AIX-MARSEILLE UNIVERSITÉ
Faculté des sciences de Luminy

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE E.D. 184

INSTITUT DE MATHÉMATIQUES DE LUMINY

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ D'AIX-MARSEILLE

Spécialité : Mathématiques

par

Virgile DUCET

Titre:

CONSTRUCTION OF ALGEBRAIC CURVES WITH MANY RATIONAL POINTS OVER FINITE FIELDS

soutenue publiquement le 23 septembre 2013
devant un jury composé de

Directeur

David R. KOHEL, professeur — Université d'Aix-Marseille

Rapporteurs

Everett HOWE, chercheur — Center for Communications Research
John VOIGHT, professeur associé — Dartmouth College

Examinateurs

Gilles LACHAUD, directeur de recherche émérite — CNRS IML
Marc PERRET, professeur — Université Toulouse 2
Christophe RITZENTHALER, professeur — Université Rennes 1
François RODIER, directeur de recherche — CNRS IML
René SCHOOF, professeur — Università di Roma Tor Vergata

To the one who stole my proof of the Riemann hypothesis[1]

[1] Give it back to me!

Arithmetic is being able to count up to twenty without taking off your shoes.

Mickey Mouse

FOREWORD

Remerciements

L'aboutissement de la thèse après le pot, enfin, les remerciements ! En réalité je pensais zapper cette section, mais Stéphane Louboutin, en farouche défenseur des protocoles sociaux, m'a convaincu de m'y soumettre.

Précision importante : le texte qui suit comporte un grand nombre d'occurences du mot "merci"[2]. Cependant, le lecteur socialement plus adapté au monde d'aujourd'hui que le mathématicien moyen est encouragé à remplacer ce terme par "high five".

Tout d'abord je tiens à exprimer ma gratitude à David Kohel pour avoir accepté d'encadrer cette thèse, pour sa patience lorsque je cherchais ma voie, et pour sa grande disponibilité. Il restera une source d'inspiration pour sa rigueur et la profondeur de son approche des mathématiques.[3]

Je suis très heureux qu'Everett Howe et John Voight aient accepté de rapporter ma thèse. Je souhaite ici les en remercier ainsi que leur exprimer ma reconnaissance pour l'intérêt qu'ils ont témoigné pour mes travaux, ainsi que de la grande disponibilité dont ils ont fait preuve.

Merci beaucoup également à Gilles Lachaud, Marc Perret, Christophe Ritzenthaler, François Rodier et René Schoof de me faire le plaisir de faire partie de ce jury, ainsi que pour leur aide amicale lorsque j'en ai eu besoin.

Je suis très reconnaissant à David Kohel, Everett Howe, John Voight, Jeroen Sijsling et Hamish Ivey-Law pour leurs relectures qui ont permis de grandement améliorer la qualité de cette thèse [4]. En particulier, un grand merci à John Voight et Jeroen Sijsling pour avoir, avec une patience infinie, répondu à mes innombrables questions sur les courbes de Shimura, comme en témoigneront aisément leur boîte de spams et la création d'un filtre adapté.

Travailler dans l'équipe ATI a été un véritable plaisir tant l'atmosphère y est bonne et le cadre scientifique stimulant. Merci donc à Yves Aubry, Christophe Ritzenthaler, Serge Vlăduţ, Gilles Lachaud, Michel Laurent, François Rodier, Stéphane Ballet, David Kohel, Stéphane Louboutin, ainsi qu'à Alexis Bonnecaze, Robert Rolland, Mireille Car, Michel Balazard et Pascal Véron pour avoir contribué à rendre mes années de thèse épanouissantes.

Les conditions de vie et de travail sont excellentes à Luminy et un grand mérite en revient à Aurélia et Éric Lozingot, Corinne Roux et Jean-Bruno Erismann, qui font vivre le laboratoire avec compétence et bonne humeur. C'est une magnifique opportunité d'avoir le CIRM à

[2] Dont la sincérité est conditionnée par l'obtention de mon diplôme.

[3] Par contre c'est un bavard invétéré, un "yes" par ci, un "ok" par là, impossible d'en placer une !

[4] Notamment pour m'avoir fait remarquer que l'on n'écrit pas "well well" en anglais, contrairement à une croyance populaire largement répandue.

cinq minutes du labo, en particulier sa bibliothèque, où l'aide de Nathalie Granottier et Fabienne Grosjean notamment, pour commander/retrouver un ouvrage de nécromancie mathématique m'aura été très utile. Merci à tous, j'espère avoir l'occasion de travailler dans des environnements de la même qualité dans le futur.

Toutes ces années ont été l'occasion de faire la rencontre de beaucoup de gens qui, modulo le fait qu'ils soient mathématiciens, peuvent être qualifiés de "très sympathiques". La liste est longue, mais je tiens à citer Ben "Drop Bear" Smith, Philippe Lebacque, Alexey Zykin, Alain Couvreur, Marc Perret, Emmanuel Hallouin, Damien Robert, Marc-Hubert Nicole, et les membres des projets CHIC et PEACE, pour leur aide ou pour avoir partagé des conversations, certaines sérieuses, et d'autres (l'écrasante majorité) pas du tout. Merci en particulier à Claus Fieker pour sa collaboration à ce qui restera mon premier article.

Le FQRNT m'a donné l'occasion d'effectuer un stage de cinq mois à Montréal ; je leur en suis très reconnaissant, ainsi qu'à Henri Darmon pour son accueil chaleureux et sa grande disponibilité. Merci aussi aux étudiants de McGill pour leur patience vis-à-vis de mon franglais, notamment Bahare, à Frédéric pour son hospitalité, et à Antoine pour des retouvailles "Ciel et Marine" bien agréables.

Ce furent quatre années fort plaisantes ma foi, et la bonne compagnie n'a pas manqué. Je tiens donc à adresser mes plus sincères remerciements[5] à turtle bob, rox et rouki, donald, mickey, sunshine 1 et sunshine 2 le retour, fioufiou "pas besoin de manger, il reste de la Guiness", fanfan le quinoa en folie, tof "on fait quoi ce huik-end ?" et Haïfa "écoute-moi", monsieur poivrons au four fournisseur officiel local de wikipédia, Florent l'unique fan d'André-Pierre Gignac sur Terre, Yih-Dar "ohlala !", Tammam "oui oui je viens ce soir, c'est sûr", pierrot la houpette, désireless, chéchile, le moustachu repenti, tortilla, Irène "j'ai mal à la rorge", Mila le dégommeur de pigeons, youyou tête de fromage, Yves ou le seul fan de Lio en liberté, Stéphane notre parrain de la pègre local très phlébiscité dans le labo, Hamish notre diable de Tasmanie fan de métal dit "hardcore" type Justin Bieber, floflo le courbeur de surfaces et sa douce râleuse miss banofee, pour des moments autant cocasses que saugrenus, à l'occasion d'un road trip californien très "simão", d'un petit déjeuner prolongé en un déjeuner puis un goûter avant d'enfin passer au sémibière[6] pour clôturer une grosse journée, d'un foot bien dynamique où les pseudo-bons tirs de donald déclenchèrent quelques hilarités, de même que les sautes d'humeur de rouki durant les parties de cartes où il avait mal (mais alors VRAIMENT MAL !!!!) joué, et lamentablement perdu. Beaucoup auront aussi partagé des conférences/vacances organisées, merci à eux pour la bonne atmosphère qu'ils auront largement contribué à instaurer.

Merci aux camarades de ma bourgade du Havre au cours de ces années passées du côté obscur, en particulier les faqueux guigui, biboule, barquette, et le groupe des rugbymen du dimanche, et Anh Tuan, Pierre-Antoine, Adrien, Angélo et Thomas, compagnons de route depuis la lointaine période du lycée, période naïve où une despé, c'était une bière.

Merci à mon professeur de seconde M. Varlet pour m'avoir redonné le goût des maths et avoir éveillé en moi un attrait puissant et obscur pour le jeu de mot douteux, dont beaucoup

[5] Par ordre de préférence ?

[6] Que mes futurs employeurs se rassurent, ces "sémibières" ne consistaient qu'en des réunions austères où nous partagions nos connaissances mathématiques autour d'un verre de bière sans alcool ou de jus de fenouil 51, spécialité marseillaise bien connue.

des personnes sus-nommées ont fait les frais. Merci aussi aux professeurs de l'université du Havre pour leur encadrement et pour m'avoir permis d'apprendre de jolies choses dans un environnement agréable et ensoleillé[7], en particulier M. Panos pour ses encouragements lors de ce périlleux apprentissage qu'est la recherche.

Rentrer en famille m'a toujours permis de recharger les batteries et de retrouver une bulle apaisante et salvatrice pour mieux repartir...mais bon, il faut bien qu'elle serve à quelque chose !

J'ai peut-être oublié des gens lors de ces remerciements, toutes mes excuses. Je leur propose d'attendre quelques années et d'utiliser une machine à remonter le temps pour me faire part de mon omission (sortie prévue en même temps que le sabre laser selon les dernières prévisions de Paco Rabanne). Si cette thèse est inchangée au moment de la soutenance, cela tendrait toutefois à prouver que le sabre laser a pris du retard dans sa commercialisation, ce qui me navre profondément.

Enfin merci à toi, cher lecteur, d'exprimer suffisamment de compassion pour venir t'ennuyer ici avec moi. Tu viens de gagner... toute mon estime.

PREUVE.
Le résultat suit par récurrence, voir ma biographie[8] pour les détails. □

Merci de signaler toute erreur en envoyant un mail au service après-soutenance, joignable à l'adresse cettethesenecontientaucuneerreur@utopie.mdr.

[7] Plusieurs fois par jour et plusieurs fois par an ! True story !

[8] Écrite par Tolstoi et éditée chez Plomb.

Conventions

We use the standard notations $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$, $\mathbb{C}$ for the non-negative integers, the rational and p-adic integers, and the rational, p-adic, real and complex numbers respectively. Similarly, $\mathbb{F}_q$ is a finite field of cardinality q. If k is a field, then $\bar{k}$ is an algebraic closure of k.

By *global field*, we mean either a number field or a global function field, and by *non-archimedean* (respectively *archimedean*) *local field*, we mean the completion of a global field at a non-archimedean (respectively archimedean) place.

If F is a number field, we denote its ring of integers by $\mathbb{Z}_F$. For a prime $\mathfrak{p}$ of F, the completion (respectively localization) of $\mathbb{Z}_F$ at $\mathfrak{p}$ will be denoted by $\mathbb{Z}_{F,\mathfrak{p}}$ (respectively $\mathbb{Z}_{F,(\mathfrak{p})}$), with local uniformizer $\pi_\mathfrak{p}$, and $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_F/\mathfrak{p} = \mathbb{Z}_{F,\mathfrak{p}}/(\pi_\mathfrak{p})$ will be the residue field at $\mathfrak{p}$, of cardinality $\mathrm{N}(\mathfrak{p})$. For any $\mathbb{Z}_F$-module M, the completion of M at $\mathfrak{p}$, which is isomorphic to $M \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$, will be denoted $M_\mathfrak{p}$. For instance, $F_\mathfrak{p}$ is the completion of F at $\mathfrak{p}$.

For a global function field, we use the notation K, and let $\mathrm{Pl}(K)$ be the set of places of K and U_K be the group of units in K. In this case, P stands for a place, K_P for the completion of K at P, and $\mathbb{F}_P$ for the residue field of K at P, of cardinality $\mathrm{N}(P)$. We also use these notations for arbitrary global fields. The ring of adeles of K is denoted by

$$\mathbb{A}_K = \prod_{P \in \mathrm{Pl}(K)} K_P^\times.$$

Unless otherwise specified, a ring A is always associative and unitary with no zero divisors, and we let $A^\times$ be the multiplicative group of invertible elements of A. For instance, the group of invertible elements of $\mathbb{A}_K$ is the idele group $\mathcal{J}_K = \mathbb{A}_K^\times$. Concerning matrix groups, $\mathrm{M}_2(A)$ is the ring of 2×2 matrices with coefficients in A, $\mathrm{SL}_2(A)$ is the group of matrices with determinant 1 and $\mathrm{GL}_2(A)$ is the group of invertible matrices, with quotient $\mathrm{PGL}_2(A) = \mathrm{GL}_2(A)/A^\times$. We denote by $\mathrm{GL}_2^+(\mathbb{R})$ the group of real matrices with positive determinant, and $\mathrm{PGL}_2^+(\mathbb{R})$ its image in $\mathrm{PGL}_2(\mathbb{R})$. If A is commutative, we let $A[(X_i)_{i\in I}]$ be the polynomial ring in the indeterminates X_i with coefficients in A.

Let $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ be the completion of $\mathbb{Z}$. If G is an abelian group, $\hat{G}$ will denote the tensor product $G \otimes_\mathbb{Z} \hat{\mathbb{Z}}$ of $\mathbb{Z}$-modules.

We denote by

$$\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$$

the Poincaré upper half-plane. If Γ is a subgroup of $\mathrm{GL}_2^+(\mathbb{R})$ or $\mathrm{PGL}_2^+(\mathbb{R})$, then Γ acts by fractional linear transformations on $\mathcal{H}$, and we let $Y(\Gamma) = \Gamma\backslash\mathcal{H}$.

Unless explicitly specified, a *curve* C over a field k is a geometrically irreducible non-singular projective curve defined over k. We let $g(C)$ be its genus, and for every field extension k'/k, we set $C_{k'} = C \times_k k'$. The homology and cohomology groups of C with respect to a sheaf $\mathscr{F}$ are denoted $H_i(C, \mathscr{F})$ and $H^i(C, \mathscr{F})$ respectively, and if D is a divisor, the space of functions whose poles are bounded by D is the *Riemann-Roch space* of D, which we denote by $\mathcal{L}(D)$. The Jacobian of C will be denoted by $\mathrm{Jac}(C)$. If k is a number field F, we say that C has *good reduction* at a prime $\mathfrak{p}$ of $\mathbb{Z}_F$ if C admits a model over $\mathbb{Z}_{F,(\mathfrak{p})}$ whose reduction modulo $\mathfrak{p}$ is a non-singular projective curve $\overline{C}$ over $\mathbb{F}_\mathfrak{p}$.

CONTENTS

Foreword **v**

Remerciements v

Conventions viii

Introduction **1**

I Upper Bounds **4**

1 Weil conjectures 4

2 The Hasse-Weil-Serre bound 6

3 The Ihara bound 7

4 The Oesterlé bound 9

5 The Drinfel'd-Vlăduţ bound 11

II Explicit Abelian Coverings **15**

1 Class field theory 15

2 Explicit cyclic extensions 21

3 Computing abelian coverings 28

4 An algorithm to find curves with many points 33

5 Results 36

III Quaternion Algebras **40**

1 Quaternion algebras over a field 40

2 Quaternion algebras over local fields 43

3 Quaternion algebras over number fields 44

4 Arithmetic groups 52

IV Shimura Curves over Finite Fields **54**
1 Shimura curves 54
2 Modular forms and Hecke operators 57
3 The trace formula 67
4 Supersingular points 71
5 Recursive towers 73

Bibliography **78**

Notations **86**

INTRODUCTION

The study of polynomial equations over finite fields can be traced back to the eighteenth century, when Gauss attempted to count the number M_p of projective solutions of the equation

$$x^3 + y^3 + z^3 = 0 \tag{1}$$

over a finite field $\mathbb{F}_p$. His result that

$$M_p = p + 1 + A,$$

for some integer A satisfying $|A| < 2\sqrt{p}$, was the first example of a more general result discovered by Hasse in 1933, namely that the number of rational points on an elliptic curve E defined over a finite field $\mathbb{F}_q$ is given by

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

where t is an integer such that $|t| \leqslant 2\sqrt{q}$ (see, for example, Silverman and Tate [ST92, Chap. IV] for a discussion of these questions). Indeed, (1) is the equation of the *Fermat curve* of degree 3, which has genus 1. In 1948, Weil proved a more general result, known as the *Riemann hypothesis* for curves by analogy with the Riemann zeta function, that every curve defined over $\mathbb{F}_q$ satisfies

$$\#C(\mathbb{F}_q) = q + 1 - t$$

for an integer t satisfying $|t| \leqslant 2g\sqrt{q}$. This led Weil to formulate a series of conjectures, known as the *Weil conjectures*, which describe the behavior of the number of rational points of a (geometrically irreducible, non-singular, projective) variety $V/\mathbb{F}_q$ of any dimension over constant field extensions of $\mathbb{F}_q$ (see Theorem I.1.1 for precise statements). These conjectures played a great role in the development of algebraic geometry, until the proof by Deligne in 1974 of the higher dimensional analogue of the Riemann hypothesis using ℓ-adic cohomology.

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

$$\frac{k}{n} + \frac{d}{n} \geq 1 + \frac{1}{n} - \frac{g}{n}. \tag{2}$$

By construction, n is bounded by the number of rational points $N(C)$ of C, and from (2), 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] or [Ser85]). 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

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

In Chapter I we present some of the techniques which lead to better upper bounds on $N_q(g)$ and $A(q)$ than Weil's result. The results we present are standard, but recent works of Howe and Lauter ([HL03] and [HL12]) give refinements of the bounds in particular cases.

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. The purpose of this thesis is to carry out these two projects in some cases. For curves of small genus, the most efficient techniques to produce curves with many rational points come from class field theory (in addition to the above references, see for instance Auer [Aue99], Lauter [Lau99a] or Niederreiter and Xing [NX01]). We continue in this direction in Chapter II, and the results presented there represent joint work with Claus Fieker [DF13]. First we explain how to compute the abelian coverings of any curve defined over a finite field, by using explicit Kummer and Artin-Schreier-Witt theories. Subsequently we describe an algorithm to look for good curves and compute their equations. The implementation of this algorithm in Magma [BCP97] allowed us to discover new curves whose number of rational points improved the preceding lower bounds on $N_q(g)$ for $q = 2$ and $q = 3$, which are the most studied cases (see [HLRVdG] for the currently best known results). An important aspect of this approach is that we are able to exhibit equations for the 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 in the general case [Iha81], and Tsfasman, Vlăduţ and Zink in the cases $q = p^2$ or $q = p^4$ for a prime p [TVZ82], 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. In Chapter III we introduce all

the necessary background on quaternion algebras in order to study, in Chapter IV, 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]. Using totally different methods than the works quoted above, we study 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 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, 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.

I

UPPER BOUNDS

Let C be a curve defined over a finite field $\mathbb{F}_q$. The number of points of C over any finite field extension of $\mathbb{F}_q$ is described by the zeta function of the curve, whose behavior is predicted by the Weil conjectures. Weil was able to prove his conjectures for curves, and he derived the first general upper bound on the number of rational points C may have. Several improvements have been obtained since, the most notable one obtained by Serre, Ihara and Oesterlé in the beginning of the 1980s. Shortly after, Drinfel'd and Vlăduţ established a sharp upper bound for curves whose genus is asymptotically large. The aim of this chapter is to explain these results. Useful references are Serre [Ser85], Stichtenoth [Sti09] and Voight [Voi05].

1 Weil conjectures

Let V be a non-singular, geometrically irreducible, projective variety over a finite field $\mathbb{F}_q$. For every integer $n \geqslant 1$, let

$$N_n = N_n(V) = \#V(\mathbb{F}_{q^n}).$$

Following Weil, one encodes the numbers N_n in the *zeta function* of V:

$$Z(V;T) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right).$$

In 1949, Weil proposed a series of deep conjectures on the behaviour of $Z(V;T)$, still called the *Weil conjectures* even though they are now theorems.

Theorem 1.1 (Weil Conjectures). *Let V be a non-singular and geometrically irreducible projective variety of dimension d defined over $\mathbb{F}_q$.*

i) RATIONALITY
$Z(V;T)$ is a rational function:

$$Z(V;T) \in \mathbb{Q}(T).$$

ii) FUNCTIONAL EQUATION
There exists an integer χ such that

$$Z\left(V; \frac{1}{q^d T}\right) = \pm q^{d\chi/2} T^{\chi} Z(V;T).$$

iii) RIEMANN HYPOTHESIS
The zeta function factors as

$$Z(V;T) = \frac{P_1(T)\dots P_{2d-1}(T)}{P_0(T)\dots P_{2d}(T)},$$

with each $P_i(T) \in \mathbb{Z}[T]$, $P_0(T) = 1 - T$, $P_{2d}(T) = 1 - q^d T$, *and for every* $1 \leqslant i \leqslant 2d-1$ *the polynomial* $P_i(T)$ *factors over* $\overline{\mathbb{Q}}$ *as*

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \omega_{i,j}T), \text{ where } |\omega_{i,j}| = q^{i/2}.$$

Furthermore, $\chi = \sum_i^{2d}(-1)^i b_i$.

iv) BETTI NUMBERS
If V *is the reduction of a variety* W *defined over a number field* F, *then* b_i *is the* i*th Betti number of the variety* $W_{\mathbb{C}}$ *and* χ *is the Euler-Poincaré characteristic of* $W_{\mathbb{C}}$.

In this thesis, we are interested only in the case of curves. Hence with our conventions, if C is a curve of genus g we see that there exists a polynomial $P(T)$ such that the zeta function of C is a rational function of the form

$$Z(C;T) = \frac{P(T)}{(1-T)(1-qT)}.$$

The polynomial $P(T)$ is of degree $2g$ because every complex algebraic curve of genus g, hence any lift of C to a non-singular curve over $\mathbb{C}$, has Betti number $b_1 = 2g$. Moreover there exist algebraic integers ω_i, for $i = 1, ..., 2g$, such that $|\omega_i| = q^{1/2}$ and

$$P(T) = \prod_{i=1}^{2g}(1 - \omega_i T).$$

Example 1.2. Let $C = \mathbb{P}^1(\mathbb{F}_q)$ be the projective line over $\mathbb{F}_q$. For every $n \geqslant 1$ we have $N_n = q^n + 1$, so in this case the zeta function is easily computable:

$$Z(\mathbb{P}^1(\mathbb{F}_q), T) = \exp\left(\sum_{n=1}^{\infty}(q^n + 1)\frac{T^n}{n}\right) = \frac{1}{(1-T)(1-qT)}.$$

Note that

$$Z\left(\mathbb{P}^1(\mathbb{F}_q); \frac{1}{qT}\right) = \frac{1}{(1-\frac{1}{qT})(1-\frac{1}{T})} = qT^2 Z(\mathbb{P}^1(\mathbb{F}_q); T),$$

as predicted with $\chi = 2$. The Betti numbers $\dim_{\mathbb{Q}} H^i(\mathbb{P}^1(\mathbb{C}), \mathbb{Z})$ for $i = 0$, 1 and 2 are respectively equal to 1, 0 and 1, so for $C = \mathbb{P}^1(\mathbb{F}_q)$ the Weil conjectures are easily verified.

Corollary 1.3. *We have the formula:*

$$N_1 = q + 1 - \sum_{i=1}^{2g} \omega_i.$$

PROOF. From the definition of the zeta function, it is clear that

$$N_1 = \left.\frac{d(\log(Z(C;T)))}{dT}\right|_{T=0}.$$

On the other hand, the Riemann hypothesis implies that

$$\begin{aligned}\left.\frac{d(\log(Z(C;T)))}{dT}\right|_{T=0} &= q + 1 + P'(0)\\ &= q + 1 - \textstyle\sum_{i=1}^{2g} \omega_i,\end{aligned}$$

which gives the result. □

Let ω_i be a root of $P(T)$, and choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Since the polynomial $P(T)$ has integer coefficients, it is invariant under complex conjugation, hence we see that $\overline{\omega}_i$ is also a root of $P(T) = 0$. From now on we assume that the ω_i are ordered in such a way that $\omega_{i+g} = \overline{\omega}_i$ for all $i = 1, \ldots, g$. We set $\alpha_i = \omega_i + \bar{\omega}_i$, so

$$N_1 = q + 1 - \sum_{i=1}^{g} \alpha_i.$$

Remark 1.4. The formula in Corollary I.1.3 can be generalized to any integer $n \geqslant 1$ as follows:

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n. \tag{I.1}$$

This can be proved in a similar manner, but the computations are more complicated. Instead, one deduces the result from the cohomological interpretation of the Weil conjectures, for which the ω_i are the eigenvalues of the ℓ-adic representation of the Frobenius endomorphism Frob on $H^1(C, \mathbb{Q}_\ell)$, for any prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$. The result follows after noting that the ω_i^n are the eigenvalues of the Frobenius endomorphism Frob^n of the curve $C_{\mathbb{F}_{q^n}}$.

2 The Hasse-Weil-Serre bound

Let $N = N_1$ be the number of $\mathbb{F}_q$-rational points of C. The following result, which gave the first bound on N, is an immediate consequence of the Riemann hypothesis for curves and Corollary I.1.3. It was first proved by Hasse for elliptic curves, and extended to all genera by Weil.

Theorem 2.1 (Hasse-Weil bound). *We have*

$$|N - (q+1)| \leqslant \lfloor 2g\sqrt{q} \rfloor.$$

Serre improved this result to produce a bound which is much sharper when the genus is sufficiently big compared to the size q of the finite field, when q is not a square.

Theorem 2.2 (Serre). *We have*

$$|N - (q+1)| \leqslant g\lfloor 2\sqrt{q}\rfloor,$$

with equality if and only if the α_i, for $i = 1, ..., g$, are all equal.

This upper bound is called the *Hasse-Weil-Serre bound*.

PROOF. We have to prove that

$$\left|\sum_{i=1}^{g} \alpha_i\right| \leqslant g\lfloor 2\sqrt{q}\rfloor.$$

For $i = 1, ..., g$, define γ_i by

$$\gamma_i = \alpha_i + \lfloor 2\sqrt{q}\rfloor + 1.$$

Then γ_i is a strictly positive (real) algebraic integer. Therefore $\prod_i \gamma_i$ is a strictly positive algebraic integer which is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, hence it is an integer greater than or equal to 1. By the arithmetic-geometric inequality, we have

$$1 \leqslant \prod_{i=1}^{g} (\gamma_i^{1/g}) \leqslant \frac{1}{g}\sum_{i=1}^{g} \gamma_i,$$

with equality between the second and third expressions if and only if the γ_i are all equal. This gives

$$g \leqslant \left(\sum_{i=1}^{g} \alpha_i\right) + g\lfloor 2\sqrt{q}\rfloor + g,$$

and thus

$$-\sum_{i=1}^{g} \alpha_i \leqslant g\lfloor 2\sqrt{q}\rfloor.$$

The other inequality follows by replacing α_i with $-\alpha_i$ in the definition of γ_i. □

Definition. A curve $C/\mathbb{F}_q$ of genus g is called *optimal* if $N(C)$ reaches the Hasse-Weil-Serre bound and *maximal*[1] if $N(C)$ equals the maximum number of rational points $N_q(g)$ among all genus g curves over $\mathbb{F}_q$.

3 The Ihara bound

By comparing the number of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$-rational points, Ihara proved the following result.

[1] In many references, the two terminologies are inverted. We prefer this one because it seems more suitable.

Theorem 3.1 (Ihara). *We have*

$$N_q(g) \leqslant \frac{1}{2}\left(\sqrt{(8q+1)g^2+4qg(q-1)}-(g-2(q+1))\right),$$

with equality if and only if the α_i, for $i=1,\dots,g$, are all equal.

The bound in the theorem is called the *Ihara bound*.

PROOF. By (I.1), we have that

$$q+1-\sum_{i=1}^{2g}\omega_i = N \leqslant N_2 = q^2+1-\sum_{i=1}^{2g}\omega_i^2.$$

By the Riemann hypothesis we obtain

$$-\sum_{i=1}^{2g}\omega_i^2 = -\sum_{i=1}^{g}(\omega_i^2+\overline{\omega}_i^2) = -\sum_{i=1}^{g}(\alpha_i^2-2q) = 2qg-\sum_{i=1}^{g}\alpha_i^2.$$

The Cauchy-Schwarz inequality applied to the real g-vectors $(\alpha_i)_i$ and $(1,\dots,1)$ gives

$$\left(\sum_{i=1}^{g}\alpha_i\right)^2 \leqslant g\sum_{i=1}^{g}\alpha_i^2,$$

and thus

$$N \leqslant q^2+1+2qg-(N-q-1)^2/g,$$

with equality if and only if the α_i, for $i=1,\dots,g$, are all equal. Writing this inequality in terms of N, we obtain

$$N^2+N(g-2(q+1))+(q+1)^2-g(q^2+2qg+1) \leqslant 0.$$

The result is obtained by solving this inequality. □

The Ihara bound is better than the Hasse-Weil-Serre bound when

$$2(q+1+g\lfloor 2\sqrt{q}\rfloor) > \sqrt{(8q+1)g^2+4qg(q-1)}-(g-2(q+1)),$$

that is when

$$g^2(1+2\lfloor 2\sqrt{q}\rfloor)^2 > (8q+1)g^2+4qg(q-1),$$

which gives, by assuming that g is non-zero,

$$g > \frac{4q(q-1)}{(1+2\lfloor 2\sqrt{q}\rfloor)^2-8q-1} = \frac{q(q-1)}{\lfloor 2\sqrt{q}\rfloor+\lfloor 2\sqrt{q}\rfloor^2-2q}.$$

The same computation with $2\sqrt{q}$ in place of $\lfloor 2\sqrt{q}\rfloor$ shows that the Ihara bound is better than the Hasse-Weil bound as soon as

$$g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}.$$

Example 3.2. Take $q=19$. The Ihara bound is sharper than the Hasse-Weil bound when

$$g \geqslant \lceil 10.05\rceil = 11.$$

It is better than the Hasse-Weil-Serre bound when

$$g > \lceil 7.321\rceil = 8.$$

4 The Oesterlé bound

When g is sufficiently large, there exist better bounds than the Hasse-Weil-Serre and Ihara bounds, called the *Oesterlé bounds*. A detailed exposition can be found in Serre [Ser85] (see also Voight [Voi05]). The method seems to come from Serre, and to have been optimized by Oesterlé, though it was never published. Let $C/\mathbb{F}_q$ be a curve and, for every $d \geqslant 1$, let $a_d = a_d(C)$ be the number of points of $C_{\overline{\mathbb{F}}_q}$ whose field of definition is $\mathbb{F}_{q^d}$. For every $i = 1, \dots, 2g$, let $\theta_i \in [0, 2\pi]$ be such that

$$\omega_i = \sqrt{q} e^{\theta_i}.$$

Hence for every integer $n \geqslant 1$ we have the formula

$$N_n = q^n + 1 - 2q^{n/2} \sum_{i=1}^{g} \cos(n\theta_i). \tag{I.2}$$

We introduce the functions $f, \psi : \mathbb{R} \to \mathbb{R}$ defined by

$$f(\theta) = 1 + 2 \sum_{n=1}^{\infty} c_n \cos(n\theta),$$

and

$$\psi_d(t) = \sum_{n=1}^{\infty} c_{nd} t^{nd},$$

for a fixed sequence $(c_n)_{n\geqslant 1}$ of real numbers such that the above series converge for every θ and t.

Note that by taking $\theta = \theta_i$, $c_n = q^{n/2}$ and $c_m = 0$ for any integer $m \neq n$, we find

$$N_n = q^n + 1 + g - \sum_{i=1}^{g} f(\theta_i).$$

Also, taking $c_{nd} = N_{nd}/nd$, we obtain $\psi_d(t) = Z(C_{\mathbb{F}_{q^d}}; t^d)$. We can therefore expect a relation between the functions f and ψ_d, and, indeed, Weil proved the following equality.

Proposition 4.1 (Weil's explicit formula). *We have*

$$\sum_{d=1}^{\infty} d a_d \psi_d(q^{-1/2}) = \psi_1(q^{1/2}) + \psi_1(q^{-1/2}) + g - \sum_{i=1}^{g} f(\theta_i).$$

PROOF. First multiply (I.2) by $c_n/q^{-n/2}$ and sum over $n \geqslant 1$. We obtain

$$\sum_{n=1}^{\infty} N_n c_n q^{-n/2} = \sum_{n=1}^{\infty} c_n q^{n/2} + \sum_{n=1}^{\infty} c_n q^{-n/2} - 2 \sum_{n=1}^{\infty} c_n \sum_{i=1}^{g} \cos(n\theta_i). \tag{I.3}$$

From the relation $N_n = \sum_{d|n} d a_d$, we see that the left hand side is of the form

$$\sum_{n=1}^{\infty} \left(\sum_{d|n} d a_d \right) c_n q^{-n/2} = \sum_{d=1}^{\infty} d a_d \sum_{n=1}^{\infty} c_{nd} q^{-nd/2} = \sum_{d=1}^{\infty} d a_d \psi_d(q^{-1/2}).$$

Now the right hand side of (I.3) is equal to

$$\psi_1(q^{1/2}) + \psi_1(q^{-1/2}) + g - \sum_{i=1}^{g} f(\theta_i),$$

and we obtain the result. □

Corollary 4.2. *Assume that the $c_n \geqslant 0$ are such that $f(\theta) \geqslant 0$ for all $\theta \in [-\pi, \pi]$ and $c_n = 0$ for all but finitely many values of n. Then for any curve C of genus g over $\mathbb{F}_q$ we have*

$$N \leqslant 1 + \frac{\psi_1(\sqrt{q}) + g}{\psi_1(1/\sqrt{q})}.$$

PROOF. By Proposition I.4.1, we have

$$N\psi_1(q^{-1/2}) = \psi_1(q^{1/2}) + \psi_1(q^{-1/2}) + g - \left(\sum_{i=1}^{g} f(\theta_i) + \sum_{d=2}^{\infty} da_d \psi_d(q^{-1/2}) \right),$$

hence the result, since by assumption $f(\theta_i)$ and $\psi_d(q^{-1/2})$ are positive for every i and d. □

Example 4.3. Take $c_1 = 1/2$ and $c_n = 0$ for $n > 1$. Then $\psi_1(t) = t/2$ and $f(\theta) = 1 + \cos(\theta)$, and thus we obtain

$$N \leqslant \frac{\sqrt{q} + 2g}{1/\sqrt{q}} + 1 = q + 1 + 2g\sqrt{q},$$

which is the Hasse-Weil bound.

Now the problem is to compute values of the c_n providing the best upper bound on N, that is to minimize

$$1 + \frac{\psi_1(\sqrt{q}) + g}{\psi_1(1/\sqrt{q})}.$$

But if we fix the number N of points a curve can have, this is equivalent to maximizing the lower bound $(N-1)\psi_1(1/\sqrt{q}) - \psi_1(\sqrt{q})$ on the genus g of the curve. Oesterlé solved this problem, although the first publication of his results is in Serre's Harvard course notes from 1985 (see Serre [Ser85], or Voight [Voi05] for a summary of the ideas occurring in the proof).

Before stating his result, we fix some notation. Let $\lambda = N - 1$, and let m be the unique integer such that $q^{m/2} < \lambda \leqslant q^{(m+1)/2}$. Set

$$u = \frac{q^{(m+1)/2} - \lambda}{\lambda\sqrt{q} - q^{m/2}}.$$

Theorem 4.4 (Oesterlé). *There exists a unique solution $\tau \in [\pi/(m+1), \pi/m]$ to the equation*

$$\cos(\tau(m+1)) + u\cos(\tau(m-1)/2) = 0.$$

For $1 \leqslant n \leqslant m-1$ let

$$c_n = \frac{(m-n)\cos(n\tau)\sin(\tau) + \sin((m-n)\tau)}{m\sin(\theta) + \sin(m\tau)}.$$

The c_n are optimal for the choice of $N = N(C)$, therefore we have the following lower bound on g:

$$g \geqslant \sum_{n=1}^{m-1} c_n(\lambda q^{-n/2} - q^{n/2}) = \frac{(\lambda - 1)\sqrt{q}\cos(\tau) + q - \lambda}{q - 2\sqrt{q}\tau - 1}.$$

Example 4.5. Kenneth Shum implemented a function in MATLAB [MAT10] which computes the Oesterlé bound for any values of q and g. Let $q = 2$.

a) For $g = 3$, we find that $N_2(3) \leqslant 7$, and this bound is sharp because the curve

$$x^3y + x^2y^2 + xz^3 + x^2z^2 + y^3z + yz^3$$

possesses 7 rational points. Note that the Ihara bound in this case is 8.

b) For $g = 12$, we find that $N_2(12) \leqslant 15$, but we do not know if this bound is sharp because until now only curves with 14 rational points have been constructed.

c) For $g = 14$, the Oesterlé bound is 16, and this bound is sharp because we will construct in the next chapter an abelian covering of degree 2 of a genus 4 curve, with genus 14 and 16 rational points.

5 The Drinfel'd-Vlăduţ bound

Until now we have explored the case where the genus of the curve is fixed, but what happens when the genus tends to infinity? In this case, as we will see, little is known and many important questions remain open. The natural extension of what has been undertaken above is to ask about the value of the Ihara constant

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

The Hasse-Weil-Serre bound (Theorem I.2.2) immediately provides that

$$A(q) \leqslant \lfloor 2\sqrt{q} \rfloor,$$

so $A(q)$ is finite, and the Ihara bound improves this result to

$$A(q) \leqslant \frac{\sqrt{8q+1} - 1}{2}.$$

Drinfeld and Vlăduţ [VD83] exhibited a much sharper bound using Weil's explicit formula (Proposition I.4.1).

Lemma 5.1. *If $f(\theta) \geqslant 0$ for every $\theta \in [0, 2\pi]$, then $c_n \leqslant 1$ for every $n \geqslant 1$.*

PROOF. By standard Fourier analysis (see for instance Rudin [Rud87, §9.4]),

$$c_n = \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\cos(n\theta)d\theta,$$

and

$$\frac{1}{2\pi}\int_0^{2\pi} f(\theta)d\theta = 1.$$

Because $|\cos(n\theta)| \leqslant 1$, we obtain

$$c_n \leqslant |c_n| = \left|\frac{1}{2\pi}\int_0^{2\pi} f(\theta)\cos(n\theta)d\theta\right| \leqslant \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\mid d\theta\,|\cos(n\theta)| \leqslant 1,$$

hence the result. □

From the lemma, we cannot expect to find a function f which is positive on the angles $[0, 2\pi]$ from a sequence $(c_n)_{n\geqslant 1}$ if any c_n is greater than 1. Instead we look at the limiting case and construct a sequence of positive functions $(f_k)_{k\geqslant 1}$ such that $\lim_{k\to\infty} c_n(f_k) = 1$ for every n.

Set $t = e^{i\theta}$, and for $k \geqslant 1$ consider the sum

$$f_k(\theta) = \frac{1}{2k+1}(t^{-k} + t^{-k+1} + \cdots + 1 + \cdots + t^k)^2.$$

Note that f_k is positive. Now we have

$$\begin{aligned} f_k(\theta) &= \frac{1}{2k+1}(t^{-2k} + 2t^{-2k+1} + \cdots + (2k+1) + 2kt + \cdots + t^{2k}) \\ &= 1 + 2\sum_{n=1}^{2k} \frac{2k-n+1}{2k+1}\cos(n\theta), \end{aligned}$$

therefore $c_n(f_k) = \frac{2k-n+1}{2k+1}$, which tends to 1^- as k tends to infinity.

Since we are interested in the asymptotic number of points, we consider a sequence $(C_i)_{i\geqslant 1}$ of curves defined over $\mathbb{F}_q$ such that $\lim_{i\to\infty} g(C_i) = \infty$.

Theorem 5.2. *Fix an integer $j \geqslant 1$. For every i, let $a_d^{(i)} = a_d(C_i)$. We have:*

$$\limsup_{i\to\infty} \frac{1}{g(C_i)} \sum_{d=1}^{j} \frac{d a_d^{(i)}}{q^{d/2}-1} \leqslant 1.$$

PROOF. From Proposition I.4.1, for every sequence of positive real numbers $(c_n)_{n\geqslant 1}$ such that f is a positive function, we know that

$$\sum_{d=1}^{j} d a_d^{(i)} \psi_d(1/\sqrt{q}) \leqslant g(C_i) + \psi_1(\sqrt{q}) + \psi_1(1/\sqrt{q}).$$

Dividing by $g(C_i)$ and taking the limit, we thus get:

$$\limsup_{i\to\infty} \frac{1}{g(C_i)} \sum_{d=1}^{j} d a_d^{(i)} \psi_d(1/\sqrt{q}) \leqslant 1. \tag{I.4}$$

Now take $f = f_k$. In this case

$$\psi_d^{(k)}(t) = \sum_{n=1}^{2k} \frac{2k - nd + 1}{2k+1} t^{nd},$$

so

$$\lim_{k\to\infty} \psi_d^{(k)}(1/\sqrt{q}) = \sum_{n=1}^{\infty} (q^{-d/2})^n = \frac{1}{q^{d/2}-1}.$$

We obtain the result by substituting this expression in (I.4) and letting k tend to ∞. □

By taking $j = 1$ in the previous theorem, we obtain the following corollary.

Corollary 5.3 (Drinfel'd-Vlăduţ bound). *Let q be a power of a prime number. Then*

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

This shows in particular that the Oesterlé bound is much sharper than the Hasse-Weil-Serre and Ihara bounds when g is large compared to q.

This bound is sharp in general because Ihara [Iha81] used sequences of modular and Shimura curves to prove that if q is a square, then

$$A(q) \geqslant \sqrt{q} - 1,$$

so in this case

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

The following year, and independantly of Ihara, the same result was obtained by Tsfasman, Vlăduţ and Zink for finite fields of the form $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$, where p is a prime [TVZ82]. They also used sequences of modular and Shimura curves respectively. We will recover these results with different techniques in chapter IV, where we study the natural analogues $X_0^+(\mathfrak{N})$ of the modular curves $X_0(N)$.

Note that finite fields $\mathbb{F}_q$ with q a square are the only cases where we know the Ihara constant exactly. For nonsquare q, one has to construct curves or function fields of arbitrary large genus such that the asymptotic ratio

$$\frac{\text{number of rational points}}{\text{genus}}$$

is the greatest possible. This way one will obtain lower bounds on $A(q)$. The best results over prime finite fields are obtained by recursively constructing sequences of abelian coverings. In

this case, the key tool to control the infiniteness of the tower is the Golod-Šafarevič theorem. For instance, Duursma and Mak [DM12] proved that

$$A(2) \geqslant 0.316999 \text{ and } A(3) \geqslant 0.492876,$$

but the Drinfel'd-Vlăduţ bound (if attainable!) is still out of reach.

For nonprime finite fields, the best lower bounds are obtained by using recursive towers [BBGS12]. A very interesting feature of these towers is that most of them have been proved to be *modular* (see for instance Elkies [Elk98a] or [Elk01]), which means that every curve in the tower is a modular curve. Here by modular, we include elliptic and Drinfel'd modular curves, as well as Shimura curves and modular curves of $\mathcal{D}$-elliptic sheaves. We will see in chapter IV that the Shimura curves of the form $X_0^+(\mathfrak{N})$ naturally form (optimal) recursive towers.

II

EXPLICIT ABELIAN COVERINGS

In the previous chapter, we have surveyed the most important upper bounds on $N_q(g)$, so the next step is to find lower bounds. The natural way to proceed is to find curves with as many rational points as possible. In this chapter we give an algorithm based on class field theory to compute curves with a large number of rational points. We also explain how the equations of the curves found can be computed using Kummer and Artin-Schreier-Witt theories. The results of this chapter represent joint work with Claus Fieker [DF13].

1 Class field theory

In this section we summarize without proofs the main theorems of class field theory that we will need later, first in the classical formulation, then using the more modern idelic language.

CLASSICAL THEORY IN TERMS OF IDEALS

The main results of class field theory in terms of ray class groups were conjectured by Weber and Hilbert, and proved in 1920 by Takagi. Artin extended Takagi's results in 1927 by describing the isomorphism between the Galois group of the abelian extension and the corresponding quotient of the ray class group. We refer to Janusz [Jan96], Childress [Chi09], or Milne [Mil11b] for more details and proofs.

Let K be a global field. Let L/K be a Galois extension of K and set $G = \mathrm{Gal}(L/K)$. Let P be a non-archimedean place of K and let Q be a place of L above P. The decomposition group $G_Q(L/K)$ of Q surjects onto $\mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ with kernel the inertia group at P. Hence if P is unramified there is a unique automorphism $(Q, L/K)$ in $G_Q(L/K)$, called the *Frobenius automorphism at* Q, such that for every $x \in L$, we have

$$(Q, L/K)(x) \equiv x^{\mathrm{N}(P)} \bmod Q.$$

The Galois group G acts on the set of places of L above K as follows: if $|\cdot|_Q$ is the norm associated to Q and if σ belongs to G, then $\sigma \cdot Q$ is the place such that

$$|x|_{\sigma \cdot Q} = |\sigma^{-1}(x)|_Q$$

for every $x \in L$. This action is transitive, so every other place of L above P is of the form $\sigma \cdot Q$ for some $\sigma \in \mathrm{Gal}(L/K)$. In this case, it is easy to see that

$$(\sigma \cdot Q, L/K) = \sigma(Q, L/K)\sigma^{-1}.$$

In particular, if L/K is abelian, as we will assume from now on, the Frobenius automorphism depends only on P, so we will henceforth refer to it as the *Frobenius automorphism at* P and denote it by $(P, L/K)$.

If K is a number field, we say that a real place *ramifies* in an extension L/K if the real embedding $\sigma : K \hookrightarrow \mathbb{R}$ corresponding to the place can be extended to at least one complex embedding of L.

Definition. A *modulus* $\mathfrak{m}$ is an effective divisor over K if the field K is a global function field, and an integral ideal if K is a number field. If K is a number field, we allow $\mathfrak{m}$ to contain real places in its support, in which case $\mathfrak{m}$ must have valuation 1 at such places.

Let $\mathfrak{m}$ be a modulus whose support contains all the (finite or infinite) places of K which ramify in L, and let $\mathrm{Div}_{\mathfrak{m}}$ be the group of divisors of K prime to $\mathfrak{m}$. The map

$$\Psi_{L/K} : \mathrm{Div}_{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$$

defined by

$$D = \sum n_P P \longmapsto (D, L/K) = \prod (P, L/K)^{n_P}$$

is called the *Artin map*. Let

$$K_{\mathfrak{m},1} = \{f \in K^\times : v_P(f-1) \geq v_P(\mathfrak{m}) \text{ for all } P \text{ in the support of } \mathfrak{m}\}$$

be the group of functions 'congruent to 1 modulo $\mathfrak{m}$', and let

$$\mathcal{P}_{\mathfrak{m},1} = \{\mathrm{div}(f) : f \in K_{\mathfrak{m},1}\}$$

be the subgroup of $\mathrm{Div}_{\mathfrak{m}}$ generated by the elements of $K_{\mathfrak{m},1}$.

Definition. Let $\mathfrak{m}$ be a modulus. A subgroup H of $\mathrm{Div}_{\mathfrak{m}}$ of finite index is called a *congruence subgroup modulo* $\mathfrak{m}$ if it contains $\mathcal{P}_{\mathfrak{m},1}$.

Let L/K be a Galois extension of global fields, and let Q be a place of L above P. We define a norm map on divisor groups

$$\mathrm{N}_{L/K} : \mathrm{Div}(L) \to \mathrm{Div}(K) \tag{II.1}$$

by extending linearly $Q \mapsto f_P P$, where f_P is the inertia degree of P.

The following theorem is a generalization of reciprocity laws known since Euler, such as the Quadratic Reciprocity Law, whence its name.

Theorem 1.1 (Artin Reciprocity Law). *Let L/K be a finite abelian extension. Then there exists a modulus $\mathfrak{m}$, whose support S contains the set of places of K which are ramified in L, and a unique congruence subgroup $H_{\mathfrak{m}}$ modulo $\mathfrak{m}$, such that the Artin map defines an isomorphism*

$$\Psi_{L/K} : \mathrm{Div}_{\mathfrak{m}}(K)/H_{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K).$$

Furthermore, the group $H_{\mathfrak{m}}$ is of the form $\mathcal{P}_{\mathfrak{m},1} \cdot \mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L))$, where $\mathfrak{m}'$ is any modulus of L whose support is the set of places above S.

A modulus $\mathfrak{m}$ as in the theorem is called an *admissible modulus for L/K*. It may not be unique (whereas for a given $\mathfrak{m}$, the second part of the theorem implies that $H_{\mathfrak{m}}$ is), but there exists an admissible modulus $\mathfrak{f}_{L/K}$ for L/K, called the *conductor of L/K*, which is smaller than the others in the sense that every defining modulus $\mathfrak{m}$ for L/K verifies $\mathfrak{f}_{L/K} \leqslant \mathfrak{m}$.

Let P be a place of K which is unramified in L and let Q be a place of L above P. The Artin map at $\mathrm{N}_{L/K}(Q)$ verifies

$$(\mathrm{N}_{L/K}(Q), L/K) = (f_P P, L/K) = (P, L/K)^{f_P},$$

and this map is the identity since $G_Q(L/K) \cong \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ has order f_P. Hence we already have that $\mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L)) \subseteq \ker(\Psi_{L/K})$. So the proof of the Artin Reciprocity Law consists in showing that there exists a modulus $\mathfrak{m}$ such that $\Psi_{L/K}(\mathcal{P}_{\mathfrak{m},1}) = 1$, and then that

$$[\mathrm{Div}_{\mathfrak{m}}(K) : \mathcal{P}_{\mathfrak{m},1} \cdot \mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L))] = [L : K].$$

One proceeds in two steps and proves each inequality separately:

$$[\mathrm{Div}_{\mathfrak{m}}(K) : \mathcal{P}_{\mathfrak{m},1} \cdot \mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L))] \geq [L : K]$$

is called the *First Inequality* whereas the other one is called the *Second Inequality*.[1]

The following fundamental theorem is a kind of converse to the Artin Reciprocity Law and constitutes the second main theorem of class field theory:

Theorem 1.2 (Existence theorem). *Let $\mathfrak{m}$ be a modulus over K. For every congruence subgroup $H_{\mathfrak{m}}$ modulo $\mathfrak{m}$ there exists a unique abelian extension L/K which is unramified outside $\mathfrak{m}$ and for which the Artin map provides an isomorphism*

$$\mathrm{Div}_{\mathfrak{m}}/H_{\mathfrak{m}} \cong \mathrm{Gal}(L/K).$$

Note also that $\mathfrak{f}_{L/K} \leqslant \mathfrak{m}$ and that modulo a finite number of exceptions (namely the totally split places P which are in the support of $\mathfrak{m}$ but not in the support of $\mathfrak{f}_{L/K}$), a place P is totally split if and only if it belongs to $H_{\mathfrak{m}}$.

[1] Historically, the Second Inequality is actually the first one which has been proved, but in the purely algebraic setting of ideles and cohomology, one first proves that $[\mathrm{Div}_{\mathfrak{m}}(K) : \mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L))] \geq [L : K]$.

Definition. The abelian extension L of K uniquely associated to the subgroup $H_{\mathfrak{m}}$ as in Theorem II.1.2 is called the *class field* of $H_{\mathfrak{m}}$.

Let $\mathfrak{m}$ be a modulus and consider the *ray class group* modulo $\mathfrak{m}$, defined by

$$\mathrm{Pic}_{\mathfrak{m}} = \mathrm{Div}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m},1}.$$

There is a bijection between the set of congruence subgroups H modulo $\mathfrak{m}$ and the set of subgroups $\bar{H} = H/\mathcal{P}_{\mathfrak{m},1}$ of $\mathrm{Pic}_{\mathfrak{m}}$, hence it is straightforward to translate the main theorems of class field theory in terms of subgroups of the ray class group, and in this case one does not need to worry about the fact that the subgroup will contain some smaller subgroup or not, as in the case of congruence subgroups. In this context, we summarize the two main theorems of class field theory as follows. Set

$$\mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L)) = (\mathcal{P}_{\mathfrak{m},1} \cdot \mathrm{N}_{L/K}(\mathrm{Div}_{\mathfrak{m}'}(L)))/\mathcal{P}_{\mathfrak{m},1}.$$

Corollary 1.3. *The Artin map induces a bijective correspondence $L \leftrightarrow \mathrm{N}(\mathrm{Pic}_{L,\mathfrak{m}})$ between the set of finite abelian extensions of K of conductor less than $\mathfrak{m}$ and the set of subgroups of finite index of $\mathrm{Pic}_{\mathfrak{m}}$. Furthermore,*

i) $L_1 \subseteq L_2 \iff \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_1)) \supseteq \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_2))$*;*

ii) $\mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_1 \cdot L_2)) = \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_1)) \cap \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_2))$*;*

iii) $\mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_1 \cap L_2)) = \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_1)) \cdot \mathrm{N}(\mathrm{Pic}_{\mathfrak{m}}(L_2))$.

Let

$$K_{\mathfrak{m}} = \{f \in K : v_{\mathfrak{p}}(f) = 0 \text{ for all } P \text{ in the support of } \mathfrak{m}\},$$

and let

$$U_{\mathfrak{m},1} = U_K \cap K_{\mathfrak{m},1}.$$

Theorem 1.4. *The ray class group $\mathrm{Pic}_{\mathfrak{m}}$ and the Picard group Pic are related by the following exact sequence:*

$$0 \to U_K/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathrm{Pic}_{\mathfrak{m}} \to \mathrm{Pic} \to 0. \tag{II.2}$$

PROOF. See Milne [Mil11b, Theo. V.1.7]. □

Assume that $K = F$ is a number field, and let $\mathfrak{m}$ be a modulus over F. The group $\mathrm{Pic}_{\mathfrak{m}}$ is finite, so by the Existence Theorem (Theorem II.1.2) there exists a unique abelian extension $F_{\mathfrak{m}}$ of F which is unramified outside $\mathfrak{m}$ and such that

$$\mathrm{Gal}(F_{\mathfrak{m}}/F) \cong \mathrm{Pic}_{\mathfrak{m}}(F).$$

The field $F_{\mathfrak{m}}$ is the maximal abelian extension of F with conductor smaller than $\mathfrak{m}$ and is called the *ray class field of F modulo $\mathfrak{m}$*.

In this case, by Theorem II.1.4, we see that the ray class group is a finite group of cardinality

$$h_{\mathfrak{m}} = \frac{h}{[U_K : U_{\mathfrak{m},1}]} 2^{r_0} \mathrm{N}(\mathfrak{m}_0) \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right), \tag{II.3}$$

where $h = h(F) = \#\mathrm{Cl}(F)$ is the *class number* of F, r_0 is the number of real places in $\mathfrak{m}$, and $\mathfrak{m}_0$ is the modulus $\mathfrak{m}$ without the infinite places.

Example 1.5. If $\mathfrak{m} = (1)$, the field $H = F_0$ is the maximal abelian extension of F unramified at finite and infinite places; it is called the *Hilbert class field* of F. Thus, by the Artin isomorphism, we have

$$\mathrm{Gal}(H/F) \cong \mathrm{Cl}(F).$$

If $\mathfrak{m}$ is the product of the (real) infinite primes of F, we obtain the maximal abelian extension F_∞ of F which is unramified everywhere except possibly at the real places of F. The field F_∞ is called the *narrow Hilbert class field* of F because its Galois group is isomorphic to the *narrow class group* $\mathrm{Cl}_\infty(F)$ of F, which is defined by

$$\mathrm{Cl}_\infty(F) = \{\text{Ideals of } F\}/\{x\mathbb{Z}_F : \iota(x) > 0 \text{ for every embedding } \iota : F \hookrightarrow \mathbb{R}\}.$$

We denote by $h_\infty(F) = \#\mathrm{Cl}_\infty(F)$ the *narrow class number* of F.

Assume now that $K/\mathbb{F}_q$ is a global function field, so K is the function field of a curve $C/\mathbb{F}_q$, and consider a modulus $\mathfrak{m}$ over K. In this case the ray class group $\mathrm{Pic}_{\mathfrak{m}}$ is no longer finite, so there is no canonical notion of ray class field as in the number field case. However K admits a divisor D_0 of degree 1 [AT09, Theo. V.5], so if we assume that $\mathfrak{m} = 0$ we obtain an isomorphism

$$\varphi_{D_0} : \mathrm{Pic}(K) \xrightarrow{\cong} \mathbb{Z} \times \mathrm{Pic}^0(K)$$

defined by $[D] \mapsto (\deg(D), [D - \deg(D)D_0])$, where

$$\mathrm{Pic}^0(K) \cong \mathrm{Pic}^0(C) \cong \mathrm{Jac}(C)(\mathbb{F}_q)$$

is the group of divisors of degree 0 of K. A subgroup H of finite index of $\mathrm{Pic}(K)$ is thus of the form $H = n\mathbb{Z} \times H_0$ for a subgroup H_0 of $\mathrm{Pic}^0(K)$. Let L be the abelian extension of K corresponding to H. By definition of the Artin map and the Artin Reciprocity Law, a place P of K splits in L if and only if P belongs to H, and in this case the residue field of any place Q of L above P is $\mathbb{F}_{q^{\deg(P)}}$. Therefore the field of constants of L is a subfield of $\mathbb{F}_{q^{\deg(P)}}$, and more generally an extension of $\mathbb{F}_q$ of degree dividing the greatest common divisor of all the degrees of the places in H, which n. In particular, the constant field extension of K from $\mathbb{F}_q$ to $\mathbb{F}_{q^n}$ is an abelian extension which is the class field of a subgroup H isomorphic to $n\mathbb{Z} \times \mathrm{Pic}^0(K)$.

We now assume that K contains places of degree 1, thus we can take D_0 equal to one of these rational places. The image by φ_{P_0} of the subgroup $H = \langle [P_0] \rangle$ generated by P_0 is equal to $\mathbb{Z} \times \{0\}$. The class field K_{P_0} corresponding to H is the largest abelian extension of K defined over $\mathbb{F}_q$ which is unramified and in which P_0 is totally split. We call K_{P_0} the *P_0-Hilbert class field* of K. It has Galois group over K

$$\mathrm{Gal}(K_{P_0}/K) \cong \mathrm{Pic}^0(K) \cong \mathrm{Jac}(C)(\mathbb{F}_q).$$

This notion of Hilbert class field is not unique, because we have one Hilbert class field for every rational place of K. Their Galois groups are all isomorphic but not necessarily equal, because if P_1 is another rational place of K such that $[P_1] \neq [P_0]$ in $\mathrm{Pic}(K)$, then the class fields K_{P_0} and K_{P_1} will be different.

The preceding discussion can be extended to the case of a modulus $\mathfrak{m}$ which is prime to D_0.

IDELIC THEORY

We now give the main results of class field theory in terms of ideles, since we will need them in Chapter IV. They are essentially idelic versions of the main theorems of class field theory stated above. We refer to Artin and Tate [AT09], Milne [Mil11b], or Neukirch [Neu99] for the proofs.

Let K be a global field, and let $\mathcal{J}_K$ be the idele group of K. For a finite extension L/K and a place P of K, we define a local norm map

$$\mathrm{N}_{L_Q/K_P}$$

at every place Q above P in the same way as (II.1). We define an adelic norm map

$$\mathrm{N}_{L/K} : \mathcal{J}_L \to \mathcal{J}_K$$

by taking the product over all the non-archimedean places P of K of all the local norm maps:

$$\mathrm{N}_{L/K} = \prod_P \prod_{Q|P} \mathrm{N}_{L_Q/K_P}.$$

Let K^{ab} be the maximal abelian extension of K inside $\bar{K}$.

Theorem 1.6 (Reciprocity Law). *There exists a homomorphism*

$$\phi_K : \mathcal{J}_K \to \mathrm{Gal}(K^{ab}/K)$$

with the following properties:

i) $\phi_K(K^\times) = 1$*;*

ii) for every finite abelian extension L *of* K*,* ϕ_K *defines an isomorphism*

$$\phi_{L/K} : \mathcal{J}_K/(K^\times \cdot \mathrm{N}_{L/K}(\mathcal{J}_L)) \xrightarrow{\cong} \mathrm{Gal}(L/K).$$

Furthermore, the group $K^\times \cdot \mathrm{N}_{L/K}(\mathcal{J}_L)$ *is open.*

The Reciprocity Law admits the following converse.

Theorem 1.7 (Existence theorem). *For every open subgroup* U *of finite index in* $\mathcal{J}_K$ *and containing* $K^\times$*, there exists a unique abelian extension* L *of* K *such that* $U = K^\times \cdot \mathrm{N}_{L/K}(\mathcal{J}_L)$.

Definition. The abelian extension L of K uniquely associated to the subgroup U as in Theorem II.1.7 is called the *class field of* U.

As in the case of ray class fields, we can express the main theorems of class field theory in terms of the *idele class group*, which is defined by

$$\mathcal{C}_K = \mathcal{J}_K / K^\times.$$

For an abelian extension L/K, let

$$\mathrm{N}(\mathcal{C}_L) = (\mathrm{N}(\mathcal{J}_L) \cdot K^\times)/K^\times.$$

Corollary 1.8. *The map ϕ_K induces a bijective correspondence $L \leftrightarrow \mathrm{N}(\mathcal{C}_L)$ between the set of finite abelian extensions of K and the set of open subgroups of finite index in $\mathcal{C}_K$. Furthermore,*

i) $L_1 \subseteq L_2 \iff \mathrm{N}(\mathcal{C}_{L_1}) \supseteq \mathrm{N}(\mathcal{C}_{L_2})$*;*

ii) $\mathrm{N}(\mathcal{C}_{L_1 \cdot L_2}) = \mathrm{N}(\mathcal{C}_{L_1}) \cap \mathrm{N}(\mathcal{C}_{L_2})$*;*

iii) $\mathrm{N}(\mathcal{C}_{L_1} \cap \mathcal{C}_{L_2}) = \mathrm{N}(\mathcal{C}_{L_1}) \cdot \mathrm{N}(\mathcal{C}_{L_2})$.

2 Explicit cyclic extensions

In certain particular cases, class field theory can be made explicit, through Kummer and Artin-Schreier-Witt theories, which we now present.

WITT VECTORS

Witt vectors were introduced by Witt in his 1936 paper [Wit36]. Two basic references are Serre [Ser79, Chap. II §6] and Lang [Lan02, pp. 330-332], but we motivate the definition of Witt vector following [Fis99] and [Rab07].

In this section we fix a prime number p. Witt vectors appear naturally when one tries to put a ring structure on $\prod_{i=0}^{\infty} \mathbb{F}_p$ such that we have a ring isomorphism

$$\mathbb{Z}_p \overset{\cong}{\to} \prod_{i=0}^{\infty} \mathbb{F}_p.$$

The representation of a p-adic integer as a sum

$$x = \sum_{i=0}^{\infty} x_i p^i$$

with x_i in $\{0, 1, \ldots, p-1\}$ does not satisfy this condition, so one needs something else.

For any element $x \in \mathbb{F}_p^\times$, Hensel's Lemma ensures the existence of an element $\tau(x)$ in $\mathbb{Z}_p^\times$, called the *Teichmüller representative* of x, such that

$$\tau(x)^{p-1} = 1.$$

If we furthermore set $\tau(0) = 0$, then by Serre [Ser79, § II.4] we obtain a map $\tau : \mathbb{F}_p \to \mathbb{Z}_p$ which is a section of the reduction map $\mathrm{red} : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ (*i.e.* $\tau \circ \mathrm{red} = \mathrm{Id}_{\mathbb{Z}_p}$ and

$\mathrm{red} \circ \tau = \mathrm{Id}_{\mathbb{F}_p}$), and which is multiplicative. Also, every p-adic integer can be uniquely written as a sum

$$\sum_{i=0}^{\infty} \tau(x_i) p^i,$$

with $x_i \in \mathbb{F}_p$.

So this gives a well defined bijective map

$$\phi : \prod_{i=0}^{\infty} \mathbb{F}_p \xrightarrow{\sim} \mathbb{Z}_p.$$

With coordinatewise addition and multiplication on the left side, this map is only a bijection. So we want to define an addition law on the left such that the map ϕ is a morphism. For two elements $x = (x_0, \dots, x_n, \dots)$ and $y = (y_0, \dots, y_n, \dots)$ in $\prod_{i=0}^{\infty} \mathbb{F}_p$, we must determine the preimage $s = (s_0, \dots, s_n, \dots)$ of $\phi(x) + \phi(y)$ in terms of x and y; s will then be "$x + y$". Equivalently, we must solve the system of equations $\phi(s) = \phi(x) + \phi(y)$:

$$\begin{aligned} \tau(s_0) &\equiv \tau(x_0) + \tau(y_0) \bmod p \\ \tau(s_0) + p\tau(s_1) &\equiv \tau(x_0) + p\tau(x_1) + \tau(y_0) + p\tau(y_1) \bmod p^2 \\ &\vdots \end{aligned}$$

Because τ is a section of red, we have $s_0 = x_0 + y_0$. For s_1, note that

$$\tau(s_0) \equiv \tau(x_0) + \tau(y_0) \bmod p$$

implies that

$$\tau(s_0)^p \equiv (\tau(x_0) + \tau(y_0))^p \bmod p^2.$$

Since $\tau^p = \tau$, by definition of the Teichmüller lift we obtain by multiplicativity

$$\tau(s_1) \equiv \tau(x_1) + \tau(y_1) + \frac{\tau(x_0^p) + \tau(y_0^p) - (\tau(x_0) + \tau(y_0))^p}{p} \bmod p,$$

which implies

$$s_1 = x_1 + y_1 + \frac{x_0^p + y_0^p - (x_0 + y_0)^p}{p}.$$

Solving the system for higher indices is much more difficult, but Witt noticed that we do not need to compute all the s_i explicitly. To see why, we first give names to the polynomials defining the s_i.

Definition. Let $(X_0, ..., X_i, ...)$ be a sequence of indeterminates. The *Witt polynomials* (relative to p) are defined by the formulas

$$\begin{aligned} W_0 &= X_0 \\ W_1 &= X_0^p + pX_1 \\ &\vdots \\ W_n &= \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + \cdots + p^n X_n \\ &\vdots \end{aligned}$$

Theorem 2.1. *Let $(Y_0, ..., Y_n, ...)$ be another sequence of indeterminates. For every polynomial $\Phi \in \mathbb{Z}[U, V]$, there exists a unique sequence $(\psi_0, ..., \psi_n, ...)$, where*

$$\psi_n \in \mathbb{Z}[X_0, ..., X_n, ...; Y_0, ..., Y_n, ...],$$

such that

$$W_n(\psi_0, ..., \psi_n) = \Phi(W_n(X_0, ..., X_n), W_n(Y_0, ..., Y_n))$$

for every $n \geqslant 0$.

PROOF. See Serre [Ser79, Theo. II.6]. □

Let $S_0, ..., S_n, ...$ and $P_0, ..., P_n, ...$ be the $\psi_0, ..., \psi_n, ...$ associated by Theorem II.2.1 to the polynomials

$$\Phi(U, V) = U + V \text{ and } \Phi(U, V) = U \cdot V$$

respectively. Of course we recover

$$S_0(X, Y) = X_0 + Y_0 \text{ and } S_1(X, Y) = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}.$$

For the product, P_0 and P_1 are given by

$$P_0(X, Y) = X_0 Y_0 \text{ and } P_1(X, Y) = X_0^p Y_1 + X_1 Y_0^p + pX_1 Y_1.$$

Now let R be any commutative ring. Let $\vec{x} = (x_0, ..., x_n, ...)$ and $\vec{y} = (y_0, ..., y_n, ...)$ be two *Witt vectors with coefficients in R*, that is $\vec{x}$ and $\vec{y}$ are elements of the free product $R^{\mathbb{N}}$ of R indexed by the natural numbers.

Theorem 2.2. *The following two composition laws endow $R^{\mathbb{N}}$ with the structure of a commutative ring with zero $(0, ..., 0, ...)$ and unity $(1, 0, ..., 0, ...)$:*

$$\begin{aligned} \vec{x} + \vec{y} &= (S_0(\vec{x}, \vec{y}), ..., S_n(\vec{x}, \vec{y}), ...), \\ \vec{x}.\vec{y} &= (P_0(\vec{x}, \vec{y}), ..., P_n(\vec{x}, \vec{y}), ...). \end{aligned}$$

This ring is denoted $\mathbb{W}(R)$ and is called the *ring of Witt vectors* with coefficients in R. It is not always integral, but in the case $R = \mathbb{F}_p$ we obtain

$$\mathbb{W}(\mathbb{F}_p) \cong \mathbb{Z}_p.$$

PROOF. By Theorem II.2.1, the map $\mathbb{W}(R) \to R^{\mathbb{N}}$ defined by

$$\vec{x} = (x_0, \dots, x_n, \dots) \mapsto (W_0(\vec{x}), \dots, W_n(\vec{x}), \dots)$$

is a ring homomorphism, and it is an isomorphism if p is invertible in R, so for instance if $R = \mathbb{Z}[p^{-1}][(T_i)_i]$ for any sequence of indeterminates T_i. By restriction the theorem is thus also true for $R = \mathbb{Z}[(T_i)_i]$, and by taking the quotient we see that is is again true for any ring R. □

It is useful in practice to work with the m first coordinates $(x_0, ..., x_{m-1})$ only. Since by construction the polynomials S_i and P_i are in $\mathbb{Z}[X_0, ..., X_i; Y_0, ..., Y_i]$, the set of such m-tuples forms a ring $\mathbb{W}_m(R)$ called the *ring of Witt vectors of length* m. Note that $\mathbb{W}_0(R) = R$, and that $\mathbb{W}(R)$ is the inverse limit of the rings $\mathbb{W}_m(R)$ with respect to the projection maps:

$$\mathbb{W}(R) = \varprojlim_m \mathbb{W}_m(R).$$

Now let k be any field of characteristic $p > 0$. In this context and for later convenience, we shift the numbering by 1, hence for instance we denote a Witt vector $\vec{\alpha} \in \mathbb{W}_m(\bar{k})$ by

$$\vec{\alpha} = (\alpha_1, \dots, \alpha_m).$$

The vector $\vec{\alpha}$ generates an algebraic extension $k(\vec{\alpha})$ of k by setting

$$k(\vec{\alpha}) = k(\alpha_1, \dots, \alpha_m).$$

This construction is equivalent to that of the tower

$$\begin{array}{rcl} k_m & = & k(\vec{\alpha}) \\ \uparrow & & \\ \vdots & & \\ \uparrow & & \\ k_2 & = & k_1(\alpha_2) \\ \uparrow & & \\ k_1 & = & k_0(\alpha_1) \\ \uparrow & & \\ k_0 & = & k \end{array}$$

ARTIN-SCHREIER-WITT THEORY

From now on we drop the notation $\vec{\cdot}$ and simply denote a Witt vector by $x = \vec{x}$. Let k be a field, and let k'/k be a finite Galois extension with Galois group G. For any $m \geqslant 1$, we let G act on $\mathbb{W}_m(k')$ as follows: For every $\sigma \in G$ and every $x \in \mathbb{W}_m(k')$ we set

$$\sigma x = \sigma(x_1, \dots, x_m) = (\sigma x_1, \dots, \sigma x_m).$$

Note that the polynomials S_n and P_n defining addition and multiplication of Witt vectors have integer coefficients, so if $y \in \mathbb{W}_m(k')$ is another Witt vector,

$$\sigma(x+y) = \sigma x + \sigma y \text{ and } \sigma(xy) = \sigma x \cdot \sigma y.$$

The *trace* of a vector $x \in \mathbb{W}_m(k')$ is defined by the rule

$$\mathrm{Tr}(x) = \sum_{\sigma \in G} \sigma x.$$

Note that Tr is a k-linear map.

The following very classical theorem is of fundamental importance:

Theorem 2.3 (Hilbert's Theorem 90). *Let k be a field of characteristic $p > 0$, and let k'/k be a cyclic extension of degree n. Let G be the Galois group of k'/k, with generator σ. For any element $\beta \in \mathbb{W}_m(k')$, $\mathrm{Tr}(\beta) = 0$ if and only if there exists an element $\alpha \in \mathbb{W}_m(k')$ such that $\beta = \sigma\alpha - \alpha$.*

PROOF. If such an element α exists, its trace is obviously equal to 0. Conversely, assume that $\mathrm{Tr}(\beta) = 0$. The extension being separable, the trace map is not identically 0 (see for instance Lang [Lan02, Theo. VI.5.2]), so there exists an element $\theta \in \mathbb{W}_m(k')$ such that $\mathrm{Tr}(\theta) \neq 0$. Set

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)}(\beta\theta^{\sigma} + (\beta + \sigma\beta)\theta^{\sigma^2} + \cdots + (\beta + \sigma\beta + \cdots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}})).$$

One easily checks that $\beta = \sigma\alpha - \alpha$. □

We let $\wp$ be the Artin-Schreier-Witt operator acting on $\alpha \in \mathbb{W}_m(\bar{k})$ by

$$\wp(\alpha) = \alpha^p - \alpha.$$

For β in $\mathbb{W}_m(k)$ the equation $\wp(\alpha) = \beta$ is algebraic over k, so as above one can consider the extension $k(\wp^{-1}(\beta))$.

Theorem 2.4 (Main Theorem of Artin-Schreier-Witt theory). *Let k be a field of characteristic $p > 0$.*

i) If k' is a cyclic extension of k of degree p^m, there exists $\alpha \in \mathbb{W}_m(k')$ such that $k' = k(\alpha)$, where α satisfies the equation $X^p - X - a = 0$ for some $a \in \mathbb{W}_m(k)$.

ii) Conversely, given $a \in \mathbb{W}_m(k)$, the polynomial $f(X) = X^p - X - a$ either has one root in $\mathbb{W}_m(k)$, in which case all its roots are in $\mathbb{W}_m(k)$, or generates a cyclic extension of degree p^m over k. This last case occurs exactly when $a_1 \notin \wp(k)$.

PROOF. Let k'/k be a cyclic extension of degree p^m and Galois group G, and let σ be a generator of G. We have $\mathrm{Tr}(1) = 0$ (it is just the sum of 1 with itself p^m times), so by Hilbert's theorem 90 there exists $\alpha \in \mathbb{W}_m(k')$ such that $\sigma\alpha - \alpha = 1$, or in other words $\sigma\alpha = \alpha + 1$. So $\sigma^i\alpha = \alpha + i$ for

every integer $i = 1, \dots, p^m - 1$. This means that α has p^m distinct conjugates, thus $k' = k(\alpha)$ because they both have degree p^m over k.

We note that

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Hence $\alpha^p - \alpha$ is fixed under σ, so it is fixed under the powers of σ and therefore under G. Therefore it lies in the fixed field k, so we have proved the first assertion of the theorem, with $a = \alpha^p - \alpha$. Conversely, let $a \in \mathbb{W}_m(k)$. If α is a root of $f(X) = \wp(X) - a$, then $\alpha + i$ is also a root for $i = 1, \dots, p^m - 1$. Thus $f(X)$ has p^m distinct roots, and it is separable. If one root lies in $\mathbb{W}_m(k)$, then all roots lie in $\mathbb{W}_m(k)$.

So assume that no root lies in $\mathbb{W}_m(k)$. It is clear that $k(\alpha)$ contains all the roots of f, therefore $k(\alpha)$ is Galois over k. Let $G = \mathrm{Gal}(k'/k)$. There exists an automorphism $\sigma \in G$ such that $\sigma\alpha = \alpha + 1$ (because $\alpha + 1$ is also a root). The powers σ^i of σ give $\sigma^i\alpha = \alpha + i$ for $i = 1, \dots, p^m$ and are distinct, therefore the Galois group consists of these powers and is cyclic.

To conclude, note that if $a_1 \in \wp(k)$, then $[k(\alpha) : k] \leqslant p^{m-1}$, so one root (hence all roots) must lie in $\mathbb{W}_m(k)$. Conversely, if $a_1 \notin \wp(k)$ then α is a root of $f(X)$ which does not belong to $\mathbb{W}_m(k)$, so $f(X)$ has p^m distinct roots and $k(\alpha)/k$ is cyclic of degree p^m. □

Now we specialize our discussion to a global function field $K/\mathbb{F}_q$ of characteristic $p > 0$. We are interested in the cyclic p-extensions of K. Let $x \in \mathbb{W}_m(K)$ be such that $x \notin \wp(\mathbb{W}_m(K))$, and let $y \in \mathbb{W}(\bar{K})$ be a solution of the equation $\wp(y) = x$. Consider the extension $L = K(y)$; it is cyclic of degree p^m over K. If P is a place of K which is unramified in L, for every $i = 1, \dots, m$ we set

$$\lambda_{P,i} = \lambda_{P,i}(x) = -v_P(x_i).$$

We define the *Witt symbol* $\left\{ \frac{x}{P} \right\}$ in $\mathbb{W}_m(\mathbb{F}_p)$ to be

$$\left\{ \frac{x}{P} \right\} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x + x^q + \cdots + x^{\frac{\mathrm{N}(P)}{q}} \bmod P).$$

Schmid [Sch36] exhibited a very explicit description of the arithmetic of the cyclic extension L/K at a given place P in terms of this symbol and the $\lambda_{P,i}$, which we summarize in the following theorem.

Theorem 2.5 (Schmid). *Let P be a place of K.*

i) Assume that $\lambda_{P,i} > 0$ or $(\lambda_{P,i}, p) = 1$ for every i, and let

$$M_P = \max\{p^{m-i}\lambda_{P,i} : 1 \leqslant i \leqslant m\}.$$

We have

$$v_P(\mathfrak{f}_{L/K}) = M_P + 1.$$

ii) If P is unramified, the Frobenius automorphism $(P, L/K)$ acts on y as follows:

$$(P, L/K)(y) = y + \left\{\frac{x}{P}\right\}.$$

Furthermore the symbol $\{\frac{\cdot}{P}\}$ is additive.

The following proposition ensures that one can always assume that the condition in Theorem II.2.5 i) is verified.

Proposition 2.6. *Let $y \in K$. For every place P of K there exists an element $u_P \in K$ such that either $v_P(y + u_P^p - u_P)$ is negative and coprime to p, or $v_P(y + u_P^p - u_P) \geq 0$.*

PROOF. If $v_P(y) \geq 0$ or $v_P(y)$ is coprime to p then $u_P = 0$ satisfies the conditions of the proposition, so we henceforth assume that $v_P(y) < 0$ and $p \mid v_P(y)$. Let $\bar{y} = (y\pi^{-v_P(y)})(P) \in \mathbb{F}_P$, where $\mathbb{F}_P$ is the residue class field of K at P and π is a uniformizing element (that is, $v_P(\pi) = 1$). Since the p-power Frobenius is surjective, we can find a $\bar{u} \in \mathbb{F}_P$ such that $\bar{u}^p = -\bar{y}$. Now let u be a lift of $\bar{u}$ in K. There exists $a \in K$ with $v_P(a) > v_P(y)$ such that $y + u^p\pi^{v_P(y)} = a$. Then, since $v_P(y) < v_P(y)/p < 0$, we have

$$v_P(y + (u\pi^{v_P(y)/p})^p - u\pi^{v_P(y)/p}) \geq \min\{v_P(a), v_P(y)/p\} > v_P(y)$$

(note that $v_P(u) = 0$), and we can recurse. □

KUMMER THEORY

In the previous section we considered cyclic p-extensions, where p is the characteristic of K. Now we are interested in cyclic n-extensions, for an integer n prime to p. The results in both cases are quite similar, as the next theorem shows:

Theorem 2.7 (Main theorem of Kummer theory). *Let k be a field, and $n > 0$ an integer not divisible by the characteristic of k. Assume that k contains a primitive n-th root of 1.*

i) If k' is a cyclic extension of k of degree n, there exists $\alpha \in k'$ such that $k' = k(\alpha)$ and α satisfies an equation $X^n - a = 0$ for some $a \in k'$.

ii) Conversely, let $a \in k$ and let $\alpha \in \bar{k}$ be a root of $X^n - a$. Then $k(\alpha)$ is cyclic over k, of degree d for an integer d dividing n such that α^d is an element of k.

PROOF. The proof follows the same steps as in the main theorem of Artin-Schreier-Witt theory, see Lang [Lan02, Theo. VI.6.2] for details. □

The following theorem is an analogue of Theorem II.2.5.

Theorem 2.8. *Let K be a global field of characteristic $p \geqslant 0$ containing a primitive n-th root of unity, where $n > 0$ is an integer such that $p \nmid n$. Let $L = K(\sqrt[n]{\alpha})$ for an element $\alpha \in K$, and let P be a non-archimedean place of K.*

i) P splits completely in K if and only if $\alpha \in (K_P^\times)^n$.

ii) P is unramified in K if and only if one can choose α such that it is a unit at P.

iii) Let ζ_n be a primitive n-th root of unity. If P is unramified, the Frobenius automorphism $(P, L/K)$ acts on $\sqrt[n]{\alpha}$ by

$$(P, L/K)(\sqrt[n]{\alpha}) = \zeta_n^{n_P} \sqrt[n]{\alpha},$$

where n_P satisfies

$$\alpha^{\lceil \mathrm{N}(P)/n \rceil} \equiv \zeta_n^{n_P} \bmod P.$$

PROOF. We follow Artin and Tate [AT09, Theo. VI.4]. The fact that P splits totally means that the completion of L at any place above P is K_P itself. Since the completion is equal to $K_P(\sqrt[n]{\alpha})$, i) follows at once. We now prove ii). Let Q be a place of L above P. The fact that P is unramified means that the valuation groups of L_Q and K_P must be the same. In L_Q we can write $\alpha = (\alpha^{1/n})^n$, so α is a n-th power in L_Q, and so its valuation at P is divisible by n, hence $v_P(\alpha) = nr$ for some r. If π is a uniformizer of K at P, then the element $\alpha(\pi^{-r})^n$ is a P-unit and can be taken for a generator of L/K.

Conversely, assume that α is a P-unit; we have to show that L/K is unramified at P. The element $\beta = \sqrt[n]{\alpha}$ is a solution of the equation $f(X) = X^n - \alpha = 0$, and $f'(\beta) = n\beta^{n-1}$ is a P-unit. A classical local criterion then gives the result (see for instance Fröhlich [Frö67, p. 30] or Stichtenoth [Sti09, Cor. 3.5.11]). Finally, let Q be a place of L above P. By definition of $(P, L/K)$, we have

$$\sqrt[n]{\alpha}^{\mathrm{N}(P)} \equiv \zeta_n^{n_P} \sqrt[n]{\alpha} \bmod Q.$$

Note that $\mathbb{F}_P$ contains the n-th roots of 1, so $\mathrm{N}(P) \equiv 1 \bmod n$. Therefore, we obtain

$$\alpha^{(N(P)-1)/n} = \alpha^{\lceil \mathrm{N}(P)/n \rceil} \equiv \zeta_n^{n_P} \bmod P,$$

as required. □

3 Computing abelian coverings

From now on, let K be a global function field defined over a finite field $\mathbb{F}_q$. Let $\mathfrak{m}$ be a modulus and let H be a congruence subgroup modulo $\mathfrak{m}$. In this section we explain how to compute the class field L of H. The similar approach for number fields has been introduced by Fieker [Fie01], where one will find more algorithmic details, and for the computations of groups of units and ray class groups, see Hess, Pauli, and Pohst [HPP03].

REDUCTION TO THE CYCLIC CASE

First, we show how to reduce the problem to the case of a cyclic extension of prime power degree. For this, we use the fundamental theorem of abelian groups to decompose $\bar{H} = \mathrm{Div}_{\mathfrak{m}}/H$ as a finite product of cyclic groups

$$\bar{H} = \prod_{i=1}^{d} \bar{H}_i,$$

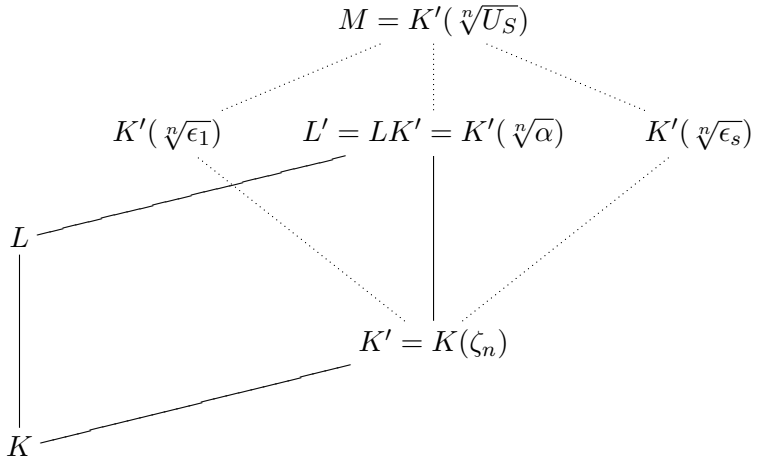


Diagram II.1: Fields used implicitly in the discussion.

where each $\bar{H}_i$ is of the form $\mathrm{Div}_{\mathfrak{m}}/H_i$ for a subgroup $H \subseteq H_i \subseteq \mathrm{Div}_{\mathfrak{m}}$ such that $\bar{H}_i \cong \mathbb{Z}/\ell_i^{m_i}\mathbb{Z}$ for some prime number p_i and some positive integer m_i. For every i, let L_i be the class field of H_i, so $\mathrm{Gal}(L_i/K) \cong \bar{H}_i$, and let L' be the composite field $L_1 L_2 \cdots L_d$. By general Galois theory, $\mathrm{Gal}(L'/K)$ is isomorphic to the subgroup of elements of $\prod_{i=1}^{d} \mathrm{Gal}(L_i/K)$ which agree on $L_1 \cap \cdots \cap L_d$. The functoriality of the Artin map implies that the previous condition is always satisfied, so

$$\mathrm{Gal}(L'/K) \cong \prod_{i=1}^{d} \mathrm{Gal}(L_i/K).$$

Thus $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$ are equal, and by the uniqueness property of the class field, we conclude that $L = \prod_{i=1}^{d} L_i$. Also, note that if we have equations for two abelian extensions L_1/K and L_2/K, then there are algorithms based on the theory of resultants to compute an equation of $L_1 L_2/K$.

CYCLIC CASE: $\ell \neq p$

Now suppose that $\bar{H}$ is cyclic of prime power degree $n = \ell^m$ for a prime ℓ different from p and an integer $m \geq 1$. As in the proof of the Existence Theorem, the idea consists of reducing to the case when K contains the n-th roots of unity, and then to use explicit Kummer theory. So let ζ_n be a primitive n-th root of unity, and let $K' = K(\zeta_n)$. Let $L' = LK'$. We will translate the problem to the extension L'/K'. (Note that the extension K'/K is a constant field extension, hence it is unramified.)

We will refer to Diagram II.1; the solid lines in the figure connect fields that are actually constructed during the execution of the algorithm, while dotted lines connect fields that are only implicitly used.

By Theorem II.2.7, since L/K is cyclic of degree n, the field $L' = L(\zeta_n) = K'L$ is a Kummer extension of K', and hence there exists a nonzero element $\alpha \in K'$ such that $L' =$

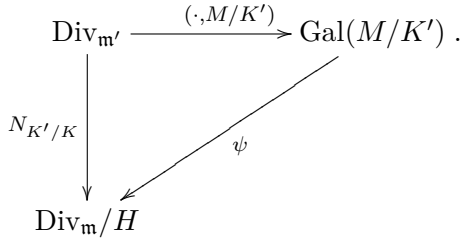


Diagram II.2: Definition of ψ.

$K'(\sqrt[n]{\alpha})$. Now by Theorem II.2.8 ii), since L'/K has to be unramified outside places in the modulus $\mathfrak{m}$ of L/K, there exists a set S of places of K', depending only on $\mathfrak{m}$ and K', such that α can be chosen as an element of the S-units U_S, that is, as an element that has no poles outside S; in particular, L'/K' is unramified outside S. Let $\mathfrak{m}'$ be an admissible modulus for L'/K', and assume without loss of generality that $\mathfrak{m}'$ is supported on S. By the Dirichlet unit theorem, we have

$$U_S = \langle \epsilon_1, \ldots, \epsilon_s \rangle$$

for independent elements ϵ_i ($1 \leq i \leq s-1$) and a torsion unit ϵ_s. Set $M = K'(\sqrt[n]{U_S})$, so that

$$\mathrm{Gal}(M/K') = (\mathbb{Z}/n\mathbb{Z})^s.$$

For any place P of K' unramified in M/K', the Frobenius $(P, M/K')$ at P is defined by its operation on the $\sqrt[n]{\epsilon_i}$. Since M/K' is unramified outside S, we see that we get a map

$$\mathrm{Div}_{\mathfrak{m}'} \to (\mathbb{Z}/n\mathbb{Z})^s$$

defined by $P \mapsto (n_i)$, where n_i satisfies

$$\epsilon_i^{\lceil \mathrm{N}(P)/n \rceil} \equiv \zeta_n^{n_i} \bmod P.$$

(Theorem II.2.8 iii)). In summary, the Artin map from $\mathrm{Div}_{\mathfrak{m}'}$ to $(\mathbb{Z}/n\mathbb{Z})^s$ is explicit and can be computed in K'!

To compute L' we need to find divisors $D \in \mathrm{Div}_{\mathfrak{m}'}$ such that $(D, M/K')$ fixes L'. By the Existence Theorem, this is equivalent to $D \in H'$, where H' is the congruence subgroup modulo $\mathfrak{m}'$ whose class field is L'. By standard properties of the Artin map, this reduces to $\mathrm{N}_{K'/K}(D) \in H$. We use this as summarized in Diagram II.2 to explicitly construct the map ψ: Computing $(P, M/K')$ on the one side and $\mathrm{N}_{K'/K}(P) + H \in \mathrm{Div}_{\mathfrak{m}}/H$ on the other, we collect (small) places outside S until the full group $\mathrm{Gal}(M/K')$ can be generated. The field L' is then obtained as the field fixed by the kernel of ψ.

In order to find α we apply a similar idea (see Fieker [Fie01, §4] for details): L'/K is abelian and the Galois group can be computed explicitly. Once the automorphisms of L'/K are known, we can easily establish again an explicit Artin map, now from $\mathrm{Div}_{\mathfrak{m}}$ to $\mathrm{Gal}(L'/K)$, and find the subgroup fixing L as above. We note that the conductor of L' can be larger than the conductor

of L/K, but since L' is obtained via a constant field extension, the ramified primes remain the same, hence the map is well defined and surjective (but the kernel may not be a congruence subgroup modulo $\mathfrak{m}$).

CYCLIC CASE: $\ell = p$

Finally we turn to the case when L/K is cyclic of degree $n = p^m$, for an integer $m \geq 1$. By Theorem II.2.4, we can assume that the cyclic extension of degree p^m of K is of the form $L = K(y)$ for some $x \in \mathbb{W}_m(K)$ and $y \in \mathbb{W}_m(\bar{K})$ satisfying $\wp(y) = x$, and we now explain how to compute x. It is clear that the extension does not change if one replaces x with $x + \wp(z)$ for some z in $\mathbb{W}_m(K)$, so we will look for x as an element of $\mathbb{W}_m(K)/\wp(\mathbb{W}_m(K))$.

We first look at the case $m = 1$; hence we assume that L/K is a cyclic extension of degree p. We also make use of the fact that the ramified places P in L/K (which appear in the support of $\mathfrak{m}$) are exactly those for which there exists a u_P as in Proposition II.2.6 such that $\lambda_P = -v_P(y + u_P^p - u_P)$ is positive and coprime to p; furthermore, the conductor $\mathfrak{f}_{L/K}$ verifies $v_P(\mathfrak{f}_{L/K}) = \lambda_P + 1$ by Theorem II.2.5 i), so λ_P does not depend on y. Thus, while Proposition II.2.6 helps us understand the ramification in L/K, if we want to explicitly compute L we need to find a Riemann-Roch space containing the generator x. With this in mind, we combine Proposition II.2.6 with the strong approximation theorem to get a global result.

Lemma 3.1. *Let y be an element of K. For every place P of K, let u_P and λ_P be as above. Let S be the set of places P of K such that $\lambda_P > 0$, and let*

$$S' = \{P \in \mathrm{Pl}_K : v_P(y) < 0\},$$

so that $S \subseteq S'$. Fix an arbitrary place $P_0 \notin S'$, and let n_0 be a positive integer such that $D = n_0 P_0 - \sum_{P \in S'} 2P$ is nonspecial. Then there exists an element $u \in K$ such that

- $v_P(y + u^p - u) = -\lambda_P$ *for $P \in S$,*
- $v_P(y + u^p - u) \geq 0$ *for $P \notin S \cup \{P_0\}$, and*
- $v_{P_0}(y + u^p - u) \geq -pn_0$.

PROOF. By the strong approximation theorem and its proof [Sti09, Theo. 1.6.5], there exists an element u in K such that $v_P(u - u_P) = 1$ for $P \in S'$, $v_P(u) \geq 0$ for $P \notin S' \cup \{P_0\}$, and $v_{P_0}(u) \geq -n_0$. We have

$$\begin{aligned} v = v_P(y + u^p - u) &= v_P(y + u_P^p - u_P + (u - u_P)^p + (u_P - u)) \\ &\geq \min\{v_P(y + u_P^p - u_P), pv_P(u - u_P), v_P(u_P - u)\}, \end{aligned}$$

which shows that $v = -\lambda_P$ if $P \in S$, and $v \geq 0$ if $P \in S' \setminus S$. In the same way,

$$\begin{aligned} v &= v_P(y + u_P^p - u_P + (u^p - u) - (u_P^p - u_P)) \\ &\geq \min\{v_P(y + u_P^p - u_P), v_P(u^p - u), v_P(u_P^p - u_P)\}, \end{aligned}$$

so $v \geq 0$ if $P \notin S' \cup \{P_0\}$, and $v \geq -pn_0$ if $P = P_0$ (note that $u_P = 0$ when $P \notin S'$). □

Thus $x = y + u^p - u$ is an element of the Riemann-Roch space

$$\mathcal{L}\left(pn_0P_0 + \sum_S \lambda_P P\right) = \left\{f \in K : \mathrm{div}(f) \geq -pn_0P_0 - \sum_S \lambda_P P\right\}.$$

We now return to our hypothesis that L/K is a cyclic extension of degree p^m for some $m \geq 1$, with primitive element x. As above, let

$$\lambda_P = -v_P(x) = (-v_P(x_1), \ldots, -v_P(x_m)).$$

By adding elements of the form $\wp(0, \ldots, 0, x, 0, \ldots, 0)$ we can assume that there exist sets $S_i \subset \mathrm{Supp}(\mathfrak{m})$, places $P_{0,i}$ not in S_i, and positive integers $n_{0,i}$ such that x_i is in $\mathcal{L}(pn_{0,i}P_{0,i} + \sum_{S_i} \lambda_{P,i}P)$, where $\lambda_{P,i} = -v_P(x_i) > 0$ and $\gcd(\lambda_{P,i}, p) = 1$ for $P \in S_i$.

Setting

$$M_P = \max\{p^{m-i}\lambda_{P,i} : 1 \leq i \leq m\},$$

we obtain $v_P(\mathfrak{f}_{L/K}) = M_P + 1$ from Theorem II.2.5 i). Given that we already know a modulus $\mathfrak{m}$ such that $\mathfrak{f}_{L/K} \leq \mathfrak{m}$, we immediately get $\lambda_{P,i} \leq (v_P(\mathfrak{m}) - 1)p^{i-m}$. If $\mathfrak{m} = \sum_P n_P P$ we set

$$D_i = pn_{0,i}P_{0,i} + \sum_{S_i}(n_P - 1)p^{i-m}P.$$

With this notation, we see that x_i is an element of $\mathcal{L}(D_i)$.

By induction, we assume that the x_i have been computed for $1 \leq i \leq m-1$ and explain how to find x_m. Set

$$M_m = K(\wp^{-1}(x_1, \ldots, x_{m-1}))$$

and $D = D_m$; as remarked above, we can identify x_m as an element of the $\mathbb{F}_q$-vector space

$$\overline{\mathcal{L}_K}(D) = \mathcal{L}_K(D)/\wp(\mathcal{L}_K(D)).$$

Let d be the dimension of this space over $\mathbb{F}_p$. We compute an $\mathbb{F}_p$-basis of $\overline{\mathcal{L}_K}(D)$ and lift it to a set of d elements $\{f_1, \ldots, f_d\}$ of $\mathcal{L}_K(D)$. Hence x_m is an element of the sub-vector space of $\mathcal{L}_K(D)$ generated by the f_i, and we have

$$x_m = \sum_{i=1}^{d} a_i f_i$$

for some unknown elements a_i of $\mathbb{F}_p$. Next, we set

$$M = K(\wp^{-1}((x_1, \ldots, x_{m-1}, \mathcal{L}_K(D)))) = M_m(\wp^{-1}(0, \ldots, 0, \mathcal{L}_K(D))),$$

so that we have a tower $K \subset M_m \subset L \subset M$. Note that as in the Kummer case, neither M nor M_m is actually ever constructed. We will use the explicit action of the Frobenius automorphisms on Witt vectors of length m, so we identify $(x_1, \ldots, x_{m-1})$ with $(x_1, \ldots, x_{m-1}, 0) \in \mathbb{W}_m(K)$

and f_i with $(0,\dots,0,f_i) \in \mathbb{W}_m(K)$. Let P be an unramified place of K; by Theorem II.2.5 ii) the Frobenius automorphism $(P, L/K)$ acts on y via the formula

$$(P, L/K)(y) = y + \left\{\frac{x}{P}\right\}.$$

We now compute $\mathrm{Gal}(M/M_m)$. We have canonical isomorphisms

$$\mathrm{Gal}(M/M_m) \cong \prod_{i=1}^{d} \mathrm{Gal}(M_m(0,\dots,0,\wp^{-1}(f_i))/M_m) \cong (\mathbb{Z}/p\mathbb{Z})^d,$$

and this is made explicit via the Frobenius: Every $\mathrm{Gal}(M_m(0,\dots,0,\wp^{-1}(f_i))/M_m)$ is generated by the isomorphisms $(Q, M_m(0,\dots,0,\wp^{-1}(f_i))/M_m)$, where Q is a place of M_m. Because of the canonical isomorphism

$$\mathrm{Gal}(M_m(0,\dots,0,\wp^{-1}(f_i))/M_m) \cong \mathrm{Gal}(K(\wp^{-1}(f_i))/K),$$

the generating isomorphisms are of the form

$$y_i \mapsto y_i + \left\{\frac{f_i}{P}\right\},$$

where y_i is a primitive element of $K(\wp^{-1}(f_i))/K$ and P is the place of K below Q. Since the symbol $\{\cdot\}$ is additive, we have

$$\mathrm{Gal}(K(\wp^{-1}(f_i))/K) \cong \left\langle \left\{\frac{f_i}{P}\right\} \right\rangle,$$

and so the isomorphism $\mathrm{Gal}(M/M_m) \cong (\mathbb{Z}/p\mathbb{Z})^d$ is made explicit via the map

$$(Q, M/M_m) \mapsto \left(\left\{\frac{f_1}{P}\right\}, \dots, \left\{\frac{f_d}{P}\right\} \right).$$

We lift the terms in $\{\cdot\}$ from $\mathbb{W}_m(\mathbb{F}_p)$ to $\mathbb{Z}_p$, and if we can find enough places P_i such that the $\mathbb{Z}_p$-vectors

$$\left(\left\{\frac{f_1}{P_i}\right\}, \dots, \left\{\frac{f_d}{P_i}\right\} \right)_i$$

form a matrix of rank d over $\mathbb{Z}_p$, then we are done, because by class field theory every element of $\mathrm{Gal}(M/M_m)$ is a Frobenius automorphism for some place Q. The generator is now obtained in exactly the same way as in the previous section for Kummer extensions, for which all that is necessary is an explicit Artin map.

4 An algorithm to find curves with many points

We now turn to the explicit applications of the theory described in the preceding sections, and we switch between the language of curves and function fields when necessary. Our aim here

is to find curves of low genus ($g \leq 50$) defined over a small finite field ($q \leq 100$) such that the number of rational points is the maximum possible; the current records can be found at `www.manypoints.org`. So we will only be interested in the abelian extensions L of K defined over the same finite field $\mathbb{F}_q$ such that the number of rational places of the field L is greater than or equal to the corresponding entry in the table[2] (as it was in June 2011). Furthermore, with the aid of the theory of §II.3, we will be able to find the equations of such extensions.

Proposition 4.1. *Let L/K be a cyclic extension of prime degree ℓ of function fields defined over a finite field $\mathbb{F}_q$. The genus of L satisfies*

$$g_L = 1 + \ell(g_K - 1) + \frac{1}{2}(\ell - 1)\deg \mathfrak{f}_{L/K}.$$

PROOF. By the Riemann-Hurwitz genus formula, this comes down to showing that the degree of the different $\mathcal{D}_{L/K}$ of L/K is $(\ell - 1)\deg \mathfrak{f}_{L/K}$. Let Q be a place of L and let P be the place of K below Q. The extension being Galois, the inertia degree of P relative to Q is independent of Q, so we denote it f_P. From the general relation $\deg Q = f_P \deg P$, we note that $\deg \mathrm{N}_{L/K}(\mathcal{D}_{L/K}) = \deg \mathcal{D}_{L/K}$. By the conductor-discriminant formula, $\mathrm{N}_{L/K}(\mathcal{D}(L_K))$ is equal to $(\ell - 1)\mathfrak{f}_{L/K}$, so by taking degrees we obtain the proposition. □

From Proposition II.4.1, the genus of a cyclic extension of global function fields L/K of prime degree is determined by its conductor $\mathfrak{f}_{L/K}$, or even simply by $\deg(\mathfrak{f}_{L/K})$. On the other hand, $\mathfrak{f}_{L/K}$ identifies L as the unique field such that the Galois group of L/K is a quotient of the ray class group modulo $\mathfrak{f}_{L/K}$ by a certain subgroup of finite index. So, starting from a prime number ℓ and a modulus $\mathfrak{m}$ defined over a global function field K with field of constants $\mathbb{F}_q$, one can enumerate all the cyclic extensions L of K of degree ℓ and of conductor $\mathfrak{f}_{L/K}$ less than $\mathfrak{m}$ by computing all the subgroups of index ℓ of $\mathrm{Pic}_{\mathfrak{m}}$. We also know in advance that the genus of these extensions will be less than

$$1 + \ell(g_K - 1) + \frac{1}{2}(\ell - 1)\deg \mathfrak{m}.$$

Since ℓ is a prime, all places which ramify have the same ramification type: Either they are all wildly ramified, or they are all tamely ramified. The following proposition describes what kind of $\mathfrak{m}$ one should test for a given ℓ.

Proposition 4.2. *Let L/K be an abelian extension of function fields. Let P be a place of K. Then P is wildly ramified in L/K if and only if P appears in the conductor of L/K with multiplicity greater than 2, that is,*

$$P \text{ is wildly ramified if and only if } \mathfrak{f}_{L/K} \geq 2P.$$

PROOF. From Milne [Mil11a, Corollary 7.59], we see that a place P is tamely ramified if and only if the first ramification group in upper numbering is trivial, and from the local-global property of the conductor, this amounts to saying that P has weight one in $\mathfrak{f}_{L_K}$. So a place with weight at least two must be wildly ramified. □

[2]Note that L will be defined over $\mathbb{F}_q$ if at least one rational place of K splits totally in L, which will be the case when we are looking for L with many rational places.

We see that if ℓ is prime to the characteristic p of K, then $\mathfrak{m}$ must be of the form

$$\mathfrak{m} = \sum_{i=1}^{n} P_i,$$

whereas if ℓ equals p, then $\mathfrak{m}$ must be of the form

$$\mathfrak{m} = \sum_{i=1}^{n} m_i P_i,$$

where $m_i \geq 2$.

Because we want the greatest possible number of rational places for the field L, and because of the formula

$$N(L) = \ell \cdot \#S + r$$

(where S is the set of rational places of K which split in L and r is the number of rational places in the support of $\mathfrak{f}_{L/K}$), it seems reasonable to start from a field K which itself has many rational points compared to its genus. In this way, we will find curves with many points and their equations recursively: We start from the projective line or a maximal elliptic curve, compute all of its 'best' coverings reaching or improving a lower bound in `www.manypoints.org`, start the process again on these coverings, and so on. We summarize the process in Algorithm 1 below. Note that a reasonable restriction, especially when the size of the constant field increases, could be to take only conductors with places of degree 1 in their support.

Algorithm 1 (Good abelian coverings)

Input: A function field $K/\mathbb{F}_q$, a prime ℓ, an integer G.

Output: The equations of all cyclic extensions of K of degree ℓ and genus less than G whose number of $\mathbb{F}_q$-rational points improves the current records.

1. Compute all the moduli of degree less than $B = (2G - 2 - \ell(2g(K) - 2))/(\ell - 1)$ using Proposition II.4.2.
2. **for** each such modulus $\mathfrak{m}$ **do**
3. Compute the ray class group $\mathrm{Pic}_{\mathfrak{m}}$ modulo $\mathfrak{m}$.
4. Compute the set S of subgroups of $\mathrm{Pic}_{\mathfrak{m}}$ of index ℓ and conductor $\mathfrak{m}$.
5. **for** every s in S **do**
6. Compute the genus g and the number of rational places n of the class field L of s.
7. **if** n is greater or equal to the known record for a genus g curve defined over $\mathbb{F}_q$ **then**
8. Update n as the new lower bound on $N_q(g)$.
9. Compute and output the equation of L.
10. **end if**
11. **end for**
12. **end for**

The complexity of the algorithm is linear in the number of fields (or pairs of divisors and subgroups) we need to consider. The total number of divisors of degree bounded by B is roughly

$O(q^B)$ since this is the estimate for the number of irreducible polynomials of degree bounded by B. The number of subgroups to consider depends on the structure of the ray class group. For tamely ramified extensions, the group is the extension of the divisor class group by the product of the multiplicative groups of the divisors (modulo constants), so the number of cyclic factors depends on the number of places such that $\ell \mid q^{\deg P} - 1$. For wild extensions, the number of ramified places provides the same information. In the wild case, the number is bounded by $B/2$, so the total number of fields to investigate is roughly $O(q^B \cdot q^{B/2})$. For each pair we have to compute the genus and the number of rational places. The computation of the genus can be seen to run in time quartic in the number of (potentially) ramified places, since for each place we need to check if it divides the conductor. This test is done by some $\mathbb{Z}$-HNF computation of a matrix whose dimension depends again on the total number of places. The computation of the number of rational places requires the computation of discrete logarithms in the divisor class group for every rational place of the base field. Assuming a small degree, this depends linearly on the number of ramified places.

In summary, the total complexity is essentially exponential in the genus bound, and is thus limited in scope.

Remark 4.3. It is possible to extend the algorithm to coverings of nonprime degrees, to include Artin-Schreier-Witt extensions for example, and this is what we have implemented in Magma. The genus and the conductor can then be computed using techniques of Hess, Pauli, and Pohst [HPP03]. Note however that the computations then are much longer. This is the reason why we presented the algorithm only for cyclic extensions of prime degree: Since their arithmetic is simpler, the algorithm works best for them and can thus be used more efficiently over finite fields of size greater than 2 or 3.

5 Results

In this section we present the explicit results we obtained by implementing our algorithm. All of our computations were carried out in Magma [BCP97], using a class field theory library implemented by Claus Fieker.

We restrict our attention here to the case where the base field is $\mathbb{F}_2$.

In Table II.1 we give the equations for the base curves to which we applied our algorithm. The curves D_g have genus g and are maximal; the curves D'_g have genus g and satisfy $\#D'_g(\mathbb{F}_2) = N_q(g) - 1$. Note that Rigato [Rig10] has shown that the maximal curves of genus 1, 2, 3, 4, and 5 over $\mathbb{F}_2$ are unique.

Table II.2 presents data on the curves we constructed that improved the previous records for the number of points on a curve of genus g over $\mathbb{F}_2$. The first two columns in the table give the genus g and the number of rational points N on the abelian coverings we construct. The third column gives the Oesterlé bound on the number of rational points of a g curve of genus g defined over $\mathbb{F}_2$; in the cases we consider this is the best upper bound known. The fourth column gives the name (from Table II.1) of the base curve used in the construction. The fifth column gives the conductor of the covering; a summand of the form $n_i P_i$ means that there is a place of degree i occurring in the conductor with weight n_i. The final four columns give the Galois group G of

Name	f
D_1	$y^2 + y + x^3 + x$
D_2	$y^2 + (x^3 + x + 1)y + x^5 + x^4 + x^3 + x$
D_3	$y^3 + x^2y^2 + (x^3 + 1)y + x^2 + x$
D_4	$y^4 + (x + 1)y^2 + (x^3 + x)y + x^7 + x^3$
D_5	$y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^7 + x^6 + x^5 + x^4$
D_6	$y^4 + (x^6 + x^5 + x^4 + 1)y^2 + (x^7 + x^4 + x^3 + x^2)y + x^{11} + x^{10} + x^3 + x^2$
D_7	$y^4 + (x^7 + x^6 + x^4 + x^2 + 1)y^2 + (x^8 + x^6 + x^5 + x^4)y + x^{10} + x^8 + x^6 + x^4$
D'_1	$y^2 + xy + x^3 + x$
D'_2	$y^2 + y + x^5 + x$
D'_3	$y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^6 + x^5$
D'_4	$y^4 + xy^2 + (x + 1)y + x^5 + x^4 + x^3 + x^2$
D'_5	$y^4 + (x^3 + 1)y^2 + (x^4 + x^2)y + x^9 + x^5$
D'_6	$y^4 + (x^3 + x + 1)y^2 + (x^3 + x)y + x^9 + x^8 + x^5 + x^4$
D'_7	$y^4 + x^7y^2 + (x^7 + 1)y + x^5 + x$

Table II.1: Equations $f = 0$ for the base curves over $\mathbb{F}_2$ used in our calculations. The curves D_g have genus g and are maximal; the curves D'_g have genus g and satisfy $\#D'_g(\mathbb{F}_2) = N_2(g) - 1$.

the covering, the number $\#S$ of totally split places, the number $\#T$ of totally ramified places, and the number $\#R$ of partially ramified places. In some cases we obtained the same values of g and N by applying our algorithm to different base curves; in these cases, we only make one entry in our table, corresponding to the construction using the base curve with the smallest genus. Finally, we mention that the average bound on the degree of the possible conductors we have tested was 14.

For each row of Table II.2, let C_g denote the covering curve of genus g corresponding to that row. We present explicit equations for each C_g below; these are equations for the C_g as coverings of their base curves, so the equations for the base curves (given in Table II.1) are left unstated here. We have attempted to present the equations so that the structure of each cover as a tower of Artin-Schreier covers is clear.

$$C_{14}\colon \begin{cases} 0 = (x^7 + x^3 + 1)(z^2 + z) \\ \qquad + y^3 + (x^4 + x)y^2 + (x^4 + x^2 + 1)y + (x^8 + x^6 + x^5 + x^4) \end{cases}$$

$$C_{17}\colon \begin{cases} 0 = z^2 + x^2z \\ \qquad + x(x + 1)(x^3 + x^2 + 1)y + x^2(x + 1)^2(x^4 + x^3 + x^2 + x + 1) \\ 0 = w^2 + xw + x(x + 1)(x^2 + x + 1)y + x^2(x + 1) \end{cases}$$

g	N	Oesterlé bound	Base curve	Conductor $\mathfrak{f}$	Galois group G	$\#S$	$\#T$	$\#R$
14	16	16	D_4	$2P_7$	$\mathbb{Z}/2\mathbb{Z}$	16	0	0
17	18	18	D_2	$4P_1 + 6P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	16	2	0
24	23	23	D_4'	$2P_1 + 4P_1 + 2P_2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	20	1	2
29	26	27	D_4	$4P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	24	2	0
41	34	35	D_3'	$4P_1 + 4P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	2	0
45	34	37	D_2	$4P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	2	0
46	35	38	D_3	$3P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	1	2

Table II.2: New results over $\mathbb{F}_2$. For each genus g in the leftmost column, we give the largest number N for which we have constructed a genus-g curve over $\mathbb{F}_2$ having N rational points. The meaning of the other columns is explained in the text.

$$C_{24}\colon \begin{cases} 0 = z^2 + x^2(x+1)z \\ \qquad + x(x^3+x^2+1)y^3 + x^3(x+1)^4y^2 + x^2(x^4+x^3+1)y \\ \qquad + x(x+1)(x^7+x^6+x^3+x^2+1) \\ 0 = w^2 + x^2w \\ \qquad + x(x+1)y^3 + x^3(x+1)^2y^2 + x^2(x+1)^2y + x(x+1)(x^2+x+1) \end{cases}$$

$$C_{29}\colon \begin{cases} 0 = z^2 + x^2(x+1)^4z \\ \qquad + (x+1)(x^6+x^5+x^4+x^3+1)y^3 \\ \qquad + x(x+1)^3(x^5+x^4+x^3+x^2+1)y^2 + (x+1)^2(x^6+x^2+1)y \\ \qquad + x^2(x+1)^3(x^5+x^4+x^3+x^2+1) \\ 0 = w^2 + x^2(x+1)^5w \\ \qquad + (x+1)(x^9+x^8+x^5+x^4+1)y^3 \\ \qquad + x(x+1)^3(x^9+x^8+x^6+x^5+x^4+x^2+1)y^2 \\ \qquad + (x+1)^2(x^9+x^8+x^3+x^2+1)y \\ \qquad + x^2(x+1)^3(x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^2+1) \end{cases}$$

$$C_{41}\colon \begin{cases} 0 = z^2 + \big[x^6(x^2+x+1)y^3 + x^7(x^4+x^3+x^2+x+1)y^2 \\ \qquad + x^6(x+1)(x^2+x+1)y + x^{10}(x+1)^4\big]z \\ \qquad + x(x+1)^7(x^{13}+x^{12}+x^{11}+x^9+x^6+x^4+1)y^3 \\ \qquad + x^2(x+1)^3(x^{17}+x^{15}+x^{12}+x^{11}+x^9+x^3+1)y^2 \\ \qquad + x(x+1)^6(x^{17}+x^{15}+x^{14}+x^{13}+x^4+x^2+1)y \\ \qquad + x^5(x+1)^4(x^{17}+x^{16}+x^{12}+x^{11}+x^6+x^3+1) \\ 0 = v^2 + x^7v + xz \\ 0 = w^2 + x^2w + xy^2 + x^2y \end{cases}$$

$$C_{45}\colon \begin{cases} 0 = z^2 + (x+1)^2(xy+1)z \\ \qquad + x^2(x^{13}+x^{11}+x^9+x+1)y + x^9(x^8+x^6+x^4+x^3+x^2+x+1) \\ 0 = v^2 + (x+1)^2 v + x(x+1)z + x^7(x^4+x+1) \\ 0 = w^2 + (x+1)^2 w + (x+1)(x^5+x^2+x)y + (x+1)(x^8+x^5+x^4) \end{cases}$$

$$C_{46}\colon \begin{cases} 0 = z^2 + \big[(x+1)y^2 + (x^3+x^2+1)y + (x^4+x^3+x^2+x+1)\big]z \\ \qquad + (x+1)^2(x^{11}+x^8+x^6+x+1)y^2 + (x+1)^6(x^9+x^2+1)y \\ \qquad + x^7(x+1)^2(x^7+x^5+x^4+x^3+1) \\ 0 = v^2 + v + x(x+1)z + x^5(x+1) \\ 0 = w^2 + w + xy^2 + x^2(x^3+x^2+1)y \end{cases}$$

Remark 5.1. After the article [DF13] was written, a preprint now published of Karl Rökaeus appeared in which he undertakes similar computations over the finite fields of size 2, 3, 4, and 5 [Rök13]. Over $\mathbb{F}_2$ he recovers our genus-17 record, and he improves our genus-45 bound to 36 points. (He obtains the record-setting genus-45 curve as an abelian cover of a genus-2 curve D with $\#D(\mathbb{F}_2) = N_2(2) - 2$.) In private communication, Rökaeus indicated that he also found a genus-46 curve over $\mathbb{F}_2$ with 36 points.

Remark 5.2. As mentioned above, we have restricted our search to curves over the field $\mathbb{F}_2$. However, our code works over other fields as well, and while we were testing it we found a curve of genus 11 over $\mathbb{F}_3$ with 21 rational points (the Oesterlé bound in this case is 22). This curve is a cover of degree 2 of the maximal curve of genus 4 defined by

$$C\colon y^4 - y^2 + x^6 + x^4 + x^2 = 0.$$

With notation as above, the conductor of the cover is of the form $P_1 + P_1 + P_1 + P_5$, and we have $\#S = 9$, $\#R = 3$, and $\#T = 0$. The resulting cover C' is given by the equation

$$\begin{aligned} z^2 = -(x^5+x^4+x^3-x^2+x-1)\cdot(y+x^2+x)\cdot(y^2+(-x+1)y+x^3-x^2-x+1) \\ \cdot\Big((x^7+x^6+x^5-x^3-1)y^3 + (-x^8+x^6+x^5-x^4-x^3-x)y^2 \\ + (-x^{10}-x^9-x^8+x^5+x^4+x^3-x^2+1)y \\ - x^{12}-x^9-x^8+x^6+x^4+x\Big). \end{aligned}$$

III

QUATERNION ALGEBRAS

In this chapter we gather the information on quaternion algebras we will need in our study of Shimura curves in the next chapter. Almost all we are going to say, together with proofs, can be found in Vignéras [Vig80]. See also the forthcoming book of Voight [Voi], or Sijsling [Sij10] for a summary.

1 Quaternion algebras over a field

Definition. An *algebra* B over a ring R is a ring with a structure of R-module and an embedding of R in the center of B such that we can identify R with its image in B. The algebra B is *simple* if the only two-sided ideals of B are B and $\{0\}$, and B is *central* if R is the center of B. A *quaternion algebra* B over a field F is a central simple algebra of dimension 4 over F.

A quaternion algebra comes naturally equipped with an F-endomorphism $x \mapsto \bar{x}$ which is an involution, and two maps $\mathrm{nrd}, \mathrm{trd} : B \to B$ defined by

$$\mathrm{nrd} : x \mapsto x\bar{x}$$

and

$$\mathrm{trd} : x \mapsto x + \bar{x},$$

which are called the *reduced norm* and *reduced trace* respectively. The reduced norm induces a group homomorphism $B^\times \to F^\times$, and the reduced trace is an F-linear map inducing a non-degenerate pairing $(x, y) \mapsto \mathrm{trd}(x\bar{y})$ on B. The Skolem-Noether theorem implies that every F-automorphism of B is an inner automorphism.

One verifies easily for all $x \in B$ that

$$x^2 - \mathrm{trd}(x)x + \mathrm{nrd}(x) = 0,$$

so any $x \notin F$ generates a commutative algebra $F[x]$ of dimension 2 over F for which the involution and identity maps are the only F-automorphisms.

The invertible elements of B are exactly those of nonzero norm, since $x\bar{x} = \mathrm{nrd}(x)$ implies $x^{-1} = \bar{x} \cdot \mathrm{nrd}(x)^{-1}$ when $\mathrm{nrd}(x) \neq 0$. Also, the group of commutators of $B^\times$ is exactly the subgroup B^1 of elements of $B^\times$ of reduced norm 1.

Example 1.1. In some cases we have a very explicit description of B:

a) If B is not a division algebra, then B is isomorphic to the matrix algebra $\mathrm{M}_2(F)$. In this case the involution is

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

so nrd and trd are the usual determinant and trace on $\mathrm{M}_2(F)$. The group of invertible elements of $\mathrm{M}_2(F)$ is $\mathrm{GL}_2(F)$, and the group of commutators is $\mathrm{SL}_2(F)$.

b) When $\mathrm{char}(k) \neq 2$, there exist $a, b \in F$ such that B is isomorphic to the quaternion algebra $\left(\frac{a,b}{F}\right)$, with basis $\{1, i, j, ij\}$ satisfying

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

The involution on $\left(\frac{a,b}{F}\right)$ is defined by

$$x + yi + zj + wij \mapsto x - yi - zj - wij,$$

so $\mathrm{nrd}(x + yi + zj + wij) = x^2 - ay^2 - bz^2 + abw^2$ and $\mathrm{trd}(x + yi + zj + wij) = 2x$. In particular, if $a = b = -1$ and $F = \mathbb{R}$, we obtain the algebra $\mathbb{H}$ of *Hamilton quaternions*, which up to $\mathbb{R}$-isomorphism is the unique division algebra of finite dimension over $\mathbb{R}$.

Note that for any field injection $F \subseteq K$, there is an isomorphism

$$\left(\frac{a,b}{F}\right) \otimes_F K \cong \left(\frac{a,b}{K}\right).$$

We call a field extension K/F a *splitting field* for B, and say that B is *split* by K, if

$$B \otimes_F K \cong \mathrm{M}_2(K).$$

The separable closure F^s of F is a splitting field of B, so in particular when F is separably closed (*e.g.* when $F = \mathbb{C}$), then $B \cong \mathrm{M}_2(F)$.

Definition. Assume that $\mathrm{char}(F) \neq 2$, and let $a, b \in F^\times$. The *Hilbert symbol* of a and b, denoted by $(a, b)_F$, is defined to be 1 if $ax^2 + by^2 - z^2 = 0$ has a nontrivial solution $(x, y, z) \in \mathbb{P}^2(F)$, and -1 otherwise.

In general, if $\mathrm{char}(F) \neq 2$ and $B = \left(\frac{a,b}{F}\right)$, then B is a matrix algebra if and only if $(a, b)_F = 1$.

IDEALS AND ORDERS

We now assume that F is either a number field or a nonarchimedean local field, and let $\mathbb{Z}_F$ be the ring of integers of F.

Definition. A *lattice* of B is a finitely generated $\mathbb{Z}_F$-submodule of B. A *full lattice* I of B is a lattice such that $I \otimes_{\mathbb{Z}_F} F = B$.

An element $b \in B$ is *integral* over $\mathbb{Z}_F$ if $\mathbb{Z}_F[b]$ is a lattice, which is the case if and only if $\mathrm{nrd}(b)$ and $\mathrm{trd}(b)$ belong to $\mathbb{Z}_F$. A ring R is *integral* over $\mathbb{Z}_F$ if all the elements of R are integral over $\mathbb{Z}_F$. The set of integral elements of B does not form a ring, so there is no canonical notion of a 'ring of integers'.

Definition. An *order* $\mathcal{O}$ of B is a full lattice which is also a ring.

In particular $\mathcal{O}$ is integral over $\mathbb{Z}_F$ and satisfies $\mathcal{O} \otimes F = B$. Every order is contained in some maximal order (for the inclusion), and we call the intersection of two (not necessarily distinct) maximal orders of B an *Eichler order*. In particular, every maximal order is an Eichler order.

The *left order* of a full lattice I is the set

$$\mathcal{O}_\ell(I) = \{b \in B : bI \subseteq I\},$$

and one can define the *right order* $\mathcal{O}_r(I)$ similarly. If $\mathcal{O}$ is an order, a full lattice I is called a *left $\mathcal{O}$-ideal* (respectively a *right $\mathcal{O}$-ideal*) if $\mathcal{O}_\ell(I) = \mathcal{O}$ (respectively $\mathcal{O}_r(I) = \mathcal{O}$).

A left or right $\mathcal{O}$-ideal I is called *integral* if $I \subseteq \mathcal{O}$, *two-sided* if it is both a left and right $\mathcal{O}$-ideal, and *principal* if there exists an element $b \in B$ such that $I = \mathcal{O}b = b\mathcal{O}$. We set

$$I^{-1} = \{b \in B : bIb \subseteq I\},$$

and say that I is *invertible* if

$$II^{-1} = I^{-1}I = \mathcal{O}.$$

We define the reduced norm $\mathrm{nrd}(I)$ of an ideal I to be the $\mathbb{Z}_F$-ideal of B generated by the reduced norm of the elements of I. In particular, the reduced norm of an integral $\mathcal{O}$-ideal is an integral $\mathbb{Z}_F$-ideal. Note that an element x of $\mathcal{O}$ is a unit in $\mathcal{O}^\times$ if and only if $\mathrm{nrd}(x)$ is a unit in $\mathbb{Z}_F^\times$, so

$$\mathrm{nrd}^{-1}(\mathbb{Z}_F^\times) \cap \mathcal{O} = \mathcal{O}^\times.$$

Two right $\mathcal{O}$-ideals I and I' are *left-equivalent* if there exists $x \in B^\times$ such that $I = xI'$. The *left classes* of an order $\mathcal{O}$ are the classes $\mathrm{Pic}_\ell(\mathcal{O})$ of invertible right $\mathcal{O}$-ideals which are left-equivalent, and we can define similarly the *right classes* $\mathrm{Pic}_r(\mathcal{O})$ of $\mathcal{O}$. The map $I \to I^{-1}$ induces a bijection between $\mathrm{Pic}_\ell(\mathcal{O})$ and $\mathrm{Pic}_r(\mathcal{O})$, so since the quantity

$$h(\mathcal{O}) = \#\mathrm{Pic}_\ell(\mathcal{O}) = \#\mathrm{Pic}_r(\mathcal{O})$$

is finite, we call $h(\mathcal{O})$ the *class number* of $\mathcal{O}$.

The *different* $\mathcal{D}(\mathcal{O})$ of an order $\mathcal{O}$ is the integral two-sided $\mathcal{O}$-ideal defined to be the inverse of the two-sided $\mathcal{O}$-ideal

$$\mathcal{C} = \{x \in B : \mathrm{trd}(x\mathcal{O}) \subseteq \mathbb{Z}_F\}.$$

The (integral) ideal $\mathfrak{d}(\mathcal{O}) = \mathrm{nrd}(\mathcal{D})$ is called the *reduced discriminant* of $\mathcal{O}$. An inclusion of orders $\mathcal{O} \subseteq \mathcal{O}'$ implies an inclusion of discriminants $\mathfrak{d}(\mathcal{O}) \subseteq \mathfrak{d}(\mathcal{O}')$, with equality if and only if $\mathcal{O} = \mathcal{O}'$.

Example 1.2. The order $\mathrm{M}_2(\mathbb{Z}_F)$ in $\mathrm{M}_2(F)$ is maximal because it has discriminant $\mathbb{Z}_F$.

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

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

Note that f is determined by its restriction to R, so one also speaks of optimal embedding of R into $\mathcal{O}$. Denote by $m(R, \mathcal{O})$ the number of classes of optimal embeddings $f : R \to \mathcal{O}$ under the equivalence relation: f is equivalent to $K : R \to \mathcal{O}$ if and only if there exists $x \in \mathcal{O}^\times$ such that $f(y) = x^{-1} f(y) x$ for all $y \in R$.

2 Quaternion algebras over local fields

The arithmetic of quaternion algebras over local fields is simpler than for general fields. For instance, if $F \neq \mathbb{C}$, then up to F-isomorphism there is only one division quaternion algebra over F (*e.g.* the Hamilton quaternions in the case $F = \mathbb{R}$). Let $B_\mathfrak{p}$ be a quaternion algebra over a non-archimedean local field $F_\mathfrak{p}$, and let $\mathbb{Z}_{F,\mathfrak{p}}$ be the ring of integers of $F_\mathfrak{p}$, with uniformizer $\pi_\mathfrak{p}$. We have $\mathrm{nrd}(B_\mathfrak{p}^\times) = F_\mathfrak{p}^\times$, but in general the arithmetic of $B_\mathfrak{p}$ is very different depending on whether $B_\mathfrak{p}$ is a matrix or division algebra. We begin with this latter case.

$B_\mathfrak{p}$ IS A DIVISION ALGEBRA

Let $B_\mathfrak{p}$ be a division algebra over $F_\mathfrak{p}$. A finite separable extension $K_\mathfrak{p}/F_\mathfrak{p}$ splits $B_\mathfrak{p}$ if and only if the degree $[K_\mathfrak{p} : F_\mathfrak{p}]$ is even. In particular a separable quadratic extension $K_\mathfrak{p}$ of $F_\mathfrak{p}$ splits $B_\mathfrak{p}$, and furthermore $K_\mathfrak{p}$ then embeds in $B_\mathfrak{p}$.

Let $v_\mathfrak{p} : F_\mathfrak{p} \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of $F_\mathfrak{p}$, normalized so that $v_\mathfrak{p}(F_\mathfrak{p}^\times) = \mathbb{Z}$. The map

$$v_{B_\mathfrak{p}} = v_\mathfrak{p} \circ \mathrm{nrd} : B_\mathfrak{p} \to \mathbb{Z} \cup \{\infty\}$$

is a discrete valuation of $B_\mathfrak{p}$. The set

$$\mathcal{O}_{B_\mathfrak{p}} = \{x \in B_\mathfrak{p} : v_\mathfrak{p}(x) \geqslant 0\}$$

is the unique maximal order of $B_\mathfrak{p}$, with unique maximal two-sided $\mathcal{O}_{B_\mathfrak{p}}$-ideal

$$P = \{x \in B_\mathfrak{p}^\times : v_{B_\mathfrak{p}}(x) > 0\}$$

such that $P^2 = \pi_\mathfrak{p} \mathcal{O}_{B_\mathfrak{p}} = \mathcal{O}_{B_\mathfrak{p}} \pi_\mathfrak{p}$. For this reason, we say that $B_\mathfrak{p}$ is *ramified*. Left or right $\mathcal{O}_{B_\mathfrak{p}}$-ideals are in fact two-sided and of the form P^n for some $n \in \mathbb{Z}$. The discriminant of $\mathcal{O}_{B_\mathfrak{p}}$ is

$$d(\mathcal{O}_{B_\mathfrak{p}}) = \mathrm{nrd}(P) = \pi_\mathfrak{p} \mathbb{Z}_{F,\mathfrak{p}}.$$

$B_\mathfrak{p}$ IS THE MATRIX ALGEBRA $\mathrm{M}_2(F_\mathfrak{p})$

Suppose $B_\mathfrak{p} \cong \mathrm{M}_2(F_\mathfrak{p})$. Then every maximal order of $B_\mathfrak{p}$ is conjugate to $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$. The unique prime $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$-ideal P of $B_\mathfrak{p}$ is $\pi_\mathfrak{p}\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$, so the two-sided $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$-ideals of $B_\mathfrak{p}$ are generated by P. In contrast with the case when $B_\mathfrak{p}$ is a division algebra, we say that $B_\mathfrak{p}$ is *split* or *unramified*. This also explains the terminology of splitting field $K_\mathfrak{p}$ for $B_\mathfrak{p}$ as a field such that $B_\mathfrak{p} \otimes_{F_\mathfrak{p}} K_\mathfrak{p}$ is split.

Theorem 2.1. *The right integral $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$-ideals of $B_\mathfrak{p}$ are the distinct ideals*

$$\begin{pmatrix} \pi_\mathfrak{p}^\ell & r \\ 0 & \pi_\mathfrak{p}^m \end{pmatrix} \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}}) \subset \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}}),$$

where ℓ and m are non-negative integers and r runs through a system of representatives of $\mathbb{Z}_{F,\mathfrak{p}}/\pi_\mathfrak{p}^m\mathbb{Z}_{F,\mathfrak{p}}$.

From Theorem III.2.1, we see that the number of right (or left) $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$-ideals of $B_\mathfrak{p}$ of reduced norm $\pi_\mathfrak{p}^d\mathbb{Z}_{F,\mathfrak{p}}$ for $d \geqslant 0$ is equal to $\sum_{i=0}^d \mathrm{N}(\pi_\mathfrak{p})^i$, where $\mathrm{N}(\pi_\mathfrak{p})$ is the cardinality of $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_{F,\mathfrak{p}}/\pi_\mathfrak{p}\mathbb{Z}_{F,\mathfrak{p}}$. This formula will be useful later when we compute the degree of Hecke operators, see (IV.9).

Recall that an Eichler order $\mathcal{O}_\mathfrak{p}$ is the intersection of two maximal ideals. In fact, there exists a unique integer $N \geqslant 0$ such that an Eichler order $\mathcal{O}_\mathfrak{p}$ is conjugate in $B_\mathfrak{p}$ to

$$\mathcal{O}_0(\pi_\mathfrak{p}^N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}}) : c \in \pi_\mathfrak{p}^N\mathbb{Z}_{F,\mathfrak{p}} \right\}.$$

Proposition 2.2. *The normalizer of $\mathcal{O}_0(\pi_\mathfrak{p}^N)$ in $B_\mathfrak{p}^\times = \mathrm{GL}_2(F_\mathfrak{p})$ is*

$$\mathrm{N}_{B_\mathfrak{p}^\times}(\mathcal{O}_0(\pi_\mathfrak{p}^N)) = \left\langle F_\mathfrak{p}^\times \mathcal{O}_0(\pi_\mathfrak{p}^N), \begin{pmatrix} 0 & -1 \\ \pi_\mathfrak{p}^N & 0 \end{pmatrix} \right\rangle.$$

3 Quaternion algebras over number fields

We now assume that F is a number field. We denote a place of F by v, or $\mathfrak{p}$ if it corresponds to a non-archimedean prime of $\mathbb{Z}_F$.

We say that a place v of F is *ramified* in B if $B_v = B \otimes F_v$ is ramified. If $B_v \cong \mathrm{M}_2(F_v)$, we say that B is *split* or *unramified* at v. Therefore $B \cong \left(\frac{a,b}{F}\right)$ is ramified at v if and only if the Hilbert symbol $(a,b)_v = (a,b)_{F_v}$ at v is equal to -1.

The following theorem is fundamental and classifies quaternion algebras over a global field, see Vignéras [Vig80, § III.3] for a proof.

Theorem 3.1 (Classification theorem). *The number of ramified places of B is finite and of even cardinality. Conversely, for any finite set S of places of F such that $\#S$ is even, there exists a quaternion algebra B over F such that S is exactly the set of places of F which ramify in B. Two quaternion algebras B and B' are isomorphic if and only they are ramified at the same places.*

As a consequence of this result, we obtain the *product formula*

$$\prod_v (a,b)_v = 1$$

for the Hilbert symbol.

Definition. We call the product $\mathfrak{D}(B)$ of the finite primes of F which ramify in B the *discriminant* of B.

A consequence of Theorem III.3.1 is that B is split if and only if B_v is split for all places of F (finite and infinite). The first of the following local-global theorems is a generalization of this result.

Theorem 3.2.

i) HASSE-MINKOWSKI THEOREM
A quadratic form has a zero over F if and only if it has a zero over F_v for all places v of F.

ii) NORM THEOREM IN QUADRATIC EXTENSIONS
Let K/F be a quadratic extension of number fields. An element of $F^\times$ belongs to the norm group $\mathrm{N}_{K/F}(K)$ if and only if it belongs to the local norm groups $\mathrm{N}_{K_w/F_v}(K_w)$ for every place v of F and every extension w of v from F to K.

iii) CHARACTERIZATION OF SPLITTING FIELDS
A finite extension of fields K/F splits B if and only if K_w splits B_v for every place v of F and every extension w of v from F to K.

iv) CHARACTERIZATION OF QUADRATIC SUB-EXTENSIONS
A quadratic extension K of F can be embedded in B if and only if K_v is a field for every place v which ramifies in B.

PROOF. See Vignéras [Vig80, § III.3]. □

Let $F^{(+)}$ be the subgroup of $F^\times$ of elements that are positive at every real place of F ramified in B. Eichler proved the following result.

Theorem 3.3 (Eichler norm theorem). *We have*

$$\mathrm{nrd}(B^\times) = F^{(+)}.$$

PROOF. See Vignéras [Vig80, Théo. III.4.1]. □

STRONG APPROXIMATION THEOREM

We now consider adelizations of our objects. We have that F and $F^\times$ have discrete images in $\hat{B}$ and $\hat{B}^\times$ respectively, and that there is a product formula $\prod_v |x|_v = 1$ for $x \in F^\times$.

For every prime $\mathfrak{p}$ of F, one can extend the reduced norm to get a local map $\mathrm{nrd}_\mathfrak{p} : B_\mathfrak{p} \to F_\mathfrak{p}$. This map is continuous by definition, and taking the product of the local norm maps gives rise to an adelic reduced norm map $\mathrm{nrd} : \hat{B} \to \hat{F}$ which is thus also continuous. Let

$$\hat{B}^1 = \{\hat{b} \in \hat{B}^\times : \mathrm{nrd}(\hat{b}) = 1\}.$$

Definition. We say that B *satisfies the Eichler condition* if the set of archimedean places of B contains at least one unramified place.

Theorem 3.4 (Strong approximation theorem). *If B satisfies the Eichler condition, then B^1 is dense in $\hat{B}^1$.*

PROOF. See Vignéras [Vig80, Théo. III.4.3] or Voight [Voi, Theo. 2.11]. □

Eichler used Theorem III.3.4 to prove the following result.

Corollary 3.5 (Eichler). *Assume that B satisfies the Eichler condition. Then if $\mathcal{O}$ is an Eichler order, a left $\mathcal{O}$-ideal is principal if and only if its reduced norm is a principal ideal.*

As can be seen from Theorem III.3.4, the arithmetic of B is greatly influenced by the fact that B satisfies the Eichler condition or not. When F is totally real, we distinguish the two situations and say that B is *indefinite* if B satisfies the Eichler condition and *definite* otherwise. If all the archimedean places of F are unramified in B, we say that B is *totally indefinite*.

LOCAL-GLOBAL DICTIONARY

The map

$$I \mapsto \hat{I} = \prod_\mathfrak{p} I_\mathfrak{p}$$

induces a bijection from the set of $\mathbb{Z}_F$-lattices in B to the set of $\hat{\mathbb{Z}}_F$-lattices in $\hat{B}$, with inverse $\hat{I} \mapsto \hat{I} \cap B$. By restriction, it also induces a bijection between the set of ideals (respectively, orders) of B and the set of ideals (respectively, orders) of $\hat{B}$. If I and J are two lattices (for instance ideals or orders) such that $I \subseteq J$, then there is a group isomorphism $I/J \cong \hat{I}/\hat{J}$.

Many global properties of lattices can be checked locally thanks to this bijection. For instance, being a maximal or an Eichler order, or an integral or two-sided ideal, are all local properties. Also, the completion at a prime $\mathfrak{p}$ of the left (or right) order of an ideal I is the left (or right) order of $I_\mathfrak{p}$, and the same is true for the norm of an ideal or the reduced discriminant of an order. In particular, an order of B is maximal if and only if its reduced discriminant is equal to $\mathfrak{D}(B)$.

The *level* of an Eichler order $\mathcal{O}$ is the integral ideal $\mathfrak{N} = \prod_{\mathfrak{p}} \mathfrak{p}^{N_{\mathfrak{p}}}$, where $N_{\mathfrak{p}}$ is the level of the local Eichler order $\mathcal{O}_{\mathfrak{p}}$ at $\mathfrak{p}$. We sometimes use the notation $\mathcal{O}_0(\mathfrak{N})$ for an Eichler order, to make the level explicit. The level $\mathfrak{N}$ of $\mathcal{O}$ is prime to the discriminant $\mathfrak{D}$ of B, and $\mathcal{O}$ has discriminant $\mathfrak{D}\mathfrak{N}$

Remark 3.6. If we take $B = \mathrm{M}_2(\mathbb{Q})$ and $\mathfrak{N} = N\mathbb{Z}$ for a positive integer N, then the classical congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \in N\mathbb{Z} \right\} \subset B$$

is an Eichler order of level N.

The use of adeles allows us to obtain a nice description of several objects.

Proposition 3.7.

i) The right locally principal $\mathcal{O}$-ideals are in bijection with the set $\hat{B}^\times/\hat{\mathcal{O}}^\times$: to the idele $(x_{\mathfrak{p}})_{\mathfrak{p}}$ one associates the $\mathcal{O}$-ideal I such that $I_{\mathfrak{p}} = x_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$.

ii) The set of locally principal two-sided $\mathcal{O}$-ideals are thus in bijection with $\mathrm{N}_{B^\times}(\hat{\mathcal{O}}^\times)/\hat{\mathcal{O}}^\times$, and $\mathrm{Pic}_r(\mathcal{O})$ is in bijection with $B^\times\backslash\hat{B}^\times/\hat{\mathcal{O}}^\times$.

The number of left (or right) classes of an order $\mathcal{O}$ is finite, and thus so is the number of two-sided classes, because it is bounded by the former quantity. When $\mathcal{O}$ is an Eichler order, we can be more precise if we assume that the Eichler condition is satisfied, as in the next section.

B SATISFIES THE EICHLER CONDITION

From now on we assume that B satisfies the Eichler condition. Let $\mathcal{O}$ be an Eichler order and consider the subgroup $\hat{\mathcal{O}}^\times$ of $\hat{B}^\times$; it is compact and open [Sij10, p. 25]. The reduced norm is open, thus in particular $\mathrm{nrd}(\hat{\mathcal{O}}^\times)$ is open in $\hat{F}^\times$. Let

$$\mathbb{Z}_{F,(+)} = \mathbb{Z}_F \cap F^{(+)}.$$

As in Vignéras [Vig80, Prop. III.5.8], we have

$$\mathrm{nrd}(\mathcal{O}^\times) = \mathrm{nrd}(\hat{\mathcal{O}}^\times \cap B^\times) = \mathrm{nrd}(\hat{\mathcal{O}}^\times) \cap \mathbb{Z}_{F,(+)}.$$

The local description of $\mathcal{O}$ of § III.2 shows that

$$\mathrm{nrd}(\hat{\mathcal{O}}^\times) = \hat{\mathbb{Z}}_F^\times,$$

hence

$$\mathrm{nrd}(\mathcal{O}^\times) = \mathrm{nrd}(\hat{\mathcal{O}}^\times) \cap \mathbb{Z}_{F,(+)} = \hat{\mathbb{Z}}_F^\times \cap \mathbb{Z}_{F,(+)} = \mathbb{Z}_{F,(+)}^\times. \tag{III.1}$$

CLASS GROUPS

By Proposition III.3.7 ii), we have a group isomorphism

$$\mathrm{Pic}_r(\mathcal{O}) = B^\times \backslash \hat{B}^\times / \hat{\mathcal{O}}^\times.$$

Let

$$F^+ = \{x \in F : \iota(x) > 0 \text{ for every real place } \iota : F \hookrightarrow \mathbb{R}\}$$

be the group of totally positive elements of F. We define $\mathbb{Z}_{F,+} = \mathbb{Z}_F \cap F^+$, and

$$B^+ = \{x \in B : \mathrm{nrd}(x) \in F^+\}.$$

The following group will naturally appear in the next chapter

$$\mathrm{Pic}_r^+(\mathcal{O}) = B^+ \backslash \hat{B}^\times / \hat{\mathcal{O}}^\times.$$

Let now

$$\mathrm{Cl}^{(+)}(F) = \{\text{Ideals of } F\}/\{x\mathbb{Z}_F : x \in F^{(+)}\}$$

be the *restricted class group* of F, and let

$$h^{(+)}(F) = \#\mathrm{Cl}^{(+)}(F)$$

be the *restricted class number* of F, relative to B. Let $\mathrm{Cl}^+(F)$ be the narrow class group of F. We have an isomorphism

$$F^+ \backslash \hat{F}^\times / \hat{\mathbb{Z}}_F^\times \xrightarrow{\cong} \mathrm{Cl}_\infty(F)$$

As a consequence of the strong approximation theorem, we have the following theorem.

Theorem 3.8. *The reduced norm map induces bijections of finite sets*

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

and

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

PROOF. See Vignéras [Vig80, p. 89]. □

Corollary 3.9. *The class number $h(\mathcal{O})$ of $\mathcal{O}$ is equal to $h^{(+)}(F)$.*

EMBEDDING NUMBERS

A *quadratic order* R is a finitely generated $\mathbb{Z}_F$-module which is also a ring whose field of fractions is a quadratic extension K of F. Let R be a quadratic order in B and let $h(R)$ be the class number of R. The number of optimal embeddings of R in an Eichler order $\mathcal{O}$ of given level $\mathfrak{N}$ is independent of $\mathcal{O}$ and equal to the product

$$m(R, \mathcal{O}) = \frac{h(R)}{h^{(+)}(F)} \prod_{\mathfrak{p}} m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p})$$

(see Vignéras [Vig80, Prop. III.5.16]).

Let $m_{\mathfrak{p}}(R,\mathcal{O}) = m(R_{\mathfrak{p}},\mathcal{O}_{\mathfrak{p}})$. We can give explicit formulas for the local embedding numbers $m_{\mathfrak{p}}(R,\mathcal{O})$, but we first need to look at the arithmetic of quadratic orders. Let $\mathfrak{F}_R$ be the *conductor* of R in $\mathbb{Z}_K$, that is

$$\mathfrak{F}_R = \{x \in \mathbb{Z}_K : x\mathbb{Z}_K \subseteq R\}.$$

We set $\mathfrak{f}_R = \mathfrak{F}_R \cap \mathbb{Z}_F$ and by abuse of terminology we also call $\mathfrak{f}_R$ the conductor of R.

The *relative discriminant* $\mathfrak{d}_R$ of R over $\mathbb{Z}_F$ is by definition the ideal of $\mathbb{Z}_F$ generated by the discriminants of all $x \in R$. By [Shi10, pp. 213-214], we have the relation

$$\mathfrak{d}_R = \mathfrak{f}_R^2 \mathfrak{d}_{K/F}. \tag{III.2}$$

Also note that an inclusion of orders $R \subseteq R'$ implies the divisibility condition $\mathfrak{f}(R') \mid \mathfrak{f}(R)$ on their conductors.

Proposition 3.10. *We can write*

$$R = \mathbb{Z}_F + \mathfrak{F}_R = \mathbb{Z}_F + \mathfrak{f}_R\mathbb{Z}_K.$$

PROOF. This result is local in nature, so we assume that F is a nonarchimedean local field and let $\mathbb{Z}_F$ be its ring of integers. The ring $\mathbb{Z}_F$ is principal, so by the corollary to Theorem 1 in [Sam70, §2.7], the $\mathbb{Z}_F$-module $\mathbb{Z}_K$ is free of rank 2. Therefore we see that $\mathbb{Z}_K = \mathbb{Z}_F[\alpha] = \mathbb{Z}_F + \mathbb{Z}_F\alpha$ for an element $\alpha \in \mathbb{Z}_K$. It is immediate that $\mathfrak{f}_R = \{x \in \mathbb{Z}_F : x\alpha \in R\}$. If $a + b\alpha \in R$ with a and b in $\mathbb{Z}_F$, then $b \in \mathfrak{f}_R$, so we can write $R = \mathbb{Z}_F + \mathfrak{f}_R\alpha = \mathbb{Z}_F + f\alpha\mathbb{Z}_F = \mathbb{Z}_F + f\mathbb{Z}_K$, where $f \in \mathbb{Z}_F$ is such that $\mathfrak{f}_R = f\mathbb{Z}_F$. □

From Proposition III.3.10, a quadratic order R is uniquely determined by $\mathfrak{f}_R$, and conversely, for every ideal $\mathfrak{a}$ of $\mathbb{Z}_F$, the ring $\mathbb{Z}_F + \mathfrak{a}\mathbb{Z}_K$ is an order in K of conductor $\mathfrak{a}\mathbb{Z}_K$. We denote it $R_{\mathfrak{a}}$.

We define the *Artin symbol* $\left(\frac{K}{\mathfrak{p}}\right)$ at a place $\mathfrak{p}$ of F 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 3.11. *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 $e = v_{\mathfrak{q}}(\mathfrak{M})$, 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). □

Remark 3.12. With the notations of the theorem, [Neu99, §III.2] and [Sam70, §2.7] imply that $d_{R_0} = (t^2 - 4n)$, so together with (III.2) we obtain

$$v_{\mathfrak{q}}(t^2-4n) - 2\rho = v_{\mathfrak{q}}\left(\frac{\mathfrak{f}_R^2}{\mathfrak{f}_{R_0}^2}\mathfrak{d}_{R_0}\right) = v_{\mathfrak{q}}(\mathfrak{f}_R^2\mathfrak{d}_{K/F}) = v_{\mathfrak{q}}(\mathfrak{d}_R).$$

In the case when B does not satisfy the Eichler condition, the local formulas remain true, but the number of optimal global embeddings is not necessarily equal to the product of the numbers of optimal local embeddings at every prime, up to a quotient of class numbers.

Now we look at the relation between $h(R)$ and $h(K)$.

Proposition 3.13. *The class numbers of an order R of conductor $\mathfrak{f}$ in K and its integral closure $\mathbb{Z}_K$ are related as follows:*

$$h(R) = \frac{h(K)}{[\mathbb{Z}_K^\times : R^\times]}\mathrm{N}(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \left(\frac{K}{\mathfrak{p}}\right)\frac{1}{\mathrm{N}\mathfrak{p}}\right),$$

PROOF. From [Neu99, Theo. 12.12], we know that

$$h(R) = \frac{h(K)}{[\mathbb{Z}_K^\times : R^\times]}\frac{\#(\mathbb{Z}_K/\mathfrak{F})^\times}{\#(R/\mathfrak{F})^\times}.$$

First note that we have group isomorphisms

$$R/\mathfrak{F} \cong (\mathbb{Z}_F + \mathfrak{F})/\mathfrak{F} \cong \mathbb{Z}_F/\mathfrak{f},$$

so $\#(R/\mathfrak{F})^\times = \#(\mathbb{Z}_F/\mathfrak{f})^\times$. By the Chinese Remainder Theorem, we obtain

$$\#(\mathbb{Z}_F/\mathfrak{f})^\times = \mathrm{N}_F(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{\mathrm{N}_F(\mathfrak{p})}\right).$$

From the ramification behavior in K/F, it is clear that we can write

$$\prod_{\mathfrak{q}|\mathfrak{F}} \left(1 - \frac{1}{\mathrm{N}_K(\mathfrak{q})}\right) = \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{\mathrm{N}_F(\mathfrak{p})}\right)\left(1 - \left(\frac{K}{\mathfrak{p}}\right)\frac{1}{\mathrm{N}_F(\mathfrak{p})}\right)$$

and that $\mathrm{N}(\mathfrak{F}) = \mathrm{N}(\mathfrak{f})^2$, so we obtain our result. □

NORMALIZERS

Let $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$ in B with reduced discriminant $\mathfrak{d} = \mathfrak{D}\mathfrak{N}$. Recall that B satisfies the Eichler condition. For an ideal $\mathfrak{a}$ of $\mathbb{Z}_F$ dividing $\mathfrak{d}$, we write $\mathfrak{a} \mid\mid \mathfrak{d}$ if $\mathfrak{a}$ and $\mathfrak{d}/\mathfrak{a}$ are coprime and call $\mathfrak{a}$ a *unitary divisor* of $\mathfrak{d}$. The set

$$\{\mathfrak{a} \mid\mid \mathfrak{d} : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\}$$

of unitary divisors of $\mathfrak{d}(\mathcal{O})$ which are squares in $\mathrm{Cl}(F)$ can be given the structure of an elementary abelian 2-group by considering it as a subgroup of $\bigoplus_{\mathfrak{p}^e \mid\mid \mathfrak{d}} \mathbb{Z}/2\mathbb{Z}$.

We abbreviate $\mathrm{N}(\mathcal{O}) = \mathrm{N}_{B^\times}(\mathcal{O})$. The set

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

is a group because $\mathcal{O}^\times$ is a normal subgroup of $\mathrm{N}(\mathcal{O})$.

Proposition 3.14. *The reduced norm induces an isomorphism of elementary abelian* 2*-groups:*

$$W(\mathcal{O}) \cong \{\mathfrak{a} \mid\mid \mathfrak{d}(\mathcal{O}) : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\} \times \mathrm{Cl}(F)[2].$$

PROOF. We reproduce the proof of Doyle, Linowitz and Voight [DLV, Prop. 1.13] for the convenience of the reader. Let $\alpha \in \mathrm{N}(\mathcal{O})$, we have that $\mathcal{O}\alpha\mathcal{O} = \mathfrak{c}J$, where $\mathfrak{c}$ is a fractional of $\mathbb{Z}_F$ and J is a two-sided $\mathcal{O}$-ideal such that $\mathrm{nrd}(J) = \mathfrak{a} \mid\mid \mathfrak{d}$ [KV10, §3]. By the Eichler norm theorem (Theorem III.3.3), we have $\mathrm{nrd}(\alpha) = \mathfrak{c}^2\mathfrak{a} = a\mathbb{Z}_F$ for an element $a \in F^{(+)} \subset F^\times$. The reduced norm thus induces a homomorphism

$$\mathrm{N}(\mathcal{O}) \quad \to \quad \{\mathfrak{a} \mid\mid \mathfrak{d}(\mathcal{O}) : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\} \tag{III.3}$$

whose kernel contains $\mathcal{O}^\times$. This map is surjective, since if $\mathfrak{a} \mid\mid \mathfrak{d}$ is such that $[\mathfrak{a}] \in \mathrm{Cl}(F)^2$ then there exists a fractional ideal $\mathfrak{c}$ satisfying $[\mathfrak{c}^2] = [\mathfrak{a}^{-1}]$ in $\mathrm{Cl}(F)$. Let $[\mathcal{O}, \mathcal{O}]$ be the group of commutators of $\mathcal{O}$. The two-sided ideal $\mathfrak{c}J$ with $J = [\mathcal{O}, \mathcal{O}] + \mathfrak{a}\mathcal{O}$ satisfies $[\mathrm{nrd}(\mathfrak{c}J)] = [\mathfrak{c}^2\mathfrak{a}] = [1]$ in $\mathrm{Cl}(F)$, therefore by Theorem III.3.8 there exists $\alpha \in \mathcal{O}^\times \subset \mathrm{N}(\mathcal{O})$ such that $\mathcal{O}\alpha\mathcal{O} = \mathfrak{c}J$. The kernel H of (III.3) is generated by the $\alpha \in \mathrm{N}(\mathcal{O})$ such that $\mathcal{O}\alpha\mathcal{O} = \mathfrak{c}\mathcal{O}$ with $[\mathfrak{c}^2] = [(1)]$ in $\mathrm{Cl}(F)$, and the image of $F^\times$ is the subgroup of principal ideals of $\mathbb{Z}_F$. We therefore obtain two exact sequences

$$1 \quad \to \quad H/F^\times \quad \to \quad \mathrm{N}(\mathcal{O})/F^\times \quad \to \quad \{\mathfrak{a} \mid\mid \mathfrak{d}(\mathcal{O}) : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\} \quad \to \quad 1$$

and

$$1 \quad \to \quad \mathcal{O}^\times/(\mathcal{O}^\times \cap F^\times) \quad \to \quad H/F^\times \quad \to \quad \mathrm{Cl}(F)[2] \quad \to \quad 1$$

induced by $\alpha \mapsto \mathfrak{a}$ and $\alpha \mapsto \mathfrak{c}$ respectively, from which we deduce the result. □

CLASS NUMBER FORMULA

Suppose now that F is totally real of degree d over $\mathbb{Q}$ and that the quaternion algebra B is definite, with discriminant $\mathfrak{D}$. Thus the discriminant d_F of F is positive.

Let

$$\Phi(\mathfrak{D}) = \#(\mathbb{Z}_F/\mathfrak{D})^\times = \mathrm{N}(\mathfrak{D}) \prod_{\mathfrak{p}|\mathfrak{D}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right)$$

and

$$\Psi(\mathfrak{N}) = \mathrm{N}(\mathfrak{N}) \prod_{\mathfrak{p}|\mathfrak{N}} \left(1 + \frac{1}{\mathrm{N}(\mathfrak{p})}\right).$$

Theorem 3.15 (Class number formula). *The number of left (or right) classes of an Eichler order $\mathcal{O}$ of level $\mathfrak{N}$ is equal to*

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

where R runs through the quadratic orders of B.

PROOF. See Vignéras [Vig80, §V.2]. □

By the Klingen-Siegel theorem, if F is a totally real number field, then $\zeta_F(-1)$ is a rational number, which by the functional equation of the Dedekind zeta function is equal to

$$\zeta_F(-1) = d_F^{3/2}(-2\pi^2)^{-d}\zeta_F(2).$$

Since $\zeta_F(2)$ is positive, we obtain

$$|\zeta_F(-1)| = d_F^{3/2}(2\pi^2)^{-d}\zeta_F(2).$$

Therefore $h(\mathcal{O})$ is also equal to

$$\frac{2}{(2\pi)^d} d_F^{3/2}\zeta_F(2)h(F)\Phi(\mathfrak{D})\Psi(\mathfrak{N}) + \frac{1}{2}\sum_R([R^\times : \mathbb{Z}_F^\times] - 1)\frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]} \prod_{\mathfrak{q}} m_{\mathfrak{q}}(R, \mathcal{O}). \quad \text{(III.4)}$$

4 Arithmetic groups

We now turn to geometric applications of the theory described in the preceding sections.

Definition. A subgroup Γ of $\mathrm{GL}_2^+(\mathbb{R})$ (or $\mathrm{PGL}_2^+(\mathbb{R})$) is a *Fuchsian group* if Γ is discrete, and *of the first kind* if the quotient $\Gamma\backslash\mathcal{H}$ has finite volume.

We will study a particular class of subgroups of $\mathrm{GL}_2^+(\mathbb{R})$. Let B be a quaternion algebra over a number field F admitting a real embedding $\iota : F \hookrightarrow \mathbb{R}$ at which B is split. Let $\mathcal{O}(1)$ be a maximal order of B and consider the group

$$\Gamma^B(1) = \iota\left(\{b \in \mathcal{O}(1) : \mathrm{nrd}(b) \text{ is totally positive}\}\right).$$

Theorem 4.1. *The group $\Gamma^B(1)$ is a Fuchsian group if and only if F is a totally real number field and there is exactly one (real) infinite place at which B is split. Furthermore, the quotient $\Gamma\backslash\mathcal{H}$ is compact if and only if B is a division algebra.*

PROOF. This comes from results of Weil, see Weil [Wei60] and Milne [Mil05, Theo. 3.3]. □

Therefore when $B = \mathrm{M}_2(\mathbb{Q})$ it is necessary to compactify the quotients $\Gamma\backslash\mathcal{H}$. We consider instead quotients of

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}),$$

where $\mathbb{P}^1(\mathbb{Q})$ is the set of *cusps* of Γ. We denote by $X(\Gamma)$ the compactification of $Y(\Gamma) = \Gamma\backslash\mathcal{H}$.

Recall that two groups G and G' are *commensurable* if $G \cap G'$ has finite index in both G and G'.

Definition. A subgroup of $\mathrm{GL}_2^+(\mathbb{R})$ is *arithmetic* if it is commensurable with $\Gamma^B(1)$ for a quaternion algebra B over a totally real number field F such that B is unramified at exactly one real place. A *Shimura curve* is a quotient of the form $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ for an arithmetic Fuchsian group $\Gamma \subset \mathrm{GL}_2^+(\mathbb{R})$.

By classical theory of Riemann surfaces (*e.g.* Katok [Kat92]), the quotient of the Poincaré upper half-plane by an arithmetic Fuchsian group can be given the structure of a connected Riemann surface and of a nonsingular and irreducible complex algebraic curve, which is projective when the quotient is compact. Therefore a Shimura curve is naturally an irreducible and nonsingular complex algebraic curve.

Definition. 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]).

Let vol be the volume with respect to the hyperbolic measure $(dx^2 + dy^2)/y^2$ on $\mathcal{H}$. By [Shi71, Theo. 2.20], we have the following formula.[1]

Theorem 4.2. *Let $\Gamma \subset \mathrm{GL}_2^+(\mathbb{R})$ be a Fuchsian group of the first kind. The genus g of the Shimura curve $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ verifies*

$$2g - 2 = \frac{1}{2\pi}\mathrm{vol}(Y(\Gamma)) - \sum_q e_q(\Gamma)\left(1 - \frac{1}{q}\right) - e_\infty(\Gamma). \tag{III.5}$$

[1] Shimura states his theorem for a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$, but his proof works for the more general case of a subgroup of $\mathrm{GL}_2^+(\mathbb{R})$.

IV

SHIMURA CURVES OVER FINITE FIELDS

The objective of this chapter is to use the theory of quaternion algebras developed in the previous chapter to study the arithmetic of Shimura curves, with an emphasis on finite fields. The modular curves $X_0(N)$ are known to give examples of asymptotically optimal sequences of curves which naturally form optimal recursive towers over finite fields, and our goal in this chapter is to look at what happens for the Shimura curves which are the natural generalizations of modular curves. We introduce the necessary background on Shimura curves and modular forms in the first two sections, before presenting our results on the arithmetic of Shimura curves over finite fields in the subsequent sections.

1 Shimura curves

In this section we introduce our main object of study from both a classical and adelic perspective. Let F be a totally real number field of degree d and absolute discriminant d_F. 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

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

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 (see § III.4). The quotient

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

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 $X_0^1(\mathfrak{N}) = X(\Gamma_0^1(\mathfrak{N}))$.

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. 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 $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$. 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

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

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

$$Y(\hat{\mathcal{O}}^{\times}) \cong \bigsqcup_{[\hat{b}] \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^{\times})} Y(\Gamma_{\hat{b}}). \tag{IV.1}$$

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 (IV.1) 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 Theorem III.3.8 implies that $Y(\hat{\mathcal{O}}^{\times})$ is naturally a disjoint union of curves indexed by $\mathrm{Cl}_{\infty}(F)$. Let $X(\hat{\mathcal{O}}^{\times})$ be the projective closure of $Y(\hat{\mathcal{O}}^{\times})$. By Theorem III.4.1 we have $X(\hat{\mathcal{O}}^{\times}) = Y(\hat{\mathcal{O}}^{\times})$ 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 (Theorem II.1.7), $\mathrm{Pic}_r^+(\mathcal{O})$ 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

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

be the set of units x of $\mathcal{O}$ with totally positive reduced norm[1]. 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

$$Y_0^+(\mathfrak{N}) = Y(\Gamma_0^+(\mathfrak{N})),$$

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_∞:

$$\mathrm{Sh}(\hat{\mathcal{O}}^\times) \times_F F_\infty \cong \bigsqcup_{\sigma \in \mathrm{Gal}(F_\infty/F)} \mathrm{Sh}_0^+(\mathfrak{N})^\sigma. \tag{IV.2}$$

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.

By (III.1) 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 Theorem II.1.4 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 $h = h(F)$ is the class number of F. When $h_\infty = h = 1$, we have isomorphisms

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

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 $Y_0^1(\mathfrak{N})$, but the curves $Y_0^+(\mathfrak{N})$.

[1]Note that this is equivalent to $\iota_1(\mathrm{nrd}(x)) > 0$, because by the Eichler norm theorem (Theorem III.3.3) the reduced norm of any element of $B^\times$ is already positive at any infinite place other than ι_1.

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 $H^0(Y(\Gamma), \Omega^1)$ of holomorphic differential 1-forms on the Shimura curve $Y(\Gamma)$, given by

$$\begin{array}{ccc} S_2(\Gamma) & \xrightarrow{\cong} & H^0(Y(\Gamma), \Omega^1) \\ f & \longmapsto & f(\tau)d\tau \end{array} . \tag{IV.3}$$

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

$$\hat{S}_2(\mathfrak{N}) = \bigoplus_{[\hat{b}] \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^{\times})} S_2(\Gamma_{\hat{b}}) \tag{IV.4}$$

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 (IV.1) and (IV.3), we obtain isomorphisms

$$\begin{array}{ccccc} \hat{S}_2(\mathfrak{N}) & \xrightarrow{\cong} & H^0(X(\hat{\mathcal{O}}^\times), \Omega^1) & \xrightarrow{\cong} & \displaystyle\bigoplus_{[\hat{b}] \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times)} H^0(X(\Gamma_{\hat{b}}), \Omega^1) \\ \hat{f} & \longmapsto & \hat{f}(\tau, \hat{b})d\tau & \longmapsto & (f_{\hat{b}}(\tau)d\tau)_{[\hat{b}]} \end{array} \tag{IV.5}$$

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

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 (IV.11)).

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

$$r_i\hat{\alpha}_\ell = b_\ell r_j k_\ell \in \mathrm{Pic}_r^+(\hat{\mathcal{O}}^\times). \tag{IV.6}$$

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 (IV.1) and (IV.4) respectively. We thus have:

$$\begin{aligned}
([\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot\hat{f})_i(\tau) &= ([\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]\cdot\hat{f})(\tau,r_i)\\
&= \sum_\ell \hat{f}(\tau, r_i\hat{\alpha}_\ell)\\
&= \sum_\ell \hat{f}(b_\ell(b_\ell^{-1}\tau, r_j k_\ell))\\
&= \sum_\ell \frac{j(b_\ell, b_\ell^{-1}\tau)^2}{\det(b_\ell)}\hat{f}(b_\ell^{-1}\tau, r_j k_\ell) \quad \text{by the transformation properties of } \hat{f}\\
&= \sum_\ell \frac{\det(b_\ell^{-1})}{j(b_\ell^{-1},\tau)^2} f_j(b_\ell^{-1}\tau) \qquad \text{by (IV.4).}
\end{aligned} \tag{IV.7}$$

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

$$[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]_i\cdot\hat{f} = [\Gamma_i\gamma\Gamma_i]\cdot\hat{f}_i, \tag{IV.8}$$

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 $\hat{\mathfrak{n}}$:

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

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

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

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 Theorem III.3.8 we see that $i = j$ in (IV.6). 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 (IV.8) 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

$$\deg(\hat{\mathrm{T}}(\mathfrak{n})) = \deg(\mathrm{T}(\mathfrak{n})) = \prod_{\substack{\mathfrak{p}^e \| \mathfrak{n} \\ \mathfrak{p} \mid \mathfrak{N}}} \mathrm{N}(\mathfrak{p})^e \prod_{\substack{\mathfrak{p}^e \| \mathfrak{n} \\ \mathfrak{p} \nmid \mathfrak{N}}} (1 + \mathrm{N}(\mathfrak{p}) + \cdots + \mathrm{N}(\mathfrak{p})^e) \tag{IV.9}$$

(note that the case $\mathfrak{N} = \mathbb{Z}_F$ follows from Theorem III.2.1).

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 (IV.6) 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 IV.2.2, we obtain the result. □

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

$$\begin{array}{ccc} & X(\hat{\mathcal{O}}^\times_{\hat{\alpha}}) & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_1' \circ m_{\hat{\alpha}}} \\ X(\hat{\mathcal{O}}^\times) & \xrightarrow[[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]]{} & X(\hat{\mathcal{O}}^\times) \end{array} \tag{IV.10}$$

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 (IV.10) 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

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

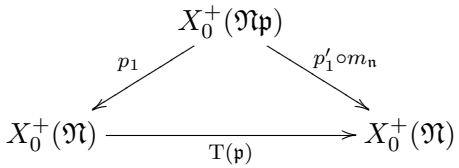
so $[\hat{\mathcal{O}}^\times\hat{\alpha}\hat{\mathcal{O}}^\times]$ is indeed the operator on $\hat{S}_2(\mathfrak{N})$ induced by the correspondence.

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

$$[\Gamma\alpha\Gamma]\circ[\Gamma\alpha\Gamma]^\vee = [\Gamma\alpha\Gamma]^\vee\circ[\Gamma\alpha\Gamma] = [\deg([\Gamma\alpha\Gamma])] = [\deg([\Gamma\alpha\Gamma]^\vee)], \tag{IV.11}$$

where $[\Gamma\alpha\Gamma]^\vee$ is the operator defined in Remark IV.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 IV.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 IV.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 IV.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 IV.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 IV.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 $X_0^+(\mathfrak{N})_{\mathbb{F}_{q^{r+1}}}$. □

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 Proposition III.3.14, the reduced norm induces maps

$$\{\mathfrak{a} \;||\; \mathfrak{d}(\mathcal{O}) : [\mathfrak{a}] \in \mathrm{Cl}(F)^2\} \times \mathrm{Cl}(F)[2] \xrightarrow{\cong} \widehat{W(\mathcal{O})} \hookrightarrow W(\hat{\mathcal{O}}^\times). \tag{IV.12}$$

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 (IV.12) 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 (IV.1), 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 $\mathbb{Z}_F[X]/P(X)$.

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 (II.3),

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

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]:

$$\mathrm{vol}(\Gamma_0^+(\mathfrak{N})\backslash\mathcal{H}) = \frac{8\pi}{(2\pi)^{2d}}\frac{h}{h_\infty}d_F^{3/2}\zeta_F(2)\Phi(\mathfrak{D})\Psi(\mathfrak{N}). \tag{IV.13}$$

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

$$\mathrm{vol}(X_0^1(\mathfrak{N})) = \frac{8\pi}{(2\pi)^{2d}}d_F^{3/2}\zeta_F(2)\Phi(\mathfrak{D})\Psi(\mathfrak{N}). \tag{IV.14}$$

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 IV.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 IV.2.7 and Theorem IV.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.

Lemma 3.3. *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. From Theorem III.3.11, 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 3.4. *We have an equality*

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

PROOF. We can decompose

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

By Lemma IV.3.3 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 Proposition III.3.13 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 3.5. *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 $\mathfrak{p}$. As noted in Remark III.3.12, 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 IV.3.4. All terms in the sum are positive, so A is positive, and therefore $\Xi(r) - q\Xi(r-2)$ is positive. □

Proposition IV.3.5 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 3.6. We have an equality $\Xi(r) = q\Xi(r-2)$ if and only if the terms A and B are zero. By Theorem III.3.11, 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:

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

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

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

d) 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 III.3.11 iii)).

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 IV.3.2 and Theorem III.4.2 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 (Corollary I.5.3).

Theorem 3.7. *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 3.8. 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 IV.3.7. 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 IV.3.7. 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 $\overline{\mathrm{Sh}}(\mathfrak{N}) \times \overline{\mathbb{F}}_\mathfrak{p}$ intersecting 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]. For the bijection between ii) and iii), see Proposition III.3.7 ii).

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 Theorem (III.4).

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 by $\overline{[\tau, \hat{b}]} \mapsto \overline{[\tau, \hat{b}\hat{\alpha}]}$, that is like the Atkin-Lehner operator $\hat{w}(\mathfrak{p})$. 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

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

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 (IV.2), 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 IV.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 III.4.2, (IV.13) and Corollary IV.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 (Corollary I.5.3). □

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 § IV.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 $C_1 = X_0^+(\mathfrak{N}\mathfrak{n})$ and $C_2 = X_0^+(\mathfrak{N}\mathfrak{n}^2)$, and for $i \geqslant 3$ let C_i be the fibre product

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

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

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

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

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

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

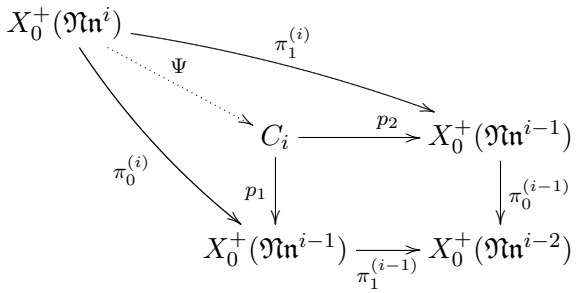


Diagram IV.1: The correspondence $X_0^+(\mathfrak{N}\mathfrak{n}^i)$.

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

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

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

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

The following theorem is a consequence of the above discussion and Theorem IV.3.7 and Theorem IV.4.5.

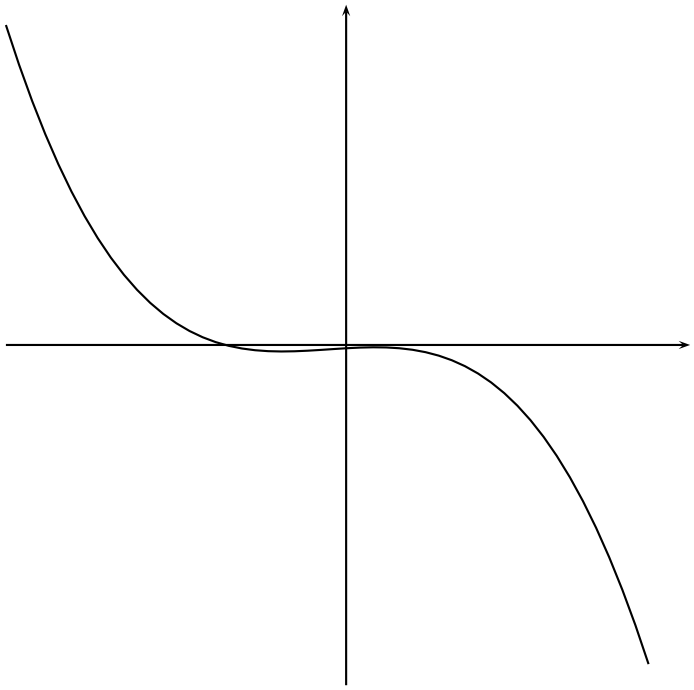
Theorem 5.2. *Let $\mathfrak{n}$ be an ideal of $\mathbb{Z}_F$ relatively prime to $\mathfrak{D}\mathfrak{N}$. Let $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}\mathfrak{n}$ be a prime of $\mathbb{Z}_F$ and let $\mathfrak{P}$ be a prime of $\mathbb{Z}_{F_\infty}$ above $\mathfrak{p}$. Let $\bar{\cdot}$ denote reduction modulo $\mathfrak{P}$. The curves $\overline{\mathrm{Sh}_0}^+(\mathfrak{N}\mathfrak{n}^i)$ 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 $X_0(1) = \mathbb{P}^1_F(j_0)$ 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 IV.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 $\mathfrak{q} \neq \mathfrak{p}$.

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

BIBLIOGRAPHY

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

[AT09] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[Aue99] Roland Auer. *Ray Class Fields of Global Function Fields with Many Rational Places*. PhD thesis, Carl-von-Ossietzky-Universität, Oldenburg, 1999.

[Aue00] Roland Auer. Curves over finite fields with many rational points obtained by ray class field extensions. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 127–134. Springer, Berlin, 2000.

[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).

[Bis11] Gaetan Bisson. *Endomorphism Rings in Cryptography*. PhD thesis, Technische Universiteit Eindhoven and Laboratoire Lorrain de Recherche en Informatique et ses Applications, 2011.

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

[Cas67] J. W. S. Cassels. Global fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 42–84. Thompson, Washington, D.C., 1967.

[Chi09] Nancy Childress. *Class field theory*. Universitext. Springer, New York, 2009.

[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`.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[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.

[DF13] V. Ducet and C. Fieker. Computing Equations of Curves with Many Points. *To appear in the proceedings of ANTS X*, 2013.

[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.

[DM12] Iwan Duursma and Kit-Ho Mak. On lower bounds for the Ihara constants A(2) and A(3). 2012. Available at "arXiv:1102.4127".

[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".

[Fie01] Claus Fieker. Computing class fields via the Artin map. *Mathematics of Computation*, 70(235):1293–1303 (electronic), 2001.

[Fie06] Claus Fieker. Applications of the class field theory of global fields. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 31–62. Springer, Berlin, 2006.

[Fis99] Benji Fisher. Notes on Witt Vectors: a motivated approach. 1999.

[Frö67] A. Fröhlich. Local fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 1–41. Thompson, Washington, D.C., 1967.

[Gar81] Dennis Garbanati. Class field theory summarized. *Rocky Mountain J. Math.*, 11(2):195–225, 1981.

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

[GS95] Arnaldo Garcia and Henning Stichtenoth. Algebraic function fields over finite fields with many rational places. *IEEE Trans. Inform. Theory*, 41(6, part 1):1548–1563, 1995. Special issue on algebraic geometry codes.

[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".

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[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.

[HL03] E. W. Howe and K. E. Lauter. Improved upper bounds for the number of points on curves over finite fields. *Ann. Inst. Fourier (Grenoble)*, 53(6):1677–1737, 2003. Available at "arXiv:math/0207101".

[HL12] E. W. Howe and K. E. Lauter. New methods for bounding the number of points on curves over finite fields. 2012. Available at "arXiv:1202.6308v2".

[HLRVdG] E. Howe, K. Lauter, C. Ritzenthaler, and G. Van der Geer. Table of Curves with Many Points. Available at `http://www.manypoints.org/`.

[HPP03] Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548 (electronic), 2003.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[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.

[Hur03] Norman E. Hurt. *Many rational points*, volume 564 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 2003. Coding theory and algebraic geometry.

[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.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[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.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lau96] Kristin Lauter. Ray class field constructions of curves over finite fields with many rational points. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 187–195. Springer, Berlin, 1996.

[Lau99a] Kristin Lauter. Deligne-Lusztig curves as ray class fields. *Manuscripta Math.*, 98(1):87–96, 1999.

[Lau99b] Kristin Lauter. A formula for constructing curves over finite fields with many rational points. *J. Number Theory*, 74(1):56–72, 1999.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[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.

[MAT10] MATLAB. *version 7.10.0 (R2010a)*. The MathWorks Inc., Natick, Massachusetts, 2010.

[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.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at `http://www.jmilne.org/math/`.

[Mil11a] James S. Milne. Algebraic number theory (v3.03), 2011. Available at `http://www.jmilne.org/math/`.

[Mil11b] 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.

[NX01] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001.

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

[Rab07] Joseph Rabinoff. The theory of Witt vectors. 2007. Available at `http://www.math.harvard.edu/~rabinoff/`.

[Rig09] Alessandra Rigato. *Uniqueness of Optimal Curves over $\mathbb{F}_2$ of Small Genus*. PhD thesis, Università Degli Studi Di Roma, 2009.

[Rig10] Alessandra Rigato. Uniqueness of low genus optimal curves over $\mathbb{F}_2$. In *Arithmetic, geometry, cryptography and coding theory 2009*, volume 521 of *Contemp. Math.*, pages 87–105. Amer. Math. Soc., Providence, RI, 2010. Available at "arXiv:1005.4591".

[Rök13] Karl Rökaeus. New curves with many points over small finite fields. *Finite Fields Appl.*, 21:58–66, 2013. Available at "arXiv:1204.4355".

[Rud87] Walter Rudin. *Real and complex analysis*. McGraw-Hill Book Co., New York, third edition, 1987.

[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.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Sch36] H.L. Schmid. Zur arithmetik der zyklischen p-körper. *Crelle's Journal*, 176:161–167, 1936.

[Sch90] René Schoof. Algebraic curves and coding theory. *Università di Trento*, 1990. Preprint 336, 38 pages.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[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.

[Ser85] Jean-Pierre Serre. *Rational Points on Curves over Finite Fields*. September to December 1985. Lecture notes given at Harvard University. Notes by Fernando Q. Gouvéa.

[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.

[Sil94] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

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

[Tat67] J. T. Tate. Global class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 162–203. Thompson, Washington, D.C., 1967.

[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.

[VD83] S. G. Vlăduţ and V. G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.

[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.

[Voi05] John Voight. Curves over finite fields with many points: an introduction. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 124–144. World Sci. Publ., Hackensack, NJ, 2005.

[Voi06] John Voight. Three lectures on Shimura curves. 2006.

[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.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

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

[Wei95] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[Wit36] Ernst Witt. Zyklische körper und algebren der characteristik p vom grad p^n. *Crelle's Journal*, 176:126–140, 1936.

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

NOTATIONS

$\mathbb{N}$ non-negative integers. viii$\mathbb{Z}$ rational integers. viii$\mathbb{Z}_p$ p-adic integers. viii$\mathbb{Q}$ rational numbers. viii$\mathbb{Q}_p$ p-adic nu

Résumé
L'étude du nombre de points rationnels d'une courbe définie sur un corps fini se divise naturellement en deux cas : lorsque le genre est petit (typiquement $g \leqslant 50$), et lorsqu'il tend vers l'infini. Nous consacrons une partie de cette thèse à chacun de ces cas. Dans la première partie de notre étude nous expliquons comment calculer l'équation de n'importe quel revêtement abélien d'une courbe définie sur un corps fini. Nous utilisons pour cela la théorie explicite du corps de classe fournie par les extensions de Kummer et d'Artin-Schreier-Witt. Nous détaillons également un algorithme pour la recherche de bonnes courbes, dont l'implémentation fournit de nouveaux records de nombre de points sur $\mathbb{F}_2$ et $\mathbb{F}_3$. Nous étudions dans la seconde partie une formule de trace d'opérateurs de Hecke sur des formes modulaires quaternioniques, et montrons que les courbes de Shimura de la forme $X_0^+(\mathfrak{N})$ forment naturellement des suites récursives de courbes asymptotiquement optimales sur une extension quadratique du corps de base. Nous prouvons également qu'alors la contribution essentielle en points rationnels est fournie par les points supersinguliers.

Abstract
The study of the number of rational points of a curve defined over a finite field naturally falls into two cases: when the genus is small (typically $g \leqslant 50$), and when it tends to infinity. We devote one part of this thesis to each of these cases. In the first part of our study, we explain how to compute the equation of any abelian covering of a curve defined over a finite field. For this we use explicit class field theory provided by Kummer and Artin-Schreier-Witt extensions. We also detail an algorithm for the search of good curves, whose implementation provides new records of number of points over $\mathbb{F}_2$ and $\mathbb{F}_3$. In the second part, we study a trace formula of Hecke operators on quaternionic modular forms, and we show that the Shimura curves of the form $X_0^+(\mathfrak{N})$ naturally form recursive sequences of asymptotically optimal curves over a quadratic extension of the base field. Moreover, we then prove that the essential contribution to the rational points is provided by supersingular points.

Discipline

MATHÉMATIQUES

Mots-clés
Courbes avec beaucoup de points, corps de fonctions, théorie explicite du corps de classe, théorie de Kummer, vecteurs de Witt, équations de revêtements abéliens, algèbres de quaternions, courbes de Shimura, formes modulaires, opérateurs de Hecke, points supersinguliers, tours récursives.

Laboratoire
INSTITUT DE MATHÉMATIQUES DE LUMINY - Campus de Luminy, 13288 Marseille Cedex 9