4,\\
j(E_3) &= 9835528416708171630595587590500112016400078250025221487899546588355628137266 5,\\
j(E_4) &= 1388066880339297988118686463466172299814501399414830259912841487232310472184.
\end{aligned}$$

5.3 Explicit computations with the Bruhat–Tits tree

To explicitly compute neighbours in the quotient of the Bruhat–Tits tree, we adapt the code from [FM14], which is also available in Sage [BTQuotient]. The module BTQuotient [FM14code] allows one to enumerate the entire graph given by the quotient of the Bruhat–Tits tree $\mathcal{T}_\ell$ by the group $\Gamma_{\ell,+}$, that in turn gives a double covering of the isogeny graph $\mathcal{G}_\ell$ (note that while their definition of $\Gamma_{\ell,+}$ is slightly different from ours, the groups are the same). The code from [FM14], also contains functions to compute many other useful things, for example the maximal order in the quaternion algebra associated to a given vertex in the Bruhat–Tits graph. As written, the code of [FM14] relies on first enumerating the entire graph before performing any other computations (as the focus of Franc and Masdeu is computing small explicit examples) but in fact this is mainly for convenience and it is easy to extend their work to cryptographic sizes. We adapt their algorithm for computing the norm form of a quaternion order corresponding to a given vertex in the Bruhat–Tits quotient in Algorithm 2 so that it can be used for examples of cryptographic size.

For simplicity, we specialize Algorithm 2 as follows: we choose $p \equiv 3 \mod 4$, for the root vertex of the Bruhat–Tits tree $\mathcal{T}_\ell$ we use the supersingular elliptic curve $E : y^2 = x^3 - x$, with the maximal order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$ with $i^2 = -1$ and $j^2 = -p$ and which can be identified with endomorphisms of E as in Example 4.1.

In Section 5.4, we discuss a way of making use of Algorithm 2 for cryptanalysis of supersingular isogeny graph cryptosystems. For this, we also need to compute the elliptic curve corresponding to a vertex of the Bruhat–Tits tree, and the ℓ-power-isogeny to it corresponding to the path in the Bruhat–Tits tree, which we have described in Algorithm 1.

Algorithm 2 Computing norm equations for cryptographic sizes with $p \equiv 3 \pmod 4$

```
Require: A vertex $v \in M_2(\mathbb{Z}_\ell)$ in the Bruhat–Tits tree.
Ensure: The norm form of the maximal order corresponding to $v$, if the root of the tree corresponds to the
    maximal order $\mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$.

1. Define $\Phi_\ell : B_{p,\infty} \to M_2(\mathbb{Q}_\ell)$ to be an embedding for which $\Phi_\ell(\mathcal{O}_0) = M_2(\mathbb{Z}_\ell)$, and compute $\Phi_\ell(i)$, $\Phi_\ell(j)$,
    and $\Phi_\ell(k)$.
2. Label the initial vertex $v^{(0)} = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ with the order $\mathcal{O}_0$.
3. Apply the basis change $v$ to the basis of $v^{(0)}$ (as elements of $M_2(\mathbb{Z}_\ell)$). The new basis $\mathcal{B}$ is the basis of the
    maximal order of $v$.
4. Row reduce the basis $\mathcal{B}$ and deduce the basis $\widetilde{\mathcal{B}} = \{\beta_0, \beta_1, \beta_2, \beta_3\}$ in terms of $1, i, j, k$ (via $\Phi_\ell$).
5. Compute the reduced norm $N$ of an element $a\beta_0 + b\beta_1 + c\beta_2 + d\beta_3$, where $a, b, c, d \in \mathbb{Z}$ are variables.
    return $N$.
```

5.4 Computing and exploiting norm equations

In this section, we explore the feasibility of using the Bruhat–Tits description to deterministically find an elliptic curve whose endomorphism ring satisfies certain desirable properties. This study is motivated by the recent paper [KMPPS20], in which it is shown that, under certain plausible heuristics, there exist exponentially many supersingular elliptic curves over $\mathbb{F}_{p^2}$ which, if used as a starting curve for the SIDH protocol, can give an improvement over the generic meet-in-the-middle attack by exploiting the public torsion point images. For simplicity, let us consider an SIDH setup in which $p = 2^{e_A}3^{e_B} - 1$, and the starting curve $E_0/\mathbb{F}_p$ has j-invariant 1728, as in Section 5.1, and additionally suppose that $2^{e_A} \leq 3^{e_B}$. In this case, a curve $E/\mathbb{F}_{p^2}$ is defined to be *insecure* if there exist $\theta \in \operatorname{End}(E)$, $\tau \in \operatorname{End}(E_0)$, $n \in \mathbb{Z}$, and $\epsilon < 2^{e_A}$ such that

$$\operatorname{nrd}(\theta) = 2^{2e_A} \operatorname{nrd}(\tau) + n^2 = \epsilon 3^{2e_B}.$$

In particular, insecure curves are characterised by the existence of such an endomorphism θ, and by the intersection of their endomorphism rings with $\operatorname{End}(E_0)$. With this in mind, we give an example in which we can parametrize the norm form of this intersection for a certain path in the Bruhat–Tits tree, with a view to using this as a tool in future cryptanalysis.

Example 5.4 *Let $p = 2^{128}3^{81} - 1$, and let $\mathcal{O}_n$ be a maximal order obtained by taking $1 \leq n \leq 81$ steps on the 3-left-ideal graph in direction 2 from the starting point $\operatorname{End}(E_0) \cong \mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$. Then the norm form of the right-ideal linking $\mathcal{O}_0$ and $\mathcal{O}_n$ is*

$$\frac{1}{4}((3^n - 1)^2 p + (3^n + 1)^2)(a^2 + b^2) + \frac{3^{2n}}{4}(p + 1)(c^2 + d^2) + \frac{3^n}{2}((3^n - 1)p + 3^n + 1)(ac + bd).$$

This example was computed using the code available at `www.martindale.info/research/BT`.

In future work we hope to parameterize all the norm forms of intersections of maximal orders corresponding to the endpoints of a chain of n isogenies in the ℓ-isogeny graph for SIKE or SIDH[5]

[5] Although we will focus at first on the SIKE parameters, it could be that the most interesting case occurs for a different parameter set within the SIDH family of protocols.

in this way. The hope is that one can determine the properties needed by an endomorphism ring for a particular cryptanalytic tool, such as insecure curves in the sense of [KMPPS20]. One can then look at the parametrization to determine if such a quaternion order appears in the required neighbourhood of the graph, and if necessary traverse the Bruhat–Tits tree to compute a path to $j = 1728$ from the order in question. Traversing the Bruhat–Tits tree is very fast and simple, involving only multiplication of matrices in $M_2(\mathbb{Z}_\ell)$, and Algorithm 1 then translates this path to an isogeny.

A final note on the potential to use this in cryptanalysis: [KMPPS20, Proposition 23] shows that it would be possible to use a path from $j = 1728$ to an insecure curve to get an attack on a protocol starting from $j = 1728$, if there is an insecure curve sufficiently close to $j = 1728$. A classification of the kind described above should allow us to say exactly where the closest insecure curve is to be found on the Bruhat–Tits tree and consequently in the isogeny graph, giving a result on the (in)security of SIDH.

6 Conclusion

Supersingular isogeny graphs underlying SIDH and SIKE have been successfully studied using quaternion algebras: Deuring's correspondence translates questions about supersingular elliptic curves to questions about maximal orders. We propose that we take this one step further: study Bruhat–Tits trees.

The main advantage of looking at supersingular isogeny graphs as quotients of Bruhat–Tits trees is that every vertex and edge can be labelled by a simple two-by-two matrix, which allows for a simple manipulation, as well as giving directions in the isogeny graph (although these directions depend on the particular SIDH/SIKE instance).

Moreover, we defined the truncated Bruhat–Tits tree and argued how these trees give an approximation to the subgraph of $\mathcal{G}_\ell$ relevant for SIKE. The truncated Bruhat–Tits tree also captures the choice of torsion basis, which is a part of the protocol set up.

We believe that the directions of a path in the Bruhat–Tits tree can give insight into the arithmetic of the endomorphism rings of the elliptic curves along that path.

References

[ACLLNSS19] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. *Adventures in Supersingularland.* Cryptology ePrint Archive, Report 2019/1056. `https://eprint.iacr.org/2019/1056`. 2019.

[AM19] Laia Amorós and Piermarco Milione. "Mumford curves covering p-adic Shimura curves and their fundamental domains". In: *Trans. Amer. Math. Soc.* 371.2 (Jan. 2019), pp. 1119–1149.

[BC91] Jean-François Boutot and Henri Carayol. "Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld". In: *Astérisque* 196-197 (1991), pp. 45–158.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations". In: *Advances in Cryptology – ASIACRYPT 2019.* Vol. 11921. Lecture Notes in Comp. Sci. Springer, 2019, pp. 227–247.

[Bra43] Heinrich Brandt. "Zur Zahlentheorie der Quaternionen". In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 53 (1943), pp. 23–57.

[BTQuotient] *BTQuotient Module.* `https://doc.sagemath.org/html/en/reference/modsym/sage/modular/btquotients/btquotient.html`.

[CD20] Wouter Castryck and Thomas Decru. "CSIDH on the Surface". In: *Post-Quantum Cryptography. PQCrypto 2020.* Vol. 12100. Lecture Notes in Comp. Sci. Springer, Cham, 2020.

[Cer76] Ivan V. Cerednik. "Uniformization of algebraic curves by discrete aithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotients". In: *Math. USSR Sbornik* 29.1 (1976), pp. 55–78.

[CFLMP18] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas. "Ramanujan graphs in cryptography". In: *Research Directions in Number Theory.* Vol. 19. Association for Women in Mathematics Series. Springer, 2018, pp. 1–40.

[CGL06] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. *Cryptographic hash functions from expander graphs.* IACR CryptologyePrint Archive 2006/021. `https://eprint.iacr.org/2006/021`. 2006.

[CGL09a] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. "Cryptographic hash functions from expander graphs". In: *J. Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790. DOI: `10.1007/s00145-007-9002-x`. URL: `https://eprint.iacr.org/2006/021`.

[CGL09b] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. "Families of Ramanujan graphs and quaternion algebras". In: *Groups and symmetries.* Vol. 47. CRM Proc. Lecture Notes. Amer. Math. Soc., Providence, RI, 2009, pp. 53–80.

[CLMPR18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *ASIACRYPT (3).* Vol. 11274. Lecture Notes in Comp. Sci. Springer, 2018, pp. 395–427. URL: `https://eprint.iacr.org/2018/383`.

[Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces.* IACR Cryptology ePrint Archive 2006/291. `https://ia.cr/2006/291`. 2006.

[DeFeo18] Luca De Feo. "Exploring Isogeny Graphs". Habilitation. Universite de Versailles Saint-Quentin-en-Yvelines, 2018.

[Deu41] Max Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." In: *Abh. Math. Sem. Hansischen Univ.* 14 (1941), pp. 197272.

[DKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. "Towards Practical Key Exchange from Ordinary Isogeny Graphs". In: *Advances in Cryptology–ASIACRYPT 2018. Part III.* Lecture Notes in Comp. Sci. Springer, 2018, pp. 365–394.

[Dri76] Vladimir G. Drinfel'd. "Coverings of p-adic symmetric regions". In: *Functional Analysis and Its Applications* 10.2 (1976), pp. 107–115.

[EHLMP18] Kirsten Eisentraeger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. "Supersingular isogeny graphs and endomorphism rings: reductions and solutions". In: *Advances in Cryptology–EUROCRYPT 2018.* Vol. 10822. Lecture Notes in Comp. Sci. Springer, 2018, pp. 329–368.

[FM14] Cameron Franc and Marc Masdeu. "Computing fundamental domains for the Bruhat-Tits tree for $\mathrm{GL}_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves". In: *LMS Journal of Computation and Mathematics* 17.01 (2014), pp. 1–23.

[FM14code] Cameron Franc and Marc Masdeu. *BTQuotient package.* `https://github.com/mmasdeu/btquotients`. accessed 09/03/2020.

[JF11] David Jao and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Post-quantum cryptography.* Vol. 7071. Lecture Notes in Comput. Sci. Springer, Heidelberg, 2011, pp. 19–34. DOI: `10.1007/978-3-642-25405-5_2`.

[JL84] Bruce W. Jordan and Ron Livné. "Local diophantine properties of Shimura curves". In: *Math. Ann.* 270.2 (1984), pp. 235–248.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion ℓ-isogeny path problem". In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 418–432. ISSN: 1461-1570. DOI: `10.1112/S1461157014000151`. URL: `https://doi.org/10.1112/S1461157014000151`.

[KMPPS20] Péter Kutas, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. *Weak instances of SIDH variants under improved torsion-point attacks.* Cryptology ePrint Archive, Report 2020/633. `https://eprint.iacr.org/2020/633`. 2020.

[Koh96] David Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkely, 1996.

[Kur79] Akira Kurihara. "On some examples of equations defining Shimura curves and the Mumford uniformization". In: *J. Fac. Sci. Univ. Tokyo, Sect. IA Math* 25.3 (1979), pp. 277–300.

[Mil15] Piermarco Milione. "Shimura curves and their p-adic uniformizations". PhD thesis. Universitat de Barcelona, 2015.

[Mor81] Yasuo Morita. "Reduction mod $\mathfrak{p}$ of Shimura curves". In: *Hokkaido Math. J.* 10.2 (1981), pp. 209–238.

[NIST] *National Institute of Standards and Technology. Post-quantum cryptography standardization, Dec. 2016.* `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

[OAT20] Hiroshi Onuki, Yusuke Aikawa, and Tsuyoshi Takagi. *The Existence of Cycles in the Supersingular Isogeny Graphs Used in SIKE.* Cryptology ePrint Archive, Report 2020/439. `https://eprint.iacr.org/2020/439`. 2020.

[Pet17] Christophe Petit. "Faster Algorithms for Isogeny Problems Using Torsion Point Images". In: *Advances in cryptology—ASIACRYPT 2017. Part II.* Vol. 10625. Lecture Notes in Comp. Sci. Springer, Cham, 2017, pp. 330–353.

[Piz80] Arnold Pizer. "An Algorithm for Computing Modular Forms on $\Gamma_0(N)$". In: *Journal of Algebra* Vol. 64, Issue 2 (June 1980).

[Piz90] Arnold Pizer. "Ramanujan graphs and Hecke operators". In: *Bull. Amer. Math. Soc. (N.S.)* 23.1 (1990), pp. 127–137. ISSN: 0273-0979.

[Rib90] Kenneth A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms". In: *Invent. Math.* 100 (1990), pp. 431–476.

[RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-key cryptosystem based on isogenies.* IACR Cryptology ePrint Archive 2006/145. `https://ia.cr/2006/145`. 2006.

[Ser77] Jean-Pierre Serre. *Arbres, amalgames,* SL_2. Cours au Collège de France, rédigé avec la collaboration de Hyman Bass. Vol. 46. Astérisque. Société Mathèmatique de France, 1977.

[Shi67] Goro Shimura. “Construction of Class Fields and Zeta Functions of Algebraic Curves”. In: *Annals of Mathematics* 85.1 (1967), pp. 58–159.

[SIKE] Reza Azarderakhsh, Brian Koziel, Matt Campagna, Brian LaMacchia, Craig Costello, Patrick Longa, Luca De Feo, Michael Naehrig, Basil Hess, Joost Renes, Amir Jalali, Vladimir Soukharev, David Jao, and David Urbanik. *Supersingular Isogeny Key Encapsulation.* Nov. 30, 2017. URL: `http://sike.org`.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition.* Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[Vél71] Jacques Vélu. “Isogénies entre courbes elliptiques”. In: *Comptes Rendus de l’Académiedes Sciences de Paris* 273 (1971), pp. 238–241.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions.* Vol. 800. Lecture Notes in Mathematics. Springer, 1980.

[Voi] John Voight. “Quaternion Algebras”. v.0.9.22, July 7, 2020, `https://math.dartmouth.edu/~jvoight/quat.html`.