Number of Rational Points of Shimura Curves over Finite Fields

Virgile Ducet

March 12, 2014

Abstract

We use a trace formula for Hecke operators to study the number of rational points of Shimura curves over finite fields, and recover a result of Ihara that sequences of such curves with asymptotically growing genus are optimal over a quadratic extension of the base field, and that the main contribution in rational points is provided by supersingular points. Generalizing a result of Elkies, we furthermore prove that Shimura curves naturally form recursive towers, and exhibit such a tower computed by John Voight.

Introduction

The introduction by Goppa [Gop77] of a geometric class of error-correcting codes became a motivation for a deeper study of the number of rational points of varieties over finite fields, especially curves. Indeed these codes, now known as *Goppa codes*, rely essentially on the structure of curves over finite fields as follows. Let C be a curve defined over $\mathbb{F}_q$. Let $D_1 = P_1 + \cdots + P_n$ and D_2 be two divisors over C with disjoint support such that the points P_i are rational and $2g(C) - 2 < \deg(D_2) < n$. Let $\Omega_C(D_1 - D_2)$ be the space of differentials ω on C such that $\mathrm{div}(\omega) \geq D_2 - D_1$ and let $\mathrm{res}_{P_i}(\omega)$ be the residue of ω at P_i. The Goppa code associated to this data is the image of the $\mathbb{F}_q$-linear map $\Omega_C(D_1 - D_2) \to \mathbb{F}_q^n$ defined by

$$\omega \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)).$$

For these codes, the Riemann-Roch theorem shows that the dimension k of the code satisfies the relation

$$k = g - 1 + n - \deg(D_2),$$

and if d is the minimal distance of the code we have the inequality

$$\frac{k}{n} + \frac{d}{n} \geq 1 + \frac{1}{n} - \frac{g}{n}. \tag{1}$$

By construction, n is bounded by the number of rational points $N(C)$ of C, and from (1), for given n and k, the smaller the genus, the more efficient the code. So one would like to find, for every n, the smallest genus g such that there exists a curve $C/\mathbb{F}_q$ with at least n rational points.

This problem served as a motivation for Serre in the beginning of the 1980s to look for a more precise estimate of the possible values of $N(C)$, in particular of the maximum number of rational points $N_q(g)$ among curves of genus g defined over $\mathbb{F}_q$ (see Serre [Ser83b], [Ser83a]). Serre looked at this question for fixed genus as well as when the genus of the curve increases to infinity. In the latter context the natural object to study is the Ihara constant

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

To have an estimate of the sharpness of the upper bounds, one needs curves with the maximal possible number of rational points, in order to have a lower bound on $N_q(g)$. And for concrete applications, for instance to coding theory, one needs the equations of these curves. When the genus grows asymptotically, techniques from class field theory still prove to be efficient, but in many cases one can obtain an exact estimation of the Ihara constant by geometric methods. Indeed, when the order of the finite field is a square, Ihara [Iha81] in the general case, and Tsfasman, Vlăduţ and Zink [TVZ82] in the cases $q = p^2$ or $q = p^4$ for a prime p, independently constructed sequences of elliptic modular curves and Shimura curves which are asymptotically *optimal*, that is, which reach $A(q) = \sqrt{q}-1$. Furthermore, asymptotically and relative to their genus, all rational points are supersingular points. We will study the asymptotic behavior of a particular class of Shimura curves, denoted $X_0^+(\mathfrak{N})$, which arise in the context of Shimura varieties as formulated by Deligne [Del71]. After two sections on preliminary background about Shimura curves and quaternionic modular forms respectively, and using different methods than the works quoted above, we study in section 3 a trace formula for the action of Hecke operators on spaces of quaternionic modular forms. Together with an explicit formula for the genus, we are able to prove the optimality of the $X_0^+(\mathfrak{N})$ in some cases. Moreover, we study separately their supersingular points in section 4 using results of Carayol [Car86], and show that relative to the genus of the curve, these points provide asymptotically all the rational points. We conclude our study by showing in the last section, after Elkies [Elk98a], that the curves $X_0^+(\mathfrak{N})$ naturally form (asymptotically optimal) recursive towers. The potential effectiveness of this approach is confirmed by an explicit equation determined by John Voight.

Acknowledgements

I am extremely grateful to John Voight and Jeroen Sijsling, who both took a lot of time to discuss technical questions with me. John Voight also computed an explicit example of recursive tower for me, I would like to warmly thank him for this.

1 Shimura curves

Let F be a totally real number field of degree d and absolute discriminant d_F, and let $\mathbb{Z}_F$ be its ring of integers. Let $\iota_1, \ldots, \iota_d$ be the real embeddings of F. We consider a quaternion algebra B over F unramified at ι_1 and ramified at the other real places.

Let $\mathfrak{N}$ be a nonzero integral ideal of $\mathbb{Z}_F$ prime to the discriminant $\mathfrak{D}$ of B, and let $\mathcal{O}_0(\mathfrak{N})$ be an Eichler order of level $\mathfrak{N}$. Consider the group

$$\mathcal{O}_0^1(\mathfrak{N}) = \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\},$$

where nrd is the reduced norm in B. The image group

$$\Gamma_0^1(\mathfrak{N}) = \iota_1(\mathcal{O}_0^1(\mathfrak{N})) \subset \mathrm{GL}_2^+(\mathbb{R})$$

is an arithmetic Fuchsian group. The quotient

$$Y_0^1(\mathfrak{N}) = \Gamma_0^1(\mathfrak{N})\backslash\mathcal{H}$$

can be given the structure of a Riemann surface which depends only on ι_1 and $\mathcal{O}_0(\mathfrak{N})$, up to isomorphism. Hence $Y_0^1(\mathfrak{N})$ is an irreducible and non-singular complex algebraic curve, whose projective closure is denoted $X_0^1(\mathfrak{N})$.

We now define Shimura curves from an adelic perspective, as it is more adapted to the local-global principle appearing in the study of quaternion algebras. So let $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ be the restricted product of all the p-adic integer rings, and let $\hat{B} = B \otimes \hat{Z}$. Let $\mathcal{H}^{\pm} = \mathbb{C} \setminus \mathbb{R}$ be the union of the upper and lower half planes. We define a left action of $B^\times$ on $\mathcal{H}^{\pm} \times \hat{B}^\times$ by

$$b(\tau, \hat{b}) = (b\tau, b\hat{b}),$$

where b acts on τ as the fractional linear transformation associated to $\iota_1(b)$.

From now on we set $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$ and let $\hat{\mathcal{O}} = \mathcal{O} \otimes \hat{\mathbb{Z}}$. The group $\hat{\mathcal{O}}^\times$ is compact open and acts on $\mathcal{H}^{\pm} \times \hat{B}^\times$ on the right by

$$(\tau, \hat{b})k = (\tau, \hat{b}k).$$

Consider the quotient space

$$Y(\hat{\mathcal{O}}^\times) = B^\times\backslash(\mathcal{H}^{\pm} \times \hat{B}^\times)/\hat{\mathcal{O}}^\times.$$

One can give $Y(\hat{\mathcal{O}}^\times)$ the structure of a Riemann surface as follows. Let $\hat{b} \in \hat{B}^\times$ be the representative of a class $[\hat{b}]$ in $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times) = B^+\backslash\hat{B}^\times/\hat{\mathcal{O}}^\times$, and set

$$\Gamma_{\hat{b}} = \iota_1(\hat{b}\hat{\mathcal{O}}^\times\hat{b}^{-1} \cap B^+) \subset \mathrm{GL}_2^+(\mathbb{R}),$$

where $\mathrm{GL}_2^+(\mathbb{R})$ is the subgroup of matrices in $\mathrm{GL}_2(\mathbb{R})$ with positive determinant. Let $Y(\Gamma_{\hat{b}}) = \Gamma_{\hat{b}}\backslash\mathcal{H}$. By Milne [Mil05, Lem. 5.13], the maps

$$\begin{array}{ccc} Y(\hat{\mathcal{O}}^\times) & \to & Y(\Gamma_{\hat{b}}) \\ [\tau, \hat{b}] & \mapsto & [\tau] \end{array},$$

for $[\hat{b}] \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$, induce a homeomorphism

$$Y(\hat{\mathcal{O}}^\times) \cong \bigsqcup_{[\hat{b}] \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)} Y(\Gamma_{\hat{b}}). \tag{2}$$

Every $\Gamma_{\hat{b}}$ is an arithmetic Fuchsian group [Shi71, Prop. 9.5], and thus each $Y(\Gamma_{\hat{b}})$ can be given the structure of a connected Riemann surface, hence an irreducible and non-singular complex algebraic curve, which is projective when $Y(\Gamma_{\hat{b}})$ is compact. Therefore (2) provides a natural way to put on $Y(\hat{\mathcal{O}}^\times)$ the structure of a (possibly disconnected) Riemann surface and also of a nonsingular complex algebraic curve. We call $Y(\hat{\mathcal{O}}^\times)$ an (adelic) *Shimura curve*. Note that by the strong approximation theorem, the reduced norm

map implies that $Y(\hat{\mathcal{O}}^\times)$ is naturally a disjoint union of curves indexed by the narrow class group $\mathrm{Cl}_\infty(F)$ of F, since it provides a bijection of finite sets

$$\mathrm{nrd} : \mathrm{Pic}_r^+(\mathcal{O}) \xrightarrow{\sim} \mathrm{Cl}_\infty(F) \tag{3}$$

(see Vignéras [Vig80, p. 89]). Let $X(\hat{\mathcal{O}}^\times)$ be the projective closure of $Y(\hat{\mathcal{O}}^\times)$. By Milne [Mil05, Theo. 3.3], we have $X_0^1(\mathfrak{N}) = Y_0^1(\mathfrak{N})$ and $X(\hat{\mathcal{O}}^\times) = Y(\hat{\mathcal{O}}^\times)$ if and only if B is a division algebra, that is if and only if $B \neq \mathrm{M}_2(\mathbb{Q})$.

The group $\mathrm{nrd}(\hat{\mathcal{O}}^\times)$ is open in $\hat{F}^\times$, so by the Existence Theorem of class field theory, $\mathrm{Pic}_r^+(\mathcal{O})$ is isomorphic to the Galois group of an abelian extension of F, which is the narrow Hilbert class field F_∞ of F. Actually, by the theory of Shimura and Deligne (see [Shi67], [Del71], [Car86] or [Mil05]), the complex curve $Y(\hat{\mathcal{O}}^\times)$ admits a model $\mathrm{Sh}(\hat{\mathcal{O}}^\times)$ over F, and every connected component admits a model over F_∞. Let B^+ be the set of elements of B with totally positive reduced norm[1], and let

$$\mathcal{O}^+ = \mathcal{O}^\times \cap B^+$$

be the set of units x of $\mathcal{O}$ with totally positive reduced norm. We let $1_{\hat{B}^\times}$ represent the trivial class in $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$, so

$$\Gamma_{1_{\hat{B}^\times}} = \hat{\mathcal{O}}^\times \cap B^+ = \mathcal{O}^+.$$

We write

$$\Gamma_0^+(\mathfrak{N}) = \iota_1(\mathcal{O}^+)$$

and

$$Y_0^+(\mathfrak{N}) = \Gamma_0^+(\mathfrak{N})\backslash\mathcal{H},$$

and let $X_0^+(\mathfrak{N})$ denote the projective closure of $Y_0^+(\mathfrak{N})$. Let $\mathrm{Sh}_0^+(\mathfrak{N})$ be the model of $Y_0^+(\mathfrak{N})$ over F_∞. The action of $\mathrm{Gal}(F_\infty/F) = \mathrm{Cl}_\infty(F)$ on the set of connected components of $\mathrm{Sh}(\hat{\mathcal{O}}^\times)$ is transitive [Sij10, Theo. 3.1.3], so we have the following isomorphism of curves over F_∞:

$$\mathrm{Sh}(\hat{\mathcal{O}}^\times) \times_F F_\infty \cong \bigsqcup_{\sigma \in \mathrm{Gal}(F_\infty/F)} \mathrm{Sh}_0^+(\mathfrak{N})^\sigma. \tag{4}$$

The model $\mathrm{Sh}(\hat{\mathcal{O}}^\times)$ is connected over F, however it is not geometrically connected in general as this last isomorphism shows.

Let $\mathbb{Z}_{F,+}$ be the subset of totally positive elements of $\mathbb{Z}_F$. As in Vignéras [Vig80, Prop. III.5.8], the reduced norm induces a surjective map $\mathcal{O}^+ \twoheadrightarrow \mathbb{Z}_{F,+}^\times$, hence a surjective map $\mathcal{O}^+/\mathbb{Z}_F^\times \twoheadrightarrow \mathbb{Z}_{F,+}^\times/{\mathbb{Z}_F^\times}^2$, with kernel $\mathcal{O}^1/(\mathcal{O}^1 \cap \mathbb{Z}_F^\times)$. By class field theory, we have an isomorphism

$$\mathbb{Z}_{F,+}^\times/{\mathbb{Z}_F^\times}^2 \cong \mathrm{Cl}_\infty(F)/\mathrm{Cl}(F),$$

so we see that $Y_0^1(\mathfrak{N})$ is a covering of $Y_0^+(\mathfrak{N})$ of degree h_∞/h, where h and h_∞ are the class number and narrow class number of F respectively. When $h_\infty = h = 1$, we have isomorphisms

$$Y(\hat{\mathcal{O}}^\times) \xrightarrow{\cong} Y_0^+(\mathfrak{N}) \xrightarrow{\cong} Y_0^1(\mathfrak{N}).$$

[1]Note that this is equivalent to $\iota_1(\mathrm{nrd}(x)) > 0$, because by the Eichler norm theorem (see Vignéras [Vig80, Théo. III.4.1]) the reduced norm of any element of $B^\times$ is already positive at any infinite place other than ι_1.

When $h_\infty > 1$, the curve $Y(\hat{\mathcal{O}}^\times)$ is no longer connected, so we cannot expect to obtain such an identification anymore. However, by Shimura's theory [Shi67], $Y_0^1(\mathfrak{N})$ admits a model $\mathrm{Sh}_0^1(\mathfrak{N})$ over F_∞, and $F_\infty = F$ when $h_\infty = 1$. But it should be emphasized that the natural way to do arithmetic with Shimura curves, as will become apparent in the next sections, is with the curve $Y(\hat{\mathcal{O}}^\times)$, for which $Y_0^+(\mathfrak{N})$ inherits many interesting properties as a connected component. The arithmetic theory developped in the next sections works nicely for the curve $Y_0^1(\mathfrak{N})$ only when $h_\infty = h$, in which case $Y_0^1(\mathfrak{N}) \cong Y_0^+(\mathfrak{N})$. Therefore, at least concerning the arithmetic theory, the natural analogues of the modular curves $X_0(N)$ are not the curves $X_0^1(\mathfrak{N})$, but the curves $X_0^+(\mathfrak{N})$ which are the compactifications of the curves $Y_0^+(\mathfrak{N})$.

2 Modular forms and Hecke operators

We now define quaternionic modular forms. For a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$$

and an element $\tau \in \mathcal{H}$, we set

$$j(\gamma, \tau) = c\tau + d.$$

Let Γ be a subgroup of $\iota_1(B^+) \subset \mathrm{GL}_2^+(\mathbb{R})$ with discrete image, and assume that the quotient $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ is compact (equivalently, $B \neq \mathrm{M}_2(\mathbb{Q})$), so $X(\Gamma) = Y(\Gamma)$. To avoid cusps and growth conditions in the definition of modular forms, we will restrict our attention to compact Shimura curves, whence the assumption on Γ (see for instance Shimura [Shi71] for an account of the theory in the elliptic modular case).

Definition. A function $f : \mathcal{H} \to \mathbb{C}$ is called a *quaternionic modular form of weight* 2 for Γ if it is holomorphic and satisfies

$$f(\gamma\tau) = \frac{j(\gamma, \tau)^2}{\det(\gamma)} f(\tau)$$

for every $\gamma \in \Gamma$ and $\tau \in \mathcal{H}$. When Γ is $\Gamma_0^1(\mathfrak{N})$ or $\Gamma_0^+(\mathfrak{N})$, we say that f has *level* $\mathfrak{N}$.

Because $Y(\Gamma)$ is compact, there are no cusps and a quaternionic modular form is thus trivially a *cusp form*. The set of cusp forms of weight 2 for Γ will be denoted $S_2(\Gamma)$. For brevity we write $S_2^+(\mathfrak{N}) = S_2(\Gamma_0^+(\mathfrak{N}))$ and $S_2^1(\mathfrak{N}) = S_2(\Gamma_0^1(\mathfrak{N}))$.

There is an isomorphism of complex vector spaces between $S_2(\Gamma)$ and the set of holomorphic differential 1-forms on the Shimura curve $Y(\Gamma)$, given by

$$\begin{array}{ccc} S_2(\Gamma) & \xrightarrow{\cong} & H^0(Y(\Gamma), \Omega^1) \\ f & \longmapsto & f(\tau)d\tau \end{array} . \tag{5}$$

Definition. Let $\hat{f} : \mathcal{H}^\pm \times \hat{B}^\times \to \mathbb{C}$ be a function that is holomorphic in the first variable and locally constant in the second variable, and let $\hat{\mathcal{O}}^\times$ be a compact open subgroup of $\hat{B}^\times$. The function $\hat{f}$ is an *adelic quaternionic cusp form of weight* 2 *and level* $\mathfrak{N}$ if it verifies

$$\hat{f}(b(\tau, \hat{b})k) = \frac{j(b, \tau)^2}{\det(b)} \hat{f}(\tau, \hat{b})$$

for all $b \in B^\times$, $(\tau, \hat{b}) \in \mathcal{H}^\pm \times \hat{B}^\times$ and $k \in \hat{\mathcal{O}}^\times$, where we consider b as embedded in $\mathrm{GL}_2(\mathbb{R})$ by ι_1. We denote the space of adelic quaternionic cusp forms of weight 2 and level $\mathfrak{N}$ by $\hat{S}_2(\mathfrak{N})$.

As in the previous paragraph, the adelic quaternionic cusp forms decompose as a direct sum of quaternionic cusp forms indexed by $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$ (and thus also $\mathrm{Cl}_\infty(F)$). More precisely, we have an isomorphism of $\mathbb{C}$-vector spaces

$$\hat{S}_2(\mathfrak{N}) = \bigoplus_{[\hat{b}]\in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)} S_2(\Gamma_{\hat{b}}) \tag{6}$$

given by $\hat{f} \mapsto (f_{\hat{b}})_{\hat{b}}$, where $\Gamma_{\hat{b}} = \hat{b}\Gamma\hat{b}^{-1}$ and $f_{\hat{b}} : \mathcal{H} \to \mathbb{C}$ is the function defined by

$$f_{\hat{b}}(\tau) = \hat{f}(\tau, \hat{b})$$

(see Sijsling [Sij10, Prop. 4.1.3]). In the case where $h_\infty = 1$, we thus have an isomorphism

$$\hat{S}_2(\mathfrak{N}) \cong S_2^+(\mathfrak{N}) \cong S_2^1(\mathfrak{N}).$$

Combining with (2) and (5), we obtain isomorphisms

$$\begin{array}{ccccc} \hat{S}_2(\mathfrak{N}) & \xrightarrow{\cong} & H^0(X(\hat{\mathcal{O}}^\times), \Omega^1) & \xrightarrow{\cong} & \displaystyle\bigoplus_{[\hat{b}]\in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)} H^0(X(\Gamma_{\hat{b}}), \Omega^1) \\ \hat{f} & \longmapsto & \hat{f}(\tau, \hat{b})d\tau & \longmapsto & (f_{\hat{b}}(\tau)d\tau)_{[\hat{b}]} \end{array} \tag{7}$$

(we have used the fact that the cohomology of a disjoint union of curves is the direct sum of the cohomologies of the curves).

2.1 Hecke operators

Our goal here, by analogy with the case $B = \mathrm{M}_2(\mathbb{Q})$, is to define Hecke operators before studying their arithmetic properties in the next sections. We begin by defining Hecke operators in the classical setting, then we extend this definition to the adelic setting.

For every α in $\mathrm{GL}_2^+(\mathbb{R})$ such that $\alpha^{-1}\Gamma\alpha$ is commensurable with Γ, there exists a positive integer d_α such that we have a finite decomposition (see Miyake [Miy06, Lem. 2.7.1])

$$\Gamma\alpha\Gamma = \bigsqcup_{\ell=1}^{d_\alpha} \alpha_\ell\Gamma,$$

with $\alpha_\ell \in \mathrm{GL}_2^+(\mathbb{R})$, and an action on the left $[\Gamma\alpha\Gamma] : S_2(\Gamma) \to S_2(\Gamma)$ defined by

$$([\Gamma\alpha\Gamma] \cdot f)(\tau) = \sum_{\ell=1}^{d_\alpha} \frac{\det(\alpha_\ell^{-1})}{j(\alpha_\ell^{-1}, \tau)^2} f(\alpha_\ell^{-1}\tau).$$

The integer d_α is called the *degree* of the operator $[\Gamma\alpha\Gamma]$. These definitions extend linearly to finite unions of double cosets $\Gamma\alpha\Gamma$.

Remark 2.1. Since Γ acts on $\mathcal{H}$ on the left, it would be more natural to decompose $\Gamma\alpha\Gamma$ as a disjoint union $\bigsqcup_{\ell=1}^{d_\alpha} \Gamma\alpha'_\ell$, and consider the operator $[\Gamma\alpha\Gamma]^\vee$ defined by

$$([\Gamma\alpha\Gamma]^\vee \cdot f)(\tau) = \sum_{\ell=1}^{d_\alpha} \frac{\det(\alpha'_\ell)}{j(\alpha'_\ell, \tau)^2} f(\alpha'_\ell\tau).$$

However it turns out that it is the operator $[\Gamma\alpha\Gamma]$ that one needs to consider in order to get a satisfying theory in the context of Shimura curves. Both $[\Gamma\alpha\Gamma]$ and $[\Gamma\alpha\Gamma]^\vee$ are related in a nice geometric way (see (13)).

One can generalize the above constructions to the adelic setting. Let $\hat{\alpha} \in \hat{B}^\times$. Because $\hat{\mathcal{O}}^\times$ is compact open, $\hat{\alpha}^{-1}\hat{\mathcal{O}}^\times\hat{\alpha}$ is commensurable with $\hat{\mathcal{O}}^\times$, hence we have a finite decomposition

$$\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times = \bigsqcup_{\ell=1}^{d_{\hat{\alpha}}} \hat{\alpha}_\ell\hat{\mathcal{O}}^\times$$

(notice that we consider decompositions in right cosets because $\hat{\mathcal{O}}^\times$ acts on the right of $\mathcal{H}^\pm \times \hat{B}^\times$). We define an operator $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ on $\hat{S}_2(\mathfrak{N})$ by

$$([\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot\hat{f})(\tau,\hat{b}) = \sum_{\ell=1}^{d_{\hat{\alpha}}} \hat{f}(\tau,\hat{b}\hat{\alpha}_\ell),$$

and define the *degree* of $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ by $d_{\hat{\alpha}}$. To see how this operator is related to the connected components of $X(\hat{\mathcal{O}}^\times)$, choose a set $(r_i)_i$ of representatives of $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$. For every i there exist elements $b_\ell \in B^+$ and $k_\ell \in \hat{\mathcal{O}}^\times$ such that

$$r_i\hat{\alpha}_\ell = b_\ell r_j k_\ell \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times). \tag{8}$$

Note that the integer j does not depend on ℓ, because for two indexes ℓ and ℓ', there exists $k \in \hat{\mathcal{O}}^\times$ such that $\hat{\alpha}_{\ell'} = \hat{\alpha}_\ell k$, so $[r_i\hat{\alpha}_{\ell'}]$ and $[r_i\hat{\alpha}_\ell]$ have the same class $[r_j]$ in $\mathrm{Pic}^+(\hat{\mathcal{O}}^\times)$. To simplify notation, if $\hat{f}$ belongs to $\hat{S}_2(\mathfrak{N})$ we write $\Gamma_i = \Gamma_{r_i}$ and $\hat{f}_i = \hat{f}_{r_i}$ in (2) and (6) respectively. We thus have:

$$\begin{aligned}
([\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot\hat{f})_i(\tau) &= ([\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot\hat{f})(\tau,r_i) \\
&= \sum_\ell \hat{f}(\tau, r_i\hat{\alpha}_\ell) \\
&= \sum_\ell \hat{f}(b_\ell(b_\ell^{-1}\tau, r_j k_\ell)) \\
&= \sum_\ell \frac{j(b_\ell, b_\ell^{-1}\tau)^2}{\det(b_\ell)}\hat{f}(b_\ell^{-1}\tau, r_j k_\ell) \quad \text{by the transformation properties of } \hat{f} \\
&= \sum_\ell \frac{\det(b_\ell^{-1})}{j(b_\ell^{-1},\tau)^2} f_j(b_\ell^{-1}\tau) \qquad \text{by (6).}
\end{aligned} \tag{9}$$

Therefore the action of $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ on $\hat{S}_2(\mathfrak{N})$ permutes the components $S_2(\Gamma_i)$, by sending a modular form for Γ_i to a modular form for Γ_j, where j is such that $[r_j] = [r_i][\hat{\alpha}]$ in $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$. So we see that $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ induces an operator $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]_i$ on each $S_2(\Gamma_i)$ if and only if $[\hat{\alpha}] = 0$. In this case we obtain

$$[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]_i\cdot\hat{f} = [\Gamma_i\gamma\Gamma_i]\cdot\hat{f}_i, \tag{10}$$

where $\gamma \in B^+$ satisfies $\Gamma_i\gamma\Gamma_i = \bigsqcup_\ell b_\ell\Gamma_i$.

Let $\mathfrak{n}$ be an integral ideal of $\mathbb{Z}_F$ prime to $\mathfrak{D}$. Consider the set of quaternionic matrices of determinant generating $\hat{\mathfrak{n}}$:

$$\hat{\Theta}(\mathfrak{n}) = \{\hat{\alpha} \in \hat{\mathcal{O}} : \mathrm{nrd}(\hat{\alpha})\hat{\mathbb{Z}}_F = \hat{\mathfrak{n}}\}.$$

We denote the completion at a prime $\mathfrak{p}$ by adding a subscript $\mathfrak{p}$. For every $\mathfrak{p} \nmid \mathfrak{D}$ we fix a splitting $B_\mathfrak{p} \cong \mathrm{M}_2(F_\mathfrak{p})$. As in Miyake [Miy06, Lem. 4.5.2], we have

$$\hat{\Theta}(\mathfrak{n}) = \bigsqcup_{\substack{\mathfrak{l}|\mathfrak{m},\ (\mathfrak{l},\mathfrak{N})=1 \\ \mathfrak{lm}=\mathfrak{n}}} \hat{\mathcal{O}}^\times\hat{\alpha}_{\mathfrak{m},\mathfrak{l}}\hat{\mathcal{O}}^\times,$$

where for two integral ideals $\mathfrak{l} = \prod \mathfrak{p}^{\ell_\mathfrak{p}}$ and $\mathfrak{m} = \prod \mathfrak{p}^{m_\mathfrak{p}}$ we define $\hat{\alpha}_{\mathfrak{m},\mathfrak{l}}$ to be the idele whose $\mathfrak{p}$-component is 1 if $\mathfrak{p} \mid \mathfrak{D}$, and

$$(\hat{\alpha}_{\mathfrak{m},\mathfrak{l}})_\mathfrak{p} = \begin{pmatrix} \pi_\mathfrak{p}^{m_\mathfrak{p}} & 0 \\ 0 & \pi_\mathfrak{p}^{\ell_\mathfrak{p}} \end{pmatrix} \in B_\mathfrak{p} \cong \mathrm{M}_2(F_\mathfrak{p})$$

otherwise. Let

$$\hat{\mathrm{T}}(\mathfrak{m},\mathfrak{l}) = [\hat{\mathcal{O}}^\times \hat{\alpha}_{\mathfrak{m},\mathfrak{l}} \hat{\mathcal{O}}^\times],$$

and define the *Hecke operator* $\hat{\mathrm{T}}(\mathfrak{n})$ by the formula

$$\hat{\mathrm{T}}(\mathfrak{n}) = \sum_{\substack{\mathfrak{l}\mid\mathfrak{m},\ (\mathfrak{l},\mathfrak{N})=1 \\ \mathfrak{l}\mathfrak{m}=\mathfrak{n}}} \mathrm{T}(\mathfrak{m},\mathfrak{l}).$$

In particular, if $\mathfrak{n} = \mathfrak{p}$ is prime, we have $\hat{\mathrm{T}}(\mathfrak{p}) = \hat{\mathrm{T}}(\mathfrak{p},1)$.

Let $\mathrm{M}_2(\hat{\mathbb{Z}}_F) \cap \hat{B}$ be the set of matrices $\gamma \in \mathrm{M}_2(\hat{\mathbb{Z}}_F)$ such that $\gamma_\mathfrak{p} = \hat{b}_\mathfrak{p} \in B_\mathfrak{p}$ at any prime $\mathfrak{p} \mid \mathfrak{D}$. Then equivalently, one has $\hat{\Theta}(\mathfrak{n}) = \bigsqcup_{\hat{\alpha}\in\hat{\Delta}_0(\mathfrak{n})} \hat{\mathcal{O}}^\times \hat{\alpha} \hat{\mathcal{O}}^\times$, where

$$\hat{\Delta}_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\hat{\mathbb{Z}}_F) \cap \hat{B} : (d,\mathfrak{N}) = 1,\ c \in \hat{\mathfrak{N}},\ (ad-bc)\hat{\mathbb{Z}}_F = \hat{\mathfrak{n}} \right\}.$$

This gives rise to a decomposition

$$\bigsqcup_{\hat{\alpha}\in\hat{\Delta}_0(\mathfrak{n})} \hat{\mathcal{O}}^\times \hat{\alpha} \hat{\mathcal{O}}^\times = \bigsqcup_{\hat{\beta}\in\hat{\Delta}'_0(\mathfrak{n})} \hat{\beta} \hat{\mathcal{O}}^\times,$$

where $\hat{\Delta}'_0(\mathfrak{n})$ is the finite set

$$\hat{\Delta}'_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{M}_2(\hat{\mathbb{Z}}_F) \cap \hat{B} : (d,\mathfrak{N}) = 1, (ad-bc)\hat{\mathbb{Z}}_F = \hat{\mathfrak{n}}, b \in \hat{\mathbb{Z}}_F / d\hat{\mathbb{Z}}_F \right\}$$

(see Zhang [Zha01, § 3] or Miyake [Miy06, p. 142]). This way one has an 'explicit' description of $\hat{\mathrm{T}}(\mathfrak{n})$.

As in Hijikata [Hij74, §5.2-5.3], if $[\mathfrak{n}] = 0$ in $\mathrm{Cl}_\infty(F)$ then the group $\hat{\Theta}(\mathfrak{n})$ admits a decomposition as a finite union of double cosets

$$\hat{\Theta}(\mathfrak{n}) = \bigsqcup_s \hat{\mathcal{O}}^\times \gamma_s \hat{\mathcal{O}}^\times$$

with $\gamma_s \in \mathcal{O}^+$, and

$$\Theta^+(\mathfrak{n}) = \hat{\Theta}(\mathfrak{n}) \cap B^+ = \{x \in \mathcal{O}^+ : \mathrm{nrd}(x)\mathbb{Z}_F = \mathfrak{n}\}$$

admits a decomposition $\Theta^+(\mathfrak{n}) = \bigsqcup_s \mathcal{O}^+ \gamma_s \mathcal{O}^+$. We can thus define a Hecke operator $\mathrm{T}(\mathfrak{n})$ on $S_2(\Gamma_0^+(\mathfrak{N}))$ by setting

$$\mathrm{T}(\mathfrak{n}) = \sum_s [\Gamma_0^+(\mathfrak{N}) \gamma_s \Gamma_0^+(\mathfrak{N})].$$

Let $\hat{\alpha} = \gamma_s \in \mathcal{O}^+$ for some s. Because $[\mathfrak{n}] = 0$ in $\mathrm{Cl}_\infty(F)$, by (3) we see that $i = j$ in (8). Thus we have a well defined operator

$$[\hat{\mathcal{O}}^\times \hat{\alpha} \hat{\mathcal{O}}^\times]_i \cdot f_i(\tau) = ([\hat{\mathcal{O}}^\times \hat{\alpha} \hat{\mathcal{O}}^\times] \cdot f)_i(\tau)$$

on $S_2(\Gamma_i)$, for every i. If $i = j = 1$, we can choose $r_1 = 1$ and so we can write $\hat{\alpha}_\ell = b_\ell k_\ell$. Therefore we see that $\Gamma_0^+(\mathfrak{N})\gamma_s\Gamma_0^+(\mathfrak{N}) = \iota_1(\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times \cap B^+) = \bigsqcup b_\ell\Gamma_0^+(\mathfrak{N})$. Consequently, if $\mathfrak{n}$ is a principal ideal of F generated by a totally positive element, then by (10) we have an equality of Hecke operators on $S_2^+(\mathfrak{N})$

$$\hat{\mathrm{T}}(\mathfrak{n})_1 = \mathrm{T}(\mathfrak{n}).$$

In particular, the traces of $\hat{\mathrm{T}}(\mathfrak{n})$ and $\mathrm{T}(\mathfrak{n})$ on the $\mathbb{C}$-vector space $S_2^+(\mathfrak{N})$ are equal.

By Hijikata [Hij74, § 5], both Hecke operators have degree

$$\deg(\hat{\mathrm{T}}(\mathfrak{n})) = \deg(\mathrm{T}(\mathfrak{n})) = \prod_{\substack{\mathfrak{p}^e||\mathfrak{n}\\ \mathfrak{p}|\mathfrak{N}}} \mathrm{N}(\mathfrak{p})^e \prod_{\substack{\mathfrak{p}^e||\mathfrak{n}\\ \mathfrak{p}\nmid\mathfrak{N}}} (1 + \mathrm{N}(\mathfrak{p}) + \cdots + \mathrm{N}(\mathfrak{p})^e)\,. \tag{11}$$

Proposition 2.2. *For all integral ideals $\mathfrak{l} \subset \mathbb{Z}_F$ admitting a totally positive generator ℓ, the operator $\hat{\mathrm{T}}(\mathfrak{l},\mathfrak{l})$ acts as the identity on $S_2(\mathfrak{N})$.*

PROOF. Indeed, the idele $\hat{\alpha}_{\mathfrak{l},\mathfrak{l}}$ is equal to $\prod_\mathfrak{p} \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{l})} \in \hat{\mathbb{Z}}_F$, so $\hat{\alpha}_{\mathfrak{l},\mathfrak{l}}$ belongs to the center of $\hat{B}$, hence the center of $\hat{\mathcal{O}}^\times$. Therefore

$$\hat{\mathcal{O}}^\times\hat{\alpha}_{\mathfrak{l},\mathfrak{l}}\hat{\mathcal{O}}^\times = \hat{\alpha}_{\mathfrak{l},\mathfrak{l}}\hat{\mathcal{O}}^\times.$$

Also, $\hat{\alpha}_{\mathfrak{l},\mathfrak{l}}/\ell \in \hat{\mathbb{Z}}_F^\times$, so we can write $\hat{\alpha}_{\mathfrak{l},\mathfrak{l}} = \ell k$ for an element $k \in \hat{\mathcal{O}}^\times$. Hence $\hat{\alpha}_{\mathfrak{l},\mathfrak{l}}\hat{\mathcal{O}}^\times = \ell\hat{\mathcal{O}}^\times$, and if we choose $r_1 = 1$ in (8) we see that $r_j = 1$ as well, thus $\hat{\mathrm{T}}(\mathfrak{l},\mathfrak{l})$ stabilizes $S_2(\mathfrak{N})$. Furthermore, for $\hat{f} \in \hat{S}_2(\mathfrak{N})$ we have

$$(\hat{\mathrm{T}}(\mathfrak{l},\mathfrak{l})\hat{f})_1(\tau,\hat{b}) = \hat{f}_1(\ell^{-1}\tau) = \hat{f}_1(\tau),$$

because any scalar matrix in $\mathrm{GL}_2^+(\mathbb{R})$ acts trivially on $\mathcal{H}$. □

Set $\mathrm{T}(\mathfrak{p}^{-1}) = 0$ and $T(1) = \mathrm{Id}$. We now give a recursive formula between Hecke operators.

Corollary 2.3. *Let $\mathfrak{p} \nmid \mathfrak{D}$ be a prime of $\mathbb{Z}_F$ such that $[\mathfrak{p}] = 0$ in $\mathrm{Cl}_\infty(F)$. For every $r \geqslant 0$ we have the following relation inside $\mathrm{End}_\mathbb{C}(\hat{S}_2(\mathfrak{N}))$:*

$$\hat{\mathrm{T}}(\mathfrak{p})\hat{\mathrm{T}}(\mathfrak{p}^r) = \hat{\mathrm{T}}(\mathfrak{p}^{r+1}) + \mathrm{N}(\mathfrak{p})\hat{\mathrm{T}}(\mathfrak{p}^{r-1}).$$

PROOF. By Shimura [Shi71, Theo. 3.24] we have

$$\hat{\mathrm{T}}(\mathfrak{p})\hat{\mathrm{T}}(\mathfrak{p}^r) = \hat{\mathrm{T}}(\mathfrak{p}^{r+1}) + \mathrm{N}(\mathfrak{p})\hat{\mathrm{T}}(\mathfrak{p},\mathfrak{p})\hat{\mathrm{T}}(\mathfrak{p}^{r-1}).$$

By applying Proposition 2.2, we obtain the result. □

2.2 Hecke correspondences

We now look at the geometric aspects of Hecke operators. We start with the adelic case and derive from it the classical case.

An element $\hat{\alpha} \in \hat{B}^\times$ induces a map

$$\begin{array}{ccc} \mathcal{H}^\pm \times \hat{B}^\times & \to & \mathcal{H}^\pm \times \hat{B}^\times \\ (\tau,\hat{b}) & \mapsto & (\tau,\hat{b}\hat{\alpha}) \end{array}.$$

The operators $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ naturally arise when attempting to define a map on

$$X(\hat{\mathcal{O}}^\times) = B^\times\backslash\mathcal{H}^\pm \times \hat{B}^\times/\hat{\mathcal{O}}^\times.$$

See Chapter 5 of Milne [Mil12] for more details on what follows. The map which sends the class $\hat{b}\hat{\mathcal{O}}^\times$ to $\hat{b}\hat{\mathcal{O}}^\times\hat{\alpha}$ (respectively $\hat{b}\hat{\alpha}\hat{\mathcal{O}}^\times$) is not well defined, because in general $\hat{b}\hat{\mathcal{O}}^\times\hat{\alpha}$ is not a $\hat{\mathcal{O}}^\times$-orbit (respectively $\hat{\alpha}$ does not normalize $\hat{\mathcal{O}}^\times$, so the orbit depends on the choice of $\hat{b}$). To obtain a $\hat{\mathcal{O}}^\times$-orbit, we consider the set $\hat{b}\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times$. Since $\hat{\mathcal{O}}^\times$ is compact open, $\hat{\alpha}\hat{\mathcal{O}}^\times\hat{\alpha}^{-1}$ is commensurable with $\hat{\mathcal{O}}^\times$, therefore we have a finite decomposition $\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times = \bigsqcup \hat{\alpha}_\ell\hat{\mathcal{O}}^\times$, and we can thus associate to the class $\hat{b}\hat{\mathcal{O}}^\times$ the set $\{\hat{b}\alpha_\ell\hat{\mathcal{O}}^\times\}_\ell$. Let $\hat{\mathcal{O}}^\times_{\hat{\alpha}} = \hat{\mathcal{O}}^\times \cap \hat{\alpha}\hat{\mathcal{O}}^\times\hat{\alpha}^{-1}$. In more geometric terms, multiplication by $\hat{\alpha}$ induces a correspondence

$$\begin{array}{ccc} & X(\hat{\mathcal{O}}^\times_{\hat{\alpha}}) & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_1'\circ m_{\hat{\alpha}}} \\ X(\hat{\mathcal{O}}^\times) & \xrightarrow[[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]]{} & X(\hat{\mathcal{O}}^\times) \end{array} \tag{12}$$

where $p_1 : X(\hat{\mathcal{O}}^\times_{\hat{\alpha}}) \to X(\hat{\mathcal{O}}^\times)$ and $p_1' : X(\hat{\mathcal{O}}^\times_{\hat{\alpha}^{-1}}) \to X(\hat{\mathcal{O}}^\times)$ are the projection maps, and $m_{\hat{\alpha}} : X(\hat{\mathcal{O}}^\times_{\hat{\alpha}}) \to X(\hat{\mathcal{O}}^\times_{\hat{\alpha}^{-1}})$ is the map induced by $\hat{b}\hat{\mathcal{O}}^\times_{\hat{\alpha}} \mapsto \hat{b}\hat{\alpha}\hat{\mathcal{O}}^\times_{\hat{\alpha}^{-1}}$, which is now well defined. By Milne [Mil05, Theo. 13.6] the correspondence (12) is defined over F.

As we have seen, an element of $\hat{S}_2(\mathfrak{N})$ is a holomorphic differential 1-form on $X(\hat{\mathcal{O}}^\times)$, that is a global section of the sheaf Ω^1. For a morphism $\phi : X \to Y$ of Riemann surfaces, let $\phi^* : H^0(Y,\Omega^1) \to H^0(X,\Omega^1)$ and $\phi_* : H^0(X,\Omega^1) \to H^0(Y,\Omega^1)$ be respectively the pullback and pushforward morphisms induced by ϕ.

As in Milne [Mil12, Lem. 5.30], one can write $\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times = \bigsqcup k_\ell\hat{\alpha}\hat{\mathcal{O}}^\times$, where $\{k_\ell\}$ is a set of representatives of the right classes of $\hat{\mathcal{O}}^\times/\hat{\mathcal{O}}^\times_{\hat{\alpha}}$. For a modular form $\hat{f} \in \hat{S}_2(\mathfrak{N})$, we have

$$\begin{aligned} (p_{1*}'\circ m_{\hat{\alpha}*}\circ p_1^*)\hat{f}(\tau,\hat{b})d\tau &= \sum_\ell (p_{1*}'\circ m_{\hat{\alpha}*})\hat{f}(\tau,\hat{b}k_\ell)d\tau \\ &= \sum_\ell p_{1*}'\hat{f}(\tau,\hat{b}k_\ell\hat{\alpha})d\tau \\ &= \sum_\ell \hat{f}(\tau,\hat{b}k_\ell\hat{\alpha})d\tau \\ &= [\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot f(\tau,\hat{b})d\tau, \end{aligned}$$

so $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ is indeed the operator on $\hat{S}_2(\mathfrak{N})$ induced by the correspondence.

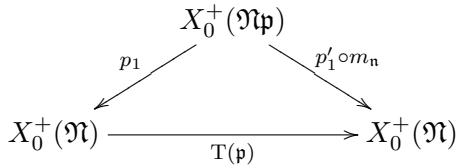
Note that the Jacobian of $X(\hat{\mathcal{O}}^\times)$ verifies

$$\mathrm{Jac}(X(\hat{\mathcal{O}}^\times)) \cong H^0(X(\hat{\mathcal{O}}^\times)^\vee,\Omega^1)/H_1(X(\hat{\mathcal{O}}^\times),\mathbb{Z}),$$

so by functoriality $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ induces an endomorphism of finite degree, hence an isogeny, of $\mathrm{Jac}(X(\hat{\mathcal{O}}^\times))$. In particular, when $\sum[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ is the Hecke operator $\hat{\mathrm{T}}(\mathfrak{n})$ for an integral ideal $\mathfrak{n}$ prime to $\mathfrak{D}$, we speak of *Hecke correspondence* for both the correspondence and the isogeny of $\mathrm{Jac}(X(\hat{\mathcal{O}}^\times))$ it induces.

Of course all that we have said can be transfered naturally to the classical case. For instance the operators $[\Gamma\alpha\Gamma]$ arise when one tries to give a sense to the map $\Gamma\backslash\mathcal{H} \to \Gamma\backslash\mathcal{H}$ sending $[\tau]$ to $[\alpha^{-1}\tau]$. When $\mathfrak{p} \nmid \mathfrak{D}$ is a prime ideal with trivial image in $\mathrm{Cl}_\infty(F)$, we

obtain the Hecke correspondence on $X_0^+(\mathfrak{N})$:



Let $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$ be such that $\alpha^{-1}\Gamma\alpha$ and Γ are commensurable. Choose a set of common representatives for the left and right classes $\Gamma\backslash\Gamma\alpha\Gamma$ and $\Gamma\alpha\Gamma/\Gamma$ respectively (this is always possible, see for instance the proof of Milne [Mil12, Lem. 5.24]). We easily check that

$$[\Gamma\alpha\Gamma] \circ [\Gamma\alpha\Gamma]^\vee = [\Gamma\alpha\Gamma]^\vee \circ [\Gamma\alpha\Gamma] = [\deg([\Gamma\alpha\Gamma])] = [\deg([\Gamma\alpha\Gamma]^\vee)], \tag{13}$$

where $[\Gamma\alpha\Gamma]^\vee$ is the operator defined in Remark 2.1, and where for an integer n, $[n]$ is the multiplication-by-n map. This means that the isogenies induced by these two operators are dual to each other. For a prime $\mathfrak{p}$ of F as above and the Hecke operator $\mathrm{T}(\mathfrak{p})$, we obtain

$$\mathrm{T}(\mathfrak{p}) \circ \mathrm{T}(\mathfrak{p})^\vee = \mathrm{T}(\mathfrak{p})^\vee \circ \mathrm{T}(\mathfrak{p}) = \begin{cases} [\mathrm{N}(\mathfrak{p}) + 1] & \text{if } \mathfrak{p} \nmid \mathfrak{N} \\ [\mathrm{N}(\mathfrak{p})] & \text{if } \mathfrak{p} \mid \mathfrak{N}. \end{cases}$$

We will now consider the reduction of all our objects over finite fields. The following fundamental result is due to Carayol [Car86].

Theorem 2.4 (Carayol). *Let $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ be a prime of $\mathbb{Z}_F$. Then $\mathrm{Sh}(\hat{\mathcal{O}}^\times)$ has good reduction at $\mathfrak{p}$.*

Let $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ be a prime of good reduction of $\mathrm{Sh}(\hat{\mathcal{O}}^\times)$, with norm $\mathrm{N}(\mathfrak{p}) = q$. Let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$. Theorem 2.4 implies that the model over F_∞ of the connected components of $X(\hat{\mathcal{O}}^\times)$, in particular $\mathrm{Sh}_0^+(\mathfrak{N})$, have good reduction at $\mathfrak{P}$. We will use the notation $\bar{\cdot}$ to speak of the reduction of the corresponding object modulo $\mathfrak{p}$ or $\mathfrak{P}$, depending on the field of definition. The following theorem was proved by Eichler in particular cases and greatly generalized by Shimura, and is a fundamental result in many arithmetical questions (a proof can be found in Shimura [Shi67, Theo. 11.17] or Zhang [Zha01, Prop. 1.4.10]). Let $\mathrm{Frob}_{\mathfrak{p}}$ (respectively, $\mathrm{Ver}_{\mathfrak{p}}$) be the Frobenius endomorphism (respectively, Verschiebung) on $\mathrm{Jac}(\overline{\mathrm{Sh}}(\hat{\mathcal{O}}^\times))$.

Theorem 2.5 (Eichler-Shimura congruence relation). *We have the following relation:*

$$\overline{\hat{\mathrm{T}}}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}} + \mathrm{Ver}_{\mathfrak{p}}.$$

Assume now that $[\mathfrak{p}] = 0$ in $\mathrm{Cl}_\infty(F)$. In particular, we have an isomorphism of residue fields $\mathbb{F}_{\mathfrak{p}} \cong \mathbb{F}_{\mathfrak{P}}$ and $\mathrm{N}(\mathfrak{P}) = \mathrm{N}(\mathfrak{p}) = q$. Consider the curve $\mathrm{Sh}_0^+(\mathfrak{N})$; it is defined over F_∞ and has good reduction at $\mathfrak{P}$. The Hecke operator $\mathrm{T}(\mathfrak{p})$ acts on $\mathrm{Jac}(X_0^+(\mathfrak{N}))$ and is defined over F_∞. By restriction, the Eichler-Shimura congruence relation gives

$$\overline{\mathrm{T}}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}} + \mathrm{Ver}_{\mathfrak{p}}$$

in $\mathrm{End}(\mathrm{Jac}(\overline{\mathrm{Sh}_0^+}(\mathfrak{N})))$.

Proposition 2.6. *The zeta function of the curve* $\overline{\mathrm{Sh}}_0^+(\mathfrak{N})$ *satisifies*

$$Z(\overline{\mathrm{Sh}}_0^+(\mathfrak{N}); T) = \frac{\det(1 - \mathrm{T}(\mathfrak{p})t + qt^2)}{(1-t)(1-qt)},$$

where $\mathrm{T}(\mathfrak{p})$ *is the Hecke operator defined by its action on the* $\mathbb{C}$*-vector space* $S_2^+(\mathfrak{N})$.

PROOF. We follow Milne [Mil12, Theo. 11.11]. For a prime $\ell \nmid \mathfrak{p}$, let

$$R_\ell : \mathrm{End}(\mathrm{Jac}(X_0^+(\mathfrak{N}))) \to \mathrm{End}_{\mathbb{Q}_\ell}(H^1(\mathrm{Jac}(X_0^+(\mathfrak{N})), \mathbb{Q}_\ell))$$

and

$$\bar{R}_\ell : \mathrm{End}(\overline{\mathrm{Jac}}(X_0^+(\mathfrak{N}))) \to \mathrm{End}_{\mathbb{Q}_\ell}(H^1(\mathrm{Jac}(X_0^+(\mathfrak{N})), \mathbb{Q}_\ell))$$

be ℓ-adic representations of $\mathrm{End}(\mathrm{Jac}(X_0^+(\mathfrak{N})))$ and $\mathrm{End}(\overline{\mathrm{Jac}}(X_0^+(\mathfrak{N})))$ respectively. Then by Shimura [Shi71, § 7.1], the numerator of $Z(\overline{\mathrm{Sh}}_0^+(\mathfrak{N}); T)$ is $\det(1 - \bar{R}_\ell(\mathrm{Frob}_\mathfrak{p}))$. Now by Shimura [Shi98, Prop. III.14], for every endomorphism $\phi \in \mathrm{End}(\mathrm{Jac}(X_0^+(\mathfrak{N})))$ we have $R_\ell(\phi) = \bar{R}_\ell(\bar{\phi})$, so the Eichler-Shimura congruence relation (Theorem 2.5) gives

$$(1 - \bar{R}_\ell(\mathrm{Frob}_\mathfrak{p})t)(1 - \bar{R}_\ell(\mathrm{Ver}_\mathfrak{p})t) = 1 - R_\ell(\mathrm{T}(\mathfrak{p}))t + qt^2.$$

The characteristic polynomials of $\mathrm{Frob}_\mathfrak{p}$ and $\mathrm{Ver}_\mathfrak{p}$ are the same[Shi71, p. 193], so by taking determinants we obtain

$$\det(1 - \bar{R}_\ell(\mathrm{Frob}_\mathfrak{p})t)^2 = \det(1 - R_\ell(\mathrm{T}(\mathfrak{p}))t + qt^2).$$

Let g be the genus of $X_0^+(\mathfrak{N})$, and let

$$R : \mathrm{End}_\mathbb{Q}(\mathrm{Jac}(X_0^+(\mathfrak{N}))) \to \mathrm{M}_g(\mathbb{C})$$

be a complex representation of $\mathrm{End}_\mathbb{Q}(\mathrm{Jac}(X_0^+(\mathfrak{N})))$. Then by Shimura [Shi98, § I.3.2] and Shimura [Shi71, § 11], R_ℓ is equivalent to the sum of R and its complex conjugate. Thus

$$\det(1 - \bar{R}_\ell(\mathrm{Frob}_\mathfrak{p})t)^2 = \det(1 - R(\mathrm{T}(\mathfrak{p}))t + qt^2)^2,$$

and the result follows by taking square roots. □

In this thesis we are mainly interested in the number of rational points of curves defined over finite fields. The following corollary to Proposition 2.6 is the main reason of our interest in Hecke operators.

Corollary 2.7. *Suppose that* $[\mathfrak{p}] = 0$ *in* $\mathrm{Cl}_\infty(F)$. *Then we have the following formula for* $r \geqslant 1$*:*

$$\#\overline{\mathrm{Sh}}_0^+(\mathfrak{N})(\mathbb{F}_{q^r}) = q^r + 1 - \mathrm{Tr}(\mathrm{T}(\mathfrak{p}^r)) + q\mathrm{Tr}(\mathrm{T}(\mathfrak{p}^{r-2})).$$

PROOF. We follow Ihara [Iha67, Lem. 5]. Let g be the genus of $X_0^+(\mathfrak{N})$ and $a_1, \ldots, a_g \in \mathbb{C}$ be the eigenvalues of $\mathrm{T}(\mathfrak{p})$ with multiplicity. Write

$$1 - a_i t + qt^2 = (1 - \alpha_i t)(1 - \bar{\alpha}_i t).$$

Then

$$\det(1 - \mathrm{T}(\mathfrak{p})t + qt^2) = \prod_{i=1}^{g}(1 - \alpha_i t)(1 - \bar{\alpha}_i t).$$

The zeta function of a curve defined over $\mathbb{F}_q$ can be uniquely written as

$$\frac{\prod_{j=1}^{2g}(1-\omega_j T)}{(1-T)(1-qT)},$$

therefore by Proposition 2.6 the α_i and $\bar{\alpha}_i$, for $i = 1, \ldots, g$, are the eigenvalues of the Frobenius.

Set $U(1) = 2$, and for $r \geqslant 1$

$$U(\mathfrak{p}^r) = \mathrm{T}(\mathfrak{p}^r) - q\mathrm{T}(\mathfrak{p}^{r-2}).$$

By using Corollary 2.3, we see that for every $r \geqslant 1$,

$$\begin{aligned} U(\mathfrak{p})U(\mathfrak{p}^r) - qU(\mathfrak{p}^{r-1}) &= \mathrm{T}(\mathfrak{p})(\mathrm{T}(\mathfrak{p}^r) - q\mathrm{T}(\mathfrak{p}^{r-2})) - q(\mathrm{T}(\mathfrak{p}^{r-1}) - q\mathrm{T}(\mathfrak{p}^{r-3})) \\ &= \mathrm{T}(\mathfrak{p}^{r+1}) - q\mathrm{T}(\mathfrak{p})\mathrm{T}(\mathfrak{p}^{r-2}) + q^2\mathrm{T}(\mathfrak{p}^{r-3}) \\ &= \mathrm{T}(\mathfrak{p}^{r+1}) - q\mathrm{T}(\mathfrak{p}^{r-1}) \\ &= U(\mathfrak{p}^{r+1}). \end{aligned}$$

We obtain the result by induction, since if $U(\mathfrak{p}^r)$ has trace $\sum_{i=1}^g \alpha_i^r + \bar{\alpha}_i^r$, then $U(\mathfrak{p}^{r+1})$ has trace

$$\sum_{i=1}^{g}(\alpha_i + \bar{\alpha}_i)(\alpha_i^r + \bar{\alpha}_i^r) - \alpha_i\bar{\alpha}_i(\alpha_i^{r-1} + \bar{\alpha}_i^{r-1}) = \sum_{i=1}^{g} \alpha_i^{r+1} + \bar{\alpha}_i^{r+1},$$

which is the trace of the Frobenius on $X_0^+(\mathfrak{N})_{\mathbb{F}_{q^{r+1}}}$. □

2.3 Atkin-Lehner operators

Let $\mathrm{N}_{\hat{B}^\times}(\hat{\mathcal{O}}^\times)$ be the normalizer of $\hat{\mathcal{O}}^\times$ in $\hat{B}^\times$. We have seen that Hecke correspondences arise when we try to interpret the map on Shimura curves induced by

$$(\tau, \hat{b}) \mapsto (\tau, \hat{b}\hat{\alpha}),$$

for an adele $\hat{\alpha} \in \hat{B}^\times$. When $\hat{\alpha}$ belongs to $\mathrm{N}_{\hat{B}^\times}(\hat{\mathcal{O}}^\times)$, the correspondence is 'natural' in the sense that this map is already well defined. The automorphism $\hat{w}(\hat{\alpha})$ of $X(\hat{\mathcal{O}}^\times)$ that it induces is called the *Atkin-Lehner operator* associated to $\hat{\alpha}$, after the work of Atkin and Lehner in the elliptic modular case [AL70].

The groups $\hat{F}^\times$ and $\hat{\mathcal{O}}^\times$ both act trivially on $S_2(\hat{\mathcal{O}}^\times)$, so when considering the action of an Atkin-Lehner operator on modular forms, we are rather interested in the group

$$W(\hat{\mathcal{O}}^\times) = \mathrm{N}_{\hat{B}^\times}(\hat{\mathcal{O}}^\times)/(\hat{F}^\times\hat{\mathcal{O}}^\times).$$

By Doyle, Linowitz and Voight [DLV, Prop. 1.13], the reduced norm induces maps

$$\{\mathfrak{a} \;||\; \mathfrak{d}(\mathcal{O}) : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\} \times \mathrm{Cl}(F)[2] \xrightarrow{\cong} \widehat{W(\mathcal{O})} \hookrightarrow W(\hat{\mathcal{O}}^\times). \tag{14}$$

For a unitary ideal $\mathfrak{a} \;||\; \mathfrak{d}(\mathcal{O})$ we define the *Atkin-Lehner operator*

$$\hat{w}(\mathfrak{a}) = [\hat{\mathcal{O}}^\times\hat{\alpha}_\mathfrak{a}\hat{\mathcal{O}}^\times],$$

where $\hat{\alpha}_\mathfrak{a}$ is a representative in $\widehat{W(\mathcal{O})} \subset W(\hat{\mathcal{O}}^\times)$ which has non-trivial image in (14) precisely at the primes dividing $\mathfrak{a}$. For instance, to every integral unitary ideal $\mathfrak{n} \;||\; \mathfrak{N}$, that

is such that $\mathfrak{n}^2 + \mathfrak{N} = \mathfrak{n}$, we can associate the operator $\hat{w}(\mathfrak{n})$ corresponding to an adele $\hat{\alpha}_\mathfrak{n} \in W(\hat{\mathcal{O}}^\times)$ defined locally at $\mathfrak{p} \nmid \mathfrak{D}$ by

$$(\hat{\alpha}_\mathfrak{n})_\mathfrak{p} = \begin{pmatrix} \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{n})} & -1 \\ \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{N})} & \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{n})} \end{pmatrix} \in B_\mathfrak{p} \cong \mathrm{M}_2(F_\mathfrak{p})$$

(and at $\mathfrak{p} \mid \mathfrak{D}$ by $(\hat{\alpha}_\mathfrak{n})_\mathfrak{p} = 1$). When $\mathfrak{n} = \mathfrak{N}$, we can take $\hat{\alpha}_\mathfrak{N}$ defined locally at $\mathfrak{p} \nmid \mathfrak{D}$ by

$$(\hat{\alpha}_\mathfrak{N})_\mathfrak{p} = \begin{pmatrix} 0 & -1 \\ \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{N})} & 0 \end{pmatrix}.$$

We denote by $\hat{\omega}(\mathfrak{n})$ both the operators $\hat{w}(\hat{\alpha}_\mathfrak{n})$ on $X(\hat{\mathcal{O}}^\times)$ and $[\hat{\mathcal{O}}^\times \hat{\alpha}_\mathfrak{n} \hat{\mathcal{O}}^\times]$ on $\hat{S}_2(\mathfrak{N})$. One checks easily that $\hat{\alpha}_\mathfrak{n}$ normalizes $\hat{\mathcal{O}}^\times$ and that $\hat{\alpha}_\mathfrak{n}^2 \in \hat{F}^\times \hat{\mathcal{O}}^\times$, therefore $\hat{w}(\mathfrak{n})$ is a nontrivial involution of $\hat{S}_2(\mathfrak{N})$ (note that $\hat{\alpha}_\mathfrak{n}$, which belongs to $\hat{\mathcal{O}}$, is not invertible in $\hat{F}^\times \hat{\mathcal{O}}$).

By definition of the map providing the isomorphism (2), it is clear that the operator $\hat{w}(\mathfrak{n})$ acts on $X_0^+(\mathfrak{N})$ (respectively $S_2^+(\mathfrak{N})$) if and only if $[\hat{\alpha}_\mathfrak{n}] = 0$ in $\mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)$, that is if and only if $[\mathfrak{n}] = 0$ in $\mathrm{Cl}_\infty(F)$. In this case, there exists an element $b \in B^+$ such that $\hat{\mathcal{O}}^\times \hat{\alpha}_\mathfrak{n} \hat{\mathcal{O}}^\times = \hat{\mathcal{O}}^\times b \hat{\mathcal{O}}^\times$ [Hij74, §5]. Therefore, as in the case of Hecke operators, we can define Atkin-Lehner operators $\omega(\mathfrak{n})$ on $X_0^+(\mathfrak{N})$ and $S_2^+(\mathfrak{N})$ by setting

$$w(\mathfrak{n})[\tau] = [b^{-1}\tau]$$

and

$$w(\mathfrak{n}) = [\Gamma_0^+(\mathfrak{N}) b \Gamma_0^+(\mathfrak{N})]$$

respectively. We once again have an equality of operators, both on $X_0^+(\mathfrak{N})$ and $S_2^+(\mathfrak{N})$:

$$\hat{w}(\mathfrak{n})_1 = w(\mathfrak{n}).$$

3 The trace formula

We now study a trace formula for Hecke operators acting on quaternionic modular forms which is due to Hijikata [Hij74, Theo. 4.6]. See also Shimizu [Shi65], Saito [Sai84] and Hijikata, Saito and Yamauchi [HSY93] for other versions of this result.

Theorem 3.1 (Eichler-Selberg trace formula). *Let $\mathfrak{n}$ be an ideal of $\mathbb{Z}_F$ coprime to $\mathfrak{D}$ and with trivial class in $\mathrm{Cl}_\infty(F)$. Then the trace of $\mathrm{T}(\mathfrak{n})$ on $S_2(\Gamma_0^+(\mathfrak{N}))$ is*

$$\mathrm{Tr}(\mathrm{T}(\mathfrak{n}) \mid S_2(\Gamma_0^+(\mathfrak{N}))) = \delta(\mathfrak{n}) \frac{\mathrm{vol}(\Gamma_0^+(\mathfrak{N}) \backslash \mathcal{H})}{4\pi} - \frac{1}{2h_\infty} \sum_{\mathcal{P}(\mathfrak{n})} \sum_R \frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R, \mathcal{O}),$$

where

- $\delta(\mathfrak{n})$ equals 1 if $\mathfrak{n} = (\alpha)^2$ with $\alpha \in \mathbb{Z}_F$, and 0 otherwise.
- $\mathcal{P}(\mathfrak{n})$ is the (finite) set of polynomials $P(X) = X^2 - tX + n \in \mathbb{Z}_F[X]$ such that n runs through a sytem of representatives of

  $$\{x \in \mathbb{Z}_{F,+} : x\mathbb{Z}_F = \mathfrak{n}\}$$

  modulo $\mathbb{Z}_F^{\times 2}$, and $t^2 - 4n$ is totally negative.

- R runs through all the orders of $K = F[X]/P(X)$ containing the order $\mathbb{Z}_F[X]/P(X)$, and $h(R)$ is the class number of R.
- vol be the volume with respect to the hyperbolic measure $(dx^2 + dy^2)/y^2$ on $\mathcal{H}$.

PROOF. We explain our formulation of Hijikata's result [Hij74, Theo. 4.6]. We start with the contributions of scalar matrices. There is a scalar matrix α of norm generating $\mathfrak{n}$ if and only if $\mathfrak{n} = (\alpha^2)$, and in this case the only double coset containing this matrix is $\Gamma_0^+(\mathfrak{N})\alpha\Gamma_0^+(\mathfrak{N})$. For the volume, note that $\mathrm{vol}(\Gamma_0^+(\mathfrak{N})\backslash\mathcal{H}^\pm) = 2 \cdot \mathrm{vol}(\Gamma_0^+(\mathfrak{N})\backslash\mathcal{H})$.

We now consider the contribution of elliptic points. With Hijikata's notation, $R = \mathcal{O}$ and $\Gamma = \mathcal{O}^+$. The reduced norm map induces an isomorphism $\mathcal{O}^\times/\mathcal{O}^+ \cong \mathbb{Z}_{F,(+)}^\times/\mathbb{Z}_{F,+}^\times$, so by Milne [Mil11, Theo. V.1.7],

$$[\mathcal{O}^\times : \mathcal{O}^+] = \frac{2^d h h_\infty^{-1}}{2^{d-1} h h^{(+)^{-1}}} = \frac{2h^{(+)}}{h_\infty}.$$

At last, we have to divide the trace by 2 by Hijikata [Hij74, Rem. 1.4] (compare with Saito [Sai72]). □

Generalizing a result of Shimizu [Shi65, Appendix], Hijikata proved the following formula for the volume of $X_0^+(\mathfrak{N})$ [Hij74, Lem. 4.5]:

$$\mathrm{vol}(\Gamma_0^+(\mathfrak{N})\backslash\mathcal{H}) = \frac{8\pi}{(2\pi)^{2d}} \frac{h}{h_\infty} d_F^{3/2} \zeta_F(2) \Phi(\mathfrak{D}) \Psi(\mathfrak{N}). \tag{15}$$

The curve $X_0^1(\mathfrak{N})$ being a covering of $X_0^+(\mathfrak{N})$ of degree h_∞/h, we have

$$\mathrm{vol}(X_0^1(\mathfrak{N})) = \frac{8\pi}{(2\pi)^{2d}} d_F^{3/2} \zeta_F(2) \Phi(\mathfrak{D}) \Psi(\mathfrak{N}). \tag{16}$$

Now let $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ be a prime of $\mathbb{Z}_F$ such that $[\mathfrak{p}] = 0$ in $\mathrm{Cl}_\infty(F)$. If $\mathfrak{P}$ is a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$, then by Theorem 2.4 $\mathrm{Sh}_0^+(\mathfrak{N})$ has good reduction at $\mathfrak{P}$ and the reduction is defined over $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$. Let $q = \mathrm{N}(\mathfrak{p})$.

Set $\Xi(-1) = 0$, and for every integer $r \geqslant 0$, let

$$\Xi(r) = \sum_{\mathcal{P}(\mathfrak{p}^r)} \sum_R \frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R, \mathcal{O}).$$

Proposition 3.2. *For every integer $r \geqslant 1$ we have*

$$\#\overline{\mathrm{Sh}_0}^+(\mathfrak{N})(\mathbb{F}_{q^r}) = q^r + 1 + \delta(r)(q-1)\frac{\mathrm{vol}(X_0^+(\mathfrak{N}))}{4\pi} + \frac{1}{2h_\infty}\left(\Xi(r) - q\Xi(r-2)\right),$$

where $\delta(r) = \delta(\mathfrak{p}^r) = 1$ if r is even, 0 else.

PROOF. This follows from Corollary 2.7 and Theorem 3.1. □

We would now like to generalize the result due to Jordan and Livné [JL85] and Skorobogatov and Yafaev [SY04] that the term $\Xi(r) - q\Xi(r-2)$ is positive. This will play a major role in our proof that the curves $X_0^+(\mathfrak{N})$ are asymptotically optimal.

Let K be a quadratic extension of F and R a $\mathbb{Z}_F$-order in K. A map $f : K \to B$ is an *embedding* if f is a morphism of F-algebras, and f is *optimal* relative to R and $\mathcal{O}$ if

$$f(K) \cap \mathcal{O} = f(R).$$

For a prime $\mathfrak{q}$ in $\mathbb{Z}_F$, we denote by $m_\mathfrak{q}(R,\mathcal{O})$ the number of classes of local optimal embeddings $f : R_\mathfrak{q} \to \mathcal{O}_\mathfrak{q}$ under the equivalence relation: f is equivalent to $K_\mathfrak{q} : R_\mathfrak{q} \to \mathcal{O}_\mathfrak{q}$ if and only if there exists $x \in \mathcal{O}_\mathfrak{q}^\times$ such that $f(y) = x^{-1}f(y)x$ for all $y \in R_\mathfrak{q}$.

The *Artin symbol* at a prime $\mathfrak{p}$ of $`\mathbb{Z}_F$ is defined by

$$\left(\frac{K}{\mathfrak{p}}\right) = \begin{cases} -1 & \text{if } \mathfrak{p} \text{ is inert in } K, \\ 0 & \text{if } \mathfrak{p} \text{ is ramified in } K, \\ 1 & \text{if } \mathfrak{p} \text{ is split in } K. \end{cases}$$

Theorem 3.3. *Let y be an integral element of $B \setminus F$ with minimal polynomial $P(X) = X^2 - tX + n \in \mathbb{Z}_F[X]$ over F. Let R_0 be the order $\mathbb{Z}_F[y] \subset B$, with conductor $\mathfrak{f}_{R_0}$, and let $K \subset B$ be the fraction field of R_0. Let $R \subset K$ be another $\mathbb{Z}_F$-order of K containing R_0, with conductor $\mathfrak{f}_R$. For a prime $\mathfrak{q}$ of F, the number $m_\mathfrak{q}(R,\mathcal{O})$ takes the following values:*

a) If $\mathfrak{q} \nmid \mathfrak{D}\mathfrak{N}$, then $m_\mathfrak{q}(R,\mathcal{O}) = 1$.

b) If $\mathfrak{q} \mid \mathfrak{D}$, then $m_\mathfrak{q}(R,\mathcal{O}) = \begin{cases} 0, & \text{if } \mathfrak{q} \mid \mathfrak{f}_R, \\ 1 - \left(\frac{K}{\mathfrak{q}}\right), & \text{otherwise.} \end{cases}$

c) Let $e = v_\mathfrak{q}(\mathfrak{N})$, and let $\rho = v_\mathfrak{q}(\mathfrak{f}_{R_0}) - v_\mathfrak{q}(\mathfrak{f}_R)$. For every integer $s \geqslant 0$, define the set

$$E(s) = \{x \in \mathbb{Z}_{F,\mathfrak{q}}/(\pi_\mathfrak{q})^{s+2\rho} : P(x) \equiv 0 \bmod (\pi_\mathfrak{q})^{s+2\rho},\, 2x \equiv t \bmod (\pi_\mathfrak{q})^\rho\}.$$

Then

$$m_\mathfrak{q}(R,\mathcal{O}) = \begin{cases} \#E(e), & \text{if } e = 0 \text{ or } v_\mathfrak{q}(t^2-4n) = 2\rho \\ \#E(e) + \#\mathrm{Im}\left(E(e+1) \to \mathbb{Z}_{F,\mathfrak{q}}/(\pi_\mathfrak{q})^{e+2\rho}\right), & \text{otherwise.} \end{cases}$$

PROOF. This result comes from Hijikata [Hij74, Theo. 2.3 and § 2.8]. See also Vignéras [Vig80, § II.3] (but note that there are a few typos). □

Lemma 3.4. *Let K/F be a quadratic imaginary extension of F. Let R be an order in K of conductor $\mathfrak{p}^i\mathfrak{a}$, with $i \geqslant 1$ and $\mathfrak{a} \subset \mathbb{Z}_F$ coprime to $\mathfrak{p}$, and let R' be an order in K of conductor $\mathfrak{a}$. For every prime $\mathfrak{q}$ we have*

$$m_\mathfrak{q}(R',\mathcal{O}) = m_\mathfrak{q}(R,\mathcal{O}).$$

PROOF. By Theorem 3.3, this is clear when $\mathfrak{q} \nmid \mathfrak{D}\mathfrak{N}$, as we have $m_\mathfrak{q}(R',\mathcal{O}) = 1 = m_\mathfrak{q}(R,\mathcal{O})$. So suppose $\mathfrak{q} \mid \mathfrak{D}\mathfrak{N}$. Then $\mathfrak{q}$ cannot be equal to $\mathfrak{p}$. If $\mathfrak{q} \mid \mathfrak{D}$, then $\mathfrak{q} \mid \mathfrak{p}^i\mathfrak{a}$ if and only if $\mathfrak{q} \mid \mathfrak{a}$, so $m_\mathfrak{q}(R',\mathcal{O}) = m_\mathfrak{q}(R,\mathcal{O})$. Finally, when $\mathfrak{q} \mid \mathfrak{N}$ we see that the dependance of $m_\mathfrak{q}(R,\mathcal{O})$ on R, or equivalently on its conductor, only occurs at the $\mathfrak{q}$-adic valuation of the relative conductor $\mathfrak{f}_{R/\Lambda} = \mathfrak{f}_\Lambda/\mathfrak{f}_R$ of Λ in R. But since $\mathfrak{q} \neq \mathfrak{p}$, multiplying by a power of $\mathfrak{p}$ does not affect this valuation, hence once again $m_\mathfrak{q}(R',\mathcal{O}) = m_\mathfrak{q}(R,\mathcal{O})$. □

Proposition 3.5. *We have an equality*

$$\sum_{\mathfrak{f} \mid \mathfrak{p}^n\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times : \mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}) = \left(1 + \sum_{i=1}^{n} \mathrm{N}(\mathfrak{p}^i)\left(1 - \left(\frac{K}{\mathfrak{p}}\right)\frac{1}{\mathrm{N}(\mathfrak{p})}\right)\right) \sum_{\mathfrak{f} \mid \mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times : \mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}).$$

PROOF. We can decompose

$$\sum_{\mathfrak{f}|\mathfrak{p}^n\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}) = \sum_{i=0}^{n} \sum_{\mathfrak{f}|\mathfrak{a}} \frac{h\left(R_{\mathfrak{p}^i\mathfrak{f}}\right)}{[R_{\mathfrak{p}^i\mathfrak{f}}:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}\left(R_{\mathfrak{p}^i\mathfrak{f}},\mathcal{O}\right).$$

By Lemma 3.4 we obtain $\prod_\mathfrak{q} m_\mathfrak{q}(R_{\mathfrak{p}^i\mathfrak{f}},\mathcal{O}) = \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O})$, so from Neukirch [Neu99, Theo. 12.12] the right hand term is equal to the sum of

$$\sum_{\mathfrak{f}|\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O})$$

and

$$\sum_{i=1}^{n} \sum_{\mathfrak{f}|\mathfrak{a}} \mathrm{N}(\mathfrak{p}^i)\left(1-\left(\frac{K}{\mathfrak{p}}\right)\frac{1}{\mathrm{N}(\mathfrak{p})}\right)\frac{h(K)}{[\mathbb{Z}_K^\times:\mathbb{Z}_F^\times]}\mathrm{N}(\mathfrak{f})\prod_{\mathfrak{q}|\mathfrak{f}}\left(1-\left(\frac{K}{\mathfrak{q}}\right)\frac{1}{\mathrm{N}(\mathfrak{q})}\right)\prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}),$$

whence the result. □

Proposition 3.6. *We have*

$$\Xi(r) - q\Xi(r-2) \geqslant 0.$$

PROOF. We follow Jordan and Livné [JL85, Prop. 2.4]. Let p be a generator of $\mathfrak{p}$ such that p^{r-2} is a totally positive generator of $\mathfrak{p}^{r-2}$ (thus p^r is a totally positive generator of $\mathfrak{p}^r$). Let $P'_p(X) = X^2 - t'X + p^{r-2}$ be a polynomial in $\mathcal{P}(\mathfrak{p}^{r-2})$, and let α' be a root of $P'_p(X) = 0$. The algebraic integer $\alpha = p\alpha'$ is a root of the polynomial $P_p(X) = X^2 - pt'X + p^r$, which belongs to $\mathcal{P}(\mathfrak{p}^r)$. Let $\mathfrak{p}^n\mathfrak{a}$ be the conductor of $\mathbb{Z}_F[\alpha]$ in $K = F(\alpha)$, for an integer $n \geqslant 1$ and an ideal $\mathfrak{a}$ prime to $\mathfrak{p}$. The orders of K containing $\mathbb{Z}_F[\alpha]$ must have conductor dividing $\mathfrak{p}^n\mathfrak{a}$, whereas the orders in $K' = F(\alpha')$ containing $\mathbb{Z}_F[\alpha']$ must have conductor dividing $\mathfrak{p}^{n-1}\mathfrak{a}$. But note that $K = K'$, so all orders are in K. Now, the root α of a polynomial $P_p(X) = X^2 - tX + p^r \in \mathcal{P}(p^r)$ can be written $\alpha = p\alpha'$ for a root α' of a polynomial $P'_p(X) = X^2 - t'X + p^{r-2}$ in $\mathcal{P}(\mathfrak{p}^{r-2})$ if and only if $p \mid t$. Thus there is a decomposition

$$\Xi(r) - q\Xi(r-2) = A + B$$

where

$$A = \sum_{\substack{P_p(X)\in\mathcal{P}(\mathfrak{p}^r)\\ p|t}} \left(\sum_{R\supseteq\mathbb{Z}_F[p\alpha']} \frac{h(R)}{[R^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R,\mathcal{O}) - q \sum_{R\supseteq\mathbb{Z}_F[\alpha']} \frac{h(R)}{[R^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R,\mathcal{O}) \right)$$

and

$$B = \sum_{\substack{P_p(X)\in\mathcal{P}(\mathfrak{p}^r)\\ p\nmid t}} \sum_{R\supseteq\mathbb{Z}_F[\alpha]} \frac{h(R)}{[R^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R,\mathcal{O}).$$

The term B is obviously positive, so it remains to prove that A is positive. We have

$$\begin{aligned} A &= \sum_{P'_p(X)} \left(\sum_{\mathfrak{f}|\mathfrak{p}^n\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}) - \mathrm{N}(\mathfrak{p}) \sum_{\mathfrak{f}|\mathfrak{p}^{n-1}\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}) \right) \\ &= \sum_{P'_p(X)} \left(1-\left(\frac{K}{\mathfrak{p}}\right)\right) \sum_{\mathfrak{f}|\mathfrak{a}} \frac{h(R_\mathfrak{f})}{[R_\mathfrak{f}^\times:\mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R_\mathfrak{f},\mathcal{O}) \end{aligned}$$

by Proposition 3.5. All terms in the sum are positive, so A is positive, and therefore $\Xi(r) - q\Xi(r-2)$ is positive. □

Proposition 3.6 implies that the contribution of elliptic points in the trace formula for $\mathrm{T}(\mathfrak{p}^r)$ is at least $\mathrm{N}(\mathfrak{p})$ times the contribution of elliptic points in the trace formula for $\mathrm{T}(\mathfrak{p}^{r-2})$.

Remark 3.7. We have an equality $\Xi(r) = q\Xi(r-2)$ if and only if the terms A and B are zero. By Theorem 3.3, this occurs precisely when for any order $R_{\mathfrak{f}} \subset K$ containing a root α of a polynomial $X^2 - tX + p^r$, where p^r runs through a system of generators of $\{x \in \mathbb{Z}_{F,+} : x\mathbb{Z}_F = \mathfrak{p}^r\}$ modulo ${\mathbb{Z}_F^\times}^2$ and $t^2 - 4p^r$ is totally negative, at least one of the following conditions is satisfied:

i) $(\mathfrak{D}, \mathfrak{f}) \neq 1$;

ii) at least one prime factor $\mathfrak{q} \mid \mathfrak{D}$ is split in $F(\alpha)$;

iii) p divides t and $\mathfrak{p}$ is split in $F(\alpha)$;

iv) for least one prime $\mathfrak{q} \mid \mathfrak{N}$ with $e = v_{\mathfrak{q}}(\mathfrak{N}) > 0$, we have $E(e) = E(e+1) = \emptyset$ (with the notation of Theorem c).

The following result is fundamental in the study of the Ihara constant:

Theorem 3.8 (Drinfel'd-Vlăduţ bound). *Let q be a power of a prime number. Then*

$$A(q) \leqslant \sqrt{q} - 1.$$

Let $\Gamma \subset \mathrm{GL}_2^+(\mathbb{R})$ be a Fuchsian group of the first kind. An *elliptic point* of order q (respectively, a parabolic point) for Γ is a fixed point of an elliptic matrix of order q (respectively, a parabolic matrix). A conjugacy class of elliptic (respectively parabolic) points of order q under Γ is called an *elliptic cycle* of order q (respectively a *parabolic cycle*). The number of elliptic cycles of order q (respectively of parabolic cycles) for Γ is denoted by $e_q(\Gamma)$ (respectively $e_\infty(\Gamma)$). Note that $e_\infty(\Gamma) = 0$ if $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ is compact (see Shimura [Shi71, Prop. 1.33]).

The genus g of the Shimura curve $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ is related to the volume by the formula

$$2g - 2 = \frac{1}{2\pi}\mathrm{vol}(Y(\Gamma)) - \sum_q e_q(\Gamma)\left(1 - \frac{1}{q}\right) - e_\infty(\Gamma) \tag{17}$$

(see [Shi71, Theo. 2.20]).

As a consequence, denoting the number of $\mathbb{F}_{q^r}$-rational points and the genus of $\overline{\mathrm{Sh}}_0^+(\mathfrak{N})$ by N_r and g respectively, Proposition 3.2 and (17) imply that, for every $r \geqslant 1$,

$$\begin{aligned} N_{2r}/(g-1) &\geqslant \frac{(q-1)\mathrm{vol}(X_0^+(\mathfrak{N}))/4\pi}{\mathrm{vol}(X_0^+(\mathfrak{N}))/4\pi} \\ &= q - 1. \end{aligned}$$

Therefore, taking $r = 1$, we obtain the following result as a consequence of the Drinfel'd-Vlăduţ theorem.

Theorem 3.9. *Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_F$ such that $[\mathfrak{p}] = 0$ in $\mathrm{Cl}_\infty(F)$, and let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$. Consider a sequence $(X_0^+(\mathfrak{N}_i))_{i\geqslant 0}$ of Shimura curves defined over F_∞ with respect to a quaternion algebra B_i/F of discriminant $\mathfrak{D}_i$. Suppose that for every index i the prime $\mathfrak{p}$ does not divide $\mathfrak{D}_i\mathfrak{N}_i$, and that*

$$\lim_{i\to\infty} g(X_0^+(\mathfrak{N}_i)) = +\infty.$$

Then for every i, the curve $\mathrm{Sh}_0^+(\mathfrak{N}_i)$ has good reduction at $\mathfrak{P}$, and the sequence $(\overline{\mathrm{Sh}}_0^+(\mathfrak{N}_i))_{i\geqslant 0}$ is asymptotically optimal over the finite field $\mathbb{F}_{q^2}$.

Remark 3.10. Let $\Xi_i(r)$ be $\Xi(r)$ for the Eichler order of level $\mathfrak{N}_i$ defining the Shimura curve $X_0^+(\mathfrak{N}_i)$ in Theorem 3.9. Then we see that

$$\lim_{i\to\infty} \frac{\Xi_i(2) - q\Xi_i(0)}{g(\overline{\mathrm{Sh}}_0^+(\mathfrak{N}_i))} \to 0.$$

4 Supersingular points

We now study supersingular points on $X_0^+(\mathfrak{N})$ and show that they asymptotically provide all the rational points which allow us to attain the Drinfel'd-Vlăduţ bound in Theorem 3.9. In this section, let $\mathfrak{p}$ be a prime with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$. Let $\mathcal{O}'$ be an Eichler order of level $\mathfrak{N}$ in the definite quaternion algebra B' over F with discriminant $\mathfrak{D}\mathfrak{p}$. Let $q = \mathrm{N}(\mathfrak{p})$.

We denote by $\mathrm{Sh}(\mathfrak{N})$ the model of the adelic Shimura curve $X(\hat{\mathcal{O}}^\times)$, and similarly $\mathrm{Sh}(\mathfrak{N}\mathfrak{p})$. The curve $\mathrm{Sh}(\mathfrak{N}\mathfrak{p})$ has bad reduction at $\mathfrak{p}$. Actually, by [Jar04, Theo. 2.2 ii)], the reduction $\overline{\mathrm{Sh}}(\mathfrak{N}\mathfrak{p}) \times \overline{\mathbb{F}}_\mathfrak{p}$ modulo $\mathfrak{p}$ is isomorphic to a disjoint union of two copies of $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_\mathfrak{p}$ interesecting transversally over a finite set of points Σ, which we can thus see as points in either $\overline{\mathrm{Sh}}(\mathfrak{N}\mathfrak{p}) \times \overline{\mathbb{F}}_\mathfrak{p}$ or $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_\mathfrak{p}$. We call these points *supersingular points*.

Theorem 4.1. *The following three sets are in bijection:*

i) the set of supersingular points of $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_\mathfrak{p}$*;*

ii) the double coset $B'^\times \backslash \hat{B}'^\times / \hat{\mathcal{O}}'^\times$*;*

iii) the set of (left or right) classes of invertible $\mathcal{O}'$*-ideals in* B'*.*

PROOF. For the bijection between i) and ii), see Carayol [Car86, § 11.2]. The bijection between ii) and iii) is an instance of the local-global dictionnary of quaternion algebras, to the class of $\hat{b}' \in \hat{B}^\times$ we associate the class of the ideal I such $I_\mathfrak{p} = \mathcal{O}'_\mathfrak{p}\hat{b}'_\mathfrak{p}$. □

As a consequence, we obtain an exact formula for the number $N^{ss} = \#\Sigma$ of supersingular points on $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_\mathfrak{p}$:

Corollary 4.2. *We have the formula*

$$N^{ss} = \frac{2}{(2\pi)^d} d_F^{3/2} \zeta_F(2) h(F) \Phi(\mathfrak{D}) \Psi(\mathfrak{N}) + \frac{1}{2} \sum_R ([R^\times : \mathbb{Z}_F^\times] - 1) \frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]} \prod_\mathfrak{q} m_\mathfrak{q}(R, \mathcal{O}).$$

PROOF. This is the formula for the number of (right or left) $\mathcal{O}'$-ideal classes in B', see Vignéras [Vig80, §V.2]. □

Now we look at the field of definition of these supersingular points.

Theorem 4.3. *Suppose that* $\mathfrak{p} = (p)$ *is principal. Then the supersingular points of* $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_q$ *are defined over* $\mathbb{F}_{q^2}$*.*

PROOF. We use results of Carayol [Car86, § 11], but see also Jarvis [Jar04, § 2] for a summary of relevant results. Let $\hat{\alpha}$ be such that $(\hat{\alpha})_\mathfrak{p} = \pi_\mathfrak{p}$ and $(\hat{\alpha})_\mathfrak{q} = 1$ at $\mathfrak{q} \neq \mathfrak{p}$. We denote the reduction modulo $\mathfrak{p}$ of a point $[\tau, \hat{b}] \in X(\hat{\mathcal{O}}^\times)$ by $\overline{[\tau, \hat{b}]}$. The Frobenius $\mathrm{Frob}_\mathfrak{p}$

acts on Σ like the Atkin-Lehner operator $\hat{w}(\mathfrak{p})$, hence $\mathrm{Frob}_{\mathfrak{p}}^2$ acts by $\overline{[\tau,\hat{b}]} \mapsto \overline{[\tau,\hat{b}\hat{\alpha}]}$. By hypothesis $\mathfrak{p}=(p)$, therefore $p^{-1}\hat{\alpha}=\hat{\beta}\in\hat{\mathbb{Z}}_F^\times\subset\hat{\mathcal{O}}^\times$. So for all $\overline{[x,\hat{b}]}\in\Sigma$ we have

$$\begin{aligned}
\mathrm{Frob}_{\mathfrak{p}}^2(\overline{[\tau,\hat{b}]}) &= \overline{[\tau,\hat{b}\hat{\alpha}]} \\
&= \overline{[\tau,\hat{b}p\hat{\beta}]} \\
&= \overline{[\tau,p\hat{b}]} && \text{since } p\in F^\times \text{ is in the center of } \hat{B}^\times \text{ and } \hat{\beta}\in\hat{\mathcal{O}}^\times \\
&= \overline{[p^{-2}\tau,\hat{b}]} && \text{since } p\in B^\times \\
&= \overline{[\tau,\hat{b}]} && \text{since } p^{-2}\in F^\times \text{ acts trivially on } \mathcal{H}^\pm.
\end{aligned}$$

Hence we see that the action of $\mathrm{Frob}_{\mathfrak{p}}^2$ on Σ is trivial, which means that the supersingular points are $\mathbb{F}_{q^2}$-rational. □

Remark 4.4. The proof also shows that the Atkin-Lehner operator $\hat{\omega}(\mathfrak{p})$ on $X(\hat{\mathcal{O}}^\times)$ is an involution when $\mathfrak{p}$ is principal.

Let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$, and let $f_{\mathfrak{p}}$ be the inertia degree of $\mathfrak{p}$ in F_∞. After reduction of (4), we obtain that the curve $\overline{\mathrm{Sh}}(\mathfrak{N})\times\mathbb{F}_{\mathfrak{P}}$ is the disjoint union of $h_\infty/f_{\mathfrak{p}}$ copies of

$$\bigsqcup_{\overline{\sigma}\in\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/F_{\mathfrak{p}})} \overline{\mathrm{Sh}_0^+}(\mathfrak{N})^{\overline{\sigma}}.$$

If we assume that $f_{\mathfrak{p}}=1$, or equivalently that $\mathfrak{p}$ is totally split in F_∞, then $\overline{\mathrm{Sh}}(\mathfrak{N})$ is isomorphic over $\mathbb{F}_q$ to h_∞ copies of the curve $\overline{\mathrm{Sh}_0^+}(\mathfrak{N})$. Therefore $\overline{\mathrm{Sh}_0^+}(\mathfrak{N})\times_{\mathbb{F}_q}\overline{\mathbb{F}}_q$ contains N^{ss}/h_∞ supersingular points, which are defined over $\mathbb{F}_{q^2}$ by Proposition 4.3.

Let g be the genus of $\overline{\mathrm{Sh}_0^+}(\mathfrak{N})$ and N_r the number of $\mathbb{F}_{q^r}$-rational points of $\overline{\mathrm{Sh}_0^+}(\mathfrak{N})$. From Theorem (17), (15) and Corollary 4.2, we have

$$\begin{aligned}
N_{2r}/(g-1) \geqslant \frac{N^{ss}/h_\infty}{g-1} &\geqslant \frac{2(2\pi)^{-2d}d_F^{3/2}\zeta_F(2)h/h_\infty\Phi(\mathfrak{D}\mathfrak{p})\Psi(\mathfrak{N})}{4\pi(2\pi)^{-2d-1}d_F^{3/2}\zeta_F(2)h/h_\infty\Phi(\mathfrak{D})\Psi(\mathfrak{N})} \\
&= \mathrm{N}(\mathfrak{p})-1.
\end{aligned}$$

Taking $r=1$, we obtain the following result, whose first part thus admits a second proof.

Theorem 4.5. *Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_F$ such that $[\mathfrak{p}]=0$ in $\mathrm{Cl}_\infty(F)$, and let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$. Consider a sequence $(X_0^+(\mathfrak{N}_i))_{i\geqslant 0}$ of Shimura curves defined over F_∞ with respect to a quaternion algebra B_i/F of discriminant $\mathfrak{D}_i$. Assume that, for every index i, the prime $\mathfrak{p}$ does not divide $\mathfrak{D}_i\mathfrak{N}_i$, and that $\lim_{i\to\infty} g(X_0^+(\mathfrak{N}_i))=+\infty$. Then:*

- *i) for every i, the curve $\mathrm{Sh}_0^+(\mathfrak{N}_i)$ has good reduction at $\mathfrak{P}$, and the sequence $(\overline{\mathrm{Sh}_0^+}(\mathfrak{N}_i))_i$ is asymptotically optimal over the finite field $\mathbb{F}_{q^2}$;*
- *ii) asymptotically, all the $\mathbb{F}_{q^2}$-rational points in the sequence are supersingular, relative to the genus:*

$$\lim_{i\to\infty}\frac{N_2(\mathrm{Sh}_0^+(\mathfrak{N}_i))}{g(\mathrm{Sh}_0^+(\mathfrak{N}_i))} = \frac{N^{ss}(\mathrm{Sh}_0^+(\mathfrak{N}_i))}{g(\mathrm{Sh}_0^+(\mathfrak{N}_i))} = q-1.$$

PROOF. This is a consequence of the Drinfel'd-Vlăduţ theorem. □

5 Recursive towers

Following the approach of Elkies [Elk98a] in the elliptic modular case, we now want to interpret sequences of Shimura curves as recursive towers. Let $\mathfrak{n}$ be an integral ideal of F, relatively prime to $\mathfrak{D}\mathfrak{N}$ and generated by a totally positive element $n \in \mathbb{Z}_F$. Then for $i \geqslant 1$, we have an Atkin-Lehner operator $w_i = w(\mathfrak{n}^i)$ on $X_0^+(\mathfrak{N}\mathfrak{n}^i)$. If $i \geqslant 2$, we consider two maps from $X_0^+(\mathfrak{N}\mathfrak{n}^i)$ to $X_0^+(\mathfrak{N}\mathfrak{n}^{i-1})$: the projection map $\pi_0^{(i)}$, and the map $\pi_1^{(i)}$ defined by

$$\pi_1^{(i)} = w_{i-1} \circ \pi_0^{(i)} \circ w_i.$$

Proposition 5.1. *If $i \geqslant 3$, then the following diagram is commutative:*

$$\begin{array}{ccc} X_0^+(\mathfrak{N}\mathfrak{n}^i) & \xrightarrow{\pi_1^{(i)}} & X_0^+(\mathfrak{N}\mathfrak{n}^{i-1}) \\ {\scriptstyle \pi_0^{(i)}}\downarrow & & \downarrow{\scriptstyle \pi_0^{(i-1)}} \\ X_0^+(\mathfrak{N}\mathfrak{n}^{i-1}) & \xrightarrow[\pi_1^{(i-1)}]{} & X_0^+(\mathfrak{N}\mathfrak{n}^{i-2}) \end{array}$$

PROOF. Write $\mathfrak{N} = \prod_{\mathfrak{p}} \mathfrak{p}^{N_{\mathfrak{p}}}$ and $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$. We consider the Atkin-Lehner operators $\hat{w}_i$ relative to the adeles $\hat{\alpha}_i$ defined locally at $\mathfrak{p} \nmid \mathfrak{D}$ by

$$(\hat{\alpha}_i)_{\mathfrak{p}} = \begin{pmatrix} \pi_{\mathfrak{p}}^{in_{\mathfrak{p}}} & -1 \\ \pi_{\mathfrak{p}}^{N_{\mathfrak{p}}+in_{\mathfrak{p}}} & \pi_{\mathfrak{p}}^{in_{\mathfrak{p}}} \end{pmatrix} \in B_{\mathfrak{p}} \cong \mathrm{M}_2(F_{\mathfrak{p}}),$$

and at $\mathfrak{p} \mid \mathfrak{D}$ by $(\hat{\alpha}_i)_{\mathfrak{p}} = 1$. The operator w_i on $X_0^+(\mathfrak{N}\mathfrak{n}^i)$ is the restriction of $\hat{w}_i$ from $X(\mathfrak{N}\mathfrak{n}^i)$ to $X_0^+(\mathfrak{N}\mathfrak{n}^i)$ (see § 2). At a prime $\mathfrak{p} \mid \mathfrak{D}$, we have

$$(\hat{\alpha}_i\hat{\alpha}_{i-1})_{\mathfrak{p}} = (\hat{\alpha}_{i-1}\hat{\alpha}_{i-2})_{\mathfrak{p}} = 1.$$

Suppose now that $\mathfrak{p} \nmid \mathfrak{D}$. For every $i \geqslant 3$, let

$$U_{i,i-1} = \begin{pmatrix} \pi_{\mathfrak{p}}^{n_{\mathfrak{p}}(i+i-1)} & 0 \\ 2\pi_{\mathfrak{p}}^{N_{\mathfrak{p}}+n_{\mathfrak{p}}(i+i-1)} & \pi_{\mathfrak{p}}^{n_{\mathfrak{p}}(i+i-1)} \end{pmatrix}$$

and

$$V_{i,i-1} = \begin{pmatrix} \pi_{\mathfrak{p}}^{N_{\mathfrak{p}}+(i-1)n_{\mathfrak{p}}} & \pi_{\mathfrak{p}}^{in_{\mathfrak{p}}} + \pi_{\mathfrak{p}}^{(i-1)n_{\mathfrak{p}}} \\ 0 & \pi_{\mathfrak{p}}^{N_{\mathfrak{p}}+in_{\mathfrak{p}}} \end{pmatrix}.$$

Then

$$(\hat{\alpha}_i)_{\mathfrak{p}}(\hat{\alpha}_{i-1})_{\mathfrak{p}} = U_{i,i-1} - V_{i,i-1} = \pi_{\mathfrak{p}}^{2n_{\mathfrak{p}}} U_{i-1,i-2} - \pi_{\mathfrak{p}}^{n_{\mathfrak{p}}} V_{i-1,i-2} \in B_{\mathfrak{p}}.$$

Now $\pi_{\mathfrak{p}} \in \mathbb{Z}_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}$, so

$$(\hat{\alpha}_i)_{\mathfrak{p}}(\hat{\alpha}_{i-1})_{\mathfrak{p}} = U_{i-1,i-2} - V_{i-1,i-2} = (\hat{\alpha}_{i-1})_{\mathfrak{p}}(\hat{\alpha}_{i-2})_{\mathfrak{p}} \in B_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}.$$

Therefore

$$(\hat{\alpha}_i)_{\mathfrak{p}}(\hat{\alpha}_{i-1})_{\mathfrak{p}} = (\hat{\alpha}_{i-1})_{\mathfrak{p}}(\hat{\alpha}_{i-2})_{\mathfrak{p}} \in B_{\mathfrak{p}}^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times},$$

and more generally

$$\hat{\alpha}_i\hat{\alpha}_{i-1} = \hat{\alpha}_{i-1}\hat{\alpha}_{i-2} \in \hat{B}^{\times}/\hat{\mathcal{O}}^{\times}.$$

Hence by restriction to $X_0^+(\mathfrak{N}\mathfrak{n}^i)$, we obtain an equality

$$\pi_0^{(i-1)} \circ w_{i-1} \circ \pi_0^{(i)} \circ w_i = w_{i-2} \circ \pi_0^{(i-1)} \circ w_{i-1} \circ \pi_0^{(i)},$$

whence the result. □

Let $C_1 = X_0^+(\mathfrak{Nn})$ and $C_2 = X_0^+(\mathfrak{Nn}^2)$, and for $i \geqslant 3$ let C_i be the fibre product

$$C_i = X_0^+(\mathfrak{Nn}^{i-1}) \times_{X_0^+(\mathfrak{Nn}^{i-2})} X_0^+(\mathfrak{Nn}^{i-1})$$

with respect to the maps $\pi_1^{(i-1)}$ and $\pi_0^{(i-1)}$. By Proposition 5.1 and the universal property of the fibre product, when $i \geqslant 3$ there exists a unique morphism $\Psi : X_0^+(\mathfrak{Nn}^i) \to C_i$ and projection maps $p_1, p_2 : C_i \to X_0^+(\mathfrak{Nn}^{i-1})$ such that we obtain the commutative diagram

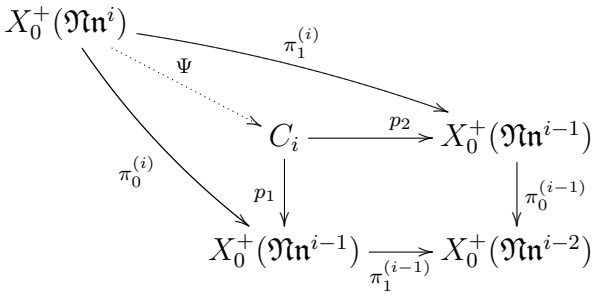


Diagram 1: The correspondence $X_0^+(\mathfrak{Nn}^i)$.

The map Ψ is a morphism of curves, hence it is surjective because $\pi_0^{(i)}$ is not constant. The maps p_1, p_2, $\pi_0^{(i)}$ and $\pi_1^{(i)}$ have the same degree $\mathrm{N}(\mathfrak{n})$, hence Ψ has degree 1 and is thus an isomorphism. Therefore, for every $i \geqslant 1$, we have a canonical isomorphism

$$X_0^+(\mathfrak{Nn}^i) \cong C_i,$$

so for every $i \geqslant 3$, the curve $X_0^+(\mathfrak{Nn}^i)$ is equal to the $(i-2)$-th iteration of the correspondence $X_0^+(\mathfrak{Nn}^3)$:

$$X_0^+(\mathfrak{Nn}^i) \cong X_0^+(\mathfrak{Nn}^3) \times_{X_0^+(\mathfrak{Nn}^2)} X_0^+(\mathfrak{Nn}^3) \times_{X_0^+(\mathfrak{Nn}^2)} \cdots \times_{X_0^+(\mathfrak{Nn}^2)} X_0^+(\mathfrak{Nn}^3).$$

By Milne [Mil05, Theo. 13.6], all the maps in Diagram 1 descend to maps over F_∞, so we see that the isomorphism $X_0^+(\mathfrak{Nn}^i) \cong C_i$ induces an isomorphism of the models over F_∞:

$$\mathrm{Sh}_0^+(\mathfrak{Nn}^i) \cong \mathrm{Sh}_0^+(\mathfrak{Nn}^{i-1}) \times_{\mathrm{Sh}_0^+(\mathfrak{Nn}^{i-2})} \mathrm{Sh}_0^+(\mathfrak{Nn}^{i-1}).$$

By reducing modulo a prime $\mathfrak{P}$ of F_∞ above a prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{Nn}$, this isomorphism descends to an isomorphism over $F_\mathfrak{P}$:

$$\overline{\mathrm{Sh}_0^+}(\mathfrak{Nn}^i) \cong \overline{\mathrm{Sh}_0^+}(\mathfrak{Nn}^{i-1}) \times_{\overline{\mathrm{Sh}_0^+}(\mathfrak{Nn}^{i-2})} \overline{\mathrm{Sh}_0^+}(\mathfrak{Nn}^{i-1}).$$

The following theorem is a consequence of the above discussion and Theorem 3.9 and Theorem 4.5.

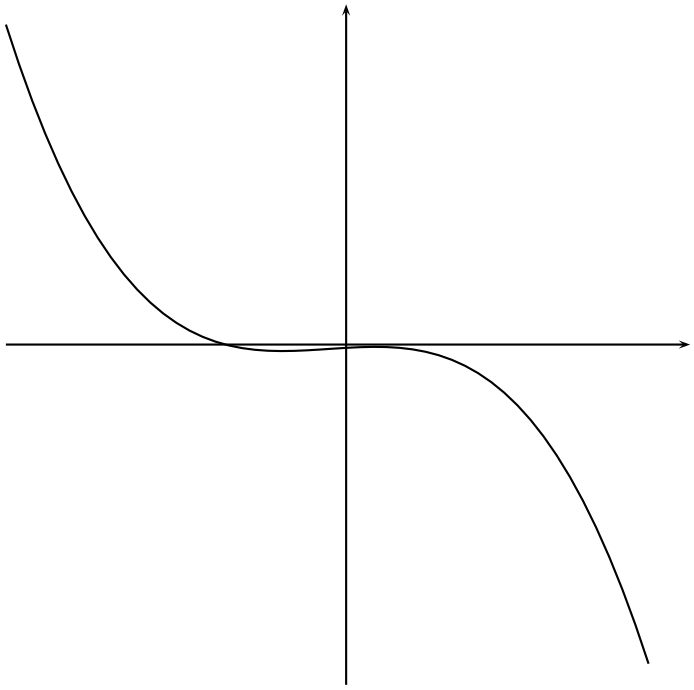
Theorem 5.2. *Let $\mathfrak{n}$ be an ideal of $\mathbb{Z}_F$ relatively prime to $\mathfrak{DN}$. Let $\mathfrak{p} \nmid \mathfrak{DNn}$ be a prime of $\mathbb{Z}_F$ and let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$. Let $\bar{\cdot}$ denote reduction modulo $\mathfrak{P}$. The curves $\overline{\mathrm{Sh}_0^+}(\mathfrak{Nn}^i)$ form a recursive tower over $\mathbb{F}_\mathfrak{P}$. If furthermore $[\mathfrak{p}] = 0$ in $\mathrm{Cl}_\infty(F)$, the tower is optimal over the quadratic extension of $\mathbb{F}_\mathfrak{p}$.*

Based on Ihara's results, Elkies proved this proposition for modular curves using the moduli interpretation of theses curves (see Elkies [Elk98a]), and extended his results to Shimura curves over $\mathbb{Q}$ (see Elkies [Elk98b, § 2.3]). However the moduli interpretation of Shimura curves when $F \neq \mathbb{Q}$ is much more complicated, and doesn't allow a direct generalization of Elkies's method.

Example 5.3. I am very grateful to John Voight for computing the following example. Let F be the totally real field of degree 3 over $\mathbb{Q}$ with discriminant 148 and defining equation $P(X) = X^3 - 3X^2 - X + 1$. Note that F has narrow class number $h_\infty = 1$. Let B be the unique quaternion algebra of discriminant $\mathbb{Z}_F$ over F (up to F-isomorphism), and let $\mathfrak{N} = \mathfrak{p}$ be the prime of $\mathbb{Z}_F$ above 2. Consider the Shimura curve $X_0(\mathfrak{p}) = X_0^1(\mathfrak{p}) = X_0^+(\mathfrak{p})$. It has genus 0 and is a covering of $X_0(1) = \mathbb{P}_F^1(j_0)$ of equation

$$j_0 = (702a^2 - 486a - 2268)j_1^3 + (486a^2 - 324a - 1566)j_1^2 + (-702a^2 + 486a + 2241)j_1 - 486a^2 + 324a + 1593,$$

where a is a root of $P(X) = 0$.



The Shimura curve $X_0^+(\mathfrak{p})$.

The curve $X_0^+(\mathfrak{p}^2)$ has defining equation $\Phi_2(j_1, j_2) = 0$, where Φ_2 is equal to

$$\Phi_2(j_1, j_2) = 23(j_1^2 j_2^2) + (2a^2 - 20a - 10)j_1 j_2 (j_1 + j_2) + (14a^2 - 2a - 24)(j_1^2 + j_1 j_2 + j_2^2).$$

The Atkin-Lehner operators on $X_0^+(\mathfrak{p})$ and $X_0^+(\mathfrak{p}^2)$ are respectively given by

$$w_1(j_1) = 1/j_1$$

and

$$w_2(j_1, j_2) = (j_2, j_1).$$

Therefore Diagram 1 implies that $X_0^+(\mathfrak{p}^3)$ is defined by

$$\Phi_2(1/j_2, j_3) = 0.$$

More generally, for $i \geqslant 2$, the curve $X_0^+(\mathfrak{p}^{i+1}) = \mathbb{P}^1(j_0, j_1, j_2, \ldots, j_{i+1})$ is recursively defined by

$$\Phi_2(1/j_i, j_{i+1}) = 0.$$

We gather below numerical data for $\mathrm{Sh}_0^+(\mathfrak{p}^i)$ for $i = 3, 4, 5$. We consider reduction modulo a prime $\mathfrak{q} \neq \mathfrak{p}$. The computations have been performed using Magma [BCP97].

i	$g(\mathrm{Sh}_0^+(\mathfrak{p}^i))$	$\#\mathrm{Sh}_0^+(\mathfrak{p}^i)(\mathbb{F}_q)$	$\#\mathrm{Sh}_0^+(\mathfrak{p}^i)(\mathbb{F}_{q^2})$	$\mathrm{Tr}(\mathrm{T}(\mathfrak{q}))$	$\mathrm{Tr}(\mathrm{T}(\mathfrak{q}^2))$
3	1	8	160	6	36
4	3	8	140	6	56
5	5	8	120	6	76

Table 1: Number of points and traces of Hecke operators, for $\mathfrak{q}$ such that $\mathrm{N}(\mathfrak{q}) = 13$.

i	$g(\mathrm{Sh}_0^+(\mathfrak{p}^i))$	$\#\mathrm{Sh}_0^+(\mathfrak{p}^i)(\mathbb{F}_q)$	$\#\mathrm{Sh}_0^+(\mathfrak{p}^i)(\mathbb{F}_{q^2})$	$\mathrm{Tr}(\mathrm{T}(\mathfrak{q}))$	$\mathrm{Tr}(\mathrm{T}(\mathfrak{q}^2))$
3	1	24	672	2	4
4	3	24	764	2	-88
5	5	24	856	2	-180

Table 2: Number of points and traces of Hecke operators, for $\mathfrak{q}$ such that $\mathrm{N}(\mathfrak{q}) = 25$.

References

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

[BBGS12] Alp Bassa, Peter Beelen, Arnaldo Garcia, and Henning Stichtenoth. Towers of Function Fields over Non-prime Finite Fields. 2012. Available at "arXiv:1202.5922".

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Car86] Henri Carayol. Sur la mauvaise réduction des courbes de Shimura. *Compositio Math.*, 59(2):151–230, 1986.

[Cla03] Pete L. Clark. *Rational points on Atkin-Lehner quotients of Shimura curves*. PhD thesis, Harvard University, 2003.

[Cla05] Pete L. Clark. Course notes on Shimura curves, 2005. Available at `http://www.math.uga.edu/~pete/expositions2012.html`.

[Del71] Pierre Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, pages 123–165. Lecture Notes in Math., Vol. 244. Springer, Berlin, 1971.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[DLV] Peter Doyle, Benjamin Linowitz, and John Voight. The smallest isospectral and nonisometric orbidolds of dimension 2 and 3. In preparation.

[DV12] Lassana Dembelé and John Voight. Explicit methods for Hilbert modular forms. 2012. Available at "arXiv:1010.5727".

[Elk98a] Noam D. Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997, T. Basar, A. Vardy, eds.)*, pages 23–32. Univ. of Illinois at Urbana-Champaign, 1998. Available at "arXiv:math.NT/0103107".

[Elk98b] Noam D. Elkies. Shimura curve computations. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 1–47. Springer, Berlin, 1998. Available at "arXiv:math/0005160".

[Elk01] Noam D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198. Birkhäuser, Basel, 2001. Available at "arXiv:math/0005140".

[Gop77] V. D. Goppa. Codes that are associated with divisors. *Problemy Peredači Informacii*, 13(1):33–39, 1977.

[GV11] Matthew Greenberg and John Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. *Math. Comp.*, 80(274):1071–1092, 2011. Available at "arXiv:0904.3908".

[Hid81] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[Hid06] Haruzo Hida. *Hilbert modular forms and Iwasawa theory*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, Oxford, 2006.

[Hij74] Hiroaki Hijikata. Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$. *J. Math. Soc. Japan*, 26:56–82, 1974.

[HSY93] Hiroaki Hijikata, Hiroshi Saito, and Masatoshi Yamauchi. Representations of quaternion algebras over local fields and trace formulas of Hecke operators. *J. Number Theory*, 43(2):123–167, 1993.

[Iha67] Yasutaka Ihara. Hecke Polynomials as congruence ζ functions in elliptic modular case. *Ann. of Math. (2)*, 85:267–295, 1967.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[Ish73] Hirofumi Ishikawa. On the trace formula for Hecke operators. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:217–238, 1973.

[Jar04] Frazer Jarvis. Correspondences on Shimura curves and Mazur's principle at p. *Pacific J. Math.*, 213(2):267–280, 2004.

[JL85] Bruce W. Jordan and Ron A. Livné. Local Diophantine properties of Shimura curves. *Math. Ann.*, 270(2):235–248, 1985.

[Kat92] Svetlana Katok. *Fuchsian groups*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[LMSE02] Wen-Ching W. Li, Hiren Maharaj, Henning Stichtenoth, and Noam D. Elkies. New optimal tame towers of function fields over small finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 372–389. Springer, Berlin, 2002.

[Mil79] J. S. Milne. Points on Shimura varieties mod p. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 165–184. Amer. Math. Soc., Providence, R.I., 1979.

[Mil05] J. S. Milne. Introduction to Shimura varieties. In *Harmonic analysis, the trace formula, and Shimura varieties*, volume 4 of *Clay Math. Proc.*, pages 265–378. Amer. Math. Soc., Providence, RI, 2005.

[Mil11] J.S. Milne. Class field theory (v4.01), 2011. Available at `http://www.jmilne.org/math/`.

[Mil12] James S. Milne. Modular functions and modular forms (v1.30), 2012. Available at `http://www.jmilne.org/math/`.

[Miy06] Toshitsune Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

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

[Oes77] Joseph Oesterlé. *Sur la trace des opérateurs de Hecke*. PhD thesis, Université de Paris-Sud, Centre d'Orsay, 1977.

[Sai72] Hiroshi Saito. On Eichler's trace formula. *J. Math. Soc. Japan*, 24:333–340, 1972.

[Sai84] Hiroshi Saito. On an operator U_χ acting on the space of Hilbert cusp forms. *J. Math. Kyoto Univ.*, 24(2):285–303, 1984.

[Ser83a] Jean-Pierre Serre. Nombres de points des courbes algébriques sur $\mathbf{F}_q$. In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.

[Ser83b] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.

[Shi62] Goro Shimura. On Dirichlet series and abelian varieties attached to automorphic forms. *Ann. of Math. (2)*, 76:237–294, 1962.

[Shi65] Hideo Shimizu. On zeta functions of quaternion algebras. *Ann. of Math. (2)*, 81:166–193, 1965.

[Shi67] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Shi98] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[Shi10] Goro Shimura. *Arithmetic of quadratic forms*. Springer Monographs in Mathematics. Springer, New York, 2010.

[Sij10] Jeroen Sijsling. *Equations for arithmetic pointed tori*. PhD thesis, Universiteit Utrecht, 2010.

[SY04] Alexei Skorobogatov and Andrei Yafaev. Descent on certain Shimura curves. *Israel J. Math.*, 140:319–332, 2004.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

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

[Voi] John Voight. *The arithmetic of quaternion algebras*. In preparation.

[Voi09] John Voight. Shimura curves of genus at most two. *Math. Comp.*, 78(266):1155–1172, 2009. Available at "arXiv:0802.0911".

[VW13] John Voight and John Willis. Computing power series expansions of modular forms. *accepted to "Computations with modular forms"*, 2013.

[Wei60] André Weil. Algebras with involutions and the classical groups. *J. Indian Math. Soc. (N.S.)*, 24:589–623 (1961), 1960.

[Zha01] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001. Available at "arXiv:math/0101269".