

**CUSP FORMS OVER FUNCTION FIELDS AND
MODULAR SYMBOLS**

BY SAŠA RADOMIROVIĆ

A dissertation submitted to the
Graduate School—New Brunswick
Rutgers, The State University of New Jersey
in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Prof. J. B. Tunnell

and approved by

New Brunswick, New Jersey

October, 2005

ABSTRACT OF THE DISSERTATION

Cusp Forms over Function Fields and Modular Symbols

by Saša Radomirović

Dissertation Director: Prof. J. B. Tunnell

Classical automorphic functions are complex valued functions on the upper half plane left invariant under a subgroup of finite index of the modular group $SL(2, \mathbb{Z})$.

We consider the analogue of this classical setting in characteristic p . In particular, we investigate the analogue of the upper half plane and analyze the structure of the fundamental domain of a Hecke congruence group of level A over a function field over a finite field. We describe two algorithms to compute spaces of cusp forms of level A and analyze their complexity. For the second algorithm we extend Manin's classical Modular Symbols method to the function field case.

Acknowledgements

I would like to thank my advisor Jerrold Tunnell, for suggesting an interesting problem, for the discussions we've had, for the compelling number theory courses, and for his patience. I wish to thank the committee members and readers of my thesis, Richard Bumby, Emanuel Kowalski, and Jacob Sturm, for their time, suggestions, and comments. Moreover, I would like to extend a warm thank you to Henryk Iwaniec for teaching me many interesting topics in analytic number theory. For mathematical discussions I gladly acknowledge Laura Ciobanu, Kia Dalili, Sujith Vijay, and Aaron Lauve. I am very grateful to Stephen Greenfield for being an approachable and inspiring teacher, and for his professional and personal advise. A part of this thesis has been written with support from DIMACS' graduate student award.

The fellow graduate students have made graduate school a really enjoyable and worthwhile experience. A heartfelt thank you to all of them, and in particular to Aaron and Maria for organizing the first get together party, Aerobie games, the annual Mardi Gras party, and the 4th of July barbecues, to name but a few. I am especially grateful to Laura, Kia, Aaron, and Maria, for having been part of the 326 Wayne Street #2 household, for moral support, enriching evenings, and for the much appreciated cooking, all of which will be sorely missed. Lastly, thank you noisy little Sir Raymond Hungerford Charles III for reminding me how important it is to enjoy the simple things in life.

Above all, I extend my deepest gratitude to my beautiful fiancée Laura, for sharing my excitement for frivolous things, for being critical, yet encouraging and understanding, and to my family, for supporting me, believing in me, and keeping me away from work for hours every Sunday.

Dedication

Мојим родитељима

To my parents

Table of Contents

Abstract	ii
Acknowledgements	iii
Dedication	iv
1. Introduction	1
2. Preliminaries	4
2.1. Notation	4
2.2. Useful Lemmas	5
2.3. Analogue of Upper Half Plane	7
2.3.1. Decomposition of G	7
2.3.2. The upper half plane as a tree	7
2.3.3. Computations in the tree	9
2.4. Automorphic Functions, Cusp Forms, and Hecke Operators	12
2.4.1. Cusp Forms	13
2.4.2. Hecke Operators	15
2.5. L -function	15
3. The Fundamental Domain	17
3.1. Right cosets of Γ_A in Γ	17
3.2. The number of points on σ -level n	20
3.2.1. The σ -level 0	20
3.2.2. σ -level $n > 0$	22
3.3. Cusps	24
3.4. The number of edges between σ -levels	27

3.5. The Shape of the Fundamental Domain	29
3.6. The Fundamental Domain and Cusp forms	30
4. Modular Symbols	33
4.1. Homology in Quotientgraphs	33
4.2. Path Integrals	34
4.3. Manin Symbols	36
4.4. Modular Symbols and Spaces of Cusp Forms	40
5. Computation of L-functions, special values and complexity	42
5.1. Complexity	42
5.1.1. Computation of the L -function and a_{Π} for a given Elliptic Curve	43
5.1.2. The Modular Symbols method	43
5.1.3. Computing the space of cusp forms directly	44
5.1.4. Special Values, other operators	45
5.2. Examples	45
References	51
Vita	53

Chapter 1

Introduction

The goal of this thesis is the construction and complexity analysis of the Modular Symbols method to compute special values of L -functions of elliptic curves defined over function fields over finite fields. The interest in doing these computations stems from the Birch and Swinnerton-Dyer conjecture which we will outline below.

It is well known that function fields over finite fields have number theoretic properties similar to the rational numbers and number fields. In general, problems over function fields are easier to tackle, and once settled, may provide new insight into their classical analogues. Some conjectures, most famously the Riemann Hypothesis, have been proved in the function field case [19, 20, 21, 22, 23], while others, for instance the Birch and Swinnerton-Dyer conjecture [2], are open in both cases, although more progress has been made in the function field case [14, 10]. Several papers by Ulmer [18, 17] show analogies between elliptic curves over number fields and function fields, and give an account on what is known today about the Birch and Swinnerton-Dyer conjecture over function fields.

The Birch and Swinnerton-Dyer conjecture relates the rank of the Mordell–Weil group of an elliptic curve E (i.e. the structure of its rational points) to a special value of the L -function $L_E(s)$ attached to the elliptic curve. $L_E(s)$ is essentially a generating function obtained by counting the number of rational points on the reduction of E over residue fields. More precisely, the Birch and Swinnerton-Dyer conjecture predicts that the order of vanishing of $L_E(s)$ at the central point $s = 1$ is equal to the rank of the Mordell–Weil group of E , and further predicts the precise value of $L^{(r)}(1)$ in terms of arithmetic constants related to E [2, 14, 18].

There is a well known relation between cusp forms and modular curves on one

side, and elliptic curves on the other side. The relation started out as a problem of Taniyama in the 1950's and after some work and partial results by Shimura and many other mathematicians turned into a very precise conjecture carrying Taniyama's and Shimura's name and was finally proved by Wiles, Breuil, Conrad, Diamond, and Taylor [26, 15, 3], in a series of papers between the mid 1990's and early 2000's, settling one of its motivations, Fermat's last theorem, as a by-product.

The function field analogue of the Taniyama–Shimura conjecture has been known to be true since the 1970's, when it was proved by Deligne [5]. This result, just like the classical version, implies for every (non-constant) elliptic curve the existence of a cusp form f on the Hecke group $\Gamma_0(A)$, of level A equal to the conductor of E , whose L -function $L_f(s)$ (defined as the Mellin transform of the Fourier expansion of f) is equal to the L -function $L_E(s)$ of E .

In 1972 Manin [9] introduced the Modular Symbol and with it a technique to compute special values of L -functions of elliptic curves (in the classical case) by integrating the cusp form related to the elliptic curve along paths between cusps on the modular curve the cusp form is defined on. This method lends itself very well to implementation on a computer. Cremona implemented the method and computed and tabulated the results [4].

In this thesis, we are using the classical methods to extend Modular Symbols and the corresponding computations to the function field case. We have learned that Teitelbaum [16] has also considered Modular Symbols over function fields, and that Tan and Rockmore [13] outline an algorithm for computing spaces of modular forms using Mazur's formula for the modular element.

The present text is organized as follows. Chapter 2 begins by setting notation, defines all non elementary terms used, states known theorems, and proves technical lemmas. In Chapter 3 we investigate the fundamental domain of $\Gamma_A \backslash G / \mathfrak{K}^3$, $A \in \mathbb{F}_q[T]$, which is the analogue of the modular curve in the classical case obtained by the action of a Hecke congruence subgroup acting on the upper half plane. In particular, we determine the structure of the fundamental domain which is useful for an algorithm that directly computes the space of cusp forms given an eigenvalue of a Hecke operator

at a certain place. We compute the index of the Hecke congruence group in the full modular group and count the number of points in the core of the fundamental domain. The complexity of any modular symbols algorithm is dominated by the former quantity, while a direct approach to computing cusp forms is dominated by the latter. We end Chapter 3 by describing an algorithm that directly computes a basis for the space of cusp forms of level A which are eigenvalues for the Hecke operator H_∞ . In Chapter 4 we introduce and investigate the modular symbol for spaces of cusp forms of level A_∞ , $A \in \mathbb{F}_q[T]$ for which the Atkin–Lehner involution at ∞ has eigenvalue -1 , and prove that the space of modular symbols is generated by the coset representatives of the Hecke congruence group in the full modular group satisfying two and three point relations very similar to the classical relations. We end Chapter 4 with a discussion about the limitations of the modular symbols method. In Chapter 5 we do a complexity analysis of methods to compute L -functions of elliptic curves and their special values and explicitly compute an example with the two algorithms considered in this thesis.

Chapter 2

Preliminaries

In this chapter we will fix the notation, define all non elementary terms and state known results. Throughout this chapter, but in particular in section 2.2, we will prove useful lemmas which would hinder the natural flow in the presentation of the main ideas if stated later.

2.1 Notation

Our notation follows Weil's [24] notation closely.

\mathbb{F}_q will denote a finite field with q elements,

$$k_\infty = \left\{ \sum_{i=N}^{\infty} a_i T^{-i} \mid a_i \in \mathbb{F}_q, N \in \mathbb{Z} \right\} \text{ the completion of } k = \mathbb{F}(T) \text{ at } T^{-1},$$

$$r_\infty = \left\{ \sum_{i=0}^{\infty} a_i T^{-i} \mid a_i \in \mathbb{F}_q \right\} \text{ a maximal compact subring of } k_\infty, \text{ and}$$

$$r_\infty^\times = \left\{ a_0 + \sum_{i=1}^{\infty} a_i T^{-i} \mid a_0 \in \mathbb{F}_q^\times, a_i \in \mathbb{F}_q \right\} \text{ the units in } r_\infty.$$

$$G = \mathrm{GL}(2, k_\infty),$$

$$\mathfrak{Z} = \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} \mid \alpha \in k_\infty, \alpha \neq 0 \right\} \text{ the center of } G,$$

$$\mathfrak{K} = \left\{ \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in G \mid P, Q, R, S \in r_\infty, \det \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in r_\infty^\times \right\} \text{ a maximal compact subgroup of } G, \text{ and}$$

$$\mathfrak{I} = \left\{ \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \mathfrak{K} \mid R \equiv 0 \pmod{T^{-1}} \right\} \text{ the Iwahori subgroup of } \mathfrak{K}.$$

$$\Gamma = \left\{ \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \mid P, Q, R, S \in \mathbb{F}_q[T], \det \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \mathbb{F}_q^\times \right\} \text{ denotes the analogue of the full modular group, and for } A \in \mathbb{F}_q[T] \text{ we write}$$

$$\Gamma_A = \left\{ \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \mid P, Q, R, S \in \mathbb{F}_q[T], R \equiv 0 \pmod{A}, \det \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \mathbb{F}_q^\times \right\} \text{ for the analogue of the congruence subgroup } \Gamma_0. \text{ Finally,}$$

$$B_1 = \left\{ \begin{bmatrix} T^n & y \\ 0 & 1 \end{bmatrix} \mid y \in k_\infty, n \in \mathbb{Z} \right\}, \text{ and we set}$$

$$\sigma_n = \begin{bmatrix} T^n & 0 \\ 0 & 1 \end{bmatrix}, n \in \mathbb{Z}.$$

For $a, b \in G$ we will write $a \equiv b \pmod{\mathfrak{K}\mathfrak{Z}}$ if a and b are in the same left coset of G modulo $\mathfrak{K}\mathfrak{Z}$, i.e. if $b^{-1}a \in \mathfrak{K}\mathfrak{Z}$. Since $\mathfrak{K}\mathfrak{Z}$ is not normal in G we will confine ourselves to operations from the left on equations of that form.

It will be convenient to let $[R, S]$ denote a matrix in Γ whose bottom row is $[R, S]$. Throughout the paper $A \in \mathbb{F}_q[T]$ is a fixed polynomial. We will write $|x| = q^{-N}$ for $x = \sum_{i=N}^{\infty} \alpha_i T^{-i} \in k_{\infty}$, thus $|x| = q^{\deg x}$ for $x \in \mathbb{F}_q[T]$.

In chapter 3 we will additionally use the following notation. For $A = \prod_i p_i^{e_i}$ written as a product of prime powers we define $[\sqrt{A}] = \prod_i p_i^{\lfloor e_i/2 \rfloor}$ and $\lceil \sqrt{A} \rceil = \prod_i p_i^{\lceil e_i/2 \rceil}$ so that $\lceil \sqrt{A} \rceil [\sqrt{A}] = A$. We let $\omega(A)$ denote the number of distinct prime divisors of A , $\Phi(A)$ the number of elements in the group $(\mathbb{F}_q[T]/(A\mathbb{F}_q[T]))^*$, and $\Phi_N(A)$ the number of polynomials relatively prime to A and of degree smaller than $\deg N$. A formula for $\Phi_N(A)$ will be given in section 2.2. Finally, for a non-negative integer n , we set $G_n = \left\{ \begin{bmatrix} a & Q \\ 0 & b \end{bmatrix} \in \text{GL}(2, \mathbb{F}_q[T]) \mid a, b \in \mathbb{F}_q, \deg Q \leq n \right\}$.

2.2 Useful Lemmas

Let $A \in \mathbb{F}_q[T]$. In this section, p, p_i will denote a *monic irreducible polynomial*.

Lemma 1. *Let $A, N \in \mathbb{F}_q[T]$, $\deg N \geq \deg A$. Then the number of polynomials relatively prime to A and of degree smaller than $\deg N$ is given by*

$$\Phi_N(A) = |N| \prod_{p|A} \left(1 - \frac{1}{|p|} \right)$$

Proof. It is easy to see from the definition of $\Phi(A)$ that

$$\Phi(A) = |A| \prod_{p|A} \left(1 - \frac{1}{|p|} \right).$$

The Lemma now follows by counting. Let $R_1, \dots, R_{\Phi(A)}$ be the $\Phi(A)$ polynomials relatively prime to A and of degree smaller than $\deg A$. There are $|N|/|A|$ polynomials Q of degree smaller than $\deg N - \deg A$, each of which gives rise to $\Phi(A)$ polynomials $QA + R_i$ ($1 \leq i \leq \Phi(A)$) relatively prime to A and of degree smaller than $\deg N$. These are all possible polynomials, since by the division algorithm, any polynomial relatively

prime to A of degree smaller than $\deg N$ can be written in the form $QA + R$ for some R of degree smaller than A and relatively prime to A . \square

It follows immediately that $\Phi_N(A)$ is a multiplicative function in the following way.

Lemma 2. *Let A and B be relatively prime, $|N| \geq |A|$, $|M| \geq |B|$. Then*

$$\Phi_N(A)\Phi_M(B) = \Phi_{NM}(AB)$$

Finally, analogous to the classical integer identity we have

Lemma 3. *Let $A \in \mathbb{F}_q[T]$. Then*

$$\sum_{d|A} \Phi(d) = |A|.$$

Proof. We can assume without loss of generality that A is a monic polynomial. Let $A = \prod_{i=1}^k p_i^{e_i}$ be the prime factorization of A .

$$\sum_{d|A} \Phi(d) = \sum_{i_1=0}^{e_1} \sum_{i_2=0}^{e_2} \cdots \sum_{i_k=0}^{e_k} \Phi(p_1^{i_1} \cdots p_k^{i_k})$$

which using multiplicativity of Φ can be written as

$$\sum_{d|A} \Phi(d) = \sum_{i_1=0}^{e_1} \Phi(p_1^{i_1}) \sum_{i_2=0}^{e_2} \Phi(p_2^{i_2}) \cdots \sum_{i_k=0}^{e_k} \Phi(p_k^{i_k})$$

and so is just a product of sums of the form

$$\begin{aligned} \sum_{i_j=0}^{e_j} \Phi(p_j^{i_j}) &= 1 + (|p_j| - 1) + (|p_j^2| - |p_j|) + \cdots + (|p_j^{e_j}| - |p_j^{e_j-1}|) \\ &= |p_j^{e_j}| \end{aligned}$$

and therefore

$$\sum_{d|A} \Phi(d) = |A|.$$

\square

2.3 Analogue of Upper Half Plane

The classical upper half plane $\mathbb{H} = \{x + iy \in \mathbb{C} | x, y \in \mathbb{R}, y > 0\}$ can be identified with $\mathrm{GL}(2, \mathbb{R})/KZ$, where $K = O(2, \mathbb{R})$ is the orthogonal group, a maximal compact subgroup of $\mathrm{GL}(2, \mathbb{R})$, and Z is the center of $\mathrm{GL}(2, \mathbb{R})$. In our setting, $G/\mathfrak{K}\mathfrak{J}$ is the analogue of the classical upper half plane and due to this analogy we will refer to it as *the* upper half plane. Just like in the classical case, Γ operates properly discontinuously on the space $G/\mathfrak{K}\mathfrak{J}$.

2.3.1 Decomposition of G

The following theorem of Weil [24, §3] constitutes the basis for the representation of points in the upper half plane used in this thesis.

Theorem 1 (Weil [24]). *Every element g of G can be written as $g = \gamma\sigma_n g_0$ with $\gamma \in \Gamma$, $n \geq 0$, $g_0 \in \mathfrak{K}\mathfrak{J}$; moreover, when g is given, the integer n in this formula is uniquely determined.*

Remark 1. Let $g = \gamma_1\sigma_n k_1 = \gamma_2\sigma_n k_2$, with $\gamma_1, \gamma_2 \in \Gamma$, $k_1, k_2 \in \mathfrak{K}\mathfrak{J}$ then, as noted by Weil [24, §4], for $n = 0$ there is an $M \in \mathrm{GL}(2, \mathbb{F}_q)$ such that $\gamma_1 = \gamma_2 M$ while for $n > 0$, there is an $M = \begin{bmatrix} a & Q \\ 0 & b \end{bmatrix}$ with $\deg Q \leq n$ and $a, b \in \mathbb{F}_q^\times$ such that $\gamma_1 = \gamma_2 M$.

Definition. We will refer to the cosets $\gamma\sigma_n\mathfrak{K}\mathfrak{J}$ as *points on σ -level n* .

Remark 2. Another way to decompose G is $G = B_1 \cdot \mathfrak{K}\mathfrak{J}$, but $B_1 \cap \mathfrak{K}\mathfrak{J} = \{ \begin{bmatrix} 1 & v \\ & 1 \end{bmatrix} \mid v \in r_\infty \}$ is not trivial. Thus we can represent the cosets $G/\mathfrak{K}\mathfrak{J}$ also by $\begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix}$ with unique $i \in \mathbb{Z}$, and $y \in k_\infty$ unique modulo $T^i r_\infty$.

2.3.2 The upper half plane as a tree

The space $G/\mathfrak{K}\mathfrak{J}$ can be represented by a $q + 1$ -regular tree, the *Bruhat-Tits tree* X of G/\mathfrak{J} , with the following description. The *vertices* of X are the cosets of $\mathfrak{K}\mathfrak{J}$ in G . Since $\mathfrak{K}\mathfrak{J}$ is its own normalizer, there is a bijection between cosets $g\mathfrak{K}\mathfrak{J}$ and conjugates $g\mathfrak{K}\mathfrak{J}g^{-1}$. Two vertices $g\mathfrak{K}\mathfrak{J}$, $h\mathfrak{K}\mathfrak{J}$ are joined by an *edge* (and called *neighbors*) if the intersection $g\mathfrak{K}\mathfrak{J}g^{-1} \cap h\mathfrak{K}\mathfrak{J}h^{-1}$ is conjugate to $\mathfrak{J}\mathfrak{J}$. Note that this relation is stable

under left G -action. There are $q + 1$ neighbors for each vertex. The Iwahori subgroup $\mathfrak{I} = \mathfrak{K} \cap \sigma_1 \mathfrak{K} \sigma_{-1}$ has index $q + 1$ in \mathfrak{K} , a set of left coset representatives being given by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & \\ \xi & 1 \end{bmatrix}$, $\xi \in \mathbb{F}_q$, it is normalized by itself, \mathfrak{I} , and $W_\infty = \begin{bmatrix} 0 & 1 \\ T^{-1} & 0 \end{bmatrix}$. The edges are indexed by the conjugates of $\mathfrak{I}\mathfrak{I}$ in G .

Lemma 4. *If $g \in G$ is a representative for a coset in $G/\mathfrak{K}\mathfrak{I}$, then the neighboring cosets have representatives $g\sigma_1$ and $g \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} = g \begin{bmatrix} 1 & \xi \\ 1 & 1 \end{bmatrix} \sigma_{-1}$ for $\xi \in \mathbb{F}_q$.*

Proof. This follows from the simple computation

$$\begin{aligned} & g\mathfrak{K}\mathfrak{I}g^{-1} \cap g \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} \mathfrak{K}\mathfrak{I} \begin{bmatrix} T & -\xi T \\ 1 & 1 \end{bmatrix} g^{-1} \\ &= g \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} \left(\begin{bmatrix} T & -\xi T \\ 1 & 1 \end{bmatrix} \mathfrak{K}\mathfrak{I} \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} \cap \mathfrak{K}\mathfrak{I} \right) \begin{bmatrix} T & -\xi T \\ 1 & 1 \end{bmatrix} g^{-1} \\ &= g \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} (\sigma_1 \mathfrak{K}\mathfrak{I} \sigma_{-1} \cap \mathfrak{K}\mathfrak{I}) \begin{bmatrix} T & -\xi T \\ 1 & 1 \end{bmatrix} g^{-1} \end{aligned}$$

and a similar computation for $g\sigma_1$. □

Remark 3. It follows from lemma 4 that points on σ -level $n > 0$ have q neighbors on σ -level $n - 1$ and one neighbor on σ -level $n + 1$. The neighbors of points on σ -level 0 are all on σ -level 1, since $\gamma\sigma_{-1} = \gamma \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \sigma_{-1} = \gamma \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \sigma_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} 1/T$ and thus $\gamma\sigma_{-1}\mathfrak{K}\mathfrak{I} = \gamma \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \sigma_1 \mathfrak{K}\mathfrak{I}$.

Remark 4. The representation of neighbors described in lemma 4 and the usefulness of the representation of $G/\mathfrak{K}\mathfrak{I}$ as the tree X are related to the Hecke operator H_∞ which will be defined in section 2.4.2.

The natural map $G/\mathfrak{I}\mathfrak{I} \rightarrow G/\mathfrak{K}\mathfrak{I}$ allows us to consider X as a tree with vertices given by the cosets $G/\mathfrak{K}\mathfrak{I}$, and *oriented* edges indexed by the cosets $G/\mathfrak{I}\mathfrak{I}$ such that the image of an edge in $G/\mathfrak{K}\mathfrak{I}$ is its *terminus*. Thus a vertex $g\mathfrak{K}\mathfrak{I}$ is the terminus of the edges $g \begin{bmatrix} 1 & \\ \xi & 1 \end{bmatrix} \mathfrak{I}\mathfrak{I}$ for $\xi \in \mathbb{F}_q$, and $g \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} \mathfrak{I}\mathfrak{I}$. The representative $h = g \begin{bmatrix} 1 & \xi \\ 1 & 1 \end{bmatrix} \sigma_{-1}$ of a neighbor of $g\mathfrak{K}\mathfrak{I}$ is the terminus of the edge $h\mathfrak{I}\mathfrak{I}$. Since

$$h\mathfrak{I}\mathfrak{I}W_\infty = hW_\infty\mathfrak{I}\mathfrak{I} = \begin{cases} g \begin{bmatrix} 1 & \\ \xi^{-1} & 1 \end{bmatrix} \mathfrak{I}\mathfrak{I} & \xi \neq 0 \\ g \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} \mathfrak{I}\mathfrak{I} & \xi = 0 \end{cases}$$

particular, given the representative $\begin{bmatrix} P & Q \\ R & S \end{bmatrix} \sigma_n$, $\begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \Gamma$, we have

$$\begin{bmatrix} P & Q \\ R & S \end{bmatrix} \sigma_n \equiv \begin{cases} \begin{bmatrix} T^{-2 \deg(R) - n} & P/R \\ 0 & 1 \end{bmatrix} & \text{if } |S| \leq |RT^n| \\ \begin{bmatrix} T^{n - 2 \deg(S)} & Q/S \\ 0 & 1 \end{bmatrix} & \text{if } |S| > |RT^n| \end{cases} \pmod{\mathfrak{K}\mathfrak{J}} \quad (\text{mod } \mathfrak{K}\mathfrak{J})$$

This is easily seen by multiplying both sides by the inverse of the matrix on the right hand side.

If we write $m = n - \deg(S/R)$, then the first case is equivalent to $m \geq 0$ and the second is equivalent to $m \leq 0$. Solving for n and plugging back in into the respective cases, we obtain

$$\begin{bmatrix} P & Q \\ R & S \end{bmatrix} \sigma_n \equiv \begin{bmatrix} T^k & y \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}}$$

$$\text{where } k = \begin{cases} -\deg(RS) - |n - \deg(S/R)| & \text{if } RS \neq 0 \\ n & \text{if } R = 0 \\ -n & \text{if } S = 0 \end{cases} \quad \text{and } y = \begin{cases} P/R & \text{if } m \geq 0 \\ Q/S & \text{if } m < 0 \end{cases}$$

- $\text{GL}(2, \mathbb{F}_q(T))$ acting from the left on the tree

More generally, computations similar to the ones performed above show that for

any $\gamma \in \text{GL}(2, \mathbb{F}_q(T))$, $\gamma = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}$, with determinant Δ ,

if $|Ry + S| \leq |RT^i|$, then

$$\gamma \begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} T^{-2 \deg(R) - i + \deg \Delta} & P/R \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}} \quad (2.1)$$

if $|Ry + S| \geq |RT^i|$, then

$$\gamma \begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} T^{i - 2 \deg(Ry + S) + \deg \Delta} & \frac{Py + Q}{Ry + S} \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}} \quad (2.2)$$

- Converting $\begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix}$ (with $i \in \mathbb{Z}, y \in k_\infty$) to the $\gamma\sigma_n$ representation.

If $y \equiv 0 \pmod{T^i r_\infty}$ then there is nothing to be done, so we can assume $y \notin T^i r_\infty$.

Suppose $i \geq 0$. Then there is a $C \in \mathbb{F}_q[T]$ such that

$$\begin{bmatrix} 1 & C \\ 0 & 1 \end{bmatrix} \sigma_i = \begin{bmatrix} T^i & C \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}}$$

and we are done.

So we can assume that $i < 0$ and $y \neq 0$. We choose relatively prime, nonzero polynomials A and B such that $\deg B \leq -i$ and $|A/B - y| \leq |T^i|$. This is clearly possible because y is determined modulo $T^i r_\infty$ only. So we have

$$\begin{bmatrix} T^i & A/B \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} T^i & y \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}}. \quad (2.3)$$

Let $n = -2 \deg B - i$ (possibly a negative integer). Since A and B are relatively prime we can find C, D with $AD - BC \in \mathbb{F}_q^\times$ and $\deg D < \deg B$.

Now we have two cases:

Case 1 $|D| \leq |BT^n|$

We are done, as either the left hand or the right hand side of

$$\begin{bmatrix} A & C \\ B & D \end{bmatrix} \sigma_n \equiv \begin{bmatrix} C & A \\ D & B \end{bmatrix} \sigma_{-n} \pmod{\mathfrak{K}\mathfrak{J}}$$

has the desired form and if $n \geq 0$ then by equation 2.1 and the fact that

$$|D| \leq |BT^n|$$

$$\begin{bmatrix} A & C \\ B & D \end{bmatrix} \sigma_n \equiv \begin{bmatrix} T^{-2 \deg B - n} & A/B \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}},$$

or if $n \leq 0$ then by equation 2.2 and the fact that $|D| \leq |BT^n|$ i.e. $|B| \geq$

$$|DT^{-n}|$$

$$\begin{bmatrix} C & A \\ D & B \end{bmatrix} \sigma_{-n} \equiv \begin{bmatrix} T^{-2 \deg B - n} & A/B \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{J}}.$$

Case 2 $|D| > |BT^n|$

Notice that in this case $D \neq 0$. We now show that $|\frac{C}{D} - y| \leq |T^i|$.

Since $\frac{A}{B} - \frac{C}{D} = \frac{\alpha}{BD}$ we have $|\frac{C}{D} - y| = |\frac{A}{B} - \frac{\alpha}{BD} - y| \leq \max(|\frac{\alpha}{BD}|, |\frac{A}{B} - y|)$ by the ultrametric inequality, but we know already that $|\frac{A}{B} - y| \leq |T^i|$, so we only have to show that $|\frac{\alpha}{BD}| \leq |T^i|$.

But $|BD| > |B \cdot BT^n| = |T^{-i}|$ since $n = -2 \deg B - i$, thus $|\frac{\alpha}{BD}| < |T^i|$.

We can now repeat the steps below equation 2.3 with C and D in place of A and B . This procedure will eventually terminate, because $\deg D < \deg B$. In fact the sequence of fractions we are computing is a subsequence of the convergents of y .

2.4 Automorphic Functions, Cusp Forms, and Hecke Operators

If one assumes an adelic point of view, then the entire theory of automorphic forms and Hecke operators can be written and treated uniformly, regardless of what global field has been chosen, and without the need for special cases for certain places. From a computational point of view however, it is much more convenient to fix a place (in our case T^{-1} , which we will refer to as the infinite place, even though it is a non-archimedean place) and work over the chosen local field. We are therefore presenting all definitions in a low level fashion customized for the choice we have made, and refer the reader to [25] for an adelic treatment.

Let Γ' be a finite-index subgroup of Γ . A complex valued function on G is called an *automorphic function for Γ'* if it is left invariant under Γ' and right invariant under \mathfrak{K} . We will exclusively consider the Hecke subgroup Γ_A and call the corresponding functions *automorphic functions of level A* .

Classically one demands that the automorphic functions are analytic, or at least eigenfunctions of the Laplace operator. In the present case, the Hecke operator H_∞ (see page 15) is analogous to the Laplace operator. It is easy to see [24] that the space of automorphic eigenfunctions for a given eigenvalue of H_∞ is a finite dimensional vector space. We will be interested in the space of cusp forms, whose dimension has been

computed by Harder et al. [7].

2.4.1 Cusp Forms

Let $N_\infty = \left\{ \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \mid x \in k_\infty \right\}$ be the standard unipotent subgroup of the standard parabolic subgroup $P_\infty = \left\{ \begin{bmatrix} \alpha & x \\ & \beta \end{bmatrix} \mid \alpha, \beta, x \in k_\infty, \alpha, \beta \neq 0 \right\}$ of G . Then the point $\infty = \lim_{n \rightarrow \infty} \sigma_n \mathfrak{K} \mathfrak{Z}$ is fixed by N_∞ , and hence for $g \in G$, $g\infty$ is fixed by $gN_\infty g^{-1}$. For $g \in G$, $N' = gN_\infty g^{-1}$ will be called Γ_A -*cuspidal*, if $N' \cap \Gamma_A \neq \{1\}$, and in that case the point $g\infty = \lim_{n \rightarrow \infty} g\sigma_n \mathfrak{K} \mathfrak{Z}$ will be called a *cuspidal* for Γ_A . The cuspidal ∞ will also be called the *cuspidal at infinity*.

Two cusps $g\infty$ and $h\infty$ are called *equivalent* if there is a $\gamma \in \Gamma_A$ such that $\gamma g\infty = h\infty$. It follows that two cusps $[R, S]\infty$ and $[R', S']\infty$ are equivalent, if there is $N \in \mathbb{Z}$ such that for all integers $n > N$ the points represented by $[R, S]\sigma_n$ and $[R', S']\sigma_n$ are in the same Γ_A -orbit. Hence the cusps $[R, S]\infty$ and $[R', S']\infty$ are equivalent if there are $\alpha, \beta \in \mathbb{F}_q^\times$ and a polynomial Q such that $[R, S] \equiv [R', S'] \begin{bmatrix} \alpha & Q \\ & \beta \end{bmatrix}$.

We let dn denote a Haar measure on $N = gN_\infty g^{-1}$, for $g \in G$. Let f be an automorphic function of level A , then f will be called a *cuspidal form* for Γ_A if

$$\int_{(N \cap \Gamma_A) \backslash N} f(ng) dn = 0 \quad (2.4)$$

for all Γ_A -cuspidal groups N and $g \in G$.

The following Lemma will be useful for computing spaces of cuspidal forms.

Lemma 5. *An automorphic form f of level A is a cuspidal form if and only if*

$$\int_{r_\infty - r_\infty^\times} f \left([R, S] \begin{bmatrix} 1 & hz \\ & 1 \end{bmatrix} g \right) dz = 0$$

for all $g \in G$, all $[R, S] \in \Gamma$, and $h = \frac{A}{(A, R^2)}$.

In the Lemma, $r_\infty - r_\infty^\times$ denotes the difference set of r_∞ and r_∞^\times .

Proof. We will use the fact that all parabolic subgroups of G are conjugates to reformulate the condition for f to be a cuspidal form. Notice that by applying the LU-decomposition, every element in \mathfrak{K} can be written as the product of a matrix $\begin{bmatrix} 1 & \\ & y \end{bmatrix}$ or

$\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$ and an upper triangular matrix. Since N_∞ is invariant under conjugation by σ_n , upper triangular matrices, and the center \mathfrak{Z} , and since $\sigma_n \begin{bmatrix} 1 & \\ y/T^n & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ y/T^n & 1 \end{bmatrix} \sigma_n$, we can obtain all conjugates of N_∞ from elements $a = \gamma l$, $\gamma = [R, S]$, $l = \begin{bmatrix} 1 & \\ y & 1 \end{bmatrix} \in \mathfrak{K}$. Let $N' = aN_\infty a^{-1}$. Then

$$\int_{(N' \cap \Gamma_A) \backslash N'} f(n'g) dn' = \mu \int_{(N_\infty \cap a^{-1} \Gamma_A a) \backslash N_\infty} f(ana^{-1}g) dn$$

where μ is the modulus introduced by the substitution $n' \rightarrow n$. We can write $n \in (N_\infty \cap a^{-1} \Gamma_A a) \backslash N_\infty$ in the form $\begin{bmatrix} 1 & hz \\ & 1 \end{bmatrix}$, $z \in r_\infty - r_\infty^\times$, and h is determined as follows. First consider the intersection and notice that $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \in a^{-1} \Gamma_A a$ if and only if $a \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a^{-1} \in \Gamma_A$. The lower left entry of $a \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a^{-1}$ is $-x(R + yS)^2$ which needs to be congruent to 0 modulo A , while all other entries need to be polynomials. Thus,

- for $y = 0$, we get $x \equiv 0 \pmod{\frac{A}{(A, R^2)}}$, hence x and thus all entries in the matrix $a \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a^{-1}$ are polynomial. So $h = \frac{A}{(A, R^2)}$ in this case.
- For nonzero $y = c/d$, with $c, d \in \mathbb{F}_q[T]$, we can assume without loss of generality that d does not divide S and we need x to be a multiple of $d^2 \frac{A}{(A, (Rd+Sc)^2)}$. It is easy to see that this choice guarantees $a \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a^{-1} \in \Gamma_A$, hence $h = d^2 \frac{A}{(A, (Rd+Sc)^2)}$. In this case, we further have

$$[R, S] \begin{bmatrix} 1 & \\ c/d & 1 \end{bmatrix} \begin{bmatrix} 1 & hz \\ & 1 \end{bmatrix} = [R', S'] \begin{bmatrix} 1 & h'z \\ & 1 \end{bmatrix} g'$$

where $h' = \frac{A}{(A, R'^2)}$, $R' = Rd + Sc$, $S' = Rb + Se$, with b, e determined by $de - bc = 1$, and $g' = \begin{bmatrix} 1/d & -b \\ & d \end{bmatrix}$.

- Finally, if $y \notin \mathbb{F}_q(T)$, then

$$a \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a^{-1} = [R, S] \begin{bmatrix} 1 - xy & x \\ -xy^2 & xy + 1 \end{bmatrix} [R, S]^{-1}$$

and since xy^2 and xy cannot be rational at the same time unless $x = 0$, the conjugated matrix is rational only if it is the identity matrix. Hence $N' \cap \Gamma_A = \{1\}$, and N is not Γ_A -cuspidal.

□

2.4.2 Hecke Operators

Let f be an automorphic function of level A , and let Π be a monic prime polynomial not dividing A . We denote by H_Π the *Hecke Operator*

$$H_\Pi : f(g) \rightarrow f_\Pi(g) = f \left(\begin{bmatrix} \Pi & 0 \\ 0 & 1 \end{bmatrix} \cdot g \right) + \sum_{\substack{M \in \mathbb{F}_q[T] \\ |M| < |\Pi|}} f \left(\begin{bmatrix} 1 & M \\ 0 & \Pi \end{bmatrix} \cdot g \right)$$

and by H_∞ the Hecke Operator attached to ∞

$$H_\infty : f(g) \rightarrow f_\infty(g) = f \left(g \cdot \begin{bmatrix} T & 0 \\ 0 & 1 \end{bmatrix} \right) + \sum_{\xi \in \mathbb{F}_q} f \left(g \cdot \begin{bmatrix} T^{-1} & \xi \\ 0 & 1 \end{bmatrix} \right).$$

We can also define Hecke operators for primes dividing the level A , by following Atkin and Lehner [1].

The *Fricke involution* $W = \begin{bmatrix} 0 & -1 \\ A & 0 \end{bmatrix}$ is another operator which preserves the spaces of automorphic functions and cusp forms. Related to it, we have for each prime p dividing A , say $p^e \parallel A$, the involution $W_p = \begin{bmatrix} p^e x & y \\ Az & p^e w \end{bmatrix}$, where $x, y, z, w \in \mathbb{F}_q[T]$ such that $\det W_p = p^e$, $W_p^2 \in \mathfrak{Z}$. The action of $\prod_{p^e \parallel A} W_p$ is equivalent to the action of W modulo Γ_A .

We will abuse notation and denote the operator and the matrix by the same letter. Thus for instance we will write $Wf(g) = f(Wg)$. All the Hecke and involution operators commute and map the space of cusp forms of level A into itself [1].

The automorphic function f is called an *eigenform* of the operator L , if $Lf = \lambda f$ for some *eigenvalue* $\lambda \in \mathbb{C}$.

2.5 L-function

Let f be a cusp form and an eigenform of H_∞ . Then

$$L(f, s) = \sum_{n=-\infty}^{\infty} f(\sigma_n) q^{ns}$$

is called the *L-function* of f .

Using the Fricke involution we obtain a functional equation analogous to the classical case, as follows. If f is an automorphic function of level A , then so is $f'(g) = f(Wg)$, and their L -functions are related by $L_f(s) = q^{s \deg A} L_{f'}(-s)$.

Chapter 3

The Fundamental Domain

Throughout this chapter A is a fixed monic polynomial and γ, γ_i are elements in Γ .

3.1 Right cosets of Γ_A in Γ

In this section we will describe a convenient set of right coset representatives of Γ_A in Γ , and we will compute the index of Γ_A in Γ .

Let $\Gamma_A\gamma_1 \cup \dots \cup \Gamma_A\gamma_k = \Gamma$ be the union of right cosets of Γ_A in Γ . Two elements $[R, S], [R', S'] \in \Gamma$ are in the same coset if and only if $RS' - R'S \equiv 0 \pmod{A}$. We will write $[R, S] \equiv [R', S']$ when this is the case.

Theorem 2. *A complete reduced set of right coset representatives for Γ_A is given by elements of the form $[R, S]$, where $(R, S) = 1$, R is monic, $R|A$, and S is unique up to multiples of A/R .*

Proof. Clearly $[R, S] \in \Gamma$ means that R and S are relatively prime, and since for $\alpha \in \mathbb{F}_q$, $[\alpha R, S] \equiv [R, \alpha^{-1}S]$, we can assume that R is monic.

If R is relatively prime to A , then $[R, S]$ is in the same Γ_A coset as $[1, S']$ where $S' \equiv SR^{-1} \pmod{A}$ and $\deg S' < \deg A$.

Now suppose $(R, A) \neq 1$. We write $R = df$ such that $(A, R) = d$, and we have $[R, S] = [df, S] \equiv [d, S']$, where $S' \equiv Sf^{-1} \pmod{A/d}$.

So we can choose R monic such that $R|A$. It remains to show that S is unique up to multiples of A/R and that the set of representatives is reduced.

For d, d' monic, both dividing A , $[d, S] \equiv [d', S']$ if and only if $d = d'$ and $S \equiv S' \pmod{A/d}$:

$Sd' - dS' \equiv 0 \pmod{A}$ implies $Sd' - dS' \equiv 0 \pmod{d}$ and $Sd' - dS' \equiv 0 \pmod{d'}$, thus $Sd' \equiv 0 \pmod{d}$ and $-dS' \equiv 0 \pmod{d'}$, but that implies $d|d'$ and $d'|d$ hence $d = d'$ since we are assuming that d, d' are monic. But then $Sd' - dS' \equiv 0 \pmod{A}$ is equivalent to $S \equiv S' \pmod{A/d}$. \square

We will refer to the set of representatives $[R, S]$ described in theorem 2 as the *standard set of coset representatives* for Γ_A in Γ , and to any element of the set as a *standard coset representative* for Γ_A in Γ .

Corollary 1. *The index of Γ_A in Γ is*

$$\sum_{\substack{d|A \\ d \text{ monic}}} \Phi_{A/d}((A/d, d))$$

where $\Phi_N(P)$ denotes the number of polynomials relatively prime to P of degree smaller than $\deg N$.

Proof. We will show that for any monic $d|A$ every polynomial S' of degree smaller than $\deg A/d$ and relatively prime to $(A/d, d)$ gives rise to an element $[d, S'] \in \Gamma$. We know already that $[d, S]$ and $[d, S']$ are equivalent if and only if $S \equiv S' \pmod{A/d}$. Thus to compute the index we need to count the number of polynomials of degree smaller than $\deg A/d$ and relatively prime to $(A/d, d)$ as claimed above.

Let $d|A$. For any $[d, S] \in \Gamma$ we can find an $S' = S + kA/d$ (by reducing S modulo A/d) of degree smaller than $\deg A/d$. Then

$$(S', (A/d, d)) = (S + kA/d, (A/d, d)) = (S, (A/d, d)) = 1.$$

Conversely, let S' be a polynomial of degree smaller than $\deg A/d$ and such that $(S', (A/d, d)) = 1$.

If $(S', d) = 1$, then $[d, S'] \in \Gamma$ and there is nothing to be shown. If $(S', d) \neq 1$ then let $g_1 = (S'^{\deg d}, d)$ and $g_2 = ((A/d)^{\deg d}, d)$. Since $1 = ((d, A/d), S') = ((d, A/d), (d, S'))$ it follows that $(g_1, g_2) = 1$. If we let $k = \frac{d}{g_1 g_2}$ then $(k, g_1) = (k, g_2) = 1$, by construction of g_1 and g_2 . Now $(S' + kA/d, d) = (S' + kA/d, g_1 g_2 k) = 1$, because g_1 divides a power of S' but $(g_1, kA/d) = 1$, and g_2 divides a power of A/d but $(g_2, S') = (k, S') = 1$. It

follows that every polynomial S' relatively prime to $(A/d, d)$ gives rise to an element $[S, d] \in \Gamma$. \square

Remark 5. Keeping the notation used in the proof, we have seen in the last paragraph that every standard coset representative $[d, S]$ can be obtained from a polynomial S' of degree smaller than $\deg A/d$ and relatively prime to $(A/d, d)$ by writing $S = S' + kA/d$ for $k = \frac{d}{(S' \deg d, d)((A/d) \deg d, d)}$. Then $[d, S] = [d, S' + \frac{A}{((A/d) \deg d, d)(S' \deg d, d)}]$ for some S' relatively prime to $(A/d, d)$ and of degree smaller than $\deg A/d$.

We can now prove the following formula for the index.

Theorem 3. *The index for Γ_A in Γ is given by*

$$[\Gamma : \Gamma_A] = \sum_{\substack{d|A \\ d \text{ monic}}} \Phi_{A/d}((A/d, d)) = |A| \prod_{\substack{p|A \\ p \text{ prime}}} \left(1 + \frac{1}{|p|}\right) \quad (3.1)$$

Proof. We first show that the index is multiplicative. Suppose A, B are relatively prime.

Then

$$\sum_{d|A, e|B} \Phi_{\frac{AB}{de}}((A/dB/e, de)) = \sum_{d|A} \Phi_{\frac{A}{d}}((A/d, d)) \sum_{e|B} \Phi_{\frac{B}{e}}((B/e, e))$$

by lemma 2 and standard laws for gcd's. Thus we can reduce our computations to the case where $A = p^k$ is a prime power. Then

$$\begin{aligned} & \sum_{p^i|A} \Phi_{A/p^i}((A/p^i, p^i)) = \sum_{p^i|A} \Phi_{p^{k-i}}((p^{k-i}, p^i)) \\ &= \sum_{p^i|A} \Phi_{p^{k-i}}(p^{\min(k-i, i)}) = |p|^k + 1 + \sum_{i=1}^{k-1} |p^{k-i}| \left(1 - \frac{1}{|p|}\right) \quad \text{by lemma 1} \\ &= |p|^k + (|p|^{k-1} - |p|^{k-2}) + (|p|^{k-2} - |p|^{k-3}) + \dots + (|p| - 1) + 1 \\ &= |p|^k + |p|^{k-1} = |p|^k \left(1 + \frac{1}{|p|}\right) = |A| \prod_{p|A} \left(1 + \frac{1}{|p|}\right) \end{aligned}$$

\square

Remark 6. We could also have followed the classical proof for the index of $\Gamma_0(N)$ in $\text{PSL}(2, \mathbb{Z})$ as can be found for example in [8, Prop. 9.3] by substituting monic conditions for conditions on positivity of integers, and replacing size relations by corresponding degree relations.

3.2 The number of points on σ -level n

It follows immediately from theorem 1 that the fundamental domain for $\Gamma \backslash G/\mathfrak{K}\mathfrak{Z}$ is given by $\{\sigma_i | i \in \mathbb{Z}, i \geq 0\}$. If $\gamma_1, \dots, \gamma_{[\Gamma:\Gamma_A]}$ are the right coset representatives for Γ_A in Γ , then the fundamental domain for $\Gamma_A \backslash G/\mathfrak{K}\mathfrak{Z}$ is given by a subset of the double coset representatives $\gamma_i \sigma_j$.

We are now going to count the number of double coset representatives for each σ -level, treating σ -level 0 separately. We will use the standard set of right coset representatives of Γ_A in Γ which was described in theorem 2.

3.2.1 The σ -level 0

Let $\gamma_1, \gamma_2 \in \Gamma$. For two points $\gamma_1 \sigma_0 \mathfrak{K}\mathfrak{Z}$ and $\gamma_2 \sigma_0 \mathfrak{K}\mathfrak{Z}$ to be in the same Γ_A orbit, it is by the remark following theorem 1 necessary that $\Gamma_A \gamma_1 = \gamma_2 M$, for some $M \in \text{GL}(2, \mathbb{F}_q)$. Thus to count the number of Γ_A orbits on this level we need to count the double cosets $\Gamma_A \backslash \Gamma / \text{GL}(2, \mathbb{F}_q)$. We will let $\text{GL}(2, \mathbb{F}_q)$ act from the right on the right cosets of Γ_A in Γ and use Burnside's Lemma to find the number of Γ_A orbits by counting the number of fixed points for each conjugacy class of $\text{GL}(2, \mathbb{F}_q)$.

Let $\alpha, \delta \in \mathbb{F}_q$, and $\bar{\beta} = \beta^q$, where $\beta \notin \mathbb{F}_q$, but in a quadratic extension of \mathbb{F}_q , so that $\beta \neq \bar{\beta}$. The following table shows the types of conjugacy classes we have in $\text{GL}(2, \mathbb{F}_q)$ [11]. The last column shows the number of fixed points for the $\text{GL}(2, \mathbb{F}_q)$ action on the right cosets of Γ_A in Γ and will be explained below the table.

	representative $g \in \text{GL}(2, \mathbb{F}_q)$	number of conjugacy classes	number of elements in each class	number of fixed points
(S1)	$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$	$q - 1$	1	$[\Gamma : \Gamma_A]$
(S2)	$\begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}, \alpha \neq \delta$	$\frac{(q-1)(q-2)}{2}$	$q^2 + q$	$2^{\omega(A)}$
(S3)	$\begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$	$q - 1$	$q^2 - 1$	$ \lfloor \sqrt{A} \rfloor $
(S4)	$\begin{bmatrix} 0 & -\beta\bar{\beta} \\ 1 & \beta+\bar{\beta} \end{bmatrix}$	$\frac{q^2-q}{2}$	$q^2 - q$	0 or $2^{\omega(A)}$

The number of fixed points in the set of cosets of Γ_A in Γ has been obtained as follows. Recall the definition of $\lfloor \sqrt{A} \rfloor$ from page 5.

(S1): $[\alpha R, \alpha S] \equiv [R, \alpha^{-1}\alpha S] = [R, S]$ thus all points are fixed points.

(S2): $[\alpha R, \delta S] \equiv [R, S]$ only if $(\alpha - \delta)RS \equiv 0 \pmod{A}$ i.e. if $A|RS$. Since for $R|A$ we have $[R, A/R] \equiv [R, mA/R]$ (any $m \in \mathbb{F}_q[T]$) it follows that for each $R|A$ there is at most one such element. And since $(R, S) = 1$ it follows that there is one such element if and only if $(R, A/R) = 1$. Thus there will be $2^{\omega(A)}$ such elements.

(S3): $[\alpha R, \alpha S + R] \equiv [R, S + \alpha^{-1}R] \equiv [R, S]$ when $\alpha^{-1}R^2 \equiv 0 \pmod{A}$, thus R needs to be a multiple of $[\sqrt{A}]$. So we need to count the number of cosets with representatives $[R, S]$ for Γ_A in Γ for which R is a multiple of $[\sqrt{A}]$. The same arguments as the ones used in the proof of corollary 1 now show that there are

$$\sum_{d|A/[\sqrt{A}]} \Phi_{A/(d[\sqrt{A}])} \left((A/(d[\sqrt{A}]), d[\sqrt{A}]) \right)$$

such cosets. Using the facts that $[\sqrt{A}][\sqrt{A}] = A$ and that $[\sqrt{A}]/d$ divides $[\sqrt{A}]d$ we can first simplify this as

$$\sum_{d|[\sqrt{A}]} \Phi_{[\sqrt{A}]/d} \left([\sqrt{A}]/d \right) = \sum_{d|[\sqrt{A}]} \Phi \left([\sqrt{A}]/d \right) = \sum_{d|[\sqrt{A}]} \Phi(d)$$

and using lemma 3 we get

$$\sum_{d|[\sqrt{A}]} \Phi(d) = \left| [\sqrt{A}] \right|$$

(S4): $[S, -\beta\bar{\beta}R + (\beta + \bar{\beta})S] \equiv [R, S]$ when $S^2 + \beta\bar{\beta}R^2 - (\beta + \bar{\beta})RS \equiv 0 \pmod{A}$. But then $(R, A) = 1$ because $(R, S) = 1$, thus we can assume without loss of generality that $R = 1$. Then $S^2 - (\beta + \bar{\beta})S + \beta\bar{\beta}$ is an irreducible polynomial over $\mathbb{F}_q[T]$ and $S^2 - (\beta + \bar{\beta})S + \beta\bar{\beta} \equiv 0 \pmod{A}$ will only have solutions if it has solutions modulo every prime divisor of A , i.e. only if $\beta, \bar{\beta} \in \mathbb{F}_q[T]/(P)$, where $P|A$, P is prime and has even degree (since the finite field \mathbb{F}_{q^2} has to be a subfield of $\mathbb{F}_{q^{\deg P}}$). Because $\beta \neq \bar{\beta}$ there will be two solutions for each such prime P , and by Hensel's Lemma the two solutions lift to two unique solutions modulo powers of

P. Combining the solutions using the Chinese Remainder Theorem we see that there will be $2^{\omega(A)}$ solutions.

Now by Burnside's Lemma and the table above the number of orbits is equal to

$$\frac{\left((q-1)[\Gamma : \Gamma_A] + \frac{(q-1)(q-2)}{2}(q^2+q)2^{\omega(A)} + (q-1)(q^2-1) \left| \lfloor \sqrt{A} \rfloor \right| + \delta_A \frac{(q^2-q)^2}{2} 2^{\omega(A)} \right)}{q(q-1)^2(q+1)}$$

which can easily be simplified to the expression in the following theorem.

Theorem 4. *The number of inequivalent points in the fundamental domain for level A on σ -level 0 is*

$$C_0(A) = \frac{[\Gamma : \Gamma_A]}{q(q-1)(q+1)} + \frac{(q-2)2^{\omega(A)-1}}{(q-1)} + \frac{\left| \lfloor \sqrt{A} \rfloor \right|}{q} + \frac{\delta_A q 2^{\omega(A)-1}}{q+1}$$

$$\text{where } \delta_A = \begin{cases} 1 & \text{if all } p|A \text{ have even degree} \\ 0 & \text{otherwise} \end{cases}$$

3.2.2 σ -level $n > 0$

Recall that $G_n = \left\{ \begin{bmatrix} a & Q \\ 0 & b \end{bmatrix} \in \text{GL}(2, \mathbb{F}_q[T]) \mid a, b \in \mathbb{F}_q, \deg Q \leq n \right\}$ and let $\gamma_1, \gamma_2 \in \Gamma$. For two points $\gamma_1 \sigma_n \mathfrak{K} \mathfrak{J}$ and $\gamma_2 \sigma_n \mathfrak{K} \mathfrak{J}$ to be in the same Γ_A orbit, it is by remark 1 necessary that $\Gamma_A \gamma_1 = \gamma_2 M$, for some $M \in G_n$. Thus to count the number of Γ_A orbits on σ -level n we need to count the double cosets $\Gamma_A \backslash \Gamma / G_n$. G_n consists of $(q-1)^2 q^{n+1}$ elements.

We will let G_n act on the set of right cosets of Γ_A in Γ and choose the standard set of coset representatives described in theorem 2. We will proceed as we did for σ -level 0 and use Burnside's Lemma to count the number of orbits.

The center of G_n consists of matrices cI , $c \in \mathbb{F}_q^\times$, I the identity matrix. For $\begin{bmatrix} \tilde{\alpha} & \tilde{Q} \\ \tilde{\beta} & \end{bmatrix}, \begin{bmatrix} \alpha & Q \\ \beta & \end{bmatrix} \in G_n$

$$\begin{bmatrix} \tilde{\alpha} & \tilde{Q} \\ \tilde{\beta} & \end{bmatrix} \begin{bmatrix} \alpha & Q \\ \beta & \end{bmatrix} \begin{bmatrix} \tilde{\alpha} & \tilde{Q} \\ \tilde{\beta} & \end{bmatrix}^{-1} = \begin{bmatrix} \alpha & \frac{\beta-\alpha}{\tilde{\beta}} \tilde{Q} + \frac{\tilde{\alpha}}{\tilde{\beta}} Q \\ \beta & \end{bmatrix}$$

thus for fixed α and β with $\alpha \neq \beta$ a conjugacy class is given by the matrices of the form $\begin{bmatrix} \alpha & Q \\ \beta & \end{bmatrix}$, for all $Q \in \mathbb{F}_q[T]$, of degree smaller or equal to n . Thus there are q^{n+1}

matrices in each of these conjugacy classes, and since $\alpha \neq \beta$ there are $(q-1)(q-2)$ classes of this type.

For fixed $\alpha = \beta$ we see that every conjugacy class is given by constant multiples of a fixed polynomial of degree smaller than or equal to n , so there are $q-1$ elements in each class, and there are $(q-1)\frac{q^{n+1}-1}{q-1}$ such classes, because there are $\frac{q^{n+1}-1}{q-1}$ monic polynomials of degree smaller than or equal to n and $q-1$ choices for α .

So we obtain the following table of conjugacy classes and numbers of fixed points in the set of cosets of Γ_A in Γ .

$g \in G_n$	representative	number of conjugacy classes	number of elements in each class	number of fixed points
(T1)	$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$	$q-1$	1	$[\Gamma : \Gamma_A]$
(T2)	$\begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}, \alpha \neq \delta$	$(q-1)(q-2)$	q^{n+1}	$2^{\omega(A)}$
(T3)	$\begin{bmatrix} \alpha & Q \\ 0 & \alpha \end{bmatrix}, Q \text{ monic}$	$q^{n+1}-1$	$q-1$	(see below)

In case (T3) we will count the number of fixed points slightly differently.

(T1): $[\alpha R, \alpha S] \equiv [R, \alpha^{-1}\alpha S] = [R, S]$.

(T2): $[\alpha R, \delta S] \equiv [R, S]$ only if $(\alpha - \delta)RS \equiv 0 \pmod{A}$ i.e. if $A|RS$. Since for $R|A$ we have $[R, A/R] \equiv [R, mA/R]$ (any $m \in \mathbb{F}_q[T]$) it follows that for each $R|A$ there is at most one such element. And since $(R, S) = 1$ it follows that there is one such element if and only if $(R, A/R) = 1$. Thus there will be $2^{\omega(A)}$ such elements.

(T3): We have $(q^{n+1}-1)(q-1)$ elements of the form $\begin{bmatrix} \alpha & Q \\ 0 & \alpha \end{bmatrix}$ with $\alpha \in \mathbb{F}_q^\times$ and $Q \neq 0$ a polynomial of degree at most n . We will count the total number of fixed points for all these elements simultaneously.

We first notice that $[R, S]$ will be a fixed point of such an element if $[\alpha R, \alpha S + QR] \equiv [R, S + \alpha^{-1}QR] \equiv [R, S]$, i.e. when $Q \equiv 0 \pmod{\frac{A/R}{(R, A/R)}}$, independent of α . Thus $[R, S]$ will be a fixed point if Q is a multiple of $\frac{A/R}{(R, A/R)}$. So the total number of fixed points will be the number of nonzero multiples of $\frac{A/R}{(R, A/R)}$ of degree smaller or equal to n , times $(q-1)$ for that many possible values of

α , times the number of standard right coset representatives of the form $[R, S]$ (fixed R), summed up over all possible R 's. If we let $M_n(P)$ denote the number of polynomials of degree at most n which are divisible by P , and use corollary 1 for the index of Γ_A in Γ , then

$$(q-1) \sum_{R|A} \left(M_n \left(\frac{A/R}{(R, A/R)} \right) - 1 \right) \cdot \Phi_{A/R}((A/R, R)).$$

It is easy to see that for $n \geq \deg P$ we have $M_n(P) = q^{n+1-\deg P}$, while for $n < \deg P$ we have $M_n(P) = 1$, as only 0 is divisible by P . Thus we can write $M_n(P) = \lceil q^{n+1-\deg P} \rceil$ for all non-negative integers n .

Applying Burnside's Lemma we get

$$\begin{aligned} C_n(A) &= \frac{1}{(q-1)^2 q^{n+1}} \left[(q-1)[\Gamma : \Gamma_A] + (q-1)(q-2)q^{n+1}2^{\omega(A)} + \right. \\ &\quad \left. (q-1) \sum_{\substack{d|A, \\ d \text{ monic}}} \left(M_n \left(\frac{A/d}{(d, A/d)} \right) - 1 \right) \Phi_{A/d}((A/d, d)) \right] \\ &= \frac{[\Gamma : \Gamma_A]}{(q-1)q^{n+1}} + \frac{q-2}{q-1} 2^{\omega(A)} + \\ &\quad \frac{1}{(q-1)q^{n+1}} \sum_{\substack{d|A, \\ d \text{ monic}}} \left(M_n \left(\frac{A/d}{(d, A/d)} \right) - 1 \right) \Phi_{A/d}((A/d, d)) \\ &= \sum_{\substack{d|A, \\ d \text{ monic}}} \Phi_{A/d}((A/d, d)) \frac{\lceil q^{n+1-\deg(A/d)+\deg((d, A/d))} \rceil}{q^{n+1}(q-1)} + \frac{q-2}{q-1} 2^{\omega(A)} \end{aligned}$$

and thus we get the following theorem.

Theorem 5. *The number of inequivalent points in the fundamental domain for the Hecke group of level A on σ -level n is*

$$C_n(A) = \sum_{d|A} \Phi_{A/d}((A/d, d)) \frac{\lceil q^{n+1-\deg(A/d)+\deg((d, A/d))} \rceil}{q^{n+1}(q-1)} + \frac{q-2}{q-1} 2^{\omega(A)}$$

3.3 Cusps

Recall that the cusps $\lim_{n \rightarrow \infty} [R, S] \sigma_n$ and $\lim_{n \rightarrow \infty} [R', S'] \sigma_n$ are equivalent if there are $\alpha, \beta \in \mathbb{F}_q^\times$ and a polynomial Q such that $[R, S] \equiv [R', S'] \begin{bmatrix} \alpha & Q \\ & \beta \end{bmatrix}$. Thus a short

computation similar to the one performed in the proof of theorem 2 shows that every cusp will be equivalent to one of the form $[d, s]$ with d, s monic, $d|A$, and s unique up to multiples of $(A/d, d)$. Thus such cusps $[d, s], [d', s']$ will be equivalent if and only if $d = d'$ and $(A/d, d)|(s - \beta s')$ for some $\beta \in \mathbb{F}_q^\times$.

Theorem 5 shows that the number of points on σ -level $n > \deg A$ remains constant, as $n \rightarrow \infty$. Thus the number of Γ_A -inequivalent cusps is an immediate corollary of the theorem. We will use theorem 5 to prove a formula for the number of inequivalent cusps of Γ_A which involves the ϕ function and thus becomes analogous to the corresponding formula in the classical case. Note however, that in our case the ϕ function is *not* multiplicative.

Theorem 6. *The number of inequivalent cusps for $\Gamma_A \setminus G/\mathfrak{K}\mathfrak{Z}$ is given by*

$$\sum_{d|A} \phi((d, A/d)) = \frac{1}{q-1} \prod_{p^e \| A} \left(q^{\deg p \lfloor \frac{e-1}{2} \rfloor} + q^{\deg p \lceil \frac{e-1}{2} \rceil} \right) + \frac{q-2}{q-1} 2^{\omega(A)}$$

where $\phi(f)$ denotes the number of monic polynomials of degree less than $\deg f$ and relatively prime to f .

Proof. For $n > \deg A$ we can simplify

$$\frac{[q^{n+1 - \deg(A/d) + \deg((d, A/d))}]}{q^{n+1}(q-1)} = \frac{1}{\left| \frac{A/d}{(d, A/d)} \right| (q-1)}$$

hence according to theorem 5

$$\begin{aligned} C(A) &= \sum_{d|A} \Phi_{A/d}((A/d, d)) \frac{1}{\left| \frac{A/d}{(d, A/d)} \right| (q-1)} + \frac{q-2}{q-1} 2^{\omega(A)} \\ &= \frac{1}{q-1} \sum_{d|A} \Phi((A/d, d)) + \frac{q-2}{q-1} 2^{\omega(A)} \\ &= \frac{1}{q-1} \left(\sum_{d|A} \Phi((A/d, d)) - 2^{\omega(A)} \right) + 2^{\omega(A)} \end{aligned}$$

Now we will show that this expression is equal to the left and the right hand side of the identity stated in the corollary. For the left hand side, notice first that we have $\phi(f) = \frac{\Phi(f)}{q-1}$ when $f \neq 1$ and $\phi(1) = \Phi(1)$. So the ϕ function is not multiplicative

for function fields over finite fields with more than 2 elements. But since the Φ function is multiplicative, and $(d, A/d)$ is multiplicative for fixed A , $\sum_{d|A} \Phi((d, A/d))$ as a summatory function is multiplicative. Since for $f \neq 1$, $\Phi(f) = (q-1)\phi(f)$,

$$\sum_{d|A} \phi((d, A/d)) = \frac{1}{q-1} \sum_{\substack{d|A \\ (d, A/d) \neq 1}} \Phi((d, A/d)) + \sum_{\substack{d|A \\ (d, A/d) = 1}} \Phi((d, A/d))$$

But

$$\sum_{\substack{d|A \\ (d, A/d) = 1}} \Phi((d, A/d)) = \sum_{\substack{d|A \\ (d, A/d) = 1}} 1 = 2^{\omega(A)}$$

Thus

$$\sum_{d|A} \phi((d, A/d)) = \frac{1}{q-1} \left(\sum_{d|A} \Phi((d, A/d)) - 2^{\omega(A)} \right) + 2^{\omega(A)}$$

which is what we had to show.

For the right hand side, it remains to compute $\sum_{d|A} \Phi((d, A/d))$. Since this sum is multiplicative it suffices to compute it for a prime power. This computation is very similar to the one we already performed in the proof of theorem 3. Let $A = p^e$, then

$$\begin{aligned} \sum_{p^i | p^e} \Phi((p^{e-i}, p^i)) &= \sum_{p^i | p^e} \Phi(p^{\min(e-i, i)}) \\ &= 2 + \sum_{i=1}^{e-1} |p^{\min(e-i, i)}| \left(1 - \frac{1}{|p|} \right) \end{aligned}$$

For convenience we compute the last sum separately. We start by splitting it up into two halves

$$\sum_{i=1}^{\lfloor (e-1)/2 \rfloor} |p^{\min(e-i, i)}| \left(1 - \frac{1}{|p|} \right) + \sum_{i=\lfloor (e-1)/2 \rfloor + 1}^{e-1} |p^{\min(e-i, i)}| \left(1 - \frac{1}{|p|} \right)$$

and consider the cases e is odd and e is even separately.

If e is odd, then the two sums are equal and we get for each of them

$$(|p| - 1) + (|p|^2 - |p|) + \dots + (|p|^{(e-1)/2} - |p|^{(e-3)/2}) = |p|^{(e-1)/2} - 1$$

thus the total comes to $2|p|^{(e-1)/2} - 2$.

If e is even, then $\lfloor (e-1)/2 \rfloor = e/2 - 1$ and the right hand sum has one term more than the left hand sum, so the total comes to $|p|^{e/2-1} + |p|^{e/2} - 2$.

So we have

$$\sum_{p^i | p^e} \Phi((p^{e-i}, p^i)) = \begin{cases} 2|p|^{(e-1)/2} & \text{if } e \text{ is odd} \\ |p|^{e/2-1} + |p|^{e/2} & \text{if } e \text{ is even} \end{cases} = |p|^{\lfloor \frac{e-1}{2} \rfloor} + |p|^{\lceil \frac{e-1}{2} \rceil}.$$

Putting everything together, we get

$$\begin{aligned} & \frac{1}{q-1} \left(\prod_{p^e \| A} \left(|p|^{\lfloor \frac{e-1}{2} \rfloor} + |p|^{\lceil \frac{e-1}{2} \rceil} \right) - 2^{\omega(A)} \right) + 2^{\omega(A)} \\ &= \frac{1}{q-1} \left(\prod_{p^e \| A} \left(q^{\deg p \lfloor \frac{e-1}{2} \rfloor} + q^{\deg p \lceil \frac{e-1}{2} \rceil} \right) - 2^{\omega(A)} \right) + 2^{\omega(A)} \\ &= \frac{1}{q-1} \prod_{p^e \| A} \left(q^{\deg p \lfloor \frac{e-1}{2} \rfloor} + q^{\deg p \lceil \frac{e-1}{2} \rceil} \right) + \frac{q-2}{q-1} 2^{\omega(A)} \end{aligned}$$

and the theorem is proved. \square

3.4 The number of edges between σ -levels

As pointed out in section 2.3.2 the neighborhood relation in X is stable under left G action. Thus Γ_A acts not only on the vertices of X , but also on the edges of X . Let X_A denote the quotient graph.

Recall from remark 3 that every point on σ -level $n > 0$ has q neighbors on σ -level $n-1$ and one neighbor on σ -level $n+1$. Thus for points on σ -level $n > 0$ we can identify the edge between two neighbors $\gamma\sigma_n\mathfrak{R}\mathfrak{Z}$, $\gamma'\sigma_{n+1}\mathfrak{R}\mathfrak{Z}$ with the vertex $\gamma'\sigma_n\mathfrak{R}\mathfrak{Z}$. Hence the number $E_n(A)$ of inequivalent edges between σ -levels n and $n+1$ in X_A is equal to the number of inequivalent points on σ -level $n > 0$. Since all neighbors of points on σ -level 0 are on σ -level 1, we will have to work a little harder to compute $E_0(A)$. We first recall from lemma 4 that $\mathfrak{R}\mathfrak{Z}$ has neighbors $\sigma_1\mathfrak{R}\mathfrak{Z}$ and $\begin{bmatrix} 1 & \xi \\ & 1 \end{bmatrix} \sigma_{-1}\mathfrak{R}\mathfrak{Z} = \begin{bmatrix} \xi & 1 \\ & 1 \end{bmatrix} \sigma_1\mathfrak{R}\mathfrak{Z}$, for $\xi \in \mathbb{F}_q$. It can be easily verified that the corresponding edges are indexed by the conjugates of $\mathfrak{Z}\mathfrak{Z}$ by $\begin{bmatrix} \xi & 1 \\ & 1 \end{bmatrix}$, and $\mathfrak{Z}\mathfrak{Z}$ itself. Since left action by any subgroup of G preserves the neighbor relation, we can use Γ to map $\mathfrak{R}\mathfrak{Z}$, its neighbors, and its edges to all points on σ -level 0, their neighbors, and their edges. Furthermore we have $\begin{bmatrix} \xi & 1 \\ & 1 \end{bmatrix} \in \Gamma$, thus all edges between σ -levels 0 and 1 are indexed by conjugates of $\mathfrak{Z}\mathfrak{Z}$ by elements in Γ . Since

$\mathfrak{J}\mathfrak{J}$ is normalized by $\Gamma \cap \mathfrak{J}\mathfrak{J} = G_0$, where G_0 denotes the upper triangular matrices in $\text{GL}(2, \mathbb{F}_q)$, the following remark follows, which we state for future reference.

Remark 7. The edges in X_A between σ -levels 0 and 1 can be represented by the double cosets $\Gamma_A \backslash \Gamma / G_0$.

Thus we need to count the number of double cosets $\Gamma_A \backslash \Gamma / G_0$ in order to find the number of Γ_A -inequivalent edges between σ -levels 0 and 1. We are again going to use Burnside's Lemma. In fact, we have already done most of the necessary work in the computations leading up to theorem 5. The table of conjugacy classes for G_0 remains unchanged in the cases (T1) and (T2). Thus we only need to work out the conjugacy classes of the form $\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}$ for $\alpha, \beta \in \mathbb{F}_q^\times$. By combining the reasoning behind the cases (S3) and (T3) we obtain (T3') below.

	representative $g \in G_0$	number of conjugacy classes	number of elements in each class	number of fixed points
(T1)	$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$	$q - 1$	1	$[\Gamma : \Gamma_A]$
(T2)	$\begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}, \alpha \neq \delta$	$(q - 1)(q - 2)$	q	$2^{\omega(A)}$
(T3')	$\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}, \beta \neq 0$	$q - 1$	$q - 1$	$ \lfloor \sqrt{A} \rfloor $

Thus by applying Burnside's Lemma, we obtain

Theorem 7. *The number of edges in the quotient graph X_A between points on σ -level 0 and points on σ -level 1 is given by*

$$E_0(A) = \frac{[\Gamma : \Gamma_A]}{q(q-1)} + \frac{(q-2)2^{\omega(A)}}{q-1} + \frac{|\lfloor \sqrt{A} \rfloor|}{q}.$$

We now have enough data about the graph X_A to compute its Euler characteristic, or equivalently the number of fundamental loops.

Theorem 8. *The rank of $H_1(X_A, \mathbb{Z})$ is $1 + E_0(A) - C(A) - C_0(A)$.*

Proof. The rank of $H_1(X_A, \mathbb{Z})$ is $1 - \chi(X_A)$ where $\chi(X_A)$ is the Euler Characteristic of the graph, which is given by the number of vertices minus the number of edges in the graph of the fundamental domain. The maximum σ -level of points in the core of

the graph is smaller than or equal to $\deg A$. Including parts of the strings does not change the Euler characteristic, so we fix an $n \geq \deg A$. Then the number of edges is $C_{n-1}(A) + C_{n-2}(A) + \dots + C_1(A) + E_0(A)$ and the number of vertices is given by $C_n(A) + \dots + C_0(A)$, thus the difference is $C_n(A) + C_0(A) - E_0(A) = C(A) + C_0(A) - E_0(A)$ since $C_n(A) = C(A)$ for $n \geq \deg A$. \square

3.5 The Shape of the Fundamental Domain

We have seen in the preceding two sections that the number of points $C_n(A)$ on a given σ -level n and the number of edges E_n between two σ -levels n and $n+1$ remain constant when $n \geq \deg A$. It follows that the fundamental domain must have $C(A)$ strings of infinite length. Thus for each point on σ -level $n > \deg A$ the q neighbors on lower σ -level are in the same Γ_A orbit. Once the σ -level drops below $\deg A$, $C_n(A)$ and $E_n(A)$ increase and thus some of the neighbors have to start branching out. The branches coming out of the individual strings will not meet until σ -level 0. This follows from the fact that for any point on σ -level $n > 0$ there is a unique neighbor on higher σ -level. On σ -level 0 however, some of the branches will have to meet to form a connected graph, since X is connected. We will now compute the exact σ -level at which a given string ends and its branches start. We will refer to the union of all branches together with the end point of the corresponding string as the *core*. The core is obviously a finite graph.

To find the σ -level on which a string starts to branch out, we need to find the largest n for which the neighbors $[R, S + RT^n\xi]\sigma_{n-1}$ of $[R, S]\sigma_n$ are not all in the same Γ_A orbit. Equivalently, we have to find the smallest $n > 0$ for which $[R, S + RT^{n+1}\xi] \in \Gamma_A[R, S]G_n$ for all $\xi \in \mathbb{F}_q$. But this is so if and only if there is $\begin{bmatrix} 1/\alpha & -Q/(\alpha\beta) \\ & 1/\beta \end{bmatrix} \in G_n$ such that $[R, S + RT^{n+1}\xi] \begin{bmatrix} \alpha & Q \\ & \beta \end{bmatrix} [R, S]^{-1} \in \Gamma_A$. For this to be true, the lower left entry $R((\alpha - \beta)S - R(Q + \beta T^{n+1}\xi))$ needs to be congruent to 0 modulo A , which is possible only if R is a multiple of A , or $\alpha = \beta$ and $\deg[A/(A, R^2)] \leq n + 1$. Thus at $n = \deg A/(A, R^2) - 1$ the string related to $[R, S]$ ends, and the core starts.

We can use this insight to count the number of points in the core of X_A . We see after a moment's thought that this number is given by the number of points in the

fundamental domain on σ -level $\deg A$ or less, minus the number of points which are on strings that go lower than $\deg A$. Our computations above showed that a string related to $[R, *]$ will go as low as $\deg A/(A, R^2) - 1$. By theorem 2, we can assume without loss of generality that $R|A$, and we know that there will be $\phi((R, A/R))$ such strings by theorem 6. Thus the number of points in the core is given by

$$\begin{aligned}
& \sum_{i=0}^{\deg A} C_i(A) - \sum_{d|A} \left(\deg A - \deg \frac{A}{(A, d^2)} + 1 \right) \phi((d, A/d)) \\
&= \sum_{i=0}^{\deg A} C_i(A) - \sum_{d|A} \deg((A, d^2)) \phi((d, A/d)) - C(A) \\
&= \sum_{i=0}^{\deg A-1} C_i(A) - \sum_{d|A} \deg((A, d^2)) \phi((d, A/d)).
\end{aligned}$$

For future reference we record this as

Lemma 6. *The number of points in the core of X_A is given by*

$$\sum_{i=0}^{\deg A-1} C_i(A) - \sum_{d|A} \deg((A, d^2)) \phi((d, A/d)).$$

The fundamental domain also exhibits some mirror symmetries thanks to the involution operators W_q . Thus the group of symmetries for the fundamental domain will have order at least $2^{\omega(A)}$.

Example. Figure 3.1 shows the fundamental domain for $A = T^4 + T^2$, over the finite field with two elements. Vertices in the graph are denoted by bullets. The dashed lines with arrows are the strings leading to the cusps, everything else belongs to the core. $A = T^2(T+1)^2$ is the product of two primes, and we can clearly see three mirror symmetries, plus the identity, which yield a group of four elements.

3.6 The Fundamental Domain and Cusp forms

We can use our understanding of the fundamental domain to prove the following theorem about cusp forms.

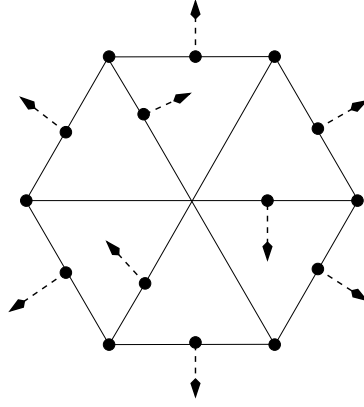


Figure 3.1: The graph X_A for $k = \mathbb{F}_2(T)$, $A = T^4 + T^2$

Theorem 9. *Let f be an automorphic function of level A and an eigenform of the Hecke operator H_∞ . Then f is a cusp form if and only if it vanishes on the strings.*

Proof. For $Y \in \mathbb{F}_q[T]$, $y \in r_\infty$, let $g = \begin{bmatrix} T^n & Y+y \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & Y \\ & 1 \end{bmatrix} \begin{bmatrix} T^n & y \\ & 1 \end{bmatrix}$. By remark 2 any $g \in G$ can be written in this form. We let $S' = YR+S$ so that $[R, S'] = [R, S] \begin{bmatrix} 1 & Y \\ & 1 \end{bmatrix} \in \Gamma$.

Now by lemma 5, f is a cusp form if and only if

$$\int_{r_\infty \setminus r_\infty^\times} f \left([R, S] \begin{bmatrix} T^n & hx + Y + y \\ & 1 \end{bmatrix} \right) dx = \int_{r_\infty \setminus r_\infty^\times} f \left([R, S'] \begin{bmatrix} T^n & hx + y \\ & 1 \end{bmatrix} \right) dx = 0,$$

where $h = \frac{A}{(A, R^2)}$. Since f is right- $\mathfrak{K}\mathfrak{Z}$ invariant we immediately obtain $f([R, S']\sigma_n) = 0$ for $n \geq \deg(h) - 1$. Thus f is a cusp form only if it vanishes on the strings by section 3.5.

For $n < \deg h - 1$ we have

$$\sum_{\substack{x=P/T^d, P \in \mathbb{F}_q[T] \\ d = \deg h - n - 1, \deg P < d}} f \left([R, S'] \begin{bmatrix} T^n & hx + y \\ & 1 \end{bmatrix} \right) = \sum_{\substack{x=P/T^d \\ \deg P < d}} f \left([R, S'] \begin{bmatrix} T^n & hx \\ & 1 \end{bmatrix} \right) = 0,$$

which, by making repeated use of the identity $\sigma_k \begin{bmatrix} T^{-1} & \xi \\ & 1 \end{bmatrix} = \begin{bmatrix} T^{k-1} & \xi T^k \\ & 1 \end{bmatrix}$, we can also write as

$$\sum_{\substack{(\xi_1, \dots, \xi_d) \in \mathbb{F}_q^d \\ d = \deg h - n - 1}} f \left([R, S'] \sigma_{\deg h - 1} \begin{bmatrix} T^{-1} & \xi_1 \\ & 1 \end{bmatrix} \cdots \begin{bmatrix} T^{-1} & \xi_d \\ & 1 \end{bmatrix} \right) = 0. \quad (3.2)$$

We now show by induction on n that vanishing on the strings implies equation 3.2 for all $d \geq 0$, via the relation $d = \deg h - n - 1$. If $d = 0$, then equation 3.2 is nothing

but the condition for vanishing on the strings. For $d = 1$ we are summing over all neighbors of $[R, S]\sigma_{h-1}$ which are on lower σ -level. But the neighbor on higher σ -level is on a string, thus f vanishes there. Since f vanishes at $[R, S]\sigma_{h-1}$, the sum over all neighbors has to vanish too, since f is an eigenform for H_∞ .

Now suppose equation 3.2 holds true for some $d > 1$, and let

$$\mathfrak{S}_d = \left\{ [R, S']\sigma_{\deg h-1} \left[\begin{smallmatrix} T^{-1} & \xi_1 \\ & 1 \end{smallmatrix} \right] \cdots \left[\begin{smallmatrix} T^{-1} & \xi_d \\ & 1 \end{smallmatrix} \right] \mid (\xi_1, \dots, \xi_d) \in \mathbb{F}_q^d \right\}.$$

For each $\mathfrak{S} \in \mathfrak{S}_d$ there are q neighbors on lower σ -level, given by $\mathfrak{S} \left[\begin{smallmatrix} T^{-1} & \eta_i \\ & 1 \end{smallmatrix} \right]$, $1 \leq i \leq q$, and one neighbor on higher σ -level $\mathfrak{S}\sigma_1$ such that

$$\lambda f(\mathfrak{S}) = f(\mathfrak{S}\sigma_1) + \sum_{i=1}^q f\left(\mathfrak{S} \left[\begin{smallmatrix} T^{-1} & \eta_i \\ & 1 \end{smallmatrix} \right]\right).$$

If we let \mathfrak{S} run through all terms in \mathfrak{S}_d then

$$\sum_{\mathfrak{S} \in \mathfrak{S}_d} \lambda f(\mathfrak{S}) = \sum_{\mathfrak{S} \in \mathfrak{S}_d} f(\mathfrak{S}\sigma_1) + \sum_{\mathfrak{S} \in \mathfrak{S}_d} \sum_{i=1}^q f\left(\mathfrak{S} \left[\begin{smallmatrix} T^{-1} & \eta_i \\ & 1 \end{smallmatrix} \right]\right). \quad (3.3)$$

But the left hand side and the first sum on the right hand side of equation 3.3 vanish by induction hypothesis for d and $d-1$, respectively, thus the double sum must vanish. But the double sum is precisely equation 3.2 for $d+1$. \square

Theorem 9 allows us to compute a basis of eigenforms for all Hecke operators of the space of cusp forms of given level $A \in \mathbb{F}_q[T]$ as follows. We start by computing a set of cusps, for instance as described at the beginning of section 3.3. We then use theorem 9 to obtain an initial set of points (the meeting points of strings and core) where we know the cusp forms will vanish. We can assume that the cusp forms are eigenforms for H_∞ and thus compute the neighbors of the initial set of points of lower σ -level, and immediately set up equations an eigenform for H_∞ needs to satisfy. We repeat this procedure with the new set of points, until we reach σ -level 0. The number of equations we obtain is equal to the number of points in the core as computed by lemma 6.

Solving these equations, we obtain a basis for the space of cusp forms consisting of eigenforms for H_∞ . To obtain a basis of simultaneous eigenforms for all Hecke operators, we need to decompose each eigenspace of H_∞ by acting with other Hecke operators.

Chapter 4

Modular Symbols

The representation of $G/\mathfrak{K}\mathfrak{J}$ as the vertices of a tree X with oriented edges indexed by the cosets $G/\mathfrak{J}\mathfrak{J}$ will be important in what follows. If we consider automorphic forms of a given level in the adelic setting, then the place ∞ can divide the level of the cusp form just as naturally as any other place. Automorphic forms of such a level $A\infty$, $A \in \mathbb{F}_q[T]$, are then functions on G left invariant under Γ_A , and right invariant under the Iwahori subgroup \mathfrak{J} of \mathfrak{K} . It follows immediately from theorem 1 that a fundamental domain is given by double coset representatives $\gamma\sigma_n\kappa$ where $\gamma \in \Gamma$ is a coset representative for $\Gamma_A \backslash \Gamma$ and $\kappa \in \mathfrak{K}$ a coset representative for $\mathfrak{K}/\mathfrak{J}$. In view of the tree X , and following Gekeler [6], we can consider functions on G right invariant under $\mathfrak{J}\mathfrak{J}$ as functions on the *oriented edges* of the tree X , rather than on the vertices, as we have done so far. We can identify $\Gamma_A \backslash G/\mathfrak{J}\mathfrak{J}$ with oriented edges of X_A .

4.1 Homology in Quotientgraphs

We define a *path* in the tree X to be a sequence of adjacent vertices. A *path* in the quotient graph X_A is then the image of the natural projection of a path in X to X_A . We will denote paths in X or X_A by square brackets. For any two points in X there is exactly one geodesic connecting them. Two paths in X will be called *homotopic* if their first vertex coincides and their last vertex coincides. Thus each homotopy class contains a unique geodesic path. Two geodesics $[a_1, a_2, \dots, a_n]$ and $[b_1, b_2, \dots, b_n]$ will be called Γ_A -*homotopic* if there is a $\gamma \in \Gamma_A$ such that $[\gamma a_1, \gamma a_2, \dots, \gamma a_n] = [b_1, b_2, \dots, b_n]$. Two paths in X will be called Γ_A -homotopic if they are homotopic to Γ_A -homotopic geodesics. Thus the fiber of the natural projection over a path in X_A consists of

Γ_A -homotopic paths in X which we will denote by $\{a, b\}$, where $[a, \dots, b]$ is any representative of the fiber. For $a, b \in X$ such that $a = \gamma b$ for some $\gamma \in \Gamma_A$ we call a path from a to b a *loop in X_A* . Two loops in X_A are *homologous* if they differ by paths which, when concatenated, are Γ_A -homotopic to a point. We let $\{a, b\}_{\Gamma_A}$ denote the class of homologous loops in X_A . The abelian group formed by the homology classes with respect to composition of paths is the first homology group and is denoted by $H_1(X_A, \mathbb{Z})$. We have the following properties which immediately follow from the definitions above. For $a, b, c \in X$, $\gamma \in \Gamma_A$,

$$\{a, a\} = 0 \tag{4.1}$$

$$\{a, b\} = -\{b, a\} \tag{4.2}$$

$$\{a, b\} + \{b, c\} + \{c, a\} = 0 \tag{4.3}$$

$$\{\gamma a, \gamma b\} = \{a, b\} \tag{4.4}$$

$$\{a, \gamma a\} = \{b, \gamma b\} \tag{4.5}$$

We have a surjective group homomorphism

$$\begin{aligned} \Gamma_A &\rightarrow H_1(X_A, \mathbb{Z}) \\ \gamma &\mapsto \{a, \gamma a\}, \end{aligned} \tag{4.6}$$

where $a \in X$ is any fixed point. Homomorphy follows from the following short computation: For $\gamma_1, \gamma_2 \in \Gamma_A$, $\gamma_1\gamma_2$ maps to $\{a, \gamma_1\gamma_2 a\} = \{a, \gamma_1 a\} + \{\gamma_1 a, \gamma_1\gamma_2 a\}$, by equation 4.3, and $\{\gamma_1 a, \gamma_1\gamma_2 a\} = \{a, \gamma_2 a\}$ by equation 4.5. Surjectivity follows from the fact that every class in $H_1(X_A, \mathbb{Z})$ can be written as a sum $\sum_i m_i \{a_i, \gamma_i a_i\}$, with $m_i \in \mathbb{Z}$, $\gamma_i \in \Gamma_A$, $a_i \in X$. By equation 4.2 we can assume without loss of generality that $m_i > 0$, and by equation 4.5 we can write the sum in the form $\sum_i m_i \{a, \gamma'_i a\}$, which can be reduced to $\{a, \gamma a\}$ for some $\gamma \in \Gamma_A$ by repeatedly applying the computation $\{a, \gamma_1 a\} + \{a, \gamma_2 a\} = \{a, \gamma_1 a\} + \{\gamma_1 a, \gamma_1\gamma_2 a\} = \{a, \gamma_1\gamma_2 a\}$.

4.2 Path Integrals

From now on, we will assume that f is a cusp form on G of level A_∞ and has an eigenvalue $\epsilon_\infty = -1$ for the Atkin-Lehner involution W_∞ (acting on the right, of course).

This assumption allows us to define path integrals for f on X_A , by summation of f over oriented edges and interpreting back-tracking on a path as summation over the opposite oriented edges.

For neighbors $a, b \in G/\mathfrak{K}\mathfrak{Z}$, we define $\int_{[a,b]} f(z)dz = f(e)$, where e is the oriented edge between a and b with terminus b , and extend this inductively to $\int_{\{a,b\}} f(z)dz$ for any points $a, b \in G/\mathfrak{K}\mathfrak{Z}$, including cusps, and call the integral the *path integral* of f over the path $\{a, b\}$. The path integral is well defined because f is finitely supported [6]. By our assumption on f , it follows immediately that $\int_{\{a,b\}} f(z)dz = -\int_{\{b,a\}} f(z)dz$. Furthermore, since f is left invariant under Γ_A , it follows that for all $\gamma \in \Gamma_A$

$$\int_{\{a,b\}} f(z)dz = \int_{\{\gamma a, \gamma b\}} f(z)dz.$$

The Hecke operators H_Π , $\Pi \neq \infty$ and relatively prime to A , and similarly the involutions W_p , $p|A$, act on $\{a, b\}$ via

$$H_\Pi : \{a, b\} \mapsto \left\{ \begin{bmatrix} \Pi & \\ & 1 \end{bmatrix} a, \begin{bmatrix} \Pi & \\ & 1 \end{bmatrix} b \right\} + \sum_{\substack{M \in \mathbb{F}_q[T] \\ |M| < |\Pi|}} \left\{ \begin{bmatrix} 1 & M \\ 0 & \Pi \end{bmatrix} a, \begin{bmatrix} 1 & M \\ 0 & \Pi \end{bmatrix} b \right\}.$$

This action commutes with the path integral, since the neighborhood relation is stable under left G -action. Thus we have

$$\int_{H_\Pi \{a,b\}} f(z)dz = \int_{\{a,b\}} H_\Pi f(z)dz.$$

In analogy with the classical case, we define for a path w between two cusps of X_A the *Modular Symbol*

$$\langle w, f \rangle = \int_w f(z)dz.$$

Remark 8. We will need to refer to the cusps of X_A frequently, so we introduce the following notation. Let $\begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \Gamma$, and $a_n = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \sigma_n$. It follows from equations 2.1 and 2.2 in section 2.3.3 that for $n > 0$ large enough $a_n \equiv \begin{bmatrix} T^{-2 \deg R - n} & P/R \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{Z}}$ and $a_{-n} \equiv \begin{bmatrix} T^{-2 \deg S - n} & Q/S \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{K}\mathfrak{Z}}$. We will denote by P/R the limit of a_n as $n \rightarrow \infty$ and by Q/S the limit of a_n as $n \rightarrow -\infty$. In particular, we will write $0 = \lim_{n \rightarrow \infty} \sigma_{-n}$ and $\infty = \lim_{n \rightarrow \infty} \sigma_n$.

Suppose additionally that f is an eigenform for H_Π , $(\Pi, A) = 1$, with eigenvalue λ_Π , and let $w = \{0, \infty\}$. Then $\langle w, H_\Pi f \rangle = \langle w, \lambda_\Pi f \rangle = \lambda_\Pi \langle w, f \rangle$, but also

$$\langle w, H_\Pi f \rangle = \langle H_\Pi w, f \rangle = \langle w, f \rangle + \sum_{\substack{M \in \mathbb{F}_q[T] \\ |M| < |\Pi|}} \left\langle \left\{ \frac{M}{\Pi}, \infty \right\}, f \right\rangle$$

and using the fact that $\{0, M/\Pi\} + \{M/\Pi, \infty\} = w$ we obtain

$$\lambda_\Pi \langle w, f \rangle = \langle w, f \rangle + |\Pi| \langle w, f \rangle - \sum_{\substack{M \in \mathbb{F}_q[T] \\ |M| < |\Pi|}} \left\langle \left\{ 0, \frac{M}{\Pi} \right\}, f \right\rangle$$

which we express as

$$(|\Pi| + 1 - \lambda_\Pi) \langle w, f \rangle = \sum_{\substack{M \in \mathbb{F}_q[T] \\ |M| < |\Pi|}} \left\langle \left\{ 0, \frac{M}{\Pi} \right\}, f \right\rangle$$

Each of the modular symbols in the right hand sum is actually an integral homology class, $\{0, M/\Pi\} \in H_1(X_A, \mathbb{Z})$, because Π is relatively prime to the level A . Write $(\Pi, AM) = s\Pi - tAM = 1$ for some $s, t \in \mathbb{F}_q[T]$. Then the matrix $\gamma = \begin{bmatrix} s & M \\ tA & \Pi \end{bmatrix} \in \Gamma_A$, and $\gamma 0 = \frac{M}{\Pi}$, hence $\{0, \gamma 0\} \in H_1(X_A, \mathbb{Z})$.

Notice that the L -function of f , $L(f, s)$, evaluated at $s = 0$ is precisely $\langle w, f \rangle$.

4.3 Manin Symbols

Following Manin, we will define distinguished classes and use the surjective homomorphism $\Gamma_A \rightarrow H_1(X_A, \mathbb{Z})$ shown in equation 4.6 with Manin's continued fractions method to prove that any class in $H_1(X_A, \mathbb{Z})$ can be written as a sum of distinguished classes.

Consider the set of right cosets of Γ_A in Γ , and let j be one such coset. Then $\xi(j) = \{g(0), g(\infty)\}$, for any representative $g \in j$, is called a *distinguished class*. In general $\xi(j) \notin H_1(X_A, \mathbb{Z})$.

Lemma 7. *Any class in $H_1(X_A, \mathbb{Z})$ can be written as a sum of distinguished classes.*

Proof. We are essentially following Manin's proof [9, Prop. 1.6.]. By the surjective homomorphism given in equation 4.6 we can write any class in $H_1(X_A, \mathbb{Z})$ as $\{0, \gamma 0\}$ where $\gamma \in \Gamma_A$. We have to show that $\{0, \gamma 0\}$ can be written as a sum of distinguished

classes. Write P/R for the cusp $\gamma 0$ and expand P/R into a continued fraction with convergents

$$\frac{P}{R} = \frac{P_n}{R_n}, \frac{P_{n-1}}{R_{n-2}}, \dots, \frac{P_0}{R_0} = \frac{P_0}{1}, \frac{P_{-1}}{R_{-1}} = \frac{1}{0}, \frac{P_{-2}}{R_{-2}} = \frac{0}{1}$$

where the last two fractions have been added formally.

The identity $P_k R_{k-1} - P_{k-1} R_k = (-1)^{k-1}$ holds true for the same reasons the analogous identity of integer continued fractions holds true, hence $g_k = \begin{bmatrix} P_k & (-1)^{k-1} P_{k-1} \\ R_k & (-1)^{k-1} R_{k-1} \end{bmatrix} \in \Gamma$.

By remark 8 we can write

$$\left\{ \frac{P_{k-1}}{R_{k-1}}, \frac{P_k}{R_k} \right\} = \{g_k(0), g_k(\infty)\}$$

and these are all distinguished classes. So by equation 4.3 we have

$$\left\{ 0, \frac{P}{R} \right\} = \sum_{k=-1}^n \left\{ \frac{P_{k-1}}{R_{k-1}}, \frac{P_k}{R_k} \right\}$$

which was to be shown. □

For $M = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \in \Gamma$ let (M) denote the class $\{M(0), M(\infty)\} = \{Q/S, P/R\}$. A representative for this class is the image under M of the path $[\dots, \sigma_{-1}, \sigma_0, \sigma_1, \dots]$. We call (M) a *Manin symbol*. Γ acts from the right on distinguished classes, since they are determined up to representatives of the right cosets $\Gamma_A \backslash \Gamma$, due to Γ_A -homotopy, hence it also acts from the right on Manin symbols.

Recall from theorem 2 that we can write all our right coset representatives in the form $[R, S]$ with monic R , and we can assume that all representatives have determinant 1. The matrices $S_{\alpha, \beta} = \begin{bmatrix} & \\ \beta & \alpha \end{bmatrix}$, $\alpha, \beta \in \mathbb{F}_q^\times$, acting from the right on distinguished classes, have the effect of reversing the path: $[R, S] S_{\alpha, \beta} = [\beta S, \alpha R]$ and the corresponding path $\{Q/S, P/R\}$ is being mapped to $\{P/R, Q/S\}$, so we have the relation

$$(M) + (MS_{\alpha, \beta}) = 0. \tag{4.7}$$

Since $[\beta S, \alpha R]$ is in the same coset as $[S, \alpha/\beta R]$, it is enough to consider $S_{\alpha, \beta}$ with $\beta = 1$.

Next, we want to consider $T_{a, b, c} = \begin{bmatrix} a & b \\ c & \end{bmatrix} \in \text{GL}(2, \mathbb{F}_q)$. It is easy to see that the matrix $T_{a, b, c}^3 \in \mathfrak{Z}$ if and only if $a^2 = -bc$. In this case we have $[R, S] T_{a, b, c} = [aR + cS, bR]$ and

$[R, S]T_{a,b,c}^2 = [acS, abR + bcS]$ so the path $\{Q/S, P/R\}$ is being mapped to $\left\{\frac{P}{R}, \frac{aP+cQ}{aR+cS}\right\}$ and then to $\left\{\frac{aP+cQ}{aR+cS}, \frac{Q}{S}\right\}$, so we have the relation

$$(M) + (MT_{a,b,c}) + (MT_{a,b,c}^2) = 0. \quad (4.8)$$

Since $[aR + cS, bR]$ is in the same coset as $[R + c/aS, b/aR]$ and $[acS, abR + bcS]$ is in the same coset as $[c/aS, b/aR + b/a c/aS]$, it is enough to consider $T_{a,b,c}$ with $a = 1$, and $bc = -1$. But since $[R, S]S_{\alpha,1}$ has to satisfy the same relation, we can fix $c = 1$, hence $b = -1$.

Theorem 10. *Let Z be the kernel of the homomorphism from the space of modular symbols with relations (4.7) and (4.8) to the formal group of cusps, $(M) \mapsto M\infty - M0$. Then $Z \cong H_1(X_A, \mathbb{Z})$.*

Proof. We will first describe the homology classes of X_A in terms of simplicial homology. It follows from the discussion in section 3.5 that if we delete points on σ -level 0 and their edges from X_A , then we are left with $C(A)$ disjoint tree's whose roots are the cusps of X_A . Thus any point P on σ -level greater than 0 uniquely represents the geodesic which connects P to the cusp of the tree P is a part of. The points on σ -level 0 and their edges establish the connections between the trees. In particular, any path between distinct cusps has to pass through one of the points on σ -level 0. Furthermore, each edge between the points P_0 and P_1 on σ -levels 0 and 1 respectively, uniquely represents the geodesic passing through it which connects P_0 with the cusp of the tree P_1 is part of. Thus every edge between σ -levels 0 and 1 has a natural unique cusp assigned to it. It follows that any geodesic connecting two cusps is uniquely described by two edges sharing the same endpoint on σ -level 0. In particular, the edges between σ -levels 0 and 1 contain all the data necessary to compute the homology classes of X_A .

We can now describe X_A as a simplicial complex K as follows. The 0-cells are the cusps of X_A . The 1-cells are indexed by ordered pairs (e_1, e_2) of distinct edges e_1, e_2 between σ -level 0 and 1 which share an endpoint on σ -level 0. They are oriented such that $(e_1, e_2) = -(e_2, e_1)$. The boundary of 1-cells are the unique 0-cells c_1, c_2 naturally assigned to the two edges e_1, e_2 , respectively via the description in the preceding paragraph. Thus the boundary homomorphism maps (e_1, e_2) to the formal difference $c_2 - c_1$.

Since X_A is a graph, we have no other cells. Thus $H_1(X_A, \mathbb{Z}) = Z_1/B_1 = Z_1$ where Z_1 is the kernel of the boundary homomorphism $\partial : C_1 \rightarrow C_0$, from 1-chains to 0-chains, and B_1 is the image of the boundary homomorphism from 2-chains to 1-chains, and hence is trivial since there are no 2-cells.

We will now show that the map $(M) \mapsto (M, MS_{1,1})$ from Manin Symbols (M) with the given relations to C_1 induces an isomorphism of the two spaces. We first notice that $(M, MS_{1,1})$ is well defined, since by remark 7 all edges between σ -level 0 and 1 can be represented by $M \in \Gamma$; M and $MS_{1,1}$ have the same endpoint on σ -level 0 since $M\sigma_0\mathfrak{K}\mathfrak{J} = MS_{1,1}\sigma_0\mathfrak{K}\mathfrak{J}$.

The map is surjective, because we can find for any point $g\sigma_0\mathfrak{K}\mathfrak{J}$, $g \in \Gamma$, on σ -level 0 and pair of distinct edges e_1, e_2 sharing the endpoint g , an $M \in \Gamma$ such that $M\mathfrak{J}\mathfrak{J}M^{-1} = e_1$ and $(MS_{1,1})\mathfrak{J}\mathfrak{J}(MS_{1,1})^{-1} = e_2$. Recall from the discussion preceding remark 7 that e_1, e_2 are given by the conjugates of $\mathfrak{J}\mathfrak{J}$ by g or $g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix}$, $\xi \in \mathbb{F}_q$. We have two cases.

1. The conjugators are g and $g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix}$, for a fixed $\xi \in \mathbb{F}_q$

We let $M = g \begin{bmatrix} 1 & \xi \\ 1 & 1 \end{bmatrix}$. Then $M\sigma_0 \in g\mathfrak{K}\mathfrak{J}$, and yields the same conjugate of $\mathfrak{J}\mathfrak{J}$ as g , since $\begin{bmatrix} 1 & \xi \\ 1 & 1 \end{bmatrix} \in \mathfrak{J} \subset \mathfrak{K}$. $MS_{1,1}$ is equal to the second conjugator, $g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix}$.

2. The conjugators are $g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix}$, $g \begin{bmatrix} \eta & 1 \\ 1 & 1 \end{bmatrix}$, for fixed but distinct $\xi, \eta \in \mathbb{F}_q$.

We let $M = g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \eta - \xi & 1 \end{bmatrix}$. The latter two matrices are in \mathfrak{K} thus M represents the same point as g . The last matrix is in \mathfrak{J} thus it represents the same edge as $g \begin{bmatrix} \xi & 1 \\ 1 & 1 \end{bmatrix}$, and $MS_{1,1} = g \begin{bmatrix} \eta & \xi \\ 1 & 1 \end{bmatrix} = g \begin{bmatrix} \eta & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \xi - \eta & 1 \end{bmatrix}$ represents the same edge as $g \begin{bmatrix} \eta & 1 \\ 1 & 1 \end{bmatrix}$ for the same reason.

Finally, we need to discuss the kernel of the map. Let $\Sigma = \sum_i m_i(M_i)$, $m_i \in \mathbb{Z}$, be in the kernel. By splitting the sum up into partial sums, if necessary, we can assume that all matrices appearing in Σ represent the same point on σ -level 0. If $M = MS_{\alpha,\beta}$ for some $\alpha, \beta \in \mathbb{F}_q^\times$, then clearly (M) is in the kernel, and we can assume Σ does not contain such elements. By construction of the map the element $(M) + (MS_{\alpha,\beta})$ is in the kernel, and we can use the identity $(M_i) = -(MS_{\alpha,\beta})$ to rewrite Σ such that all m_i are positive

integers. By the surjectivity of the map we can further simplify Σ by relations of the form $(J) + (K) = (M)$ whenever J, K are such that $(J) \mapsto (e_1, e_2)$, $(K) \mapsto (e_2, e_3)$, by choosing (M) to be the symbol mapping to (e_1, e_3) . This clearly reduces Σ successively to 0. But if $(J) + (K) = (M)$, write for convenience $L = MS_{1,1}$ so that $(J) + (K) + (L) = 0$, then $J = KGL(2, \mathbb{F}_q) = LGL(2, \mathbb{F}_q)$, because they represent the same point at σ -level 0, and $JS_{1,1} \in KG_0$, $KS_{1,1} \in LG_0$, $LS_{1,1} \in JG_0$ because their edges correspond in a cyclic manner. Solving these equations, we obtain solutions equivalent to $JT_{a,b,c} = K$, $JT_{a,b,c}^2 = L$, $T_{a,b,c}^3 \in \mathfrak{Z}$, and the relation $(J) + (JT_{a,b,c}) + (JT_{a,b,c}^2) = 0$ follows.

Now the kernel of the homomorphism from the space of modular symbols to the formal group of cusps, $(M) \mapsto M_\infty - M_0$ is obviously isomorphic to Z_1 which concludes the proof. \square

4.4 Modular Symbols and Spaces of Cusp Forms

The implementation of the Modular Symbols method is completely analogous to the classical case which has been described by Cremona [4]. The main steps are setting up the two and three point relations from the coset representatives of Γ_A in Γ , solving the linear system of equations, and keeping track with a look-up table.

As stated in section 4.2 our definition of path integral works only for cusp forms whose level is divisible by ∞ and no higher power of ∞ , and which are eigenfunctions of W_∞ with eigenvalue -1 . These cusp forms are related to elliptic curves with split multiplicative reduction at ∞ . It would be highly desirable to obtain a more general version of Modular Symbols without this limitation, but it is not clear at all how this could be done [18, 16, §3.8]. The challenge is to produce a path integral which on the one hand satisfies equations 4.1 through 4.6 (and in particular 4.2 and 4.3), and on the other hand commutes with the Hecke operators.

The only restriction that can presumably be lifted is that the prime we have singled out above is the prime ∞ . Let p be any prime in $\mathbb{F}_q[T]$, and let $A \in \mathbb{F}_q[T]$ be divisible by p , but not by p^2 . If we consider $G/\mathfrak{R}\mathfrak{Z}$ as a tree, but with neighborhood relations given by the Hecke operator H_p rather than H_∞ we can construct a quotient graph

$X_{A/p}$ where p plays much the same role as ∞ does in our work above.

Chapter 5

Computation of L -functions, special values and complexity

In this chapter we will compute the complexity for determining the coefficients of an L -function of a given elliptic curve directly, with modular symbols method, and with the algorithm outlines at the end of Chapter 3. The three methods cannot be compared directly, since they have different purposes. Both algorithms discussed in this thesis obtain much more information about the space of cusp forms of a given level than the L -function of an elliptic curve. The modular symbols method has a strong condition on the level, and hence can only reveals partial information about the space of cusp forms of level $A\infty$, $A \in \mathbb{F}_q[T]$. The method outlined in chapter 3 has the restriction that ∞ does not divide the level, but this restriction can be lifted with a loss in performance. We have learned that Tan and Rockmore outline an algorithm in [13] which works particularly well if the level is square free.

After discussing the complexities of the methods, we compute a small example, and list the decomposition of the spaces of cusp forms for levels $A \in \mathbb{F}_2[T]$ of small degree.

5.1 Complexity

Let E be an elliptic curve over a function field k over a finite field \mathbb{F}_q with conductor A . It is well known that there is a cusp form f of level A , an eigenform for all Hecke operators, whose L -function L_f is identical to the L -function L_E of E .

The L -function L_E by definition is an infinite product over all places Π of k , with factors $(1 - a_\Pi u + q^{\deg \Pi} u^2)^{-1}$, at places of good reduction, where $u = q^{-s \deg \Pi}$, $a_\Pi = q^{\deg \Pi} + 1 - N_E(\Pi)$, and $N_E(\Pi)$ is the number of points on E after reduction mod Π . a_Π is the eigenvalue of the Hecke operator H_Π applied to f . It is also known that L_E is a polynomial in u of degree $\deg A + 4g - 4$, where g is the genus of k . For details see

[12, 14, 18, 17].

5.1.1 Computation of the L -function and a_Π for a given Elliptic Curve

One way to compute the coefficients a_Π defined above is straight from the definition by counting the number of solutions of E over all the finite fields $\mathbb{F}_{q^{\deg v}}$ for all places of degree no larger than $\deg A + 4g - 4$. If $k = \mathbb{F}_q(T)$, $g = 0$, we have roughly q^n/n places of degree no larger than $n = \deg A - 4$ to consider. Most of these places will be of degree n , so most of the computations will be performed over the finite field \mathbb{F}_{q^n} , and the most naive way of counting solutions will be of the order of q^n polynomial multiplications with polynomials of degree n over $\mathbb{F}_q[T]$ representing elements in \mathbb{F}_{q^n} . Thus we need $O(q^{2n}/n)$ polynomial multiplications with polynomials of degree less than n over $\mathbb{F}_q[T]$. Polynomial multiplication costs no more than n^2 multiplications with elements in \mathbb{F}_q , thus we have $O(q^{2n}n)$ multiplications over \mathbb{F}_q .

5.1.2 The Modular Symbols method

Let $A \in \mathbb{F}_q[T]$, and A_∞ be the conductor of an elliptic curve E , such that E has split multiplicative reduction at ∞ . We can then use the Modular Symbol approach, for which we have to compute in a first stage the Manin Symbols (M) which requires a consideration of $[\Gamma : \Gamma_A]$ distinguished classes which by theorem 3 is of the order of $O(q^{\deg A})$ classes. Finding the generators thus amounts to a null space computation of the order of a $[\Gamma : \Gamma_A]/q$ squared, sparse matrix where we save a factor q by taking advantage of the $\text{GL}(2, \mathbb{F}_q)$ -invariance seen in equation 4.7. A lower bound for the number of generators is given by the rank of $H_1(X_A, \mathbb{Z})$ which has been computed in theorem 8, and from the proof of theorem 10 we see that an upper bound is given by the number of edges between σ -levels 0 and 1, which has been computed in theorem 7. In both cases the number of generators is roughly $[\Gamma : \Gamma_A]/q^2$. Given the $m = O([\Gamma : \Gamma_A]/q^2)$ generators, the action of a Hecke operator H_Π requires $q^{\deg \Pi} + 1$ matrices of dimension 2×2 over $\mathbb{F}_q[T]$. Direct computation of eigenvalues from this data would require applying all the matrices to each generator in a first step, and expressing the obtained data in terms of the generators in a second step. We can assume the second step has a negligible cost,

since the work mostly consists of table lookups. In the first step, each matrix multiplication consists of 8 polynomial multiplications with polynomials over $\mathbb{F}_q[T]$ of degree less than $\deg \Pi$ in the Hecke operator matrices, and less than $\deg A = n + 3$ in the generators, thus we have $8(n + 3)(\deg \Pi)$ multiplications with elements in \mathbb{F}_q for each matrix, and hence $O(q^{\deg \Pi} n \deg \Pi)$ for each operator and generator. Since the number of generators is roughly $[\Gamma : \Gamma_A]/q^2$, which is $O(q^{\deg A - 2})$, the computation of applying a Hecke operator to a modular symbol via Manin Symbols costs $O(q^{\deg(\Pi) + n + 2} n \deg \Pi)$. If we do this for all operators of degree no larger than n (of which there are roughly q^n/n) to obtain all eigenvalues needed for the L -function, we end up with $O(q^{3n+2}n)$ multiplications over \mathbb{F}_q , since again most of the operators will be for places of degree n . This is assuming a fixed (albeit high) cost for the pre-computation of the Manin Symbols.

5.1.3 Computing the space of cusp forms directly

Let $A \in \mathbb{F}_q[T]$, E an elliptic curve with conductor A . We can compute the cusp form f corresponding to E using the method outlined at the end of Chapter 3. If k denotes the number of points in the core of X_A as computed in lemma 6, then any cusp form is completely determined by its values at these points. We can estimate k to be $\deg A \frac{[\Gamma : \Gamma_A]}{q(q-1)(q+1)}$ which is roughly $O(nq^{n+1})$ points. To be able to choose the right cusp form, we need information about a few eigenvalues which we can obtain by counting points for low degree places. Applying the corresponding Hecke operator to the k points in the fundamental domain amounts to matrix multiplication and table lookup of equal cost as for Modular Symbols, thus the cost amounts to $O(q^{\deg \Pi} n \deg \Pi)$ multiplications over F_q for each matrix of the operator and point in the domain, and $O(q^{2 \deg \Pi + n + 1} n^2 \deg \Pi)$ for the entire fundamental domain, and all matrices of the operator. This is followed by a null-space computation performed on the $k \times k$ matrix containing the result of the Hecke operator applied to all points in the fundamental domain. For Hecke operators of low degree places this is a sparse matrix. The complexity of this step in general is $O(k^3)$ but since the operations are not on elements in \mathbb{F}_q , the effect of this computation on the overall estimate depends on the implementation. Note

that the size of this matrix is smaller than the size of the matrix needed to compute generators for the Manin Symbols, but in general this step has to be performed several times, once for each given eigenvalue.

Once an eigenform f has been obtained, the computation of a Hecke eigenvalue λ_Π can be reduced to the evaluation of $H_\Pi f$ at a single point which takes $O(q^{2 \deg \Pi} n \deg \Pi)$ multiplications over \mathbb{F}_q which is faster than the corresponding operation on Modular Symbols, as long as $\deg \Pi \leq n + 2$.

Once a cusp form corresponding to an elliptic curve E has been found, the L -function can be computed simply by evaluating the cusp form at the $\deg A - 4$ points $\sigma(-2), \dots, \sigma(-\deg A + 2)$.

5.1.4 Special Values, other operators

While the computation of the Hecke operators H_Π is quite expensive, computing the Fricke and other involutions is extremely fast, as it requires the action of a single matrix, as opposed to $q^{\deg \Pi} + 1$ matrices. The eigenvalue of the Fricke involution immediately reveals whether the central value of L_E vanishes or not. The computation of the action of one Hecke operator, relatively prime to the level A , with the Modular Symbol method also yields information about the central value, but only up to rational multiples.

5.2 Examples

Let us consider the curve $E : y^2 + xy = x^3 - T^2$ over the field $\mathbb{F}_5(T)$. This curve is one out of a class of curves for which Ulmer [17] has verified the Birch and Swinnerton-Dyer conjecture. The curve E has rank 1 curve, so the validity of the conjecture is known in this case even without Ulmer's proof. We will analyze this curve with the algorithms from Chapters 3 and 4.

The discriminant of E is $3T^2(T^2 + 2)$, it has split multiplicative reduction at T and $T^2 + 2$, and additive reduction at $1/T$. We make a change of variables sending T to $1 - 1/T$ to obtain the curve $E' : y^2 + Txy = x^3 - T^4(T - 1)^2$. It has conductor $A' = T^2(T^2 + T + 2)(T - 1)$. The index of $\Gamma_{A'}$ in Γ is $[\Gamma : \Gamma_{A'}] = 4680$, there are 12 cusps

and 108 points in the core of $X_{A'}$. Thus to compute the space of eigenfunctions for H_∞ using the algorithm from chapter 3 we need to solve a system of 108 linear equations. The dimension of the space of cusp forms of level A' is 74. We compute eigenfunctions for H_∞ with integer eigenvalues only, and find a 4-dimensional space for each of the eigenvalues $\pm 3, \pm 1$, and 0 and a 3-dimensional space for the eigenvalues ± 2 . We then use the Hecke operator H_{T+1} to decompose each of the spaces further and obtain 1 and 2-dimensional subspaces, and subspaces we can discard due to non-integer eigenvalues. We further split the 2-dimensional subspaces using the involutions W_T and W_{T+1} . We obtain the decomposition shown in the following table. λ_p denotes the eigenvalue for the Hecke operator H_p and ϵ_p the eigenvalue for the involution W_p , and ϵ for the Fricke involution W . The table lists at most 2 eigenforms on each row.

λ_∞	λ_{T+1}	ϵ_T	ϵ_{T-1}	ϵ
3	-2	1	± 1	± 1
3	0	-1	± 1	1
2	-2	± 1	1	∓ 1
2	0	1	-1	1
1	-4	-1	-1	-1
1	-2	-1	1	-1
0	-2	1	± 1	± 1
0	2	1	± 1	± 1
-1	2	-1	-1	1
-1	4	-1	1	1
-2	0	1	1	-1
-2	2	± 1	-1	± 1
-3	0	-1	± 1	-1
-3	2	1	± 1	± 1

Counting the number of points of the elliptic curve at the places $1/T$ and $T+1$ immediately reveals the cusp form related to E' as the one with $\lambda_\infty = 1$, $\lambda_{T+1} = -4$. Its Fricke involution has a negative eigenvalue, hence the L -function will vanish at the central value.

Since the curve E has split multiplicative reduction at T , we can also use the

Modular Symbol algorithm from chapter 4. Starting again from E we make the change of variables $T \rightarrow 1/T$ and obtain the curve $E'' : y^2 + Txy = x^3 - T^4$ with conductor $T^2(T^2 + 3)\infty$ and split multiplicative reduction at ∞ . In this case the index of $\Gamma_{A''}$ in Γ is $[\Gamma : \Gamma_{A''}] = 780$, and we will obtain a system of 396 equations using the Modular Symbols algorithm. Solving the system, we obtain 34 generators. The modular symbols method will be much faster since it only computes the space corresponding to the -1 -subspace of W_{T-1} in the table above.

We conclude this section by listing the decomposition of spaces of cusp forms over the field $\mathbb{F}_2(T)$ of level $A \in \mathbb{F}_2[T]$, $\deg A \leq 5$, which are simultaneous eigenfunctions with integer eigenvalues for all Hecke operators. Similar tables could be computed for other fields. The table has been created using the algorithm described in Chapter 3. It lists the following data. In the first column the factorization of the level is shown, in the second column the dimension of the space of cusp forms. The third column lists the eigenvalue of the Fricke involution, and the following columns list the eigenvalues for the Hecke operators H_Π if Π does not divide the level, or the Atkin-Lehner involution W_Π , if it does. The primes p_i appearing in the tables are primes of degree i . The three places of degree 1 are denoted by ∞ , p_1 , and p'_1 .

Level	Dim	W	∞	p_1	p'_1	p_2	p_3	p'_3
p_1^4	0							
$p_1^3 p'_1$	2	1	-1	-1	-1	1	1	-3
		1	1	1	1	1	-1	3
$p_1^2 p_1'^2$	1	1	0	-1	-1	2	0	0
$p_1^2 p_2$	2							
$p_1 p_1' p_2$	4	1	-2	-1	-1	1	-1	-1
		1	0	-1	1	-1	3	-3
		1	0	1	-1	-1	-3	3
		1	2	1	1	1	1	1
$p_1 p_3$	4							
p_2^2	0							
p_4	4	1	-2	1	1	3	1	1
		1	2	-1	-1	3	-1	-1

Level	Dim	W	∞	p_1	p'_1	p_2	p_3	p'_3
p_1^5	4	-1	-2	-1	0	0	0	-4
		-1	0	-1	-2	0	-4	0
		1	0	1	2	0	4	0
		1	2	1	0	0	0	4
$p_1^4 p'_1$	6	1	-1	-1	-1	1	1	-3
		-1	-1	-1	1	-1	-1	-3
		-1	-1	1	-1	1	1	-3
		1	1	-1	-1	-1	1	3
		-1	1	-1	1	1	-1	3
		1	1	1	1	1	-1	3
$p_1^3 p_1'^2$	8	-1	-2	1	-1	-2	-4	0
		1	-1	-1	-1	1	1	-3
		-1	-1	-1	1	1	1	-3
		1	0	-1	-1	2	0	0
		-1	0	1	-1	2	0	0
		-1	1	1	-1	1	-1	3
		1	1	1	1	1	-1	3
		1	2	-1	-1	-2	4	0
$p_1^3 p_2$	10	-1	-1	1	-1	-1	-3	-3
		1	1	-1	1	-1	3	3
$p_1^2 p_1' p_2$	14	1	-2	-1	-1	1	-1	-1
		-1	-2	1	-1	1	-1	-1
		-1	-1	-1	1	1	-5	1
		-1	0	-1	-1	-1	-3	3
		1	0	-1	1	-1	3	-3
		1	0	1	-1	-1	-3	3
		-1	0	1	1	-1	3	-3
		1	1	-1	-1	1	5	-1
		-1	2	-1	1	1	1	1
		1	2	1	1	1	1	1
$p_1^2 p_3$	12							

Level	Dim	W	∞	p_1	p'_1	p_2	p_3	p'_3
$p_1 p'_1 p_3$	20	-1	-2	-1	1	-3	1	-3
		1	0	-1	-1	-1	1	3
		-1	0	1	1	-1	-1	-3
		1	2	1	-1	-3	-1	3
$p_1 p_2^2$	4							
$p_1 p_4$	16	-1	-2	-1	-1	-1	-5	-1
		-1	-2	-1	1	3	1	1
		1	-2	1	1	3	1	1
		-1	2	-1	-1	3	-1	-1
		1	2	1	-1	3	-1	-1
		1	2	1	1	-1	5	1
$p_1 p'_4$	16	-1	-1	-1	-1	3	-1	-1
		1	-1	1	-1	3	-1	-1
		-1	1	-1	1	3	1	1
		1	1	1	1	3	1	1
$p_2 p_3$	12							
p_5	12							

References

- [1] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.
- [2] B. Birch and H. Swinnerton-Dyer. Notes on elliptic curves II. *J. Reine Angew. Math.*, 218:79–108, 1965.
- [3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.
- [4] J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. Also available online at <http://www.maths.nott.ac.uk/personal/jec/book/fulltext/index.html>.
- [5] P. Deligne. Les constantes des équations fonctionnelles des fonctions L . In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973. See also corrections in book IV, Lecture Notes in Math., Vol. 476, p. 149.
- [6] E.-U. Gekeler. Automorphe Formen über $\mathbf{F}_q(T)$ mit kleinem Führer. *Abh. Math. Sem. Univ. Hamburg*, 55:111–146, 1985.
- [7] G. Harder, W. Li, and J. Weisinger. Dimensions of spaces of cusp forms over function fields. *J. Reine Angew. Math.*, 319:73–103, 1980.
- [8] A. Knapp. *Elliptic Curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.
- [9] Ju. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.
- [10] B. Mazur and J. Tate. Refined conjectures of the “Birch and Swinnerton-Dyer type”. *Duke Math. J.*, 54(2):711–750, 1987.
- [11] I. Piatetski-Shapiro. *Complex representations of $GL(2, K)$ for finite fields K* , volume 16 of *Contemporary Mathematics*. American Mathematical Society, Providence, R.I., 1983.
- [12] J. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 1994.
- [13] K.-S. Tan and D. Rockmore. Computation of L -series for elliptic curves over function fields. *J. Reine Angew. Math.*, 424:107–135, 1992.

- [14] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analogue. In *Séminaire Bourbaki*, volume 9 of *Exposés*, pages 415–440. Soc. Math. France, Paris, 1995.
- [15] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
- [16] J. Teitelbaum. Modular symbols for $\mathbf{F}_q(T)$. *Duke Math. J.*, 68(2):271–295, 1992.
- [17] D. Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002.
- [18] D. Ulmer. Elliptic curves and analogies between number fields and function fields. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 285–315. Cambridge Univ. Press, Cambridge, 2004.
- [19] A. Weil. Sur les fonctions algébriques à corps de constantes fini. *C. R. Acad. Sciences Paris*, 210:592–594, 1940.
- [20] A. Weil. On the Riemann hypothesis in function fields. *Proc. Nat. Acad. Sci. U. S. A.*, 27:345–347, 1941.
- [21] A. Weil. *Foundations of Algebraic Geometry*. American Mathematical Society Colloquium Publications, vol. 29. American Mathematical Society, New York, 1946.
- [22] A. 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 & Cie., Paris, 1948.
- [23] A. Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.
- [24] A. Weil. On the analogue of the modular group in characteristic p . In *Functional Analysis and Related Fields (Proc. Conf. for M. Stone, Univ. Chicago, Chicago, Ill., 1968)*, pages 211–223. Springer, New York, 1970.
- [25] A. Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.
- [26] A. Wiles. Modular elliptic curves and Fermat’s last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Vita

Saša Radomirović

- 1987-1993** Attended Kantonschule Freudenberg in Zürich
- 1993** Matura typus B
- 1993-1998** Attended ETH Zürich
- 1998** Dipl. Math., *ETH Zürich*
- 1999-2005** Attended Rutgers University
- 2005** Ph.D. in Mathematics, *Rutgers University*