INAUGURAL DISSERTATION

zur

Erlangung der Doktorwürde

der

Naturwissenschaftlich-Mathematischen Gesamtfakultät

der

Ruprecht-Karls-Universität
Heidelberg

vorgelegt

von

M.Sc. Yamidt Bermúdez Tobón
aus Montebello (Ant.), Kolumbien

Tag der mündlichen Prüfung:

Thema

An efficient algorithm to compute an elliptic curve from a corresponding function field automorphic form

Gutachter:

Prof. Dr. Gebhard Böckle

Acknowledgements

I thank my supervisor Prof. Dr. Gebhard Böckle for his guidance and support. Also I would like to thank to Dr. Juan Cerviño, he provided sound support and was always willing to help whenever I asked, during the whole core of this work. We had a lot of interesting and enthusiastic discussions which often contained useful ideas. Without their help this thesis would not have been possible.

During this work I was supported by the DAAD for three and one half years and the DFG project Nr D.110200/10.005 from 01.01.2013 to 30.04.2014.

Abstract

Elliptic modular forms of weight 2 and elliptic modular curves are strongly related. In the rank-2 Drinfeld module situation, we have still modular curves that can be described analytically through Drinfeld modular forms. In [GR96] Gekeler and Reversat prove how the results of [Dri74] can be used to construct the analytic uniformization of the elliptic curve attached to a given automorphic form. In [Lon02] Longhi, building on ideas of Darmon, defines a multiplicative integral that theoretically allows to find the corresponding Tate parameter. In this thesis we develop and present a polynomial time algorithm to compute the integral proposed by Longhi. Also we devised a method to find a rational equation of the corresponding representative for the isogeny class.

Zusammenfassung

Elliptische Modulformen von Gewicht 2 und elliptische Modulkurven stehen in enger Verbindung. Im Fall eines Drinfeld-Moduls von Rang 2 haben wir noch Modulkurven, die durch Drifeldsche Modulformen analytisch beschrieben werden können. Gekeler und Reversat [GR96] beweisen, wie die Ergebnisse von [Dri74] genutzt werden können, um die analytische Uniformisierung der, einer gegeben automorphen Form eingeordneten elliptischen Kurve, zu konstruieren. Auf Darmons Ideen aufbauen definiert Lonhi [Lon02] ein multiplikatives Integral, das es erlaubt, den entsprechenden Tate-Parameter zu finden. In der vorliegenden Arbeit wird ein Polynomialzeitalgorithmus entwickelt und vorgestellt, um das von Longhi vogeschlagene Integral zu berechnen. Ausserdem wird eine Methode entwickelt, mit der eine rationale Gleichumg der entsprechenden Vertreter der Isogenieklasse gefunden werden kann.

Contents

1. Introduction

The theory of modular forms and their relation to the arithmetic of elliptic curves is a central subject in modern mathematics, where most diverse branches of mathematics come together: complex analysis, algebraic geometry, representation theory, algebra and number theory. One of the most exciting and widely mathematical discoveries is the proof, by Andrew Wiles, of "Fermat last's theorem", its solution draws an incredible range of modern mathematics, which is precisely the relation between modular forms and elliptic curves.

There are a number of analogies between on the one hand, the integers $\mathbb{Z}$ and the rational numbers $\mathbb{Q}$ and on the other hand, $\mathbb{F}_q[T]$ and its field of fractions $\mathbb{F}_q(T)$. Frequently a problem posed in number fields or, in other words, in finite extensions of $\mathbb{Q}$, admits an analogous problem in function fields, and the other way around. For example, since the appearance of Drinfeld's work [Dri74], we know that all elliptic curves which are semistable at the place ∞ are modular, that is, they appear as a factor of the Jacobian of a Drinfeld modular curve. We are interested in number theory over function fields, particularly in elliptic curves over $\mathbb{F}_q(T)$.

In order to get a better idea of the function field case, it is worth to start with a short description of the classical case, that is, over the rational numbers $\mathbb{Q}$. Let $f : \mathcal{H} \longrightarrow \mathbb{C}$ be a cuspidal modular form of weight two for the Hecke congruence subgroup $\Gamma_0(N)$ which is also a new eigenform with rational Hecke eigenvalues, we call it for short "a $\mathbb{Q}$-rational newform" of level N. From the Eichler-Shimura theory, with f one can associate an elliptic curve E with conductor N and a morphism defined over $\mathbb{Q}$ form the modular curve $X_0(N)$ to the elliptic curve E. Such an elliptic curve E is called a *Weil curve.*

On the other hand, since the 60's (after the work of Shimura, Taniyama, and Weil) emerged the conjecture that all elliptic curves over $\mathbb{Q}$ (up to isogeny) should be obtainable from the Eichler-Shimura construction. The conjecture known as the *Shimura-Taniyama-Weil conjecture*, is now a theorem called the *modularity theorem* [BCDT]. Basically it states that there are canonical bijections between the sets of

1) Normalized $\mathbb{Q}$-rational newforms f of level N with rational Hecke eigenvalues;

2) One dimensional isogeny factors of the new part of the Jacobian of the modular curve $X_0(N)$;

3) Isogeny classes of elliptic curves E over $\mathbb{Q}$ with conductor N.

The previous correspondence yields an effective method to determine all elliptic curves $E/\mathbb{Q}$ with a given conductor N, since the modular parametrization is explicitly and effectively computable (c.f. [Cre97]). For tables and numerical results see ([*Ibid.,* Ch. 4]).

For some applications it is convenient to consider other kind of parametrizations instead of the modular one, for example the *Shimura parametrization*, introdued in [BC91] and [BD98]. Let E be an elliptic curve of conductor N and suppose that N is square free and factorizes as $N = N^-N^+$ where N^- has a even number of factors. Then there exits a parametrization of E by the Shimura curve $X_{N^-N^+}$ (cf. §3.4), that is a non constant morphism from the Jacobian of the Shimura curve to E. However the lack of q-expansions for modular forms on non-split quaternion algebras, forces one to consider p-adic uniformizations of E by certain discrete arithmetic subgroups of $SL_2(\mathbb{Q}_p)$ at the primes p dividing N^-.

The modular forms considered here may be regarded as functions on oriented edges of certain Bruhat-Tits tree $\mathcal{T}$ (cf. §3.4), called harmonic cocycles, which can be identified with measures on $\mathbb{P}^1(\mathbb{Q}_p)$. Using these measures Bertolini and Darmon are able to define a multiplicative p-adic integral defined over $\mathbb{P}^1(\mathbb{Q}_p)$, which theoretically gives rise to the modular parametrization of the Tate curve attached to a given harmonic cocycle.

In [Gre06], Greenberg gives an algorithm, running in polynomial time, for evaluating this p-adic integral up to a given precision. The key of his algorithm is a method devised by Pollack and Stevens [PS11] for explicitly lifting standard modular symbols to overconvergent ones. Although Greenberg is able to compute with good accuracy the Tate parameter, he does not give an explicit method to find an equation defided over $\mathbb{Q}$ for the elliptic curve as Cremona does. However in a recent preprint [GMS] Guitart et al, get p-adic approximations to the algebraic invariants of the elliptic curve, allowing for the recovery of the Weierstrass equation.

In the function field case, we want to describe a similar relationship between elliptic curves and automorphic forms. Although this result was proved for more general global fields (cf. [GR96]), we consider here the case where $\mathbb{Q}$ is replaced by the rational function field $K = \mathbb{F}_q(T)$.

The automorphic forms considered, may be regarded also as functions on the oriented edges of the Bruhat-Tits tree for $GL_2(K_\infty)$, where K_∞ is the completion of K at the place $\infty = 1/T$. In analogy with the classical case, in [GR96] Gekeler and Reversat prove that every elliptic curve E over $\mathbb{F}_q(T)$ with conductor $\mathfrak{n}\infty$, where $\mathfrak{n}$ is an ideal of $\mathbb{F}_q[T]$, is isogenous to a factor of the Jacobian of the Drinfeld modular curve $M_0(\mathfrak{n})$ or equivalently E is a Weil curve. One can also establish a canonical bijection between the sets of:

1) $\mathbb{Q}$ rational new eigencocycles of level $\mathfrak{n}$ with rational eigenvalues;

2) Isogeny factors of dimension one of the Jacobian of the Drinfeld modular curve $M_0(\mathfrak{n})$;

3) K-isogeny classes of elliptic curves E/K with conductor $\mathfrak{n}\infty$.

This modular parametrization is explicitly constructed using a Theta function, however, this construction requires to calculate certain infinite product (cf. (2.6)), which makes it computationally hard to find the Tate parameter. On the other hand, Longhi [Lon02] working on function field analogues of Bertolini-Darmon [BD98], defines a multiplicative integral over $\mathbb{P}^1(K_\infty)$ and constructs a theta function in a different way as the one of Gekeler and Reversat. This approach does not give either an explicit method to calculate such integral.

In this thesis we develop an effective method to compute the multiplier of Gekeler's theta function using the integral proposed by Longhi. We are able to calculate the Tate parameter $\mathbf{q}$ up to an accuracy of π^M in running time $O(M^7)$ operations; this is the main result of this thesis (c.f. Thm. B.2.1). In contrast to Greenberg‘s work, we go even further and find the corresponding elliptic curve defined over $\mathbb{F}_q(T)$ in the isogeny class of the Tate curve corresponding to $\mathbf{q}$. The importance of the these results, is that we now have a method to construct, at least for small primes and polynomials N of small degree, tables as Cremona does in the classical case.

We start with a harmonic cocycle φ as above, that is, a new eigencocycle of level $\mathfrak{n}$ with rational Hecke eigenvalues. From §3.1.1 we know that there is a measure μ_φ on $\mathbb{P}^1(K_\infty)$ associated to φ. We use it, following Longhi, to define a multiplicative integral (3.9) which is very similar to the one used by Greenberg in the p-adic uniformization.

Motivated by the work of Greenberg, Darmon and pollack, we develop an algorithm to calculate our integral up to a given fixed precision of M digits. A crucial tool in Greenberg's calculation is the logarithm, which allows him to pass from a multiplicative integral to an additive one. In the function field case we had to replace the use of logarithm by a different method which lead us to calculate several integrals of functions in the ring $1 + \pi\mathbb{F}_q[\![\pi, t]\!]$ defined on O_∞ (cf. (4.3)), instead of $\mathbb{P}(K_\infty)$ (cf. (4.1)). This idea and the concepts involved were sketched to me by Prof. Böckle.

In order to calculate the integral we define a Hecke operator over certain set $\mathcal{S}$ (cf. (4.7)) of functions which are $\mathcal{I}_\infty$-equivariant. We show that the integral over any edge of the tree $\mathcal{T}$ can be regarded as an element of $\mathcal{S}$ and they are eigen-functions with eigenvalue 1. The last property allows us to calculate the integral over all edges in $\mathcal{T}$ and functions on $1 + \pi\mathbb{F}_q[\![\pi, t]\!]$ modulo π^M.

The calculation of the Hecke operator U_∞ requires to work with the edges of the quotient graph $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$, where N is a polynomial in $\mathbb{F}_q[T]$ that generates the ideal $\mathfrak{n}$, which is a covering of double the quotient $GL_2(A) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$. Since most of the algorithms available in the literature are made to work with the vertices of the quotient graph, we need to describe sets of representatives for the edges of the quotient graphs above and implement algorithms that allow us to work with such as sets (c.f Appendix A). The algorithms and the proofs that appear in the Appendices A and B, were made with the help of Dr. Cerviño.

Once we have the Tate parameter $\mathbf{q}$ we proceed to find a representative of the elliptic curve in the isogeny class defined over $\mathbb{F}_q(T)$. Unfortunately the coefficients $a_4(\mathbf{q})$ and $a_6(\mathbf{q})$ of the Tate curve (5.12) are not rational (cf. Example 5.7.4). So we need to find an appropriate change of variables to transform the Tate curve into a rational model.

In the case of characteristic 2 and 3 a simple change of variables to transform the Tate curve was enough to find the rational model. In characteristic greater than 3 we need to consider the Eisenstein form $y^2 = 4x^3 - g_2x - g_3$ of the curve. Following a suggestion of Prof. Böckle, we prove that there are powers of g_2 and g_3 that are rational functions (cf. Proposition 5.7.9). Hence after an appropriate change of variables we get a model defined over the field $\mathbb{F}_p(T)$. A direct consequence of this is that the Eisenstein series are algebraic over $\mathbb{F}_q(T)$.

This thesis is organized as follows:

In chapter 2 we give all the preliminaries from the article of Gekeler-Reversat [GR96], which include a short introduction to graphs in §2.2. We give the basic definitions of the Drinfeld upper half plane, Bruhat-Tits trees, ends, the reduction map, the quotient graph and harmonic cocycles in sections §§2.3-2.9. In Section 2.5, where the ends of the tree $\mathcal{T}$ are defined, we explain how they are identified with $\mathbb{P}^1(K_\infty)$ (cf. Lemma 2.5.4) and how each edge induces a partition of $\mathbb{P}^1(K_\infty)$ into two disjoint open sets. Besides the definion of the harmonic cocycles in §2.9 we show how they can be constructed using the homology of the quotient graph (cf. Lemma 2.9.4).

The construction of Gekeler and Reversat of theta series is given in §2.10. Theorem 2.10.2 gives their main properties. There it is stated that the multiplier of the theta series induces a symmetric bilinear pairing, this is used latter to find the integral with the minimal valuation, which is precisely the Tate parameter. Theorem 2.10.4, mostly due to Van der Put, gives the relation between theta functions and the harmonic cocycles. This relation allows us latter to construct the theta series by means of a multiplicative integral. We finish this chapter with the definition of the Hecke operator in §2.11 and the applications to the Shimura-Taniyama-Weil uniformisation §2.12, which is the main result of [GR96].

In Chapter 3 the definition of Longhi's multiplicative integral (cf. Def. 3.1) over any compact X is given. In §3.1.1 we state the relation between harmonic cocycles and measures, which is a direct consequence of Lemma 2.5.4. In §3.1.2 we give the definition of the multiplicative integral when X is $\mathbb{P}^1(K_\infty)$ and the measure is the one induced from the harmonic cocycle. The theta function as a multiplicative integral is the content of Theorem 3.2.1, which allows us to show that the multiplier of the theta function can be given as a multiplicative integral (cf. (3.9)). This is the integral that we are interested in, since it allows us to determine the Tate parameter. This chapter also includes two sections with the classical complex uniformisation in §3.3 and the p-adic uniformisation in §3.4 with a short explanation of Greenberg's algorithm.

In Chapter 4 we explain our algorithm to calculate the integral. This is the main theoretical contribution of this thesis. In §4.2 we define $\mathcal{F}_I$, the set of fundamental functions. We show in Lemma 4.2.1 that $\mathcal{F}_I$ is a group and we define the action of the Iwahori subgroup on it (cf. (4.6)). We introduce in §4.3 the Hecke operator U_∞ and the set $\mathcal{S}$ (4.7) on which the operator U_∞ acts. The main results of this section are Lemma 4.3.7 and Proposition 4.3.8 in which we prove that the integrals regarded as elements of $\mathcal{S}$ are $\mathcal{I}_\infty$-equivariant and eigenfunctions of the operator U_∞, respectively. At end of section §4.3 we explain how to calculate the Table by applying the Hecke operator U_∞. This section finishes with the example 4.3.13 of how to apply the operator U_∞.

As we already explained we need to transform our integral (3.9) into one of the form (4.1) defined over O_∞. In §4.4 we explain how to carry out this change of variables and we perform carefully all the computations over all possible open sets arising from the partition of the border $\mathbb{P}^1(K_\infty)$.

Chapter 5 deals with the applications of our algorithm to calculate the integral (3.9). We start this chapter with some definitions and results on elliptic curves, modular forms and the Tate curve (cf. §§5.1-5.5). We explain in §5.6 how to calculate the Tate parameter. This includes a calculation of the valuation of $\mathbf{q}$ and Theorem 5.6.1 which states that we can compute the Tate parameter $\mathbf{q}$ up to accuracy π^M in time $O(M^9)$.

In §5.7.1 we explain how to find the rational model for the Tate curve in characteristic 2 and 3 and write the corresponding algorithm and give some examples. Section §5.7.2 deals with characteristic $p > 3$. We show first the rationality or certain powers of the Eisenstein series g_2 and g_3 (cf. Proposition 5.7.9) over the field $\mathbb{F}_q(\mathbf{q})$. We also give the algorithm to find curves in characteristic $p > 3$ and we give examples for $p = 5, 7, 11$ and 13.

In the appendices A and B we explain the implementations for algorithms to deal with the quotient graph and the table respectively, as well as the running time for the main algorithms and the proof of Theorem 5.6.1. Appendix C includes tables for some primes and small degree of $\mathfrak{n}$.

Implementations of the algorithms described in this thesis, were done on the algebra system Magma [BCP97] and are available upon request.

2. Background

2.1 Notation

We recall some facts on the Drinfeld upper half plane, the Bruhat-Tits tree, harmonic cocycles and theta functions[1]. We fix throughout this work the following notation, assuming the reader to be familiar with [GR96].

$\mathbb{F}_q$	$=$	the finite field of characteristic p with q elements
A	$=$	$\mathbb{F}_q[T]$
K	$=$	$\mathbb{F}_q(T)$
∞	$=$	the fixed place of K of degree one corresponding to $v_{1/T}$
val	$=$	the valuation $v_{1/T}$
K_∞	$=$	$\mathbb{F}_q((\pi)), \quad \pi = T^{-1}$
O_∞	$=$	$\mathbb{F}_q[[\pi]], \quad$ the ∞-adic integers
C_∞	$=$	the completion of an algebraic closure of K_∞
$\lvert \cdot \rvert$	$=$	the multiplicative norm on C_∞ that extents $q^{\mathrm{val}(\cdot)} : K \to \mathbb{R}_{\geqslant 0}$.

2.2 Notions from graph theory

Definition 2.2.1. Let $\mathbf{S}$ be a non empty countable set.

(a) A *(directed multi-)graph* $\mathcal{G}$ is a pair $(\mathrm{X}(\mathcal{G}), \mathrm{Y}(\mathcal{G}))$ where $\mathrm{X}(\mathcal{G})$ is a (possibly infinite) non-empty set and $\mathrm{Y}(\mathcal{G})$ is a subset of $\mathrm{X}(\mathcal{G}) \times \mathrm{X}(\mathcal{G}) \times \mathbf{S}$ such that

1. if $e = (v, v', s)$ lies in $\mathrm{Y}(\mathcal{G})$, then so does its opposite $\bar{e} = (v', v, s)$,

[1] The theta functions considered here are the rigid analytic functions defined in [GR96, §5]

2. for any $(v, v') \in \mathrm{X}(\mathcal{G}) \times \mathrm{X}(\mathcal{G})$, the set $\{s \in \mathbf{S} \mid (v, v', s) \in \mathrm{Y}(\mathcal{G})\}$ is a finite set whose cardinality is denoted by $n_{v,v'}$,
3. for any $v \in \mathrm{X}(\mathcal{G})$, the set $\mathrm{Nbs}(v) := \{v' \in \mathrm{X}(\mathcal{G}) \mid (v, v', s) \in \mathrm{Y}(\mathcal{G})$ for some $s \in \mathbf{S}\}$ is finite.

(b) A subgraph $\mathcal{G}' \subset \mathcal{G}$ is a graph $\mathcal{G}'$ such that $\mathrm{X}(\mathcal{G}') \subset \mathrm{X}(\mathcal{G})$ and $\mathrm{Y}(\mathcal{G}') \subset \mathrm{Y}(\mathcal{G})$.

(c) Suppose $\mathrm{X}(\mathcal{G}) = \{v_1, v_2, ..., v_m\}$ is finite. Then $(n_{v_i,v_j})_{1 \leqslant i,j \leqslant m}$ is called *the adjacency matrix* of $\mathcal{G}$.

Notation 2.2.2. An element $v \in \mathrm{X}(\mathcal{G})$ is called a *vertex* and an element $e \in \mathrm{Y}(\mathcal{G})$ is called an *oriented edge*. If the cardinality of $\mathbf{S}$ is one, we simply write (v, v') instead of (v, v', s).

Definition 2.2.3. (a) For each edge $e = (v, v', s) \in \mathrm{Y}(\mathcal{G})$ we call $o(e) := v$ the *origin* of e and $t(e) := v'$ the *target* of e.

(b) Two vertices v, v' are called *adjacent*, if $\{v, v'\} = \{o(e), t(e)\}$ for some edge e.

Definition 2.2.4. An edge e with $o(e) = t(e)$ is called a *loop*. A vertex v with $\# \mathrm{Nbs}(v) = 1$ is called *terminal*.

Definition 2.2.5. Assume $\mathcal{G}$ to be a graph.

(a) Let $v, v' \in \mathrm{X}(\mathcal{G})$. A *path* ω from v to v' is a finite subset $\{e_1, \ldots, e_k\}$ of $\mathrm{Y}(\mathcal{G})$ such that $t(e_i) = o(e_{i+1})$ for all $i = 1, \ldots, k-1$ and $o(e_1) = v, t(e_k) = v'$.

(b) The *length* of a path ω is the number of edges contained in it.

(c) The *distance* from v to v', denoted $d(v, v')$, is the minimal length among all paths from v to v' (or ∞ if no such path exists).

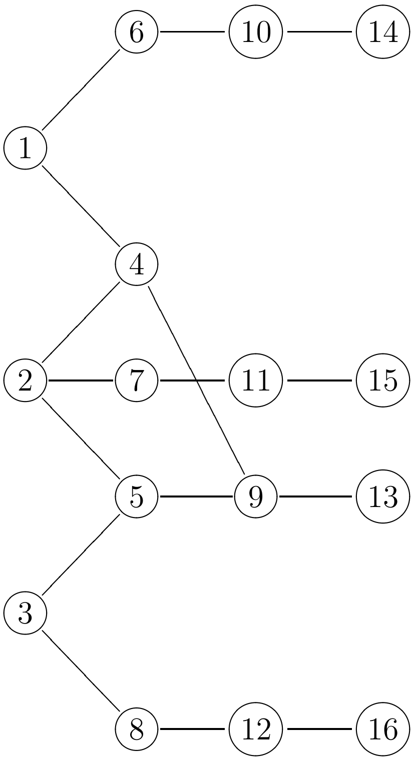
(d) A path $\{e_1, \ldots, e_k\}$ from v to v' without backtracking, i.e., such that for no i we have $e_i = \bar{e}_{i-1}$, is called a *geodesic*.

Note that the length of a geodesic need not be $d(v, v')$ but that $d(v, v')$ is attained for a geodesic.

Example 2.2.6. Consider the set $\mathbf{S} = \{*\}$ and the set of vertices

$$X(\mathcal{G}) = \{1, 2, ..., 16\}.$$

If the graph $\mathcal{G}$ is represented by



,

then the set of edges is

$$\{(1,6),(1,4),(2,4),(2,7),(2,5),(3,5),(3,8),(6,10),(4,9),\\ (7,11),(5,9),(8,12),(10,14),(11,15),(9,13),(12,16)\};$$

here due to Definition 2.2.1 only one of (v,v') (or (v',v)) is written since either both are elements of $Y(\mathcal{G})$ or none.

A graph $\mathcal{G}$ is *connected* if for any two vertices $v,v' \in \mathrm{X}(\mathcal{G})$ there is a path from v to v'. A *cycle* of $\mathcal{G}$ is a geodesic from some vertex v to itself. Therefore a loop is a cycle of length one. A graph $\mathcal{G}$ is *cycle-free* if it contains no cycles.

Definition 2.2.7. A graph $\mathcal{G}$ is called a *tree* if it is connected and cycle-free.

If $\mathcal{G}$ is a tree, then any two vertices of $\mathcal{G}$ are connected by a unique geodesic. Any subgraph $\mathcal{T} \subseteq \mathcal{G}$ which is a tree is called *subtree*. A *maximal subtree* in a graph $\mathcal{G}$ is a subtree which is maximal under inclusion among all subtrees of $\mathcal{G}$.

Definition 2.2.8. The *degree* of $v \in \mathrm{X}(\mathcal{G})$ is

$$\deg(v) := \#\{e \in Y(\mathcal{G}) \,|\, o(e) = v\}.$$

Thus v is terminal precisely if $\deg(v) = 1$. A graph $\mathcal{G}$ is called *k-regular* if for all vertices $v \in \mathrm{X}(\mathcal{G})$ we have $\deg(v) = k$.

A graph $\mathcal{G}$ is *finite* if $\# \mathrm{X}(\mathcal{G}) < \infty$. Then also $\# \mathrm{Y}(\mathcal{G}) < \infty$, since $\deg(v)$ is finite for all $v \in \mathrm{X}(\mathcal{G})$. The *diameter* of a (finite) graph $\mathcal{G}$ is

$$\operatorname{diam}(\mathcal{G}) := \max_{v,v' \in \mathrm{X}(\mathcal{G})} d(v, v').$$

2.3 The Drinfeld upper half plane

The Drinfeld upper half plane is the set

$$\Omega := \mathbb{P}^1(C_\infty) \setminus \mathbb{P}^1(K_\infty)$$

on which $GL_2(K_\infty)$ acts through fractional linear transformations by

$$\gamma\langle z \rangle := \frac{az + b}{cz + d},$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K_\infty)$ and $z \in \Omega$. This action is well defined since $GL_2(K_\infty)$ preserves K_∞. We define the *boundary* of Ω, denoted by $\partial\Omega$, to be $\mathbb{P}^1(K_\infty)$.

In order to define the algebra of rigid analytic functions on Ω, we consider the following sets that form an admissible cover of Ω (cf. [FvdP81, Ch. II] for details). Define the imaginary absolute value on Ω as the distance from K_∞:

$$|z|_i := \inf \{|z - x| \mid x \in K_\infty\}.$$

Definition 2.3.1. Let $z \in \Omega$ and $n \in \mathbb{N}$, a *basic affinoid* is a set of the form

$$\mathcal{A}_n := \left\{ z \in \Omega | \; q^{-n} \leqslant |z|_i, |z| \leqslant q^n \right\}.$$

A function $f : \mathcal{A}_n \to C_\infty$ is *holomorphic* if it is the uniform limit of rational functions without poles in $\mathcal{A}_n$. The collection of such functions is denoted by $\mathcal{O}_\Omega(\mathcal{A}_n)$. With the norm

$$\|f\|_{\mathcal{A}_n} := \sup \{|f(z)| \mid z \in \mathcal{A}_n\},$$

the space $\mathcal{O}_\Omega(\mathcal{A}_n)$ is a Banach algebra and $\mathcal{O}_\Omega(\Omega) := \varprojlim \mathcal{O}_\Omega(\mathcal{A}_n)$ is a Fréchet space [FvdP81, Ch. III].

2.4 The Bruhat-Tits tree

In this section we recall the definition of a graph $\mathcal{T}$ called the Bruhat-Tits tree of $PGL_2(K_\infty)$, which is a basic combinatorial object for the arithmetic of K_∞. For more details see [Ser03, Ch. II].

A lattice in K_∞^2 is a free O_∞-submodule of rank 2. We say that two lattices L_1 and L_2 are *homothetic* if L_1 is a $K_\infty^\times$-multiple of L_2. Homothety is an equivalence relation. The set of vertices $X(\mathcal{T})$ of $\mathcal{T}$ consists of the homothety classes of O_∞-lattices. Two vertices are joined by an edge if and only if they can be represented by lattices L_1, L_2 such that there are strict inclusions $\pi L_2 \subsetneq L_1 \subsetneq L_2$. The set of oriented edges of $\mathcal{T}$ is denoted by $Y(\mathcal{T})$.

Thus the vertices and edges of $\mathcal{T}$ may be described as follows:

$$X(\mathcal{T}) \;= \{\text{ Vertices of } \mathcal{T} \text{ }\} = \left\{ \begin{array}{l} \text{Classes } [L_1] \text{ of } O_\infty\text{-lattices } L_1 \\ \text{in } K_\infty^2 \end{array} \right\},$$

$$Y(\mathcal{T}) \;= \{\text{ Oriented edges of } \mathcal{T} \text{ }\} = \left\{ \begin{array}{l} \text{Ordered pairs } ([L_1],[L_2]) \text{ with representatives} \\ L_1,\, L_2 \text{ such that } L_1 \subset L_2 \text{ and} \\ \text{with } \pi L_2 \subsetneq L_1 \subsetneq L_2 \end{array} \right\}.$$

It is well known that the graph $\mathcal{T}$ is a connected regular tree of degree $q+1$, where q is the cardinality of the residue field of K_∞ [Ser03, Ch. II. Thm. 1].

The group $GL_2(K_\infty)$ acts naturally on lattice classes by left multiplication $(g,[L]) \mapsto [gL]$. This induces a transitive action on the vertices of $\mathcal{T}$ which preserves the incidence relations $\pi L_2 \subsetneq L_1 \subsetneq L_2$. In this way one obtain an action of $GL_2(K_\infty)$ on $\mathcal{T}$.

For $i \in \mathbb{Z}$ let v_i be the vertex $[\pi^i O_\infty \oplus O_\infty]$ of $\mathcal{T}$. Since the vertex $v_0 = [O_\infty \oplus O_\infty]$ has stabilizer $K_\infty^\times GL_2(O_\infty)$ in $GL_2(K_\infty)$, we have the following

Proposition 2.4.1. *There is a canonical bijection*

$$\begin{aligned} GL_2(K_\infty)/K_\infty^\times GL_2(O_\infty) &\longrightarrow X(\mathcal{T}) \\ \gamma \cdot K_\infty^\times GL_2(O_\infty) &\longmapsto \gamma[O_\infty \oplus O_\infty], \end{aligned}$$

equivariant for the left action of $GL_2(K_\infty)$.

Definition 2.4.2. We define the *Iwahori subgroup* of $GL_2(K_\infty)$ as

$$\mathfrak{I} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(O_\infty) \quad \text{such that} \quad c \equiv 0 (\mathrm{mod}\ \pi) \right\}. \tag{2.1}$$

Similarly, we label the edges e_i $(i \in \mathbb{Z})$ such that $t(e_i) = o(e_{i+1}) = v_i$. Each edge is taken by $GL_2(K_\infty)$ to $e_0 = (v_{-1}, v_0)$, so it follows that $Y(\mathfrak{I}) \cong GL_2(K_\infty)/\mathrm{Stab}_{GL_2(K_\infty)}(e_0)$. A simple computation shows $\mathrm{Stab}_{GL_2(K_\infty)}(e_0) = K_\infty^\times \mathfrak{I}$.

Proposition 2.4.3. *There is a canonical bijection*

$$\begin{aligned} GL_2(K_\infty)/K_\infty^\times \mathfrak{I} &\longrightarrow Y(\mathfrak{I}) \\ \gamma \cdot K_\infty^\times \mathfrak{I} &\longmapsto (\gamma[\pi^{-1} O_\infty \oplus O_\infty], \gamma[O_\infty \oplus O_\infty]), \end{aligned}$$

equivariant for the left action of $GL_2(K_\infty)$.

From now on given a $\gamma \in GL_2(K_\infty)$ we denote its class in $GL_2(K_\infty)/K_\infty^\times GL_2(O_\infty)$ as $[\gamma]_0$ and its class in $GL_2(K_\infty)/K_\infty^\times \mathfrak{I}$ as $[\gamma]_1$. We may implicitly use by abuse of notation the bijections above and understand $[\gamma]_0$ and $[\gamma]_1$ as vertex and edge respectively. The vertex $v_0 = [O_\infty \oplus O_\infty]$ is called the *standard vertex*, analogously the edge $e_0 = ([\pi^{-1} O_\infty \oplus O_\infty], [O_\infty \oplus O_\infty])$ is called the *standard edge*.

The next two lemmas will help us to identify the vertices of the tree with explicitly given matrices. Furthermore, they will show which matrices correspond to adjacent vertices in the tree.

Lemma 2.4.4. *Every class of* $GL_2(K_\infty)/K_\infty^\times GL_2(O_\infty)$ *has a unique representative of the form*

$$\begin{pmatrix} \pi^n & u \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}$ *and* $u \in K_\infty/\pi^n O_\infty$.

One can find a constructive proof in [But12, Lemma 2.7]. We call this representative the *vertex normal form*. In what follows we will denote the vertex represented by the matrix in normal form $\left(\begin{smallmatrix} \pi^k & u \\ 0 & 1 \end{smallmatrix}\right)$ as $[k, u]$.

Lemma 2.4.5. *Consider the two matrices in vertex normal form*

$$A := \begin{pmatrix} \pi^n & u \\ 0 & 1 \end{pmatrix}, \quad B := \begin{pmatrix} \pi^{n+1} & u + a\pi^n \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}$, $a \in \mathbb{F}_q$, $u \in K_\infty/\pi^n O_\infty$ and let L_1 and L_2 be the two lattices

$$L_1 := AO_\infty^2, \; L_2 := BO_\infty^2.$$

Then $L_1 \supset L_2$ and $L_1/L_2 \cong \mathbb{F}_q$.

Recall that $\mathcal{T}$ is a regular tree of degree $q+1$. The previous lemma only displays q vertices adjacent to $[L_1]$. The remaining one is the class of $\left(\begin{smallmatrix} \pi^{n-1} & u \bmod \pi^{n-1}O_\infty \\ 0 & 1 \end{smallmatrix}\right) O_\infty^2$.

The subgroup $\mathcal{J}$ is not normal in $GL_2(K_\infty)$. Denoting by $\mathcal{N}$ the normalizer of $\mathcal{J}$ in $GL_2(K_\infty)$, we have that $\mathcal{N}/\mathcal{J}K_\infty \cong \mathbb{Z}/2$. As one can easily see, $\delta := \left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right)$ is a representative of the non-trivial quotient class of $\mathcal{N}/\mathcal{J}$. Let $\gamma \in GL_2(K_\infty)$ such that $[\gamma]_1 = e$, then multiplication from the right with δ corresponds to the map

$$\begin{aligned} Y(\mathcal{T}) &\longrightarrow Y(\mathcal{T}) \\ e &\longmapsto \bar{e} \end{aligned}$$

that is $[\gamma\delta]_1 = \bar{e}$.

There are two canonical projection maps from $X(\mathcal{T}) \times X(\mathcal{T}) \times \mathbf{S}$ to $X(\mathcal{T})$, which induce two maps from $Y(\mathcal{T})$ to $X(\mathcal{T})$. We choose the first projection map that associates to each e its origin $o(e)$, *i.e.*,

$$\mathrm{pr}_1 : Y(\mathcal{T}) \longrightarrow X(\mathcal{T}) \tag{2.2}$$

$$e = (v, v') \longmapsto o(e) = v\ . \tag{2.3}$$

This map is also compatible with multiplication by δ that is, $\mathrm{pr}_1(\delta e) = o(\delta e) = t(e)$.

2.5 Ends of the tree

Before relating the Bruhat-Tits tree to the Drinfeld upper half plane, we need to define the ends of the tree.

Let $\{e_1, e_2\}$ the standard basis of K_∞^2 as a column vector.

Definition 2.5.1. Let $([L_0],[L_1],...)$ and $([L'_0],[L'_1],...)$ be two non-backtracking infinite sequences of adjacent vertices. We say that they are equivalent if $[L_n]=[L'_{n+m}]$ for some $m\in\mathbb{Z}$ and all n large enough. An *end* of $\mathfrak{T}$ is an equivalence class of such sequences. The collection of ends of $\mathfrak{T}$ is denoted by $\mathrm{Ends}(\mathfrak{T})$.

From the *elementary divisor theorem* we obtain the following. (cf. [Bos09, Ch. 6] for details).

Proposition 2.5.2. *Let L and L' be two lattices in K_∞^2. Then there exists a O_∞-basis $\{e_1,e_2\}$ of L and integers a,b such that $\{\pi^a e_1,\pi^b e_2\}$ is a O_∞-basis of L'. The numbers a and b are independent of the choice of the basis of L and L'.*

Remark 2.5.3. *i) If $L'\subset L$ then the numbers a and b from the previous proposition are positive. Furthermore, we can find in the class $[L']$ a lattice L'', namely $L''=L'\pi^{-\min\{a,b\}}$ such that if $\{f_1,f_2\}$ is a basis of L then L'' is generated by one of the f_i and the other one multiplied by a positive power of π.*

ii) Given an end s there is a unique representative sequence starting with the lattice $L_0=O_\infty e_1\oplus O_\infty e_2$, were e_i is the standard basis of K_∞^2.

Lemma 2.5.4. *There is a canonical $GL_2(K_\infty)$-equivariant bijection*

$$\phi: \mathit{Ends}(\mathfrak{T})\to\mathbb{P}^1(K_\infty).$$

Proof. Given $s\in\mathrm{Ends}(\mathfrak{T})$ represented by the sequence $([L_0],[L_1],...)$ we can construct a representing sequence of lattices

$$L_0\supset L_1\supset L_2\supset ...$$

such that $L_n/L_{n+1}\cong O_\infty/\pi O_\infty$ for all n and πL_0 does not contain any of the L_n's, since there is no backtracking. Therefore $\cap_n L_n$ is a O_∞-submodule of K_∞^2 spanning a K_∞-line. For any n, by the Remark 2.5.3, there exists a basis $\{x_n,y_n\}$ of L_0 such that $\{x_n,\pi^n y_n\}$ is a basis of L_n, analogously for L_{n+1}. Since $L_{n+1}\subset L_n$ we can write x_{n+1} in terms of the basis of L_n, that is $x_{n+1}=x_n a_n+\pi^n b_n y_n$ for some $a_n,b_n\in O_\infty$ and $a_n\notin\pi O_\infty$. Then $x_{n+1}-x_n a_n=\pi^n b_n y_n$ and since $a_n\notin\pi O_\infty$ we may replace x_{n+1} by $a_n x_{n+1}$ to get $x_{n+1}\equiv x_n \pmod{\pi^n}$. Continuing in this way, we can construct a Cauchy sequence $(x_n)_{n\geqslant 1}$ which converges to a nonzero element $x=\left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right)$ of $\cap_n L_n\subset K_\infty^2$.

The bijection

$$\begin{aligned} \phi : \mathrm{Ends}(\mathcal{T}) \to \quad & \mathbb{P}(K_\infty^2) \quad \cong \mathbb{P}^1(K_\infty) \\ & \langle e_1x_1 + e_2x_2 \rangle \mapsto (x_1 : x_2) \end{aligned}$$

is established by associating to the end $s = ([L_n])$ the line in K_∞^2 generated by $\cap_n L_n$, that is $\phi(s) = O_\infty(e_1x_1 + e_2x_2)$, where $\{e_1, e_2\}$ is the standard basis of K_∞^2 as column vectors.

The map ϕ is surjective. Let l be a line in K_∞^2 generated by $x = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right)$, that is $l = O_\infty(x_1e_1 + x_2e_2)$. Define the sequence of lattices $L_n = O_\infty x \oplus \pi^n y O_\infty$ with y a vector in K_∞^2 linearly independent of x. Let s be $([L_n])_{n\geqslant 1}$, clearly $L_{n+1} \subset L_n$ and $\phi(s) = l$.

The map ϕ is injective. Let s and s' be two ends and let $\{L_n\}$ and $\{L'_n\}$ be two sequences of lattices representing s and s', respectively, whose intersection generate the same line. Then up to multiplication by an scalar $\cap L_n = \cap L'_n = O_\infty x$ for some $x \in K_\infty^2$. Eliminating, if necessary, the first terms of the sequences, one can assume that $L_0 = O_\infty x \oplus O_\infty y$ and $L'_0 = O_\infty x \oplus O_\infty y'$. Since $x \in L_n$ for all n and $[L_0 : L_n] = q^n$ we have that L_n is generated by $\{x, \pi^n y\}$ and similarly L'_n is generated by $\{x, \pi^n y'\}$. Since $\pi^k y' = ax + by$ for $a, b \in O_\infty$ for k large enough one finds that L'_{k+m} is generated by x and $\pi^m bw$ and therefore coincides with L_{j+m} for some j, that is the ends $([L_n])$ and $([L'_n])$ are equal, hence ϕ is injective.

Finally, the map ϕ is equivariant. If $\cap_n L_n$ is generated by the vector $\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right)$, for a $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K_\infty)$ the generator of $\cap \gamma L_n$ is $\gamma \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax_1+bx_2 \\ cx_1+dx_2 \end{smallmatrix}\right)$.

On the other hand $GL_2(K_\infty)$ acts on $\mathbb{P}^1(K_\infty)$ by Möbius transformations, that is
$\gamma(x_1 : x_2) = (ax_1 + bx_2 : cx_1 + dx_2)$ and the equivariance follows.

□

Remark 2.5.5. *In [GR96] the elements of K_∞^2 are taken as row vectors and the action of $GL_2(K_\infty)$ on the lattices is given by right multiplication $L\gamma^{-1}$. So if $\cap L_n$ is generated by the row vector (x_1, x_2) and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K_\infty)$ then $\cap \gamma L_n$ is generated by $(x_1d - x_2c, -x_1b + x_2a)$. Which does not correspond to $\gamma(x_1 : x_2) = (ax_1+bx_2 : cx_1+dx_2)$. In order to make the map ϕ compatible with the action of $GL_2(K_\infty)$, it needs to be composed with the canonical map $(x_1 : x_2) \mapsto (-x_2 : x_1)$, that is the Möbius transformation $z \mapsto -z^{-1}$ on $\mathbb{P}^1(K_\infty)$ (cf. [GR96, §1.3.2]).*

From the bijection in Lemma 2.5.4, we have in particular that

- the image of the semi-line whose vertices are represented by $\{[k, 0]\}_{k<0}$ is

$\infty = (1:0) \in \mathbb{P}^1(K_\infty)$. To see this note that the line represented by $\{[k,0]\}_{k<0}$ is in the class of the sequence of lattices L_k whose basis are the columns of the matrix $\left(\begin{smallmatrix} 0 & 1 \\ \pi^k & 0 \end{smallmatrix}\right)$.

- the semi-line whose vertices are represented by $\{[k,0]\}_{k\geqslant 0}$ goes to $0 = (0:1) \in \mathbb{P}^1(K_\infty)$.

We will denote by $\mathcal{A}(0,\infty)$ the "line" whose vertices are represented by $\{[k,0]\}_{k\in\mathbb{Z}}$.

From the normalization the edge e_0 may be identified with the compact open set $U_{e_0} = O_\infty \subset \mathbb{P}^1(K_\infty)$ by considering the ends passing through e_0. These are represented by sequences of lattices whose basis are the columns of the matrix $\left(\begin{smallmatrix} \pi^n & u \\ 0 & 1 \end{smallmatrix}\right)$ with $n \geqslant 1$ and $u \in K_\infty/\pi^n O_\infty$ with positive valuation. This extends by equivariance to an assignment of a compact open subset of $\mathbb{P}^1(K_\infty)$ to each oriented edge of the tree by

$$U_{\gamma e_0} := \gamma\langle O_\infty\rangle \subset \mathbb{P}^1(K_\infty) \quad \forall \gamma \in GL_2(K_\infty). \tag{2.4}$$

Since the action of $GL_2(K_\infty)$ on the disks of $\mathbb{P}^1(K_\infty)$ is transitive, every disk of $\mathbb{P}^1(K_\infty)$ is the image of an edge on $Y(\mathcal{T})$. We observe some essential properties of the assignment:

i) Given any oriented edge e, then for the opposite edge $\bar{e}$, the associated open set satisfies $U_{\bar{e}} = \mathbb{P}^1(K_\infty) - U_e$.

ii) For any vertex v the set $\{U_e\}$, where e runs over all edges e with initial vertex v, form a disjoint covering of $\mathbb{P}^1(K_\infty)$.

iii) The sets $\{U_e\}$ form a basis of compact open subsets of $\mathbb{P}^1(K_\infty)$.

Given two vertices v and v' on the tree, there is a unique oriented path ω from v to v' joining them. The open set associated to these two vertices is the union of all ends containing ω. Given an edge e and a vertex v, we say that e points away from v if the unique path with origin v and containing $o(e)$ and $t(e)$ contains e (and not $\bar{e}$).

Remark 2.5.6. *The end ∞ defines an "orientation" of the tree $\mathcal{T}$, that is a decomposition of $Y(\mathcal{T}) = Y^+(\mathcal{T}) \,\dot{\cup}\, Y^-(\mathcal{T})$, where an edge $e = (v_1, v_2)$ belongs to $Y^+(\mathcal{T})$ if it points to ∞ and it is called* positive *and* negative *($e \in Y^-(\mathcal{T})$) otherwise. From this we get a section*

$$\begin{tikzcd} X(\mathcal{T}) \arrow[r, "\cong"] & Y^+(\mathcal{T}) \arrow[r, hook] & Y(\mathcal{T}) \\ v \arrow[r, mapsto] & e & \end{tikzcd}$$

such that $o(e) = v$ and e is positive.

Note that multiplication by δ allows us to change from $Y^+(\mathcal{T})$ to $Y^-(\mathcal{T})$ and the other way around. In terms of matrices, we have that the map $e \mapsto \bar{e}$ is given by $[g]_1 \mapsto [g\delta]_1$ for a $g \in GL_2(K_\infty)$. Then each edge e of $Y(\mathcal{T})$ is uniquely represented by either $\left(\begin{smallmatrix} \pi^k & u \\ 0 & 1 \end{smallmatrix}\right)$ (if e is positive) or $\left(\begin{smallmatrix} \pi^k & u \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right)$ (if e is negative).

2.6 The reduction map

As constructed so far, the Bruhat-Tits tree $\mathcal{T}$ is a combinatorial object. Next we will associate to it a geometrical object. For this, we identify each edge with a copy of the real unit interval endowed with the usual topology. Then we glue edges according to the relations on $\mathcal{T}$ using the quotient topology and we denote by $\mathcal{T}(\mathbb{R})$ this new tree and it is called the *geometrical realization* of $\mathcal{T}$. Let e be an edge of $\mathcal{T}(\mathbb{R})$ joining the vertices $[L_0]$ and $[L_1]$, any point on e is determined by its *barycentric coordinates*, *i.e.*, for $t \in [0,1]$ we write $x = (1-t)[L_0] + t[L_1]$ to indicate that x is the point "at distance t from the vertex $[L_0]$ in the direction of $[L_1]$". Denote by $\mathcal{T}(\mathbb{Q})$ the $\mathbb{Q}$-points of the geometrical realization of $\mathcal{T}$ defined as $t \in [0,1] \cap \mathbb{Q}$ and also $\mathcal{T}(\mathbb{Z})$ to be the vertices of $\mathcal{T}$.

The geometric realization of the tree $\mathcal{T}$ parametrizes norms on the two dimensional vector space K_∞^2, as is stated by Goldman and Iwahori [GI63], which allows us to define the reduction map.

Definition 2.6.1. A real *non-archimedean norm* on K_∞^2 is a map $\nu : K_\infty^2 \to \mathbb{R}$ which satisfies

1. $\nu(x) \geqslant 0$ and $\nu(x) = 0 \Leftrightarrow x = 0$,
2. $\nu(ax) = |a|\nu(x)$ for $a \in K_\infty$,
3. $\nu(x+y) \leqslant max\{\nu(x), \nu(y)\}$.

Given a lattice L on K_∞^2, one can associate the norm

$$\nu_L(x) := \inf\left\{|a| \;\middle|\; a \in K_\infty^\times, x \in aL\right\}.$$

We say that two norms ν and ν' are similar if there is a constant $t \in \mathbb{R}$ such that $\nu = t\nu'$. Moreover, the group $GL_2(K_\infty)$ acts on the space of norms by $(\gamma\nu)(x) := \nu(\gamma x)$ for all $\gamma \in GL_2(K_\infty)$ (cf. [GR96, §1.4.2]).

Theorem 2.6.2 (Goldman-Iwahori). *There is a canonical bijection compatible with the right action of $GL_2(K_\infty)$*

$$\left\{\textit{Similarity classes of real non-archimedean norms } \nu \textit{ on } K_\infty^2\right\} \longleftrightarrow \mathcal{T}(\mathbb{R}).$$

In particular,

$$\{\textit{Classes of norms whose unit ball is an } O_\infty\textit{-lattice}\} \longleftrightarrow \mathcal{T}(\mathbb{Z}).$$

For $z \in \Omega$ we define the norm ν_z on K_∞^2 as follows:

$$\begin{aligned} \nu_z : K_\infty^2 &\longrightarrow \mathbb{R}_{\geq 0} \\ (u,v) &\longmapsto \nu_z((u,v)) := |uz+v| \end{aligned}$$

and *the reduction map* is defined by

$$\begin{aligned} \lambda : \Omega &\longrightarrow \mathcal{T}(\mathbb{R}) \\ z &\longmapsto [\nu_z]. \end{aligned}$$

Since $|C_\infty^\times| = q^{\mathbb{Q}}$, it is not difficult to prove the following (cf. [Gek99]):

Proposition 2.6.3. *One has a surjection $\lambda : \Omega \twoheadrightarrow \mathcal{T}(\mathbb{Q})$.*

The previous proposition yields the following well known properties of the reduction map:

- $\lambda^{-1}(\textit{vertex}) = \mathbb{P}^1(C_\infty^\times) - (q+1)$ disjoint balls, in particular,
- $\lambda^{-1}(v_0) = \{z \in C_\infty^\times \mid |z| \leq 1, \quad |z-c| \geq 1 \quad \forall c \in \mathbb{F}_q\}$.

We will refer to last set as the *standard affinoid.*

Remark 2.6.4. *From the $GL_2(K_\infty)$-equivariance of the reduction map we can in principle find the fiber of any vertex and any edge on the tree from $\lambda^{-1}(v_0)$ and $\lambda^{-1}(e_0)$.*

2.7 Drinfeld modular curves

An *arithmetic subgroup* Γ of $GL_2(K_\infty)$ is a subgroup commensurable with $\Gamma(1) := GL_2(A)$ (cf. [Gek97, §3.1]), *i.e.*, such that $\Gamma \cap \Gamma(1)$ has finite index in both Γ and $\Gamma(1)$. The main examples are the principal congruence subgroups defined as follows.

Definition 2.7.1. Let N be any monic polynomial in $A = \mathbb{F}_q[T]$ and consider the set

$$\Gamma(N) = \left\{ \gamma \in GL_2(A) \,\middle|\, \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\text{mod } N) \right\}.$$

A subgroup of $GL_2(A)$ that contains $\Gamma(N)$ is called a *congruence subgroup.* Special cases are

$$\Gamma_0(N) = \left\{ \gamma \in GL_2(A) \,\middle|\, \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\text{mod } N) \right\}$$

and

$$\Gamma_1(N) = \left\{ \gamma \in GL_2(A) \,\middle|\, \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\text{mod } N) \right\}.$$

Most of the properties stated in this chapter for arithmetic subgroups Γ are proved for $\Gamma = \Gamma(1)$ in [Ser03] or in [Non01], and they can be proved for general arithmetic subgroups as defined above.

Let Γ be a congruence subgroup, it acts on Ω by fractional linear transformations with finite stabilizers. The quotient $\Gamma \setminus \Omega$ is a rigid analytic space over K_∞. Moreover, it is smooth of dimension one. In fact, the analytic curve $\Gamma \setminus \Omega$ can be shown to arise from an algebraic curve (cf. [Gek86, Ch. V]).

Theorem 2.7.2 (Drinfeld)**.** *There exists a smooth irreducible affine algebraic curve* Y_Γ *defined over* C_∞ *such that* $\Gamma\backslash\Omega$ *and the underlying analytic space are canonically isomorphic as analytic spaces over* C_∞*.*

The curve Y_Γ can be compactified by adding the finite set of *cusps* $\Gamma \setminus \mathbb{P}^1(K)$. We denote this compactification by X_Γ, that is

$$X_\Gamma = \Gamma \setminus \Omega \ \dot\cup\, \Gamma \setminus \mathbb{P}^1(K).$$

The curves X_Γ will be referred to as *Drinfeld modular curves.* If $\Gamma = \Gamma_0(N)$ we write $X_0(N)$ instead of X_Γ.

2.8 The quotient graph

As already mentioned, the group $GL_2(K_\infty)$ acts on the tree. Since $GL_2(A)$ is discrete in $GL_2(K_\infty)$, the stabilizers in $GL_2(A)$ of edges and vertices are finite. As is proved in [Ser03], the quotient $GL_2(A) \setminus \mathcal{T}$ is a "half line". In particular, it is isomorphic to the subtree of $\mathcal{T}$ whose vertices are represented by $\{[k,0]\}_{k \geqslant 0}$.

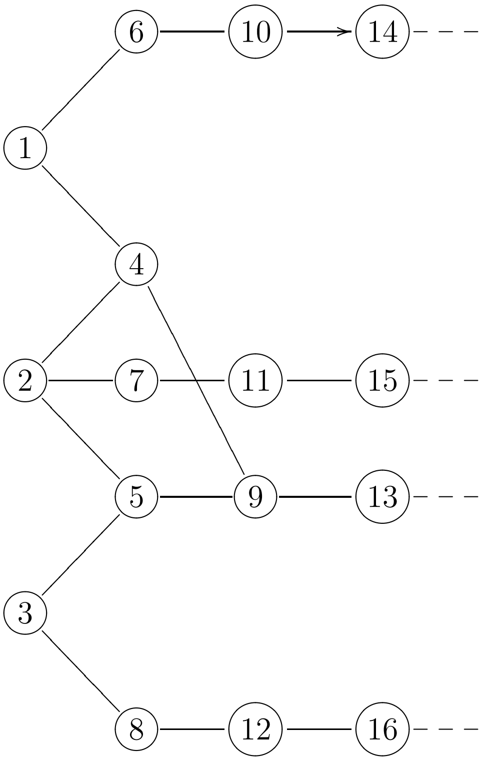
As proved in [Non01] for Γ a congruence subgroup, the quotient $\Gamma \setminus \mathcal{T}$ is a connected graph which is the union of a finite graph with a finite number of "half lines" attached to it. These are in one-to-one correspondence with the cusps of the corresponding Drinfeld modular curve and will be henceforth called *cusps*.

For a congruence subgroup Γ the quotient graph $\Gamma \setminus \mathcal{T}$ is a "ramified covering"

$$\pi : \Gamma \setminus \mathcal{T} \longrightarrow GL_2(A) \setminus \mathcal{T}.$$

Given any edge $e \in \mathcal{T}$, we will denote by $\tilde{e}$ its class on the quotient graph, analogously for any vertex v its class in the quotient is denoted by $\tilde{v}$. Also we say that a vertex in $\Gamma \setminus \mathcal{T}$ has level i if its projection under the map π is Λ_i.

Observe that the figure below shows the quotient graph for $\Gamma_0(N)$ with $N = T^3$ over $\mathbb{F}_2$.



is a covering of

$$\Lambda_0 \text{———} \Lambda_1 \text{———} \Lambda_2 \text{———} \Lambda_3 \text{———} \cdots$$

where $\Lambda_n = [\pi^n O_\infty \oplus O_\infty]$.

Denote by $(\Gamma \setminus \mathcal{T})^\circ$ the subgraph of $\Gamma \setminus \mathcal{T}$ obtained by removing all the edges starting at level $\deg(N)$ and the vertices starting at level $\deg(N)+1$, (we know (cf. [Non01]) that at level $\deg(N)$ there is no more identifications between edges).

2.9 Harmonic cocycles

In this section Γ will be a congruence subgroup.

Definition 2.9.1. Let G be an abelian group. A *G-valued harmonic cocycle* on the tree $\mathcal{T}$ is a map $\varphi : X(\mathcal{T}) \longrightarrow G$ that satisfies

i) $\varphi(\bar{e}) = -\varphi(e)$ for all $e \in Y(\mathcal{T})$,

ii) $\sum_{t(e)=v} \varphi(e) = 0$ for all $v \in X(\mathcal{T})$.

The group of harmonic cocycles on $\mathcal{T}$ with values in G is denoted by $\underline{H}(\mathcal{T}, G)$. We denote by $\underline{H}_!(\mathcal{T}, G)^\Gamma$ the subspace of $\underline{H}(\mathcal{T}, G)$ that also satisfies the following conditions

iii) $\varphi(\gamma e) = \varphi(e)$ for all $\gamma \in \Gamma$,

iv) φ has compact support modulo Γ, *i.e.* modulo Γ, the set of edges were φ takes non-zero values is finite.

We are interested in $\mathbb{Z}$-valued harmonic cocycles. From the property iii) the elements of $\underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$ may be regarded as invariant functions on the oriented edges of the quotient graph $\Gamma \setminus \mathcal{T}$. Let us denote by $\tilde{\Gamma} := \Gamma/(\Gamma \cap Z(K_\infty))$ and $\tilde{\Gamma}_{t(\tilde{e})} := \mathrm{Stab}_{\tilde{\Gamma}}(t(e))$ for some lift e to $\mathcal{T}$ of $\tilde{e}$, similarly we define $\tilde{\Gamma}_{\tilde{e}}$ and the quantity $m(\tilde{e}) := [\tilde{\Gamma}_{t(\tilde{e})} : \tilde{\Gamma}_{\tilde{e}}]$. The condition ii) is equivalent to the following sum condition (with multiplicities that count how many edges of $\mathcal{T}$ are identified modulo Γ):

$$\sum_{t(\tilde{e})=\tilde{v}} m(\tilde{e})\varphi(\tilde{e}) = 0 \quad \text{for all } \tilde{v} \in X(\Gamma \setminus \mathcal{T}). \tag{2.5}$$

Before constructing explicitly the space of harmonic cocycles, we need to recall definitions of some further groups. First the maximal torsion-free abelian quotient of Γ, namely $\bar{\Gamma} := \Gamma^{\mathrm{ab}}/\mathrm{tor}(\Gamma^{\mathrm{ab}})$. Also Γ_{f} will denote the normal subgroup generated by elements of finite order. This two groups are related by the following lemma, which holds for any congruence subgroup [Non01].

Lemma 2.9.2. *The groups $\bar{\Gamma}$ and $(\Gamma/\Gamma_{\mathfrak{f}})^{\mathrm{ab}}$ are isomorphic.*

In [Ser03, Ch. I, Thm. 13] is proved that the group $\Gamma/\Gamma_{\mathrm{f}}$ is canonically identified with the fundamental group of the graph $\Gamma \setminus \mathcal{T}$, so $\Gamma/\Gamma_{\mathrm{f}}$ is free (cf. [Ser03, p. 43]). The group $\bar{\Gamma}$ is isomorphic to the homotopy group of the quotient graph, indeed we have the following:

Lemma 2.9.3. *Let v be a vertex of $\mathcal{T}$, there exists an isomorphism*

$$\begin{aligned} i : \bar{\Gamma} &\rightarrow H_1(\Gamma \setminus \mathcal{T}, \mathbb{Z}) \\ \alpha &\longmapsto \psi_{\alpha,v} \end{aligned}$$

where $\psi_{\alpha,v}$ is given by

$$\psi_{\alpha,v}(\tilde{e}) := \#\left\{e \in (v, \alpha v)|\ e \equiv \tilde{e} \ (\mathrm{mod}\ \Gamma)\right\} - \#\left\{e \in (v, \alpha v)|\ -e \equiv \tilde{e} \ (\mathrm{mod}\ \Gamma)\right\}$$

and this map is independent of the vertex v, where $(v, \alpha v)$ denotes the path without backtracking from v to αv.

For a proof of this lemma see [Non01, Thm. 2.34]. Here we give a short explanation of the meaning of the map $\psi_{\alpha,v}$. Given any $\alpha \in \Gamma$, the path on the tree $\mathcal{T}$ that goes from v to αv is non back-tracking. However, its projection to the quotient graph is a cycle which in general is not reduced. Given any $\tilde{e}$ in the cycle determined by v and αv, there are many edges $e \in \mathcal{T}$ mapping to $\tilde{e}$. So the map $\psi_{\alpha,v}$ counts how many edges of the path $v, \alpha v$ in $\mathcal{T}$ have the image in the cycle.

Lemma 2.9.4. *There exists an injective homomorphism*

$$\begin{aligned} \iota : H_1(\Gamma \setminus \mathcal{T}, \mathbb{Z}) &\rightarrow \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma} \\ \psi &\longmapsto \varphi \end{aligned}$$

defined by $\varphi(e) := n(e)\psi(\tilde{e})$, where $n(e) := \#Z(\Gamma)^{-1}\#Stab_{\Gamma}(e)$.

Finally, the following lemma connects the groups $\bar{\Gamma}$ and $\underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma}$.

Lemma 2.9.5. *There is a canonical homomorphism*

$$\begin{aligned} j:\bar{\Gamma} \;&\to\; \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma} \\ \alpha \;&\longmapsto\; \varphi_{\alpha,v} \end{aligned}$$

where $\varphi_{\alpha}(e) := \varphi_{\alpha,v}(e) = \frac{1}{\#(Z\cap\Gamma)}\sum_{\gamma\in\Gamma}\delta(e,\alpha,v,\gamma)$ *with* v *any fixed vertex and the function* $\delta(e,\alpha,v,\gamma)$ *given by:*

$$\delta(e,\alpha,\gamma,v) = \begin{cases} 1 & \text{if} \quad \gamma(e)\in(v,\alpha v), \\ -1 & \text{if} \quad \gamma(e)\in(\alpha v, v), \\ 0 & \text{otherwise.} \end{cases}$$

This homomorphism is independent of the choice of the vertex v*.*

The map j defined above is actually the composition of i and ι, so it is injective. We show here the surjectivity of j (cf. [Non01, Cor. 2.37]) which will give us a way to construct the space of harmonic cocycles. Here we will use the homology of the graph to construct a basis of $\underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma}$ and then we get the surjectivity.

Let T be the maximal tree[1] in $(\Gamma\setminus\mathcal{T})^{\circ}$ and $\{\tilde{e_1},\tilde{e_2},...,\tilde{e_g}\}$ be a set of representatives of the edges of the tree $(\Gamma\setminus\mathcal{T})^{\circ}-T$. It is proved in [Non01, Cor. 2.38] that the set $\{\tilde{e_1},\tilde{e_2},...,\tilde{e_g}\}$ consist of edges attached to vertices of level 0 of degree $q+1$ (cf. §.2.8 for the definition of level).

Let $\tilde{v}_i = o(\tilde{e}_i)$, $\tilde{w}_i = t(\tilde{e}_i)$ the origin and target of $\tilde{e}_i$, respectively. Then there exists a unique geodesic $\tilde{c_i}'$ in the tree T joining $\tilde{w}_i$ and $\tilde{v}_i$. In this way $\tilde{c_i}'$ gives rise to a closed path c_i in $\Gamma\setminus\mathcal{T}$ by composing $\tilde{e}_i$ and $\tilde{c_i}'$.
Consider

$$\varphi_i : Y(\Gamma\setminus\mathcal{T}) \longrightarrow \mathcal{T}$$

defined as follows

[1] It exists since $(\Gamma\setminus\mathcal{T})^{\circ}$ is finite and connected.

$$\varphi_i(\tilde{e}) = \begin{cases} n(e) & \text{if} \quad \tilde{e} \quad \text{appears in} \quad \tilde{c}_i, \\ -n(e) & \text{if} \quad \bar{\tilde{e}} \quad \text{appears in} \quad \tilde{c}_i, \\ 0 & \text{otherwise.} \end{cases}$$

From (2.5), we see that actually φ_i lifts to a function on $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ and form a basis of $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$. Finally let $c_i = (e_{i,0}, e_{i,1}, ...e_{i,l})$ be a lift of $\tilde{c}_i$, then there is a $\alpha_i \in \Gamma$ such that $\alpha_i o(e_{i,0}) = t(e_{i,l})$ so we can find a $\alpha \in \Gamma$ such that $j(\alpha) \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$.

In summary, to construct the space of harmonic cocycles for the graph $\Gamma \setminus \mathcal{T}$, we need to find the maximal subtree T of $(\Gamma \setminus \mathcal{T})^\circ$, also called *maximal spanning tree.* For this we use the algorithm given in [Non01, §3] to find a set of representatives $\{\tilde{e_1}, \tilde{e_2}, ..., \tilde{e_g}\}$ of the edges of the tree $(\Gamma \setminus \mathcal{T})^\circ - T$. Finally we define for each i the φ_i as above.

2.10 Theta functions for arithmetic groups

Let Γ be an arithmetic subgroup of $GL_2(K_\infty)$.

Definition 2.10.1. A *holomorphic theta function* for $\Gamma \subset GL_2(K_\infty)$ is an invertible rigid analytic function $(u : \Omega \longrightarrow C_\infty^\times) \in \mathcal{O}_\Omega(\Omega)^\times$ such that for each $\gamma \in \Gamma$, u satisfies the functional equation

$$u(\gamma z) = c_u(\gamma) u(z)$$

for some constant $c_u(\gamma) \in C_\infty^\times$ independently of z.

The map $c_u : \gamma \mapsto c_u(\gamma)$ is a homomorphism from Γ to $C_\infty^\times$ called the *multiplier* of u.

We denote by $\Theta_{\mathrm{h}}(\Gamma)$ the space of holomorphic theta functions for Γ.

In [GR96, §5], the authors give a way to construct a holomorphic theta function for Γ as follows. Let ω be fixed element of Ω and $\alpha \in \Gamma$, put

$$\theta_\alpha(\omega, z) := \prod_{\gamma \in \tilde{\Gamma}} \frac{z - \gamma\omega}{z - \alpha\gamma\omega}. \tag{2.6}$$

Theorem 2.10.2 ([GR96, Thm. 5.4.1])**.** *The product $\theta_\alpha(\omega, z)$ converges to a holomorphic theta function for Γ on Ω. The value of $c_\alpha(\gamma) := \frac{\theta_\alpha(\omega,\gamma z)}{\theta_\alpha(\omega,z)}$ induces a group homomorphism $\bar{c} : \bar{\Gamma} \longrightarrow Hom(\bar{\Gamma}, C_\infty^\times)$ by $\alpha \mapsto c_\alpha$. Moreover, the map $\bar{\Gamma} \times \bar{\Gamma} \longrightarrow C_\infty^\times$ defined by $(\alpha, \beta) \mapsto c_\alpha(\beta)$ is a symmetric bilinear pairing.*

Corollary 2.10.3 ([GR96, Cor. 5.4.12])**.** *The constant $c_\alpha(\beta)$ lies in $K_\infty^\times \subset C_\infty^\times$.*

In the next chapter we will see another way to construct theta functions by means of certain multiplicative integrals.

2.10.1 Theta functions and harmonic cocycles

In this subsection we relate the theta function for an arithmetic group Γ and the $\mathbb{Z}$-valued harmonic cocycles by means of the following result due (mostly) to Van der Put [VdP82].

Theorem 2.10.4. *The map*

$$r : \mathcal{O}_\Omega(\Omega)^\times \longrightarrow \underline{H}_!(\mathcal{T}, \mathbb{Z}), \quad \text{given by} \qquad r(f)(e) := \log_q \frac{\|f\|_{t(e)}}{\|f\|_{o(e)}}$$

is a continuous surjective group homomorphism with kernel $C_\infty^\times$ where $\|\cdot\|_v$ is the spectral norm on $\mathcal{O}_\Omega(\lambda^{-1}(v))$ defined by

$$\|f\|_v := \sup\left\{|f(z)| \mid z \in \lambda^{-1}(v)\right\}$$

for $v \in X(\mathcal{T})$.

The next result is a refinement of the previous one, since it relates theta functions to Γ-invariant harmonic cocycles (cf. [GR96, Thm. 5.6.1]).

Theorem 2.10.5. *Let $\alpha \in \Gamma$ be given then $r(\theta_\alpha) = \varphi_\alpha$.*

The map r yields a map

$$\bar{r} : \Theta_{\mathrm{h}}(\Gamma)/C_\infty^\times \longrightarrow \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma.$$

Let further

$$\bar{u} : \bar{\Gamma} \longrightarrow \Theta_{\mathrm{h}}(\Gamma)/C_\infty^\times$$

be the map induced from $\alpha \mapsto \theta_\alpha$, then we have the following:

Theorem 2.10.6 ([GR96, §6])**.** *For $\alpha \in \Gamma$ with class $\bar{\alpha}$ in $\bar{\Gamma}$ we have that $\bar{r}(\theta_\alpha) = j(\bar{\alpha})$. In other words, the following diagram is commutative*

$$\begin{tikzcd}
\bar{\Gamma} \arrow[d, "\bar{u}"'] \arrow[dr, "j"] & \\
\Theta_h(\Gamma)/C_\infty^\times \arrow[r, "\bar{r}"] & \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma.
\end{tikzcd} \tag{2.7}$$

From the theorem we see that we have two different constructions of Γ-invariant $\mathbb{Z}$-valued harmonic cocycles from $\alpha \in \Gamma$:

i) using the function φ_α given in Lemma 2.9.5 and

ii) by evaluating the map $\bar{r}$ in θ_α.

From now by abuse on notation, we will write r instead of $\bar{r}$.

2.11 Hecke operators

There exist Hecke operators acting on each of the groups that appear in (2.7). For the definition of the operators on $\bar{\Gamma}$ and $\Theta(\Gamma)/C_\infty^\times$ see [GR96, §9.3], we will give an explicit description of the operator on $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ for the case $\Gamma = \Gamma_0(N)$.

Let $\mathfrak{m}$ be a non zero ideal of $\mathbb{F}_q[T]$. We recall from the definition of the Bruhat-Tits tree that the edges are given by classes of $GL_2(K_\infty)/K_\infty^\times \mathcal{I}$. Hence functions on $Y(\mathcal{T})$ can be seen as functions on $GL_2(K_\infty)$ right invariant under $\mathcal{I}$. For φ on $GL_2(K_\infty)$ we put

$$T_\mathfrak{m}\varphi(\alpha) := \sum_{\gamma \in \mathcal{R}_\mathfrak{m}} \varphi(\gamma\alpha)$$

where

$$\mathcal{R}_\mathfrak{m} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) \;\middle|\; a, d \text{ monic } (ad) = \mathfrak{m},\ \gcd(a, N) = 1, \deg b < \deg d \right\}. \tag{2.8}$$

The following properties of $T_\mathfrak{m}$ are standard:

i) $T_\mathfrak{m} : \varphi \mapsto T_\mathfrak{m}\varphi$ maps $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ into itself,

ii) all $T_\mathfrak{m}$ commute,

iii) if $\mathfrak{m}$ and $\mathfrak{n}$ are coprime, then $T_{\mathfrak{m}\mathfrak{n}} = T_\mathfrak{m} \circ T_\mathfrak{n}$,

iv) if $\gcd(\mathfrak{p}, N) = 1$ then $T_{\mathfrak{p}^{n+1}} = T_{\mathfrak{p}^n} \circ T_\mathfrak{p} - q^{\deg \mathfrak{p}} T_{\mathfrak{p}^{n-1}}$ for $\mathfrak{p}$ a prime ideal of A,

v) if gcd$(\mathfrak{m}, N) = 1$ then $T_{\mathfrak{m}}$ is hermitian with respect to the *Peterson inner product* defined as follows:

$$(\varphi_1, \varphi_2)(e) = \sum_{e \in \Gamma \backslash \mathcal{T}} \varphi_1(e)\varphi_2(e).$$

Hecke operators $T_{\mathfrak{m}}$ with $gcd(\mathfrak{m}, N) = 1$ are called *unramified.* As in the classical case we can also construct the space of new and old forms. Indeed suppose that M divides N. For each monic divisor a of N/M we have an embedding $i_{a,M} : \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(M)} \longrightarrow \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ given by

$$i_{a,M}(\varphi)(g) = \varphi(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g).$$

We set then $(\underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} \otimes \mathbb{Q})^{new}$ to be the orthogonal complement in $\underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} \otimes \mathbb{Q}$ with respect to the Perterson inner product to the images of all the $i_{a,M} \otimes \mathbb{Q}$, where M runs through the proper divisors of N and through the divisors of N/M. We further put

$$\underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} = \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} \ \cap \ (\underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} \otimes \mathbb{Q})^{new}.$$

2.12 Application to the Shimura-Taniyama-Weil uniformization

In order to establish the analog of the classical Shimura-Taniyama-Weil, we need to explain how $\mathbb{Q}$-harmonic cocycles may be regarded as automorphic forms of a certain type. For a deeper discussion of automorphic forms we refer the reader to [Gel75].

In what follows, $\mathcal{A}$ will be the adèle ring of K with ring of integers $\mathcal{O}$ and I the idèle group. Having fixed the place ∞ of K, these rings decompose into a “finite” and an “infinite” part

$$\begin{array}{rcl} \mathcal{A} & = & \mathcal{A}_{\mathrm{f}} \times K_\infty \\ \mathcal{O} & = & \mathcal{O}_{\mathrm{f}} \times O_\infty \\ I & = & I_{\mathrm{f}} \times K_\infty^\times. \end{array}$$

We define an *automorphic cusp form* for an open subgroup $\mathcal{K}$ of $GL_2(\mathcal{O})$ to be a $\mathbb{C}$-valued function φ on $Y(\mathcal{K}) := GL_2(K) \setminus GL_2(\mathcal{A})/\mathcal{K} \cdot Z(K_\infty)$.

Let S be a set of representatives for $GL_2(K) \setminus GL_2(\mathcal{A}_{\mathrm{f}})/\mathcal{K}_{\mathrm{f}}$ and define for $x \in S$

$$\Gamma_x := GL_2(K) \cap x\mathcal{K}_{\mathrm{f}} x^{-1}.$$

In [GR96, §4] the following isomorphism is shown:

$$\begin{aligned} GL_2(K) \setminus GL_2(\mathcal{A})/\mathcal{K}_{\mathrm{f}} \times Z(K_\infty) \cdot \mathcal{I} \ &\xrightarrow{\cong} \ \textstyle\bigsqcup_{x \in S} \Gamma_x \setminus GL_2(K_\infty)/Z(K_\infty) \cdot \mathcal{I} \\ &= \ \textstyle\bigsqcup_{x \in S} X(\Gamma_x \setminus \mathcal{T}). \end{aligned}$$

We have the following theorem.

Theorem 2.12.1 (Drinfeld)**.** *Let $\mathcal{K}$ be an open subgroup of $GL_2(\mathcal{O})$ of the form $\mathcal{K} = (\mathcal{K}_{\mathtt{f}}) \times \mathcal{I}$ and let F be a field of characteristic zero. Under the previous bijection the module of harmonic cochains*

$$\bigoplus_{x \in S} \underline{H}_!(\mathcal{T}, F)^{\Gamma_x}$$

corresponds to the space $W_{sp}(\mathcal{K}, F)$ of F-valued cuspidal automorphic forms φ on $G(K) \setminus GL_2(\mathcal{A})/\mathcal{K}_{\mathtt{f}} \times Z(K_\infty) \cdot \mathcal{I}$ that transform like π_{sp} under $GL_2(K_\infty)$.

Here π_{sp} is the so-called special representation of $GL_2(K_\infty)$, *i.e.*, the irreducible representation of $GL_2(K_\infty)$ on the space of locally constant F-valued functions on $\mathbb{P}^1(K_\infty)$. For more details see [GR96, §4.7].

So the space of harmonic cocycles has a natural interpretation as a space of automorphic functions in the sense of Jacquet-Langlands [JL70].

Let E be an elliptic curve defined over $K = \mathbb{F}_q(T)$ with conductor $N\infty$, where N is an ideal of A and assume E to have split multiplicative reduction at ∞. By combining results of Jacquet-Langlands [JL70], E corresponds to an automorphic eigenform φ_E in the new part of $\underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ with rational integral eigenvalues. The elliptic curve E is an isogeny factor of the new part of the Jacobian of the Drinfeld modular curve $X_0(N)$. This is the content of [GR96, §8.3].

Applying well known facts from the theory of automorphic forms there are canonical bijections between the following three sets

i) K-isogeny classes of elliptic curves with conductor $N\infty$,

ii) one-dimensional isogeny factors of $J_0^{new}(N)$,

iii) normalized Hecke eigenforms φ in $\underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ with rational eigenvalues.

Thus one would like to have a procedure to construct an elliptic curve within the isogeny class that corresponds to the newform φ.

Let $\varphi \in \underline{H}_!^{new}(\mathcal{T}, G)^{\Gamma_0(N)}$ be a Hecke eigenform with rational eigenvalues. We will construct the elliptic curve E_φ associated to it. By means of (2.7) we identify $\underline{H}_!(\mathcal{T}, G)^{\Gamma_0(N)}$ with $\bar{\Gamma}$.

Proposition 2.12.2 ([Gek95, Thm. 3.2])**.** *Let $\varphi \in j(\overline{\Gamma})$ be an harmonic cocycle, regarded as the class of some element, also denoted by φ, of Γ. Put $\Delta \subset K_\infty^\times$ for the subgroup $\{c_\varphi(\alpha) | \alpha \in \Gamma\}$ of $K_\infty^\times$, where $c_\varphi(\alpha)$ is the multiplier associated to the theta function of Γ. Then there exists $\mathbf{q} \in K_\infty^\times$ such that $|\mathbf{q}| < 1$ and $\mathbf{q}^{\mathbb{Z}} = \Delta$.*

For general A, the conclusion of Proposition 2.12.2 is that there exists $\mathbf{q} \in K_\infty^\times$ with $|\mathbf{q}| < 1$ such that $\Delta \supseteq \mathbf{q}^{\mathbb{Z}}$ and the incluision is of finite index (cf. [GR96, Prop 9.5.1]).

Then the elliptic curve E_φ associated with an automorphic Hecke eigenform, can be analytically recovered as a Tate curve (cf. Ch. 5, §5.5 for a definition) as $E_\varphi^{an}(C_\infty) = C_\infty^\times / \mathbf{q}^{\mathbb{Z}}$. It is shown in [Roq70, §3] that E_φ may be described by means of an analytic equation defined over a finite extension of K. However, this is not enough to recognize the isogeny class of the elliptic curve E_φ.

The aim of this thesis is calculate by means of a certain multiplicative integral the Tate period $\mathbf{q}$ and then using the analytic equation of the Tate curve and an appropriate model of an elliptic curve that by means of change of variables allows us to find the algebraic equation of the elliptic curve E_φ over K.

3. Integration, Theta function and uniformizations

3.1 Integration

As described in the previous chapter, Gekeler and Reversat develop in [GR96] the theory of theta functions to construct an explicit analytic parametrization of an elliptic curve with semi-stable reduction at the place ∞. However, their construction of the theta function requires to compute the infinite product (2.6), which makes it computationally hard to find the Tate parameter. In [Lon02], Longhi defines a multiplicative integral over $\mathbb{P}^1(K_\infty)$ which is a multiplicative version of Teiltebaum's Poisson formula [Tei91], and uses this to construct a theta function in a different way as the one of Gekeler-Reversat. Around the same time Pal gives a similar construction in [Pál06]. In this section we briefly recall the main facts of the machinery of integration along the lines of Longhi [Lon02].

Let X be a topological space such that its compact open subsets form a basis for the topology.

Definition 3.1.1. A $\mathbb{Z}$-valued function μ on compact-open subsets of X is a *distribution* on X if $\mu(X) = 0$ and if it is finitely additive, *i.e.*, if, whenever A and B are disjoint compact open sets of X, one has $\mu(A \cup B) = \mu(A) + \mu(B)$. We denote the space of $\mathbb{Z}$-valued distributions by $\mathcal{M}(X, \mathbb{Z})$.

Definition 3.1.2. A *measure* on X is a bounded distribution, *i.e.*, a distribution μ for which there is a constant C satisfying $|\mu(U)| < C$ for all compact open $U \subset X$. We denote the space of $\mathbb{Z}$-valued measures on X by $\mathcal{M}_0(X, \mathbb{Z})$.

From now on, we assume that X is compact, so in particular $\mathbb{Z}$-valued distributions on X are measures.

Definition 3.1.3. Given a continuous function $f : X \to C_\infty^\times$, its multiplicative integral with respect to the measure $\mu \in \mathcal{M}_0(X, \mathbb{Z})$ is

$$\times\!\!\!\!\!\!\int_X f(t)\, d\mu(t) := \varinjlim_{\alpha} \prod_{U \in \mathcal{C}_\alpha} f(u)^{\mu(U)} \tag{3.1}$$

where $\{\mathcal{C}_\alpha\}_\alpha$ is the direct system of finite covers of X by compact open subsets U and u is an arbitrary point in U.

Under the crucial assumption that X is compact, we have

Proposition 3.1.4 ([Lon02, Prop. 5])**.** *The limit in (3.1) exists and is independent of the choice of the u's. Furthermore*

$$\times\!\!\!\!\!\!\int_X \_\, d\mu : \mathcal{C}(X, C_\infty^\times) \to C_\infty^\times \tag{3.2}$$

is a continuous homomorphism, where $\mathcal{C}(X, C_\infty^\times)$ is the set of continuous functions from $C_\infty^\times$ to X.

3.1.1 Measures and harmonic cocycles

We know from Lemma 2.5.4 that the set of ends of the tree $\mathcal{T}$ is in 1-1 correspondence with $\mathbb{P}^1(K_\infty)$.

Proposition 3.1.5. *The map*

$$\begin{aligned} \mathcal{M}_0(X, \mathbb{Z}) &\longrightarrow \underline{H}(\mathcal{T}, \mathbb{Z}) \\ \mu &\longmapsto (e \mapsto \mu(U_e)) \end{aligned}$$

is an isomorphism of $\mathbb{Z}$-modules.

Proof. Let e be an oriented edge of the tree $\mathcal{T}$ and let the open subset U_e of $\mathbb{P}^1(K_\infty)$ be defined as in Section 2.5. For every open compact subset U of $\mathbb{P}^1(K_\infty)$ there is a finite set Y_U of oriented edges such that $U = \dot{\bigcup}_{e \in Y_U} U_e$. So, a φ in $\underline{H}(\mathcal{T}, \mathbb{Z})$ defines a finite additive measure $\mu_\varphi \in \mathcal{M}_0(X, \mathbb{Z})$ by putting $\mu_\varphi(U) = \sum_{e \in Y} \varphi(e)$.

Conversely given a $\mathbb{Z}$-valued measure $\mu \in \mathcal{M}_0(X,\mathbb{Z})$ one defines the harmonic cocycle $\varphi_\mu(e) := \mu(U_e)$. From $U_e \dot{\bigcup} U_{\overline{e}} = \mathbb{P}^1(K_\infty)$ and $\mu(\mathbb{P}^1(K_\infty)) = 0$ it follows that $\varphi(e) = -\varphi(\overline{e})$. Let now v be a vertex in $\mathcal{T}$, then $\mathbb{P}^1(K_\infty)$ is the disjoint union of U_e's, where the union is taken over the oriented edges starting at v. Again from the fact that $\mu(\mathbb{P}^1(K_\infty)) = 0$ and $\mu(U \cup V) = \mu(U) + \mu(V)$ if $U \cap V = \emptyset$ we get $\sum_e \varphi_\mu(e) = 0$. We conclude that φ_μ is indeed a harmonic cocycle. □

3.1.2 The integral over $\partial\Omega$

We are interested in the particular case where $X = \partial\Omega$. In this case the computation of a multiplicative integral can be accomplished as follows. Choose a vertex $v \in X(\mathcal{T})$. Usually the vertex v is taken to be v_0 as we will do, and for each $e \in Y(\mathcal{T})$ pointing away from v_0, define $l(e)$ to be the distance between the origin $o(e)$ of e and v_0. Then according to the definition of the integral (3.1) and the discussion in Subsection 3.1.1 we have that

$$\times\!\!\!\!\!\!\int_{\partial\Omega} f(t)\, d\mu_\varphi(t) = \lim_{n\to\infty} \prod_{l(e)=n} f(t_e)^{\mu(U_e)} \tag{3.3}$$

is independent of the choice of v_0.

3.1.3 Change of variables

Note that the group $GL_2(K_\infty)$ acts naturally on the space $\mathcal{M}_0(\mathbb{P}^1(K_\infty),\mathbb{Z})$ by $\gamma * \mu(U) := \mu(\gamma^{-1}U)$ for any $\mu \in \mathcal{M}_0(\mathbb{P}^1(K_\infty),\mathbb{Z})$ and U an open in $\mathbb{P}^1(K_\infty)$. In the same way $GL_2(K_\infty)$ acts on the space of harmonic cocycles $H(\mathcal{T},\mathbb{Z})$ by $(\gamma * \varphi)(e) := \varphi(\gamma^{-1}e)$. As in the classical case, we have the formula of change of variables formula given by

$$\times\!\!\!\!\!\!\int_{\gamma U} f\, d(\gamma * \mu) = \times\!\!\!\!\!\!\int_U (f \circ \gamma)\, d\mu$$

or equivalently

$$\times\!\!\!\!\!\!\int_{\gamma^{-1}U} (\gamma^{-1} * f)\, d(\gamma^{-1} * \mu) = \times\!\!\!\!\!\!\int_U f\, d\mu \tag{3.4}$$

where $(\gamma^{-1} * f)\,(t) = (f \circ \gamma)(t) = f(\gamma\langle t\rangle)$.

3.2 Theta function

As already observed in [Sch84], the machinery of integration on $\partial\Omega$ can be used to construct an inverse of the Van der Put's map r defined in the equation (2.10.4). In [Lon02], Longhi uses the multiplicative integral to give a multiplicative version of Teitelbaums's Poisson formula [Tei91, Thm. 11] and then such an inverse of r. In the following paragraphs we will describe the Poison formula stated by Longhi and then the integral that we are interested in.

Theorem 3.2.1 ([Lon02, Thm. 6])**.** *Let $u \in \mathcal{O}_\Omega(\Omega)$, $\varphi = r(u)$ and fix $z_0 \in \Omega$. Then for $z \in \Omega$*

$$u(z) = u(z_0) \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z-t}{z_0-t}\, d\mu_\varphi(t). \tag{3.5}$$

We are now ready to prove

Proposition 3.2.2. *The map r induces an isomorphism $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma \cong \Theta_h(\Gamma)/C_\infty$.*

Proof. Given a $u \in \Theta_h(\Gamma)/C_\infty$ then by Theorem 2.10.4 we have that $r(u)$ is a harmonic cocycle, Γ-invariant and cuspidal.

Conversely given a harmonic cocycle $\varphi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ we denote by μ_φ its corresponding measure. Fix a z_0 in Ω. Consider now the function

$$u(z) = \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z-t}{z_0-t}\, d\mu_\varphi(t). \tag{3.6}$$

By Theorem 3.2.1 we know that $u \in \mathcal{O}_\Omega(\Omega)^\times$. It remains to check that $u(z)$ satisfies the functional equation

$$u(\gamma z) = c_u(\gamma)u(z) \tag{3.7}$$

for all $\gamma \in \Gamma_0(N)$ and some constant $c_u(\gamma) \in C_\infty^\times$.

It is a straightforward calculation to see that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the ratio

$$\frac{\frac{t-\gamma z}{t-\gamma z_0}}{\frac{\gamma^{-1}t-z}{\gamma^{-1}t-z_0}} = \frac{cz+d}{cz_0+d} \tag{3.8}$$

does not depend on t. So we have

$$\begin{aligned} u(\gamma z) &= \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t-\gamma z}{t-z_0}\, d\mu_\varphi(t) \\ &= \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t-\gamma z_0}{t-z_0}\, d\mu_\varphi(t) \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t-\gamma z}{t-\gamma z_0}\, d\mu_\varphi(t) \\ &= \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t-\gamma z_0}{t-z_0}\, d\mu_\varphi(t) \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \left(\frac{cz+d}{cz_0+d}\right)\left(\frac{\gamma^{-1}t-z}{\gamma^{-1}t-z_0}\right) d\mu_\varphi(t). \end{aligned}$$

Using the fact that the integral is multiplicative and $\mu_\varphi(\partial\Omega) = 0$ we get that

$$\mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{cz_0+d}{cz+d}\, d\mu_\varphi(t) = 1,$$

since it is constant on t. The functional equation follows taking

$$c_u(\gamma) = \mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t-\gamma z_0}{t-z_0}\, d\mu_\varphi(t) \tag{3.9}$$

which does not depends on z.

□

We recall the diagram (2.7) from Chapter 2.

$$\begin{tikzcd} \bar{\Gamma} \arrow[d, "\bar{u}"'] \arrow[dr, "j"] & \\ \Theta_h(\Gamma)/C_\infty^\times \arrow[r, "\bar{r}"] & \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma. \end{tikzcd}$$

So given a harmonic cocycle $\varphi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ and $\alpha \in \bar{\Gamma}$ so that $j(\alpha) = \varphi$, we have that the multiplier $c_u(\gamma)$ is actually $c_\alpha(\gamma)$ defined in Theorem 2.10.2.

3.3 Complex uniformization

In this section we consider an elliptic curve $E/\mathbb{Q}$ with conductor N. We will briefly describe how to parametrize the curve E over the complex field $\mathbb{C}$. The main reference here is [Sil09, Ch. VI].

Let $\Gamma_0(N)$ be the group of matrices in $SL_2(\mathbb{Z})$ which are upper triangular modulo N. It acts as a discrete group by Möbius transformations on the Poincare upper half-plane

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

A *cusp form of weight 2* for $\Gamma_0(N)$ is an analytic function f on $\mathcal{H}$ satisfying the relation

$$f(\gamma\langle z\rangle) = (cz+d)^2 f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \tag{3.10}$$

together with suitable growth conditions on the boundary of $\mathcal{H}$. The invariance equation (3.10) implies in particular that the function f is periodic of period 1 and thus f can be written as a power series in $q = e^{2\pi i}$ with no constant term:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n.$$

The associated L-series is defined as $L(f,s) := \sum_{n=1}^{\infty} a_n n^{-s}$.

From the Eichler-Shimura theory given a cuspidal eigenform whose Fourier coefficients are integers, there exists an elliptic curve E_f such that the two L-series coincide

$$L(f,s) = L(E_f,s).$$

Here $L(E_f,s)$ is the L-series defined as the infinite Euler product

$$L(E_f,s) = \prod_{p\nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \prod_{p\mid N} (1 - a_p p^{-s})^{-1} := \sum a_n n^{-s}$$

with $a_p = \#E(\mathbb{F}_p)$ ([Dar04, §1.4]).

On the other hand, let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Then there exists a cuspidal Hecke eigenform of weight 2 for $\Gamma_0(N)$ such that the L functions coincide

$$L(f,s) = L(E,s)$$

and E is isogenous to the elliptic curve E_f obtained form Eichler-Shimura theory.

In summary, given an integer $N > 1$ and a cuspidal Hecke eigenform of weight 2, one would like to have a procedure to construct an elliptic curve within the isogeny class that correspond to the form f. Actually such as procedure exists and we will briefly give some things related to it (a good reference here is [Cre97]).

Let $X_0(N)$ be the modular elliptic curve for cyclic N-isogenies. By the work of Wiles et.al., E is equipped with a non constant dominant morphism defined over $\mathbb{Q}$, commonly referred as the *Weil parametrization* attached to E:

$$\Phi_N : X_0(N) \longrightarrow E$$

mapping the cusp ∞ to the identity element of E. The complex uniformization of $E(\mathbb{C})$ provides a method for calculating the Weil parametrization. Namely, the compact Riemann surface $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$, where Λ is a lattice generated by the periods of a Néron differential ω on E. Then we have the following commutative diagram

$$\begin{tikzcd}
\Gamma \setminus \mathcal{H}^* \arrow[r, "z_0 \mapsto \int_\infty^{z_0} f_E(z)dz"] \arrow[d, "j"] & \mathbb{C}/\Lambda \arrow[d, "\eta"] \\
X_0(N)(\mathbb{C}) \arrow[r, "\Phi_N"] & E(\mathbb{C})
\end{tikzcd} \tag{3.11}$$

where $\eta : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ is the complex analytic isomorphism described by the formula $\eta = (\wp_\Lambda : \wp'_\Lambda : 1)$ where $\wp_\Lambda$ is the Weierstrass $\wp$-function attached to Λ. Explicit formulas for Λ and $\wp_\Lambda$ can be found in [Sil09].

In this case a good approximation of the integral $\int_\infty^\tau f_E(z)dz$ reduces to calculate a finite sum which depends on the calculation of the a_n's in the Fourier expansion of f_E where f_E is the modular form attached to E.

Obtaining equations for the curves

The integrals $\int_\infty^{z_0} f_E(z)dz$ allow to compute periods ω_1 and ω_2 which generate the period lattice Λ_f of the modular curve $E_f = \mathbb{C}/\Lambda_f$. Letting $\tau = \omega_1/\omega_2$, we may assume that $\mathrm{Im}(\tau) > 0$ interchanging ω_1 and ω_2 if necessary. Set $q = e^{2\pi i\tau}$ and define

$$\begin{aligned}
c_4(q) &= \left(\frac{2\pi}{\omega_2}\right)^4 \left(1 + 240\sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n}\right) \quad \text{and} \\
c_6(q) &= \left(\frac{2\pi}{\omega_2}\right)^6 \left(1 - 504\sum_{n=1}^{\infty} \frac{n^5 q^n}{1-q^n}\right).
\end{aligned}$$

Then the following theorem is crucial in the calculation of the equation of the curve E (cf. [Cre97, §2.14]).

Theorem 3.3.1 (Edixhoven). *The quantities c_4 and c_6 defined above are in $\mathbb{Z}$, so the elliptic curve*

$$y^2 = 4x^3 - c_4 x - c_6$$

is defined over $\mathbb{Z}$.

This theorem allows Cremona to find equations for all elliptic curves of conductor up to 130.000 [Cre97]. The series c_4 and c_6 converge extremely rapidly. Thus, assuming that ω_1 and ω_2 are known to sufficient precision, Cremona can compute c_4 and c_6 also with sufficient precision and thus he is able to recognize the corresponding exact integer values.

3.4 p-adic Uniformization

From the previous section, we have that any elliptic curve $E/\mathbb{Q}$ with conductor N is equipped with a non constant parametrization

$$\Phi_N : X_0(N) \longrightarrow E. \tag{3.12}$$

However for some applications, like the calculation of Heegner points, (cf. [Dar04, Ch. 3-4]) it is convenient to enlarge the repertoire of modular parametrizations to include *Shimura curve parametrizations.* For more details on the results stated here, the reader is referred to [Dar04],[BC91],[Voi] and [Vig80].

Assume that the positive integer N is square free and $N = N^-N^+$ is a factorization of N such that N^- has an even number of prime factors. Let C be the *indefinite quaternion $\mathbb{Q}$-algebra* ramified precisely at the primes dividing N^- and let S be an *Eichler $\mathbb{Z}$-order* in C of level N^+. Fix an identification

$$\iota_\infty : C \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}).$$

Denote by Γ_{N^-,N^+} the image under ι_∞ of the group of units in S of reduced norm 1. Then Γ_{N^-,N^+} acts properly discontinuously on $\mathcal{H}$ with compact quotient $X_{N^-,N^+}(\mathbb{C})$. By Shimura theory, the compact Riemann surface $X_{N^-N^+}(\mathbb{C})$ has a canonical model X_{N^-,N^+} over $\mathbb{Q}$ as in the classical case. This is done by interpreting X_{N^-,N^+} as a moduli space for abelian surfaces over $\mathbb{Q}$ with endomorphism rings containing S, together with some auxiliary level N^+-structure (cf. [AB04]).

Let J_{N^-,N^-} denote the Jacobian of X_{N^-,N^+}. By the modularity theorem for elliptic curves defined over $\mathbb{Q}$ and the Jacquet-Langlands correspondence, there exists a surjective morphism

$$\Phi_{N^-,N^+} : J_{N^-,N^+} \longrightarrow E \tag{3.13}$$

defined over $\mathbb{Q}$ (cf. [Dar04, Ch. 4]).

However, we do not dispose here of Fourier coefficients, since modular forms on non-split quaternion algebras do not admit q-expansions, there is no known explicit formula for the map Φ_{N^-,N^+}. In order to handle with this issue, it is necessary to turn to the p-adic uniformization. In this section we will succinctly explain how to use the uniformization Φ_{N^-,N^+} to construct an explicit p-adic uniformization of E at the primes p dividing N^-.

Let us assume $N^- > 1$ and p be a prime dividing N^-. Consider now the definite quaternion algebra $\mathcal{B}$ ramified precisely at the infinity place together with the primes dividing N^-/p and let R be an Eichler $\mathbb{Z}$-order in $\mathcal{B}$ of level pN^+. Choose an identification

$$\iota_p : \mathcal{B} \otimes_{\mathbb{Q}} \mathbb{Q}_p \longrightarrow M_2(\mathbb{Q}_p).$$

Let $\Gamma^{(p)}_{N^-,N^+} \subset GL_2(\mathbb{Q}_p)$ be the image under ι_p of the group of units in R of reduced norm 1. In the remaining part of this section we will write Γ instead of $\Gamma^{(p)}_{N^-,N^+}$.

Let p be a fixed prime and let N be a square-free integer that factorizes as pN^-N^+ such that N^- has an odd number of prime factors. Such a factorization is called an *admissible factorization.*

We recall here some objects already defined in the function fields case, like the upper half plane, the Bruhat Tits tree, distributions, measures, etc. These concepts are necessary to define our p-adic integral.

Let $\mathbb{C}_p$ be a p-adic completion of an algebraic closure of $\mathbb{Q}_p$. As in Chapter 2, we define the p-adic upper half plane to be

$$\mathcal{H}_p := \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$$

with the action of $GL_2(\mathbb{Q}_p)$ by linear fractional transformations. Similarly as in Chapter 2, one has definitions of admissible covering by sets $\mathcal{A}_n$ and the space of rigid analytic functions on $\mathcal{H}_p$.

The group Γ acts on $\mathcal{H}_p$ with compact quotient $\Gamma\backslash\mathcal{H}_p$, which is equipped with the structure of a rigid analytic curve over $\mathbb{Q}_p$. It can be identified with an algebraic curve $X^{(p)}_{\Gamma_{N^-,N^+}}$ over $\mathbb{Q}_p$ (cf. [GvdP80]).

The Bruhat Tits tree $\mathcal{T}_p$ of $\mathrm{PGL}_2(\mathbb{Q}_p)$ is a connected $p+1$-regular tree with set of vertices $X(\mathcal{T}_p)$ defined as classes of homothety $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$. The set of edges $Y(\mathcal{T}_p)$ consists of pair of vertices (v_0, v_1) represented by lattices λ_1 and Λ_2 such that $p\Lambda_2 \subsetneq \Lambda_1 \subsetneq \Lambda_2$.

The corresponding identifications given by Propositions 2.4.1 and 2.4.3 are still valid for vertices and edges, respectively.

Let Γ be as above. A Γ-*invariant harmonic cocycle* with values in an abelian group B is a map $\varphi : X(\mathcal{T}_p) \longrightarrow B$ such that

1) $\varphi(\bar{e}) = -\varphi(e)$ for all $e \in Y(\mathcal{T}_p)$,
2) For all $v \in X(\mathcal{T}_p)$ we have $\sum_{t(e)=v} \varphi(e) = 0$,
3) $\varphi(\gamma e) = \varphi(e)$ for all $\gamma \in \Gamma$.

Definition 3.4.1. Let f be a rigid analytic function of $\mathcal{H}_p$ with values in $\mathbb{C}_p$, we say that f is a *rigid analytic modular form* of weigh k on $\Gamma \setminus \mathcal{H}_p$ if

$$f(\gamma\langle\tau\rangle) = (c\tau + d)^k f(\tau)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $\tau \in \mathcal{H}_p$.

The $\mathbb{C}_p$-vector space of rigid analytic modular forms of weight k with respect to Γ is denoted by $S_k(\Gamma)$.

Definition 3.4.2. (Distribution and measure) A *p-adic distribution* on $\mathbb{P}^1(\mathbb{Q}_p)$ is a finitely addictive $\mathbb{C}_p$-valued function μ on the compact open sets of $\mathbb{P}^1(\mathbb{Q}_p)$ satisfying $\mu(\mathbb{P}^1(\mathbb{Q}_p)) = 0$. If μ is p-adically bounded then it is called a *p-adic measure.* The space of all measures on $\mathbb{P}^1(\mathbb{Q}_p)$ is denoted by $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)$.

As in the case of function fields, we have an action of $GL_2(\mathbb{Q}_p)$ on the space of measures and on the space of harmonic cocycles (cf. §3.1.3 for the definition) and the corresponding identification between the space of measures on $\mathbb{P}^1(\mathbb{Q}_p)$ and the space of harmonic cocycles.

Let f be any continuous function on $\mathbb{P}^1(\mathbb{Q}_p)$ then we define the integral of f with respect to a measure μ on $\mathbb{P}^1(\mathbb{Q}_p)$ as

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} f(t)\, d\mu(t) = \varinjlim_{\alpha} \sum_{U \in \mathcal{C}_\alpha} f(u)\mu(U)$$

where the limit is taken over increasing fine covers $\{\mathcal{C}_\alpha\}_\alpha$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by disjoint open compact subsets U.

Denote by $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma$ the space of all Γ-invariant measures on $\mathbb{P}^1(\mathbb{Q}_p)$. There is a well known theorem due to Schneider and Teitelbaum that gives the following isomorphism (cf. [Dar04, Thm.5.9])

$$\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma \cong S_2(\Gamma).$$

We have that $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z})^\Gamma \subset \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma$ given by the $\mathbb{Z}$-valued harmonic cocycles. It thus, gives rise via the Scheneider-Teitelbaum isomorphism to an integral structure $S_2(\Gamma)^\mathbb{Z} \subset S_2(\Gamma)$, it plays a role somewhat similar to that of modular forms with integral Fourier coefficients in the theory of classical modular forms.

Fix an extension[1] $\log_p : \mathbb{C}_p^\times \longrightarrow \mathbb{C}$ of the p-adic logarithm to all $\mathbb{C}^\times$.

Definition 3.4.3. Let f be a rigid analytic modular form of weight two for Γ and μ_f be the measure attached to it by the Scheneider-Teitelbaum isomorphism. Fix $\tau_1, \tau_2 \in \mathcal{H}_p$. The p-adic line integral attached to $f(z)dz$ is defined to be

$$\int_{\tau_1}^{\tau_2} f(z)\, dz := \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log_p \left(\frac{t - \tau_2}{t - \tau_1} \right) \, d\mu_f(t). \tag{3.14}$$

If we formally exponentiate the expression (3.14) we get the multiplicative line integral

$$⨰_{\tau_1}^{\tau_2} f(z)\, d(z) = ⨰_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t - \tau_2}{t - \tau_1} \, d\mu_f(t). \tag{3.15}$$

This multiplicative integral is more canonical than its additive counterpart since it does not depend on a choice of a branch of the p-adic logarithm. In fact one should define the right hand side of (3.15) as in (3.1).

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, which admits an admissible factorization as N^-N^+ with p dividing N^- and let $\Gamma \subset SL_2(\mathbb{Q}_p)$ be the discrete subgroup arising from this factorization as explained above. The rigid variety $X^{(p)}_{\Gamma_{N^-,N^+}}$ and the curve $X_{\Gamma_{N^-,N^+}}$ are connected by the following theorem due to Cerednik and Drinfeld.

Theorem 3.4.4. *There is a canonical rigid analytic isomorphism*

$$CD : X^{(p)}_{\Gamma_{N^-,N^+}}(\mathbb{C}_p) \longrightarrow X_{\Gamma_{N^-,N^+}}(\mathbb{C}_p).$$

[1] By imposing $\log_p(wz) = \log_p(w) + \log_p(z)$ and setting $\log_p(p) = 0$.

The Cerednik-Drinfeld theorem together with the following isomorphisms ([GvdP80, Ch. VI and VIII])

$$\begin{gathered}\mathrm{Div}^0(\Gamma_{N^-,N^+} \setminus \mathcal{H}) \cong J_{N^-,N^+} \\ \mathrm{Div}^0(\Gamma^{(p)}_{N^-,N^+} \setminus \mathcal{H}_p) \cong J^{(p)}_{N^-,N^+},\end{gathered}$$

gives rise to a map $\mathrm{Div}^0(\Gamma^{(p)}_{N^-,N^+} \setminus \mathcal{H}_p) \longrightarrow J_{N^-,N^+}(\mathbb{C}_p)$ also denoted CD by abuse of notation.

On the other hand, we can use the multiplicative integral (3.14) to define a p-adic Abel-Jacobi map

$$\begin{aligned}\Phi_{AJ} : \mathrm{Div}^0(\Gamma^{(p)}_{N^-,N^+} \setminus \mathcal{H}_p) &\longrightarrow \mathrm{Hom}(S_2(\Gamma)^{\mathbb{Z}}, \mathbb{C}_p^\times) \simeq \mathbb{C}_p^\times \\ \tau_2 - \tau_1 &\longmapsto (f \mapsto \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} f(z)\, dz)).\end{aligned}$$

Let $\Phi_{\mathrm{Tate}} : \mathbb{C}_p^\times \longrightarrow E_q(\mathbb{C}_p)$ be the Tate parametrization of E (cf. [Sil94]). Assume that the curve E is a strong Weil curve, if not replace it by an isogenous curve. Then we have the following result

Proposition 3.4.5. *The following diagram commutes*

$$\begin{tikzcd}\mathrm{Div}^0(\Gamma^{(p)}_{N^-,N^+} \setminus \mathcal{H}_p) \arrow[r, "\Phi_{AJ}"] \arrow[d, "CD"] & \mathbb{C}_p^\times \arrow[d, "\Phi_{Tate}"] \\ J_{N^-,N^+}(\mathbb{C}_p) \arrow[r, "\Phi_N"] & E(\mathbb{C}_p).\end{tikzcd}$$

For a discussion of this result, see [BD98]. Compare with the diagram (3.11).

Following the ideas of Pollack and Stevens [PS11], Greenberg [Gre06] is able to give an algorithm, running in polynomial time, for evaluating the p-adic integral (3.15). In the remaining of this chapter, we will briefly describe the method devised by Greenberg.

Let

$$A_{\mathrm{rig}} := \left\{ v(x) = \sum_{n\geqslant 0} a_n x^n \;\middle|\; a_n \in \mathbb{Q}_q,\ a_n \to 0 \,\text{as}\, n \to \infty \right\}. \tag{3.16}$$

Elements of A_{rig} are rigid analytic functions on the closed unit disk in $\mathbb{C}_p$ which are defined over $\mathbb{Q}_p$.

Definition 3.4.6. A *rigid analytic distribution* μ is an element of the continuous dual of A_{rig}. The space of rigid analytic distributions is denoted by D_{rig}.

There is no problem in defining the distribution in this way since it "restricts" to a distribution as one of Definition 3.4.2 (cf. [Kob84, Ch. II, §3]).

Let $\mu \in D_{\text{rig}}$, $v \in A_{rig}$ and consider the integral $\int_{\mathbb{Z}_p} v(x)\, d\mu(x)$. According to [PS11] the problem to compute it reduces to the calculation of the moments

$$\mu(x^n) = \int_{\mathbb{Z}_p} x^n \, d\mu(x) \; n \geqslant 0.$$

Then we say that μ *is known to precision* $M \geqslant 1$ if $\int_{\mathbb{Z}_p} v(x)\, d\mu(x)$ is known modulo p^{M+1-n} for $n = 0, ..., M$.

Definition 3.4.7. A map $\Phi : \Gamma \setminus GL_2(\mathbb{Q}_p) \to D_{\text{rig}}$ that is $\mathcal{I}_p$-equivariant (for Iwahori $\mathcal{I}_p$ subgroup) under the right action is called a *overconvergent modular form for* Γ. The space of overconvergent modular forms for Γ is denoted by $\widetilde{M_2}(\Gamma)$.

In [PS11] Pollack and Stevens define a Hecke operator U_p on the space $\widetilde{M_2}(\Gamma)$. It is also proved there that its U_p^2-invariant subspace is Hecke-isomorphic to the space of rigid analytic modular forms for Γ. Then, given a rigid analytic modular form f with rational Hecke eigenvalues, one can find its corresponding $\mathbb{Z}$-valued harmonic cocycle φ_f and the measure μ_f with $U_p f = \pm f$ (cf. [Gre06, §5]). In order to calculate the moments attached to the distribution μ_f it is enough to calculate the values of the corresponding element $\Phi_f \in \widetilde{M_2}(\Gamma)$ which can be computed up to precision M from $\varphi_f \pmod p$ by iterating the operator U_p in time $O(M)$.

We come back now to the calculation of the p-adic line integral. Denote by

$$J(\tau_2, \tau_1) = \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t-\tau_2}{t-\tau_1}\, d\mu_f.$$

Under some technical hypothesis, it is enough to compute $\log J(\tau_2, \tau_1)$. Write

$$\log J(\tau_2,\tau_1) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_p)} \log J_a(\tau_2,\tau_1) \;\text{ where } J_a(\tau_2,\tau_1) = \times\!\!\!\!\!\!\int_{b_a} \frac{t-\tau_2}{t-\tau_1}\, d\mu_f \tag{3.17}$$

and b_a is the standard residue disk around a (cf. [Gre06, §8]) defined as

$$b_a := \{x \in \mathbb{Q}_p \;\mid\; |x-a| < 1/p\}.$$

Note that $b_a = U_e$ after identifying $\mathbb{P}^1(\mathbb{F}_p)$ with the edges with target v_0.

These $p+1$ integrals can be calculated in polynomial time by evaluating certain moments coming from the expansion of the function logarithm as a series (cf. [Gre06, Prop. 14]).

Remark 3.4.8. *The use of the logarithm to calculate the p-adic multiplicative line integral is crucial. We do not dispose of this function in the function field case and this is one of the main difficulties we have to overcome.*

Let N be an integer which admits a factorization N^-N^+ with a prime p dividing N^- and let f be a rigid analytic modular form for $\Gamma^{(p)}_{N^-,N^+}$ with rational Hecke eigenvalues. Define the set $\Lambda_f = \left\{ \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t-\gamma\tau_1}{t-\tau_1}\, d\mu_f \;\middle|\; \gamma \in \Gamma \right\}$, which is discrete in $\mathbb{C}_p^\times$. Set q_f as the generator of Λ_f. Then q_f is the Tate parameter attached to the form f.

As in the complex case one would like to have a procedure to find the elliptic curve E_f with coefficients in $\mathbb{Q}$. Even though Greenberg managed to calculate with good accuracy q_f, it is not clear whether one can compute from it an equation for the elliptic curve E_f with coefficients in $\mathbb{Q}$ as Cremona does.

4. The Algorithm

4.1 Motivation

Let φ be an automorphic (eigen) newform for the congruence subgroup $\Gamma_0(N)$ with rational Hecke eigenvalues. We saw in Chapter 2 that there exists an elliptic curve E_φ semistable at ∞ defined over $K = \mathbb{F}_q(T)$ with conductor $N\infty$. As in the cases of complex and p-adic uniformization (§§ 3.3 and 3.4), one would like to have a procedure that allows to calculate the elliptic curve E_φ by giving explicit equations over K.

Over the complex numbers (cf. §3.3) we saw that there exists an efficient algorithm that allows to calculate the Tate parameter and the periods with high accuracy and therefore the calculation of the equations of the corresponding elliptic curve over $\mathbb{Q}$ (cf. [Cre97]). In the p-adic case, although Greenberg ([Gre06]) devised an algorithm to calculated the Tate parameter from the corresponding automorphic form by means of certain multiplicative integral, it seems not known if one can compute from the Tate parameter an equation for the corresponding elliptic curve.

In the function field case, to find the Tate parameter we need to calculate the multiplicative integral (3.9). The problem of computing such integral up to an accuracy of M digits of exact precision is a priori of exponential complexity. In this work we follow the ideas of Darmon and Pollack ([DP06]) and Greenberg ([Gre06]) to develop an algorithm that allows us to calculate the Tate parameter up to a given accuracy in polynomial time. In their algorithm we have to replace the use of the logarithm by a different method, which leads us to compute several integrals of the form

$$\times\!\!\!\!\!\!\int_{O_\infty} (1+at)\, d\mu_\varphi(t) \tag{4.1}$$

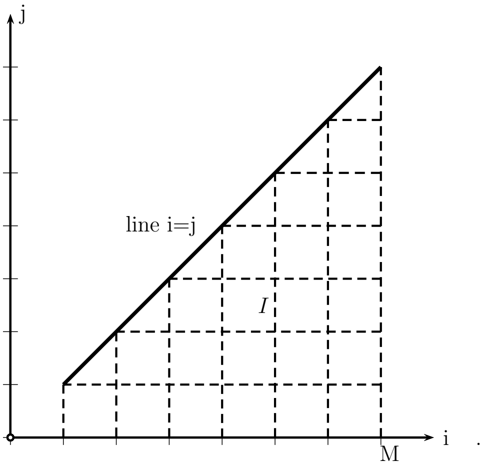
for $a \in \pi\mathbb{F}_{q^2}[[t]]$. We calculate this integral by iterating a certain Hecke operator as in Greenberg's work.

In this chapter we will define the functions to be integrated, the above mentioned Hecke operator, its properties and the algorithm that allows us to calculate the integral (3.9) up to a priori given accuracy M.

In the function field case the coefficients of the Tate curve are not rational in general, as in the complex case, however using some tools from the reduction of modular forms modulo p and appropriate models for the elliptic curves, we manage to find equations for E_φ over K – this is done in the next chapter.

4.2 Elementary functions

Let I be the subset of $\mathbb{N} \times \mathbb{N}_0$ given by $I := \{(i, j) \in \mathbb{N} \times \mathbb{N}_0 | j \leq i\}$. Graphically, the elements of I are the points with integral coordinates in the encircled area in



This set I has the properties:

- I is closed under coordinate-wise addition; we denote this by $I + I \subset I$.
- For any $(i_0, j_0) \in I$, the set I contains the set

$$I_{(i_0,j_0)} := \{(i^{'}, j^{'})|\, i^{'} \geq i_0, j^{'} \leq j_0 + i^{'} - i_0\}. \tag{4.2}$$

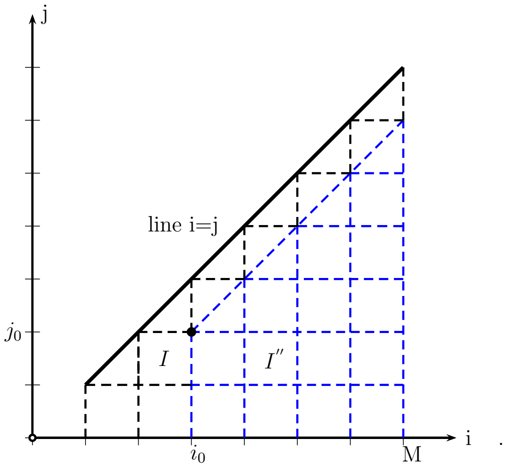


Figure 4.1: The set I''

One associates to I the set

$$\mathfrak{F}_I := \left\{ 1 + \sum_{(i,j)\in I} a_{ij}\pi^i t^j \mid a_{ij} \in \mathbb{F}_{q^2} \right\}. \tag{4.3}$$

Elements of $\mathfrak{F}_I$ are called *elementary functions* in t. We may consider its elements as those of the group $(1 + \pi\mathbb{F}_{q^2}[[\pi, t]], \times)$ for which each term has the π-power bigger or equal than the t-power.

Lemma 4.2.1. *The subset $\mathfrak{F}_I$ of $(1 + \pi\mathbb{F}_{q^2}[[\pi, t]], \times)$ is a subgroup.*

Proof. We need to check that if $f, g \in \mathfrak{F}_I$, $fg \in \mathfrak{F}_I$ and $g^{-1} \in \mathfrak{F}_I$.

For the first statement, consider $f = 1 + \sum_{(i,j)\in I} a_{ij}\pi^i t^j$ and $g = 1 + \sum_{(k,l)\in I} b_{kl}\pi^k t^l$ with a_{ij} and $b_{kl} \in \mathbb{F}_{q^2}$. From the multiplication of series

$$fg = 1 + \sum_{(r,s)\in\mathbb{N}\times\mathbb{N}_0} \left(\sum_{\substack{(i,j)\in I,\ (k,l)\in I, \\ i+k=r,\ \ j+l=s}} a_{ij}b_{kl} \right) \pi^r t^s + \sum_{(i,j)\in I} a_{ij}\pi^i t^j + \sum_{(k,l)\in I} b_{kl}\pi^k t^l$$

and since $I + I \subset I$ we have that $(r, s) \in I$ and then $fg \in \mathfrak{F}_I$ follows.

For the second statement, we have that g is invertible in $1+\pi\mathbb{F}_{q^2}[[\pi, t]]$. We need to check that $g^{-1} \in \mathcal{F}_I$. Let $g^{-1} = 1 + \sum_{(i,j)\in\mathbb{N}\times\mathbb{N}_0} c_{ij}\pi^i t^j$, then $gg^{-1} = 1$ implies

$$\sum_{(k,l)\in I} b_{kl}\pi^k t^l + \sum_{(i,j)\in\mathbb{N}\times\mathbb{N}_0} c_{ij}\pi^i t^j + \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N}_0,\ (k,l)\in I,\\ i+k=r,\quad j+l=s}} c_{ij} b_{kl}\pi^r t^s = 0. \tag{4.4}$$

Consider the set $\mathcal{E} := \{(i,j) \in \mathbb{N}\times\mathbb{N}_0 \setminus I \mid c_{ij} \neq 0\}$.

We claim $\mathcal{E}$ to be empty. If it were not empty, as $\mathcal{E} \subset \mathbb{N}\times\mathbb{N}_0$ has a lexicographic total order, then there exists a $(i_0, j_0) \in \mathcal{E}$ minimal. From the equation (4.4) the coefficient of $\pi^{i_0}t^{j_0}$ is 0 and from the left hand side this is

$$c_{i_0j_0} + \sum_{\substack{(m,n)\in\mathbb{N}\times\mathbb{N}_0,\ (k,l)\in I,\\ m+k=i_0,\quad n+l=j_0}} b_{kl}c_{mn} = 0. \tag{4.5}$$

If some $c_{mn} \neq 0$, then since $k \geqslant 1$, $m < i_0$ which implies that $(m,n) \in \mathcal{E}$, and contradicts the minimality of (i_0, j_0). Hence (4.5) becomes $c_{i_0j_0}$ and so $(i_0, j_0) \notin \mathcal{E}$ which is a contradiction.

□

Now define

$$\Gamma_0(\infty) := \left\{\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in M_2(O_\infty) \middle| \; c \equiv 0 \,(\mathrm{mod}\ \ \pi)\ , d \in O_\infty^\times \text{ and } \det(\gamma) \in O_\infty \setminus \{0\}\right\}.$$

Note that $\Gamma_0(\infty)$ is not the Iwahori subgroup, it was defined to contain at least the Iwahori subgroup and matrices of the form $\left(\begin{smallmatrix}\pi & a\\ 0 & 1\end{smallmatrix}\right)$. However, $\Gamma_0(\infty)$ is a semigroup since it is closed under the usual multiplication. Namely, let

$$\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix}, \quad \gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1\end{pmatrix} \in \Gamma_0(\infty) \quad \text{and} \quad \gamma\gamma_1 = \begin{pmatrix} aa_1 + cc_1 & ab_1 + bd_1 \\ ca_1 + dc_1 & cb_1 + dd_1\end{pmatrix}$$

then $ca_1 + dc_1 \equiv 0 \pmod{\pi}$ since $c \equiv 0$, $c_1 \equiv 0 \pmod{\pi}$. Also $\det(\gamma\gamma_1) \in O_\infty \setminus \{0\}$. It remains to prove that $cb_1 + dd_1 \in O_\infty^\times$ which is equivalent to $\mathrm{val}(cb_1 + dd_1) = 0$ where $\mathrm{val} = v_{1/T}$. From the properties of the valuation one sees that

$$\mathrm{val}(cb_1 + dd_1) \geq \inf\{\mathrm{val}(cb_1), \mathrm{val}(dd_1)\}$$

but $\mathrm{val}(dd_1) = 0$ and $\mathrm{val}(cb_1) \geq 1$, therefore $\mathrm{val}(cb_1 + dd_1) = 0$ which implies $\gamma\gamma_1 \in \Gamma_0(\infty)$ as desired.

The group $\mathcal{F}_I$ is equipped with a left action of $\Gamma_0(\infty)$ defined by

$$(\kappa * f)(t) := f(\kappa^{-1}\langle t\rangle) \quad \text{for } \kappa \in \Gamma_0(\infty) \text{ and } f \in \mathcal{F}_I \tag{4.6}$$

where $\langle\cdot\rangle$ is the usual Moebious trasnformation.

Lemma 4.2.2. *The action defined in (4.6) is well defined.*

Proof. We need to check that for $f \in \mathcal{F}_I$ and $\kappa \in \Gamma_0(\infty)$ we have $(\kappa * f) \in \mathcal{F}_I$.

Set $f = 1 + \sum_{(i,j)\in I} a_{ij}\pi^i t^j$ and $\kappa^{-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then from the definition of the action we have $(\kappa * f)(t) = 1 + \sum_{(i,j)\in I} a_{ij}\pi^i \left(\frac{at+b}{ct+d}\right)^j$. So $(\kappa * f)(t) \in \mathcal{F}_I$ if and only if for each term $\pi^i \left(\frac{at+b}{ct+d}\right)^j$ the exponents $(i,j) \in I$. Hence it is enough to check it for $\pi^i t^j$, $(i,j) \in I$.

First it is convenient to write

$$\begin{aligned} \frac{at+b}{ct+d} &= (at+b)\frac{1}{d\left(1 - (\frac{-c}{d})t\right)} \\ &= (a't+b')\frac{1}{1-\pi c't} \end{aligned}$$

where $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ and $c' = \frac{c}{\pi d}$.

Therefore

$$\begin{aligned} \pi^i\left(\frac{at+b}{ct+d}\right)^j &= \pi^i(a't+b')^j(1-\pi c't)^{-j} \\ &= \pi^i(a't+b')^j\sum_{n=0}^{\infty}(-c')^n\binom{-j}{n}(\pi t)^n \\ &= (a't+b')^j\sum_{n=0}^{\infty}(-c')^n\binom{-j}{n}\pi^{i+n}t^n \\ &= \sum_{k=0}^{j}\binom{j}{k}(a't)^k(b')^{j-k}\sum_{n=0}^{\infty}(-c')^n\binom{-i}{n}\pi^{i+n}t^k \\ &= \sum_{n=0}^{\infty}(-c')^n\binom{j}{n}\pi^{i+n}t^n\left(\sum_{k=0}^{j}\binom{j}{k}(a')^k t^k(b')^{j-k}\right) \\ &= \sum_{n=0}^{\infty}(-c')^n\binom{j}{n}\pi^{i+n}\left(\sum_{k=0}^{j}(a')^k t^{k+n}(b')^{j-k}\right) \end{aligned}$$

$$= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{j} (a')^k (b')^{j-k} (-c')^n \binom{j}{n} \right) \pi^{i+n} t^{k+n},$$

finally if we take $i' = i + n$ and $j' = k + n$ we get the conditions given for the set I'' and the lemma holds. □

Remark 4.2.3. *One can define $\mathcal{F}_I$ for arbitrary subsets $I \subset \mathbb{N} \times \mathbb{N}_0$. It is a group whenever $I + I \subset I$ and is stable under the action of $\Gamma_0(\infty)$ if $I \subset I''$.*

4.3 A Hecke operator

Fix a positive integer M. We want to compute the integral (4.1) to a precision π^M.
For a fixed $k \leq M$ we define the multiplicative group

$$U_{k,M} := \left(\frac{1 + \pi^k \mathbb{F}_{q^2}[[\pi]]}{1 + \pi^{M+1} \mathbb{F}_{q^2}[[\pi]]} \right).$$

Note that if $k' \leq k$ then $U_{k',M} \supset U_{k,M}$.

An important and crucial property of $\mathcal{F}_I$ is the following, which will be proved in the Appendix 7.

Lemma 4.3.1. *Given any function $f \in \mathcal{F}_I$ and any integer $M \geqslant 1$, then there exists a finite set of indices $J \subseteq I$ and $m_{ij\delta} \in \{1, 2, ..., p-1\}$ such that*

$$f \equiv \prod_{(i,j) \in J} (1 + \xi^\delta \pi^i t^j)^{m_{ij\delta}} \pmod{\pi^{M+1}}$$

where $\xi \in \mathbb{F}_{q^2}$ is a primitive element for the extension over $\mathbb{F}_p$, $\delta \in \{0, ..., d-1\}$ with d the degree of the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$. The representation is unique modulo p powers of $f_{ij} = 1 + \pi^i t^j$, so the set

$$\mathcal{B}_M := \{1 + \xi^\delta \pi^i t^j \; |(i,j) \in \mathcal{F}_I, i \leq M, \; \delta = 0, ..., d-1\}.$$

is a multiplicative pseudo basis.

Lemma 4.3.1 says that the representation is unique modulo p powers of $f_{ij} = 1 + \pi^i t^j$, this means that if f_{ij} is a factor of a function f with $p | \gcd(i,j)$, then the p-th roots of f_{ij} are in $\mathcal{B}_M$ and they give "other" representation of f.

Remark 4.3.2. *Let now $f_{ij} = 1 + \xi^\delta \pi^i t^j \in \mathfrak{B}_M$. From the definition of the integral*

$$\mathop{\times\!\!\!\!\!\!\int}_{O_\infty} (1 + \xi^\delta \pi^i t^j)\, d\mu \pmod{\pi^{M+1}} = \varinjlim_{l} \prod_{t_l \in U_l \subset O_\infty} (1 + \xi^\delta \pi^i t_l^j)^{\mu(U_l)} \pmod{\pi^{M+1}},$$

we can interchange modulo with the integral since the powers in the product do not decrease, in particular the integral is continuous with respect to the π-adic topology. We obtain that $\mathop{\times\!\!\!\!\!\!\int}_{O_\infty} (1 + \xi^\delta \pi^i t^j)\, d\mu \pmod{\pi^{M+1}} \in U_{i,M}$.

This leads us to define the following sets. For an integer $k > 1$ we consider

$$I_k := \{(i,j) \in \mathbb{N} \times \mathbb{N}_0 | i \geq k\}.$$

Note that by Remark 4.2.3 the set $\mathfrak{F}_{I \cap I_k}$ is a group, moreover it is a subgroup of $\mathfrak{F}_I$.

Remark 4.3.3. *As in Lemma 4.2.2 one proves that $\kappa * \mathfrak{F}_{I \cap I_k} \subset \mathfrak{F}_{I \cap I_k}$ for all $\kappa \in \Gamma_0(\infty)$.*

Let us define also the set

$$\operatorname{Hom}'(\mathfrak{F}_I, U_{1,M}) := \left\{ \begin{array}{c|l} F : \mathfrak{F}_I \longrightarrow U_{1,M} & F \textit{ is a group homomorphism} \\ & \\ & \textit{s.t. } F(\mathfrak{F}_{I \cap I_k}) \subseteq U_{k,M}, \text{ for all } k \geq 1 \end{array} \right\}.$$

It is worth pointing out that the condition on F only makes sense for $k \leq M$ and $F(\mathfrak{F}_{I \cap I_k}) \subseteq U_{k,M}$ means that we evaluate in elements $f \in \mathfrak{F}_I$ such that $\operatorname{val}(f - 1) \geq k$ and its image under F has the property $\operatorname{val}(F(f) - 1) \geq k$. Since the group $\mathfrak{J}$ acts on $\mathfrak{F}_I$ by Moebius transformations and on $U_{k,M}$ trivially, we may also define a left action of $\mathfrak{J}$ on $\operatorname{Hom}'(\mathfrak{F}_I, U_{1,M})$ by

$$(\kappa * F)(f) := F(\kappa^{-1} * f) \text{ for } \kappa \in \mathfrak{J} \text{ and } f \in \mathfrak{F}_I.$$

Lemma 4.3.4. *The previous action is well defined.*

Proof. Let κ_1 and $\kappa_2 \in \mathfrak{J}$ then we have that

$$\begin{aligned} ((\kappa_1 \kappa_2) * F)(f) &= F((\kappa_2^{-1} \kappa_1^{-1}) * f) \\ &= F((\kappa_2^{-1} * (\kappa_1^{-1} * f)) \\ &= (\kappa_2 * F)(\kappa_1^{-1} * f) \\ &= \kappa_1 * (\kappa_2 * F)(f). \end{aligned}$$

Also, using Remark 4.3.3, κ maps $\operatorname{Hom}'(\mathfrak{F}_I, U_{1,M})$ to itself. And so the lemma holds. □

Let Γ be a congruence subgroup of $PGL_2(K_\infty)$. Unless otherwise stated we will take Γ to be $\Gamma_0(N)$ for some non zero ideal $N \subset \mathbb{F}_q[T]$ and define the set

$$\mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_I, U_{1,M})) := \left\{ \phi : \Gamma \setminus PGL_2(K_\infty) \longrightarrow Hom^{'}(\mathcal{F}_I, U_{1,M}) \;\middle|\; \phi \text{ is } \mathcal{J}\text{-equivariant} \right\}. \tag{4.7}$$

For simplicity of notation we will denote this set by $\mathcal{S}$. The $\mathcal{J}$-equivariance means that for any $\gamma \in PGL_2(K_\infty)$ and $\kappa \in \mathcal{J}$, we have

$$\phi(\Gamma\gamma\kappa)(f)(t) = \phi(\Gamma\gamma)(\kappa * f)(t).$$

Writing $(\kappa \star \phi)(\Gamma\gamma) := \phi(\Gamma\gamma\kappa)$, we can also see $\mathcal{J}$-equivariance as

$$(\kappa \star \phi)(\Gamma\gamma)(f) = \phi(\Gamma\gamma)(\kappa * f).$$

Remark 4.3.5. *a) From Chapter 3 we have that the group $GL_2(K_\infty)$ acts on the space $\mathcal{M}_0(X, \mathbb{Z})$ so the integral $\oint_{O_\infty} f \; d(\gamma^{-1} * \mu)$ makes sense for any $\gamma \in GL_2(K_\infty)$ and $f \in \mathcal{F}_I$.*

b) The integral $\oint_{O_\infty} f \; d(\gamma^{-1} * \mu) \pmod{\pi^{M+1}}$ lies in $Hom^{'}(\mathcal{F}_I, U_{1,M})$ (cf. 4.3.2) then the map $\gamma \mapsto \oint_{O_\infty} \_d(\gamma^{-1} * \mu) \pmod{\pi^{M+1}}$ is in $\mathcal{S}$, so $\mathcal{S}$ is not empty.

c) From the $\mathcal{J}$-equivariance we have that any $F \in \mathcal{S}$ is uniquely determined by its values on any set of representatives (a "fundamental domain") of the double class $\Gamma \setminus PGL_2(K_\infty)/\mathcal{J}$, which is in canonical bijection with the edges of the quotient tree $\Gamma \setminus \mathcal{T}$.

From now on we write $\phi(\gamma)$ instead of $\phi(\Gamma\gamma)$.

The set $\mathcal{S}$ is endowed with an action of the Hecke operator

$$\left(U_\infty \phi\right)(\gamma)(f(t)) := \prod_{a \in \mathbb{F}_q} \phi\left(\gamma \begin{pmatrix} \pi & a \\ 0 & 1 \end{pmatrix}\right) f(\pi t + a)$$

for $f \in \mathcal{F}_I$ and $\gamma \in \Gamma \setminus PGL_2(K_\infty)$.

Lemma 4.3.6. *The Hecke operator U_∞ is well defined.*

Proof. We define $\tau_a = \left(\begin{smallmatrix} \pi & a \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in \mathbb{F}_q$. Then for all $a \in \mathbb{F}_q$ we have $\mathcal{I}\tau_a\mathcal{I} = \coprod_{a' \in \mathbb{F}_q} \tau_{a'}\mathcal{I}$, so that for each $a \in \mathbb{F}_q$ and $\kappa \in \mathcal{I}$ we can find unique $a' \in \mathbb{F}_q$ and $\kappa' \in \mathcal{I}$ such that $\kappa\tau_a = \tau_{a'}\kappa'$. Moreover for κ fixed and a variable, the map $a' \longmapsto a$ is a bijection of $\mathbb{F}_q$.

Let $\phi \in \mathcal{S}$, we need to check that $U_\infty\phi$ is in $\mathcal{S}$, *i.e.*, $U_\infty\phi$ is $\mathcal{I}$-equivariant. Let $\gamma \in \Gamma \setminus PGL_2(K_\infty)$, $f \in \mathcal{F}_I$ and $\kappa \in \mathcal{I}$. Then applying the U_∞ operator and using that ϕ is $\mathcal{I}$-equivariant we get

$$\begin{aligned}
(\kappa \star U_\infty\phi)(\gamma)(f) &= (U_\infty\phi)(\gamma\kappa)(f) \\
&= \prod_{a \in \mathbb{F}_q} \phi(\gamma\kappa\tau_a) f(\tau_a\langle t\rangle) \\
&= \prod_{a \in \mathbb{F}_q} \phi(\gamma\tau_{a'}\kappa') f(\tau_a\langle t\rangle) \\
&= \prod_{a \in \mathbb{F}_q} \phi(\gamma\tau_{a'}) f(\tau_a{\kappa'}^{-1}\langle t\rangle) \\
&= \prod_{a \in \mathbb{F}_q} \phi(\gamma\tau_{a'}) f(\kappa^{-1}\tau_{a'}\langle t\rangle) \\
&= \prod_{a' \in \mathbb{F}_q} \phi(\gamma\tau_{a'}) (\kappa * f)(\tau_{a'}\langle t\rangle) \\
&= (U_\infty\phi)(\gamma)(\kappa * f).
\end{aligned}$$

□

We recall that any Γ-invariant harmonic cocycle φ gives rise to a measure μ_φ on $\mathcal{M}_0(\mathbb{P}^1(O_\infty), \mathbb{Z})^\Gamma$ and conversely φ can be recovered from such a measure μ. From now on we will denote by μ_φ the measure associated to $\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$.

We have the following map

$$\begin{array}{ccc}
\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma & \longrightarrow & \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_I, U_{1,M})) \\
\varphi & \longmapsto & \Phi_{\mu_\varphi}
\end{array}$$

defined by $\Phi_{\mu_\varphi}(\gamma) := \times\!\!\!\!\!\!\int_{O_\infty} \_\, d(\gamma^{-1} * \mu)$.

Lemma 4.3.7. *The map Φ_{μ_φ} defined above is $\mathcal{I}$-equivariant.*

Proof. The map Φ_{μ_φ} is well defined since it defines an homomorphism $\mathcal{F}_I \to U_{1,M}$ (cf. Remark 4.3.5 b)), then Φ_{μ_φ} lies in $Hom^{'}$.

Let $\gamma \in \Gamma \setminus PGL_2(K_\infty)$, $f \in \mathcal{F}_I$ and $\kappa \in \mathcal{I}$. We need to check the equality

$$\Phi_{\mu_\varphi}(\gamma\kappa)(f) = \Phi_{\mu_\varphi}(\gamma)(\kappa * f). \tag{4.8}$$

By the definition of the map and the change of variables formula we have

$$\begin{aligned}
\Phi_{\mu_\varphi}(\gamma\kappa)(f) &= \times\!\!\!\!\!\!\int_{O_\infty} f(t)\, d((\gamma\kappa)^{-1} * \mu)(t)\\
&= \times\!\!\!\!\!\!\int_{\kappa^{-1}(\kappa O_\infty)} \kappa^{-1} * (\kappa * f)(t)\, d(\kappa^{-1} * (\gamma^{-1} * \mu))(t)\\
&= \times\!\!\!\!\!\!\int_{\kappa O_\infty} (\kappa * f)(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \times\!\!\!\!\!\!\int_{O_\infty} (\kappa * f)(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \Phi_{\mu_\varphi}(\gamma)(\kappa * f).
\end{aligned}$$

In the fourth equality we use the fact that $\kappa O_\infty = O_\infty$, it can be seen from the identification of the open O_∞ with the ends passing trough the edge e_0 and the Iwahori subgroup stabilizes the lattice class corresponding to e_0. □

A crucial property of the function Φ_{μ_φ} is that it is an eigenfunction of the Hecke operator.

Proposition 4.3.8. *The functions Φ_{μ_φ} are eigenfunctions of U_∞ with eigenvalues* 1, *i.e.* $U_\infty \Phi_{\mu_\varphi} = \Phi_{\mu_\varphi}$.

Proof. Let f be a function on $\mathcal{F}_I$ and Φ_{μ_φ} as defined above. Then by definition of U_∞ we have

$$\begin{aligned}
(U_\infty \Phi_{\mu_\varphi})(f) &= \prod_{a \in \mathbb{F}_q} \Phi_{\mu_\varphi}(\gamma\tau_a)(\tau_a^{-1} * f)\\
&= \prod_{a \in \mathbb{F}_q} \times\!\!\!\!\!\!\int_{O_\infty} f(\tau_a\langle t\rangle)\, d((\gamma\tau_a)^{-1} * \mu)(t)\\
&= \prod_{a \in \mathbb{F}_q} \times\!\!\!\!\!\!\int_{\tau_a^{-1}(\tau_a O_\infty)} (\tau_a^{-1} * f)(t)\, d(\tau_a^{-1} * \gamma^{-1} * \mu)(t)\\
&= \prod_{a \in \mathbb{F}_q} \times\!\!\!\!\!\!\int_{\tau_a(O_\infty)} f(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \prod_{a \in \mathbb{F}_q} \times\!\!\!\!\!\!\int_{a + \pi O_\infty} f(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \times\!\!\!\!\!\!\int_{\dot\bigcup_{a \in \mathbb{F}_q}(a + \pi O_\infty)} f(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \times\!\!\!\!\!\!\int_{O_\infty} f(t)\, d(\gamma^{-1} * \mu)(t)\\
&= \Phi_{\mu_\varphi}(f).
\end{aligned}$$

□

The important thing to note here is that the set $1+\pi\mathbb{F}_{q^2}[[\pi]]$ can be seeing as the subset $\mathcal{F}_{I_0}$ of $\mathcal{F}_I$ for $I_0 := \mathbb{N}\times\{0\}$. The set $\mathcal{F}_{I_0}$ is preserved under the action of $\mathcal{J}$ since the action is trivial. Given any $f \in Hom^{'}(\mathcal{F}_I, U_{1,M})$ we may restrict it to $\mathcal{F}_{I_0}$ and therefore induce a restriction map

$$\begin{aligned} Hom^{'}(\mathcal{F}_I, U_{1,M}) &\xrightarrow{\text{res}} Hom^{'}(\mathcal{F}_{I_0}, U_{1,M}) \\ f &\longmapsto f|_{\mathcal{F}_{I_0}}. \end{aligned}$$

This map induces naturally another restriction map res^*, which by abuse of notation will be also denoted by res, between the following spaces

$$\mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_I, U_{1,M})) \xrightarrow{\text{res}} \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_{I_0}, U_{1,M})).$$

Finally consider the map Φ_{0,μ_φ} defined as follows

$$\begin{array}{ccc} \varphi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma & \longrightarrow & \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_{I_0}, U_{1,M})) \\ \varphi & \longmapsto & \Phi_{0,\mu_\varphi}\ , \end{array}$$

where $\Phi_{0,\mu_\varphi}(\gamma)(f) := f^{(\gamma^{-1}*\mu_\varphi)(O_\infty)} \mod \pi^{M+1}$, for $f \in \mathcal{F}_{I_0}$.

The map is well defined since $f \in \mathcal{F}_{I_0}$ is constant, and then its integral is actually $f^{\gamma^{-1}*\mu_\varphi(O_\infty)} = f^{\varphi(\gamma e_0)}$, where e_0 is the standard edge.

These considerations lead us to

Lemma 4.3.9. *The following diagram is commutative.*

$$\begin{tikzcd} \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma \arrow[d, "\Phi_{\mu *}"'] \arrow[dr, "\Phi_{0,\mu *}"] & \\ \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_I, U_{1,M})) \arrow[r, "\text{res}"] & \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_{I_0}, U_{1,M})). \end{tikzcd}$$

Proof. The proof is straightforward. We need to check that $\text{res}\circ\Phi_{\mu_\varphi} = \Phi_{0,\mu_\varphi}$ holds for all $\varphi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$.

In order to calculate $\text{res}\circ\Phi_{\mu_\varphi}$, we need to evaluate $⨍_{O_\infty} f\ d(\gamma^{-1}*\mu)(t)$ for $f \in \mathcal{F}_{I_0}$ and since f is constant

$$⨍_{O_\infty} f\ d(\gamma^{-1}*\mu)(t) = f^{(\gamma^{-1}*\mu)(O_\infty)}.$$

Taking modulo π^{M+1} this is precisely $\Phi_{0,\mu_\varphi}(f)$. □

Now, we are ready to describe the algorithm that allows us to calculate the integral $\oint_{O_\infty} f\, d\mu(t)$ for $f \in \mathcal{F}_I$.

Suppose that we have $\phi \in \mathcal{S}(\Gamma, Hom^{'}(\mathcal{F}_I, U_{1,M}))$ such that it is an eigenfunction for the Hecke operator U_∞ with eigenvalue 1 and also that $\mathrm{res} \circ \phi = \phi_0$ (one candidate for ϕ is Φ_{μ_φ} for some Γ-invariant harmonic cocycle φ) and we want to evaluate ϕ at $1 + \xi^\delta \pi^M t^j \in \mathcal{B}_M$. Then for any $\gamma \in \Gamma$ we have

$$\begin{aligned}(U_\infty \phi)\,(\gamma)(1 + \xi^\delta \pi^M t^j) &= \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a)(1 + \xi^\delta \pi^M (a + \pi t)^j) \\ &= \prod_{a \in \mathbb{F}_q} \phi_0(\gamma \tau_a)(1 + \pi^M \xi^\delta a^j). \end{aligned} \tag{4.9}$$

In particular, when ϕ is Φ_{μ_φ} the last product equals

$$\prod_{a \in \mathbb{F}_q} (1 + \pi^M \xi^\delta a^j)^{\varphi(\gamma \tau_a e_0))}.$$

We compute now

$$\begin{aligned} U_\infty(\phi)(\gamma)(1 + \xi^\delta \pi^{M-1} t^j) &= \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a) \left(1 + \xi^\delta \pi^{M-1} (a + \pi t)^j\right) \\ &= \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a) \left(1 + \xi^\delta \pi^{M-1} \sum_{n=0}^{j} \binom{j}{n} (\pi t)^n a^{j-n}\right) \\ &= \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a) \left(1 + \xi^\delta \pi^{M-1} (a^j + j \pi t a^{j-1} + \ldots + \pi^j t^j)\right). \\ &= \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a) \left((1 + \xi^\delta \pi^{M-1} a^j)(1 + \xi^\delta j a^{j-1} \pi^M t)(1 + O(\pi^{M+1}))\right). \end{aligned}$$

From the previous calculation we see that the value of $\phi(\gamma \tau_a)(1 + \xi^\delta \pi^{M-1} a^j)$ is easy to calculate since it does not depend on t. The calculation of the value of $\phi(\gamma \tau_a)(1 + \xi^\delta \pi^M a^{j-1} j t)$ reduces hence to the previous case (4.9). The above method can be continued inductively.

Summarizing, given any function $f \in \mathcal{F}_I$, $M \geqslant 1$ and $\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma$, to calculate the integral $\oint_{O_\infty} f\, d\mu_\varphi$ up to accuracy of M digits of exact precision, we decompose f as

$$f \equiv \prod_{f_{ij} \in \mathcal{B}_M} f_{ij}^{m_{ij}} \pmod{\pi^{M+1}}$$

where $f_{ij} = 1 + \xi^\delta \pi^i t^j$.

So it is enough to know the value of the integral at the functions f_{ij}, that is the value of $\Phi_{\mu_\varphi}(\gamma)(f_{ij})$ for all $f_{ij} \in \mathcal{B}_M$ and all $\gamma \in \Gamma \setminus PGL_2(K_\infty)$. By Remark 4.3.5 we only need to calculate this value for each $f_{ij} \in \mathcal{B}_M$ and finitely many. Hence as a first step, we produce tables with all the values for $\Phi_{\mu_\varphi}(\gamma)(f_{ij})$. In the following lines we describe the algorithm which computes such table.

Let us define an order relation on $\mathcal{B}_M$. We say that $1+\xi^\delta\pi^i t^j \geqslant 1+\xi^{\delta'}\pi^{i'}t^{j'}$ if and only if their exponents satisfy one of the following two conditions:

1) If $j > 0$ and $j' > 0$

   1.1) $i < i'$ or

   1.2) $(i = i'$ and $j < j')$ or

   1.3) $(i = i'$ and $j = j'$ and $\delta' \leqslant \delta)$.

2) If $j' = 0$

   2.1) $j > 0$ or

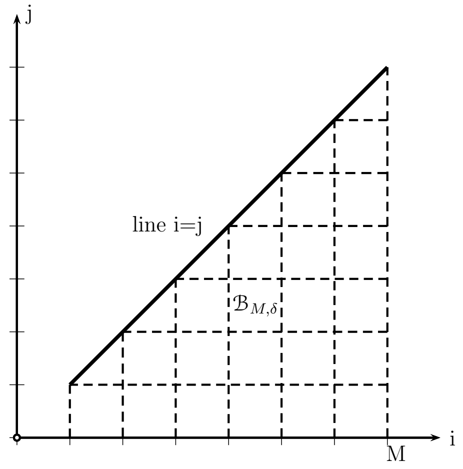
   2.2) $(j = 0$ and $i < i')$ or

   2.3) $(j = 0$ and $i = i'$ and $\delta \leqslant \delta')$.

Note that we can induce a partition of the set $\mathcal{B}_M$ in the following way. For a fixed δ we define the following subset of $\mathcal{B}_M$

$$\mathcal{B}_{M,\delta} := \{f \in \mathcal{B}_M \mid f = 1+\xi^\delta\pi^i t^j\} \tag{4.10}$$

Clearly $\mathcal{B}_M = \dot{\bigcup}_{\delta\in\{0,\dots,d-1\}}\mathcal{B}_{M,\delta}$. Note also that we can identify the elements of $\mathcal{B}_{M,\delta}$ with the points with integer coordinates of the graph



We will see later how to use this representation to explain the algorithm.

From the definition of the operator U_∞, given a representative γ of a class in $\Gamma\backslash PGL_2(K_\infty)/\mathcal{I}$, if e is the edge in $\mathcal{T}$ corresponding to $[\gamma]_1$, we have that $\gamma\tau_a$ represents all the edges in $\mathcal{T}$ with terminal $o(e)$.

Remark 4.3.10. *For γ and e as above we have that the classes of $\gamma\tau_a$ for $a \in \mathbb{F}_q$ in the quotient graph are identified, so we do not need to calculate the integral q times.*

If we apply the operator M times, then we move in the tree $\mathcal{T}$ distance M from the starting edge. So we need representatives for the quotient tree up to level M. Let us denote by $\mathcal{R}$ such a set of representatives.

For each $\gamma \in \mathcal{R}$ we need to calculate the integral $\Phi_{\mu_\varphi}(\gamma)(f_{ij})$ for all $f \in \mathcal{B}_M$. To each γ we attach d "triangular matrices" $\mathbb{T}_{\gamma,\delta}$ whose entries are the values of the integral at all functions f of $\mathcal{B}_{M,\delta}$, that is $\mathbb{T}_{\gamma,\delta}[i,j] = \Phi_{\mu_\varphi}(\gamma)(1+\xi^\delta\pi^i t^j)$.

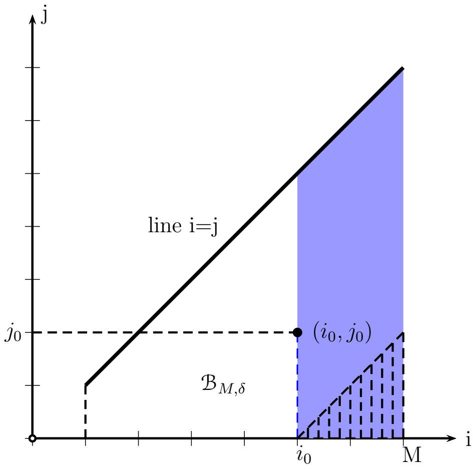
Observe that the constants corresponds to the points located over the i-axis of the graphic representation of $\mathcal{B}_{M,\delta}$. We start by filling the tables $\mathbb{T}_{\gamma,\delta}$ with the value $\Phi_{\mu_\varphi}(\gamma)(f)$ for $f \in \mathcal{B}_{M,\delta}$ constant for all $\delta \in \{0, 1, ..., d-1\}$.

First for $\gamma \in \mathcal{R}$ we calculate the value $\varphi(\gamma e_0)$ and then $\Phi_{\mu_\varphi}(\gamma)(f) = f^{\varphi(\gamma e_0)}$. We store this value at the corresponding place of $\mathbb{T}_{\gamma,\delta}$. That is at first stage all the values for functions over the axis i of $\mathcal{B}_{M,\delta}$ are known for all $\gamma \in \mathcal{R}$ and $\delta \in \{0,1,...,d-1\}$, this corresponds to the last file of the tables $\mathbb{T}_{\gamma,\delta}$, since we can identify the entries of the table with the points of $\mathcal{B}_{M,\delta}$.

Remark 4.3.11. *When we apply the U_∞ to Φ_{μ_φ} evaluated at a representative γ we move with τ_a to other representatives, so we need to fill the tables $\mathbb{T}_{\gamma,\delta}$ simultaneously for a fixed $f \in \mathcal{B}_M$ and running over $\gamma \in \mathcal{R}$.*

We start with the smallest $f \in \mathcal{B}_M$ and calculate $\Phi_{\mu_\varphi}(\gamma)(f)$, that is we start by filling the table $\mathbb{T}_{\gamma,\delta}$ by the upper right corner. Since the power of π and t is M, when we apply the operator, it reduces immediately to constants. Whose values were already calculated.

Let suppose that $f_{i_0 j_0} = 1 + \xi^\delta \pi^{i_0} t^{j_0} \in \mathcal{B}_M$ and we know the value of $\Phi_{\mu_\varphi}(\gamma)(g_{ij})$ in all $g_{ij} \in \mathcal{B}_M$ with $g_{ij} > f_{i_0 j_0}$. We can interpret this situation with a graphic in the following way



were the shaded area[1] represents the functions $f \in \mathcal{B}_{M,\delta}$ for which we know the value of $\Phi_{\mu_\varphi}(\gamma)(f)$ and the dashed blue line represents the functions in $\mathcal{B}_{M,\delta}$ with exponent i_0 in π to be integrated.

Applying the U_∞ operator to $\Phi_{\mu_\varphi}(\gamma)(f_{i_0 j_0})$ we have

$$U_\infty(\Phi_{\mu_\varphi}(\gamma)(f_{i_0 j_0})) = \prod_{a \in \mathbb{F}_q} \Phi_{\mu_\varphi}(\gamma\tau_a)(f_{i_0 j_0}(\pi t + a)).$$

[1] Although is a discrete set we use solid color to understand better the method.

Writing for every $a \in \mathbb{F}_q$ $\gamma\tau_a = \sigma_a\widetilde{\gamma}_a\kappa_a$ with $\sigma_a \in \Gamma$, $\widetilde{\gamma}_a \in \mathcal{R}$ and $\kappa_a \in \mathcal{J}$ and using the Iwahori equivariance of Φ_{μ_φ} and the Γ-invariance we have

$$\begin{aligned}\Phi_{\mu_\varphi}(\gamma\tau_a)(f_{i_0j_0}(\pi t + a)) &= \Phi_{\mu_\varphi}(\sigma_a\widetilde{\gamma}_a\kappa_a)(f_{i_0j_0}(\pi t + a)) \\ &= \Phi_{\mu_\varphi}(\widetilde{\gamma}_a)(f_{i_0j_0})(\tau_a\kappa_a^{-1}\langle t\rangle) \\ &= \Phi_{\mu_\varphi}(\widetilde{\gamma}_a)(1 + \xi^\delta\pi^{i_0}(\tau_a\kappa_a^{-1}\langle t\rangle)^{j_0}.\end{aligned}$$

Now we need to decompose the function $1 + \xi^\delta\pi^{i_0}(\tau_a\kappa_a^{-1}\langle t\rangle)^{j_0}$ as a product of elements in the pseudo-basis $\mathcal{B}_M$

$$1 + \xi^\delta\pi^{i_0}(\tau_a\kappa_a^{-1}\langle t\rangle)^{j_0} \equiv \prod_{f_{ij}\in\mathcal{B}_M} f_{ij}^{m_{ij}} \pmod{\pi^{M+1}}.$$

This decomposition has the property that each f_{ij} in it satisfies $f_{ij} > f_{i_0j_0}$, moreover the exponents of f_{ij} are in the set I'' (see figure 4.1), then we know its integral which is stored in one of the tables corresponding to $\widetilde{\gamma}_a$.

Remark 4.3.12. *At* (i_0, j_0) *need only values in the blue shaded area.*

Example 4.3.13. Let $N = T^3$ over $\mathbb{F}_2$, in Chapter 2 §2.8 we showed the corresponding graph. Let φ be the unique harmonic cocycle with rational Hecke eigenvalues (observe that there is only one cycle in the quotient graph) and let $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & T^2+T \end{smallmatrix}\right) \in \mathcal{R}$ be the representing matrix of the edge $e = (2,5)$. Working with $M = 7$ and $f = 1 + \pi^3t^2 \in \mathcal{B}_7$, to calculate $\Phi_{\mu_\varphi}(\gamma)(f)$ we apply the operator U_∞.

$$U_\infty(\Phi_{\mu_\varphi}(\gamma)(1 + \pi^3t^2)) = \prod_{a\in\mathbb{F}_2} \Phi_{\mu_\varphi}(\gamma\tau_a)(1 + \pi^3(\pi t + a)).$$

We need to decompose the matrices $\gamma\tau_0$ and $\gamma\tau_1$ as $\gamma_a\widetilde{\gamma}_a\kappa_a$, so we have

$$\begin{aligned}\gamma\tau_0 &= \left(\begin{smallmatrix} 0 & 1 \\ 1/T & T^2+T \end{smallmatrix}\right) \\ &= \begin{pmatrix} T^2+T+1 & 1 \\ T^3 & T+1 \end{pmatrix}\begin{pmatrix} T^2 & T^3+T \\ T^4+T^3+T^2+1 & T^5+T^4+T^2 \end{pmatrix}\begin{pmatrix} 1/T & 0 \\ 1/T^2 & 1/T \end{pmatrix}\end{aligned}$$

and the matrix $\widetilde{\gamma}_0 = \begin{pmatrix} T^2 & T^3+T \\ T^4+T^3+T^2+1 & T^5+T^4+T^2 \end{pmatrix}$ is a representative for the edge $(7,2)$ and

$$\kappa_0 = \begin{pmatrix} 1/T & 0 \\ 1/T^2 & 1/T \end{pmatrix} = \left(\begin{smallmatrix} 1 & 0 \\ 1/T & 1 \end{smallmatrix}\right)\begin{pmatrix} 1/T & 0 \\ 0 & 1/T \end{pmatrix}.$$

We can take κ_0 to be $\left(\begin{smallmatrix} 1 & 0 \\ 1/T & 1 \end{smallmatrix}\right)$ then

$$\begin{aligned} 1+\pi^3(\tau_0\kappa_0^{-1}\langle t\rangle)^2 &= 1+\pi^5t^2+\pi^7t^4+\pi^9t^6+... \\ &\equiv (1+\pi^5t^2)(1+\pi^7t^4) \pmod{\pi^8}. \end{aligned}$$

Both functions $(1+\pi^5t^2)$ and $(1+\pi^7t^4)$ belong to $\mathcal{B}_{7,0}$ and are smaller than $f=1+\pi^3t^2$, so its integral is stored in the table $\mathbb{T}_{\widetilde{\gamma}_0,0}$, moreover they are $\mathbb{T}_{\widetilde{\gamma}_0,0}[5,2]$ and $\mathbb{T}_{\widetilde{\gamma}_0,0}[7,4]$, respectively.

Analogously the matrix $\gamma\tau_1$ may be decomposed as above, in this case we have that the representative corresponds to the edge $(4,2)$ and $\kappa_1=\left(\begin{smallmatrix} 1 & 0 \\ 1/T & 1 \end{smallmatrix}\right)$, we have

$$\begin{aligned} 1+\pi^3(\tau_1\kappa_1^{-1}\langle t\rangle)^2 &= 1+\pi^3+\pi^5t^2+\pi^7t^4+\pi^9t^6... \\ &\equiv (1+\pi^3)(1+\pi^5t^2)(1+\pi^7t^4) \pmod{\pi^8}. \end{aligned}$$

Again the values of $(1+\pi^3)$,$(1+\pi^5t^2)$ and $(1+\pi^7t^4)$ are $\mathbb{T}_{\widetilde{\gamma}_1,0}[3,0]$, $\mathbb{T}_{\widetilde{\gamma}_1,0}[5,2]$ and $\mathbb{T}_{\widetilde{\gamma}_1,0}[7,4]$, respectively.

4.4 The change of variables and calculation of the integral

In this section we will see that the calculation of the multiplier $c_\alpha(\gamma)$ defined in Chapter 3, reduces to integrate functions on $\mathcal{F}_I$. Recall that $c_\alpha(\gamma)$ is defined by the following integral

$$\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{t-\gamma z_0}{t-z_0}\, d\mu_\varphi(t) \quad \text{for} \quad z_0\in\Omega. \tag{4.11}$$

Using the partition induced from the ends, we will break up the domain of integration in a finite union of disjoint open compacts and then by the change of variables formula, transform each integral resulting from the partition, in one of the form

$$\times\!\!\!\!\!\!\int_{O_\infty} f\, d(\mu)(t)$$

for some $f\in\mathcal{F}_I$.

Before describing the change of variables (since the integral (4.11) does not depend on the choice of z_0) we will describe briefly in Subsection 4.4.1 a way to construct a suitable z_0 using the reduction map. After this, in Subsection 4.4.2, we construct explicitly the partition of $\partial\Omega$ induced from a fixed edge e of the tree.

4.4.1 Choosing the z_0

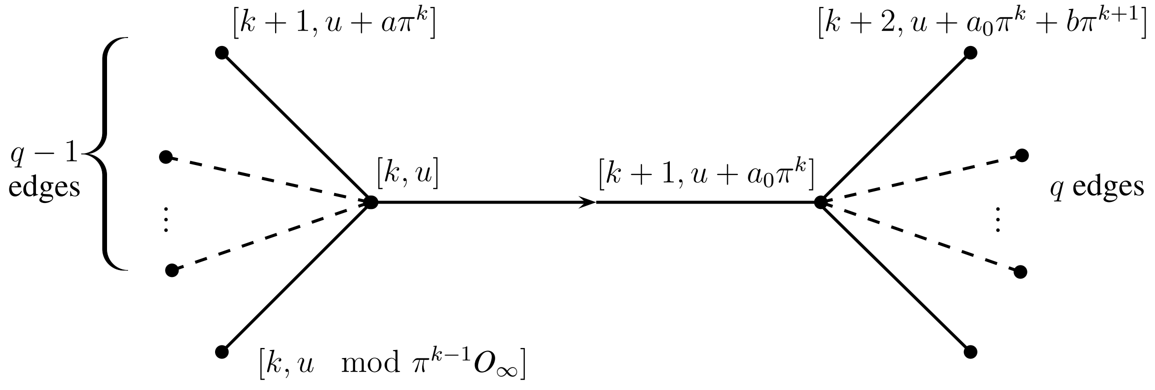
Let ξ be a generator of a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$, then ξ is in the standard affinoid $\{z \in C| \; |z| \leq 1 \quad |z-c| \geq 1 \quad \forall c \in \mathbb{F}_q\}$, *i.e.* it is a lifting of the standard vertex under the reduction map, that is $\lambda(\xi) = v_0$. So we may take $z_0 = \xi$. Moreover, given any vertex v on the tree $\mathcal{T}$, we know that there is a $\gamma \in GL_2(K_\infty)$ such that $\gamma v_0 = v$, where v_0 is the standard edge. From the $GL_2(K_\infty)$-invariance of the reduction map, we have that $z = \gamma z_0$ is a lifting of the vertex v under the reduction map .

It is straightforward to prove that given any vertex v and $\gamma = \left(\begin{smallmatrix}\pi^k & u \\ 0 & 1\end{smallmatrix}\right)$ the normal form representing v, lifting to Ω is just giving by applying γ to ξ as a Moebius transformation, namely, $z = \xi\pi^k + u$, and so $\operatorname{val}(z) < k$.

Let z and w be two different points in Ω such that $\lambda(z) \neq \lambda(w)$ then we say that they are *consecutive* if $\lambda(z)$ and $\lambda(w)$ are consecutive vertices in the tree.

4.4.2 The partition of the border

Let e be any edge of the tree, we know from (2.4) that it induces a partition of $\partial\Omega$. In order to construct explicitly such partition, it is convenient to write the vertices that determine e in normal form. So without loss of generality we may assume that the vertices v and v' are represented by $v = [k, u]$ and $v' = [k+1, u + a\pi^k]$ for $a \in \mathbb{F}_q$, respectively. Also suppose that v is closer than v_1 to the "line" $\mathcal{A}(0, \infty)$ in other words, the edge (v', v) points to infinity. We know from Lemma 2.4.5 that all the neighbors of v different from v' are given by $[k+1, u + a\pi^k]$ for $a \in \mathbb{F}_q \setminus a_0$ and the neighbors of v' are of the form $[k+2, u + a_0\pi^k + b\pi^{k+1}]$ with $b \in \mathbb{F}_q$. Graphically we have the following



From the Lemma 2.5.4 we have that to a vertex v of the form $[k,u]$ we attach the open set $u+\pi^k O_\infty$ which corresponds to the ends associated to edges e having v as terminal. Therefore

$$u+\pi^k O_\infty = \bigcup_{a\in\mathbb{F}_q}(u+a\pi^k+\pi^{k+1}O_\infty)$$

and one can easily observe

Lemma 4.4.1. *Given two neighbor vertices $[k,u]$ and $[k+1,u+a_0\pi^{k+1}]$ with $u\in O_\infty(\mathrm{mod}\ \pi^k)$ and $k\geqslant 0$ and $a_0\in\mathbb{F}_q$, then*

$$\left\{u+a\pi^k+\pi^{k+1}O_\infty\right\}_{a\in\mathbb{F}_q,a\neq a_0}\dot{\cup}\left\{u+a_0\pi^k+b\pi^{k+1}+\pi^{k+2}O_\infty\right\}_{b\in\mathbb{F}_q}\dot{\cup}\,\mathbb{P}^1(K_\infty)\setminus u+\pi^k O_\infty$$

is the partition of $\partial\Omega$ induced from the identification given by then ends.

Finally, in this partition we can identify three kinds of open sets:

i) $q-1$ of the form $u+a\pi^k+\pi^{k+1}O_\infty$ $a\in\mathbb{F}_q, a\neq a_0$, which we denote by $\mathcal{W}_a$.

ii) q of the form $u+a_0\pi^k+b\pi^{k+1}+\pi^{k+2}O_\infty$, $b\in\mathbb{F}_q$, which we denote by $\mathcal{W}_{a_0,b}$.

iii) One of the form $\mathbb{P}^1(K_\infty)\setminus(u+\pi^k O_\infty)$ denoted by $\mathcal{W}_\infty$.

4.4.3 The change of variables

Let $\varphi\in\underline{H}_!(\mathcal{T},G)^{\Gamma_0(N)}$, let μ_φ be the corresponding measure associated to it and let $\alpha\in\Gamma$ be a lifting of φ, that is, $j(\alpha)=\varphi$. Consider also $v_0,v_1,...,v_r$ to be a path in the tree which is the lifting of a cycle c of the quotient tree $\Gamma\setminus\mathcal{T}$. Then there exists a $\gamma\in\Gamma$ such that $\gamma v_0=v_r$ and let $z_0,z_1,...,z_r=\gamma(z_0)$ be consecutive points on Ω above $v_0,v_1,...,v_r$. Since the integral is multiplicative, we have

$$\begin{aligned} c_\alpha(\gamma) &= \times\!\!\!\!\!\!\int_{\partial\Omega}\frac{z_0-t}{\gamma z_0-t}\,d\mu_\varphi(t)\\ &= \times\!\!\!\!\!\!\int_{\partial\Omega}\prod_{i=0}^{r-1}\frac{z_i-t}{z_{i+1}-t}\,d\mu_\varphi(t)\\ &= \prod_{i=0}^{r-1}\times\!\!\!\!\!\!\int_{\partial\Omega}\frac{z_i-t}{z_{i+1}-t}\,d\mu_\varphi(t). \end{aligned}$$

Therefore, we will concentrate in how to calculate an integral of the form

$$\times\!\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu(t).$$

Using the partition of the border from Lemma 4.4.1, we can break up the integral in $2q$ integrals:

$$\times\!\!\!\!\!\!\!\int_{\partial\Omega} f(t)\, d\mu(t) = \prod_{a\in\mathbb{F}_q, a\neq a_0} \times\!\!\!\!\!\!\!\int_{\mathcal{W}_a} f(t)\, d\mu(t) \prod_{b\in\mathbb{F}_q} \times\!\!\!\!\!\!\!\int_{\mathcal{W}_{a_0,b}} f(t)\, d\mu(t) \times\!\!\!\!\!\!\!\int_{\mathcal{W}_\infty} f(t)\, d\mu(t)$$

where $f(t) = (z_i - t)/(z_{i+1} - t)$.

Integrating over $\mathcal{W}_a$

Consider the map

$$\begin{aligned} \gamma : O_\infty &\longrightarrow \mathcal{W}_a = u + a\pi^k + \pi^{k+1} O_\infty \\ t &\longmapsto \gamma(t) = u + a\pi^k + t\pi^{k+1}. \end{aligned}$$

It is given by the invertible Moebius transformation $\left(\begin{smallmatrix} \pi^k & u+a\pi^{k+1} \\ 0 & 1 \end{smallmatrix}\right)$, and hence a bijection. By abuse of notation we also write γ for this matrix. Note that the matrix γ represents one of the neighbors of the vertex v.

By the previous lines, the inverse of the map γ is given by the inverse of the matrix γ acting on $\mathcal{W}_a$ by Moebius transformations *i.e.*,

$$\begin{aligned} \gamma^{-1} : \mathcal{W}_a &\longrightarrow O_\infty \\ t &\longmapsto a + u\pi^{-k} + \pi^{-(k+1)}t. \end{aligned}$$

We make now the change of variables,

$$\begin{aligned}
\mathop{\times\!\!\!\!\!\!\int}_{\mathcal{W}_a} \frac{z_i - t}{z_{i+1} - t}\, d\mu(t) &= \mathop{\times\!\!\!\!\!\!\int}_{O_\infty} \frac{z_i - \gamma(t)}{z_{i+1} - \gamma(t)}\, d(\gamma^{-1} * \mu)(t) \\
&= \mathop{\times\!\!\!\!\!\!\int}_{O_\infty} \frac{z_i - (u + a\pi^k + t\pi^{k+1})}{z_{i+1} - (u + a\pi^k + t\pi^{k+1})}\, d(\gamma^{-1} * \mu)(t) \\
&= \mathop{\times\!\!\!\!\!\!\int}_{O_\infty} \frac{z_i - u - a\pi^k - t\pi^{k+1}}{z_{i+1} - u - a\pi^k - t\pi^{k+1}}\, d(\gamma^{-1} * \mu)(t) \\
&= \mathop{\times\!\!\!\!\!\!\int}_{O_\infty} \frac{(z_i - u - a\pi^k)(1 - t\pi^{k+1}/(z_i - u - a\pi^k))}{(z_{i+1} - u - a\pi^k)(1 - t\pi^{k+1}/(z_{i+1} - u - a\pi^k))}\, d(\gamma^{-1} * \mu)(t) \\
&= \left(\frac{z_i - u - a\pi^k}{z_{i+1} - u - a\pi^k}\right)^{\mu(\gamma O_\infty)} \frac{\mathop{\times\!\!\!\!\!\!\int}_{O_\infty} 1 - \frac{t\pi^{k+1}}{z_i - u - a\pi^k}\, d(\gamma^{-1} * \mu)(t)}{\mathop{\times\!\!\!\!\!\!\int}_{O_\infty} 1 - \frac{t\pi^{k+1}}{z_{i+1} - u - a\pi^k}\, d(\gamma^{-1} * \mu)(t)}.
\end{aligned}$$

The quantity $\frac{\pi^{k+1}}{(z_{i+1} - u - a\pi^k)}$ has positive valuation since $\mathrm{val}(z_i) \leqslant k$ hence the function $1 - \frac{\pi^{k+1}}{(z_i - u - a\pi^k)} t$ is an element of $\mathcal{F}_I$. Analogously, $1 - \frac{\pi^{k+1}}{(z_{i+1} - u - a\pi^k)} t \in \mathcal{F}_I$.

Integrating over $\mathcal{W}_\infty$

We will write the corresponding change of variables as a composition of two maps. In order to construct the first one, note that the following open sets are canonically isomorphic

$$\begin{array}{rcl}
\pi^k O_\infty & \longrightarrow & u + \pi^k O_\infty \\
t & \longmapsto & u + t,
\end{array}$$

$$\begin{array}{rcl}
u + \pi^k O_\infty & \longrightarrow & \pi^k O_\infty \\
t' - u & \longmapsto & t'
\end{array}$$

where u is thesame as in the case $\mathcal{W}_a$. These two maps are preserved under complement with respect to $\mathbb{P}^1(K_\infty)$,

$$\begin{array}{rcl}
\mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty & \longrightarrow & \mathbb{P}^1(K_\infty) \setminus (u + \pi^k O_\infty) \\
t & \longmapsto & u + t,
\end{array}$$

$$\begin{aligned} \mathbb{P}^1(K_\infty) \setminus (u + \pi^k O_\infty) &\longrightarrow \mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty \\ t' - u &\longmapsto t'. \end{aligned}$$

For the second one, let us now consider a map from $\mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty$ as follows

$$\begin{aligned} \mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty &\longrightarrow O_\infty \\ t &\longmapsto \ \pi^{k-1}/t. \end{aligned}$$

This map is a bijection and is well defined since if $t \in \mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty$ then $\mathrm{val}(t) \leqslant k-1$ and $\mathrm{val}(\pi^{k-1}/t) \geqslant 0$. As a Moebius transformation the map is given by the matrix $\left(\begin{smallmatrix} 0 & \pi^{k-1} \\ 1 & 0 \end{smallmatrix}\right)$ whose inverse is $\left(\begin{smallmatrix} 0 & 1 \\ \pi^{k-1} & 0 \end{smallmatrix}\right)$. So the inverse of the map above is

$$\begin{aligned} O_\infty &\longrightarrow \mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty \\ t &\longmapsto \ 1/t\pi^{-(k-1)}. \end{aligned}$$

Then we get the change of variables that we are interested in by composing the maps in the diagram

$$\begin{array}{ccccc} \mathcal{W}_\infty & \longrightarrow & \mathbb{P}^1(K_\infty) \setminus \pi^k O_\infty & \longrightarrow & O_\infty \\ t & \longmapsto & t-u & \longmapsto & \dfrac{\pi^{k-1}}{t-u}. \end{array}$$

In summary we have that the change of variables is given by the following map

$$\begin{aligned} \gamma^{-1} : \mathcal{W}_\infty &\longrightarrow O_\infty \\ t &\longmapsto \frac{\pi^{k-1}}{t-u} \end{aligned}$$

and its inverse given by

$$\begin{aligned} \gamma : O_\infty &\longrightarrow \mathcal{W}_\infty \\ t' &\longmapsto \frac{\pi^{k-1}}{t'} + u. \end{aligned}$$

Finally applying the formula of change of variables with $\gamma = \left(\begin{smallmatrix} u & \pi^{k-1} \\ 1 & 0 \end{smallmatrix}\right)$, we have

$$\begin{aligned}
\times\!\!\!\!\!\!\int_{\mathcal{W}_\infty} \frac{z_i - t}{z_{i+1} - t}\, d\mu(t) &= \times\!\!\!\!\!\!\int_{O_\infty} \frac{z_i - \gamma(t)}{z_{i+1} - \gamma(t)}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{z_i - (\frac{\pi^{k-1}}{t} + u)}{z_{i+1} - (\frac{\pi^{k-1}}{t} + u)}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{tz_i - \pi^{k-1} - tu}{tz_{i+1} - \pi^{k-1} - tu}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{\pi^{k-1}(1 - t\frac{(z_i - u)}{\pi^{k-1}})}{\pi^{k-1}(1 - t\frac{(z_{i+1} - u)}{\pi^{k-1}})}\, d(\gamma^{-1} * \mu)(t) \\
&= \frac{\times\!\!\!\!\!\!\int_{O_\infty} \left(1 - \frac{z_i - u}{\pi^{k-1}} t\right)\ d(\gamma^{-1} * \mu)(t)}{\times\!\!\!\!\!\!\int_{O_\infty} \left(1 - \frac{z_{i+1} - u}{\pi^{k-1}} t\right)\ d(\gamma^{-1} * \mu)(t)}.
\end{aligned}$$

Again $\frac{z_i - u}{\pi^{k-1}}$ and $\frac{z_{i+1} - u}{\pi^{k-1}}$ have both positive valuation since $\mathrm{val}(z_i - u) \geqslant k$ and $\mathrm{val}(z_{i+1} - u) > k$. Hence the functions $1 - \frac{z_i - u}{\pi^{k-1}} t$ and $1 - \frac{z_{i+1} - u}{\pi^{k-1}} t$ are in $\mathcal{F}_I$.

Integrating over $\mathcal{W}_{a_0,b}$

Consider the map

$$\begin{aligned}
\gamma : O_\infty &\longrightarrow \mathcal{W}_{a_0,b} \\
t &\longmapsto \gamma(t) = u + a_0\pi^k + b\pi^{k+1} + t\pi^{k+2}.
\end{aligned}$$

This map is a change of variables, the proof is similar as the one for the open $\mathcal{W}_a$. So making the change of variable we have

$$
\begin{aligned}
\times\!\!\!\!\!\!\int_{\mathcal{W}_{a_0,b}} \frac{z_i - t}{z_{i+1} - t}\, d\mu(t) &= \times\!\!\!\!\!\!\int_{O_\infty} \frac{z_i - \gamma(t)}{z_{i+1} - \gamma(t)}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{z_i - (u + a_0\pi^k + b\pi^{k+1} + t\pi^{k+2})}{z_{i+1} - (u + a_0\pi^k + b\pi^{k+1} + t\pi^{k+2})}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{z_i - u - a_0\pi^k - b\pi^{k+1} - t\pi^{k+2}}{z_{i+1} - u - a_0\pi^k - b\pi^{k+1} - t\pi^{k+2}}\, d(\gamma^{-1} * \mu)(t) \\
&= \times\!\!\!\!\!\!\int_{O_\infty} \frac{\left(z_i - u - a_0\pi^k - b\pi^{k+1}\right)\left(1 - \frac{t\pi^{k+2}}{(z_i - u - a_0\pi^k - b\pi^{k+1}}\right)}{\left(z_{i+1} - u - a_0\pi^k - b\pi^{k+1}\right)\left(1 - \frac{t\pi^{k+2}}{z_{i+1} - u - a_0\pi^k - b\pi^{k+1}}\right)}\, d(\gamma^{-1} * \mu)(t) \\
&= \left(\frac{z_i - u - a_0\pi^k - b\pi^{k+1}}{z_{i+1} - u - a_0\pi^k - b\pi^{k+1}}\right)^{\mu(\gamma O_\infty)} \frac{\times\!\!\!\!\!\!\int_{O_\infty} 1 - \frac{t\pi^{k+2}}{z_i - u - a_0\pi^k - b\pi^{k+1}}\, d(\gamma^{-1} * \mu)(t)}{\times\!\!\!\!\!\!\int_{O_\infty} 1 - \frac{t\pi^{k+2}}{z_{i+1} - u - a_0\pi^k - b\pi^{k+1}}\, d(\gamma^{-1} * \mu)(t)}
\end{aligned}
$$

The quantity $\frac{\pi^{k+2}}{z_i - u - a_0\pi^k - b\pi^{k+1}}$ has positive valuation since $\mathrm{val}(z_i) \leqslant k$ hence the function $1 - \frac{\pi^{k+2}}{z_i - u - a_0\pi^k - b\pi^{k+1}} t$ is an element of $\mathcal{F}_I$. Analogously for $1 - \frac{\pi^{k+2}}{z_{i+1} - u - a_0\pi^k - b\pi^{k+1}} t$.

Remark 4.4.2. *Note that the integral over the open sets $\mathcal{W}_a$ and $\mathcal{W}_{a_0,b}$ have positive valuation.*

5. Applications and examples

In Chapter 4 we described an algorithm to compute the integrals needed to find the Tate period. Here we describe how to obtain the Tate period explicitly from the integral and we use it to obtain elliptic curves defined over $\mathbb{F}_q(T)$ with the desired conductor. The chapter is organized as follows, in §§1-5 we make a short review of the theory of elliptic curves, supersingular curves, Eisenstein series, reduction modulo p of modular forms and the Tate curve. In §6 we describe how to calculate the Tate parameter and in §7 we give algorithms to obtain from the Tate parameter, the equations for elliptic curves over $\mathbb{F}_q(T)$.

5.1 Elliptic curves

We recall some basic facts from the theory of elliptic curves. Proofs for most of the theorems can be found in [Sil09].

Let K be a field, and let us consider projective curves in $\mathbb{P}^2_K$ defined by

$$ZY^2 + a_1ZXY + a_3Z^2Y = X^3 + a_2ZX^2 + a_4Z^2X + a_6Z^3 \tag{5.1}$$

with coefficients $a_i \in K$. We may usually consider the corresponding affine curve for $(Z \neq 0, x := X/Z, y := Y/Z)$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{5.2}$$

The only missing point $(0 : 1 : 0)$ is always smooth.

Definition 5.1.1. An *elliptic curve over a field K* is a smooth projective curve E given by the equation (5.1).

The equation (5.2) is called *a (long) Weierstrass equation* for E.

Let us define the quantities

$$\begin{aligned}
b_2 &= a_1^2 + 4a_4,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_4,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta.
\end{aligned}$$

Definition 5.1.2. Given a projective curve E over a field K as above, the quantity Δ is called the *discriminant* and in case $\Delta \neq 0$ the quantity j is called the *j-invariant* of E.

Observe that a projective curve defined by the equation (5.1) is not singular if and only if its discriminant $\Delta \neq 0$. That is, a curve given by the equation (5.1) is an elliptic curve if and only if $\Delta \neq 0$.

If the characteristic of K is not 2, then the change of variables $y \mapsto y - \frac{a_1}{2}x - \frac{a_3}{2}$ transforms a Weierstrass equation in one of the form

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{4}x + \frac{b_6}{4}.$$

If in addition the characteristic of K is not 3 then a further change of variables $x \mapsto x + \frac{b_2}{12}$ gives the equation

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

Finally with the change of variables $y \mapsto y/2$ the equation becomes

$$y^2 = 4x^3 - g_2x - g_3 \tag{5.3}$$

with $g_2 = 108c_4$ and $g_3 = 216c_6$.

Remark 5.1.3. *The last equation is not a Weierstrass equation since the coefficient of x^3 is not* 1. *However, it is a convenient expression (*e.g. *when one studies elliptic curves over $\mathbb{C}$). This form will be used later in this chapter.*

In summary, if the characteristic of K is not 2 or 3, we may and will assume that our elliptic curve has Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B \tag{5.4}$$

by considering the change of variables $y \mapsto 2y$ with $A = -\frac{g_2}{4}$ and $B = -\frac{g_3}{4}$. This form is called *the (short) Weierstrass form.* In the following we may simply say Weierstrass form, for short or long equation.

In characteristic 2 the discriminant and the j-invariant of an elliptic curve in Weierstrass form are given explicitly by

$$\Delta = a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_3^4 + a_2^3 + a_3^3$$

and

$$j = a_1^{12}/\Delta.$$

Note that the discriminant and the j-invariant of an elliptic curve given by a short Weierstrass equation are given by the formulas

$$\Delta = -16(4A^3 + 27B^2)$$

and

$$j(E) = -1728\frac{64A^3}{\Delta}.$$

Two elliptic curves E and E' defined by the Weierstrass equations with variables x and y and with variables x' and y', respectively, are isomorphic over K if and only if there exists $r, s, t, u \in K$ with $u \neq 0$ such that the change of variables

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t. \end{aligned} \tag{5.5}$$

The transformation in (5.5) is referred to as *an admissible change of variables.* Clearly, this transformation is invertible and its inverse also defines an admissible change of variables that transforms E' into E.

Theorem 5.1.4. *Let E and E' be two elliptic curves defined over an algebraically closed field K. Then E is K-isomorpic to E' if and only if they have the same j-invariant.*

If we apply to a Weierstrass equation the change of variables given by (5.5) the coefficients of the new curve and its associated quantities (denoted with primes) are compiled in the following list:

$$\begin{aligned}
ua'_1 &= a_1 + s^2,\\
u^2a'_2 &= a_2 - sa_1 + 3r - s^2,\\
u^3a'_3 &= a_3 + ra_1 + 2t,\\
u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1,\\
u^2b'_2 &= b_2 + 12r,\\
u^4b'_4 &= b_4 + rb_2 + 6r^2,\\
u^6b'_6 &= b_6 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
u^4c'_4 &= c_4,\\
u^6c'_6 &= c_6,\\
u^{12}\Delta' &= \Delta,\\
j' &= j.
\end{aligned}$$

The group law

The set of points $E(K)$ on an elliptic curve has a natural structure of an abelian group. The group law can be characterized in a number of equivalent ways. We characterize it by the following two rules:

1) The point $O = (0 : 1 : 0)$ is the identity of the group.

2) If a line L intersects E in three K-points $P, Q, R \in E(K)$ (taking multiplicities into account), then $P + Q + R = O$ in the group law.

From these one can deduce

a) The point $-P$ is the third intersection point of the line through O and P.

b) Given $P, Q \in E(K)$ not equal to O, the line through P and Q (if $P = Q$ then take the tangent line at P) intersects E at P, Q and a third point $R \in E(K)$. If $R = O$, then $P + Q = O$; otherwise $P + Q = -R$ where $-R$ can be constructed as in a).

It is easy to see that, at least generically, the coordinates of $P + Q$ can be expressed as rational functions in the coordinates of P and Q. For example, if $P = (x, y)$ and $Q = (x', y')$ are in the curve given by a Weierstrass form $y^2 = x^3 + Ax + B$, then

$$x(P+Q) = \left(\frac{y'-y}{x'-x}\right)^2 - x - x'$$

and

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Singular curves

Let E be a cubic curve given by the equation (5.2) with discriminant $\Delta = 0$, then E has a singular point (cf. [Sil09, Prop. 1.4 a)]). Actually one can easily show, that there is only one singular point, let say P. Let c_4 be the quantity associated to the Weierstrass equation of E, there are two possibilities for the singularity at P:

1) If $c_4 \neq 0$ then P has two distinct tangent directions. In this case P is called *a node.*

2) If $c_4 = 0$ then P has only a single tangent direction. In this case P is called *a cusp.*

Definition 5.1.5. Let E be a (possibly singular) cubic curve given by a Weierstrass equation (5.2). The *non-singular part* of E, denoted by E_{ns}, is the curve with its singular point removed. Similarly, if E is defined over K, then $E_{ns}(K)$ is the set of non-singular points of $E(K)$.

The set $E_{ns}(K)$ has a particularly simple structure described in the following proposition.

Proposition 5.1.6. *Let E be a cubic curve given by a Weierstrass equation with discriminant $\Delta = 0$ with E singular point P. Then the group law makes $E_{ns}(K)$ into an abelian group.*

a) Suppose E has a node, and let

$$y = \alpha_1 x + \beta_1 \quad \textit{and} \quad y = \alpha_2 x + \beta_2$$

be the two distinct tangent lines to E at P. Then the map

$$\begin{aligned} E_{ns}(\bar{K}) &\longrightarrow \bar{K}^{\times} \\ (x,y) &\longmapsto \frac{y-\alpha_1 x-\beta_1}{y-\alpha_2 x-\beta_2} \end{aligned}$$

is an isomorphism (of abelian groups).

b) Suppose E has a cusp, and let

$$y = \alpha x + \beta$$

be the tangent line to E at P. Then the map

$$\begin{aligned} E_{ns}(\bar{K}) &\longrightarrow \bar{K}^{+} \\ (x,y) &\longmapsto \frac{x-x(P)}{y-\alpha x-\beta} \end{aligned}$$

is an isomorphism.

Isogenies

We turn now to the definition of morphisms between elliptic curves.

Definition 5.1.7. Let E_1 and E_2 be two elliptic curves over K. Let L/K be a field extension, an *isogeny* (over L) between E_1 and E_2 is a non-constant morphism $\phi : E_1 \longrightarrow E_2$ defined over L that satisfies $\phi(O) = O$. We say that two curves E_1 and E_2 are *isogenous* if there exists an isogeny from E_1 to E_2.

Remark 5.1.8. *If the extension L of K is not specified then we are assuming that the isogeny is defined over the algebraic closure $\bar{K}$ of K.*

From the definition one can see that the relation of isogeny is an equivalence relation on elliptic curves. We have also

Proposition 5.1.9. *Every isogeny $\phi : E_1 \longrightarrow E_2$ is a group homomorphism.*

The set of isogenies from E_1 to E_2 together with the zero map is denoted by $\operatorname{Hom}(E_1, E_2)$. It is a group under addition. The group $\operatorname{Hom}(E, E)$ is a ring which we denote by $\operatorname{End}(E)$. It is called the *endomorphism ring* of E. The operations in $\operatorname{End}(E)$ are given by

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \quad \text{and} \quad (\phi\psi)(P) = \phi(\psi(P)).$$

The invertible elements of $\operatorname{End}(E)$ form the automorphism group of E which is denoted by $\operatorname{Aut}(E)$.

Theorem 5.1.10. *a) Let E_1 and E_2 two elliptic curves over K, then the group of isogenies, defined over $\bar{K}$, $\operatorname{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module.*

b) Let E be an elliptic curve over K, then the endomorphism ring End(E) is a (not necessarily commutative) ring of characteristic 0 with non zero divisors.

c) Let E be an elliptic curve defined over a field K. Then the endomorphism ring of E is one of the following

$$End(E) = \begin{cases} \mathbb{Z}, \\ \textit{an order in a imaginary quadratic field}, \\ \textit{a maximal order in a quaternion algebra}. \end{cases}$$

The last case only happens if $char(K) = p > 0$.

Elliptic curves over finite fields

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q = p^n$, p a prime. The first important result dealing with elliptic curves over finite fields is the following fact established by Lang and Weil [LW54].

Theorem 5.1.11. *Any smooth cubic curve E defined over a finite field $\mathbb{F}_q$ has a $\mathbb{F}_q$-rational point.*

The set of $\mathbb{F}_q$-rational points of an elliptic curve defined over a finite field $\mathbb{F}_q$ is finite. Hasse's theorem on elliptic curves, also referred to as the *Hasse bound*, provides an estimate of the number of points on an elliptic curve over a finite field.

Theorem 5.1.12 (Hasse). *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Definition 5.1.13. Let E be an elliptic curve defied over a finite field $\mathbb{F}_q$. The *Frobenious endomorphism* is given by

$$\begin{aligned} \Phi_E : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

The Frobenious endomorphism is strongly related with $\#E(\mathbb{F}_q)$ by the following

Theorem 5.1.14. *Let E be an elliptic defined over a finite field $\mathbb{F}_q$ and let $\#E(\mathbb{F}_q) = q + 1 - a$. Then the Frobenious endomorphism satisfies the equality*

$$\Phi_E^2 - a\Phi_E + q = 0.$$

Definition 5.1.15. The quantity a from the theorem is called the *Frobenious trace.*

Elliptic curves over local fields

Let K be a complete local field with normalized valuation $\nu : K^\times \longrightarrow \mathbb{Z}$. Let R be the ring of integers of K with maximal ideal $\mathfrak{p}$ and residue field $k = R/\mathfrak{p}$. Let also ϖ be a uniformizer for R, that is $\mathfrak{p} = \varpi R$.

For a given elliptic curve over K with equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, the substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ leads to a new equation in which each coefficient a_i is replaced by $u^i a_i$. If we choose u to be divisible by a sufficiently large power of ϖ, we obtain a Weierstrass equation with coefficients in R.

Definition 5.1.16. Let E/K be an elliptic curve defined by the affine Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.6}$$

with $a_i \in R$. We say that (5.6) is a *minimal Weierstrass equation* for E if $\nu(\Delta)$ is minimal among all Weierstrass equations defining E with coefficients in R.

The minimal Weierstrass equation always exists, since ν is discrete and we can choose among all Weierstrass equations with coefficients in R, one that minimalizes $\nu(\Delta)$. If the equation for an elliptic curve is not minimal, there is a coordinate change giving a new equation with discriminant $\Delta' = u^{-12}\Delta \in R$. Thus $\nu(\Delta)$ can only be changed by adding or subtracting multiples of 12. Similarly we have $c_4' = u^{-4}c_4$ and $c_6' = u^{-6}c_6$ and by the same argument $\nu(c_4)$ and $\nu(c_6)$ can only be changed by adding or subtracting a multiple of 4 and 6, respectively. So we conclude:

1) If $a_i \in R$ and $\nu(\Delta) < 12$, then the equation is minimal.

2) If $a_i \in R$ and $\nu(c_4) < 4$ (or $\nu(c_6) < 6$), then the equation is minimal.

Now we look at the "reduction modulo ϖ". Let us consider the natural reduction map $R \longrightarrow k = R/\mathfrak{p}$. Let us denote by $\tilde{a}_i \in k$ the reduction of a_i modulo ϖ and by $\widetilde{E}$ the equation obtained from E by reducing its coefficients modulo ϖ, that is

$$\widetilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

The curve $\widetilde{E}$ is called *the reduction modulo ϖ*. Note that $\widetilde{E}/k$ is an elliptic curve if $\tilde{\Delta} \neq 0$, this occurs when $\nu(\Delta) = 0$.

Definition 5.1.17. Let E/K be an elliptic curve and $\widetilde{E}$ its reduction modulo ϖ. We say that

a) E has *good (or stable) reduction* if $\widetilde{E}$ is non-singular (in which case $\widetilde{E}$ is an elliptic curve).

b) E has *multiplicative (or semi stable) reduction* if $\widetilde{E}$ has a node. The reduction is called *split* if the tangent directions are defined over k, otherwise is *non-split.*

c) E has *additive (or unstable) reduction* if $\widetilde{E}$ has a cusp.

Twists

Definition 5.1.18. Let E and E_1 be two elliptic curves defined over a field K. We say that E_1 is a twist of E if E and E_1 are isomorphic over an algebraic closure of K.

Remark 5.1.19. *Two twists have the same j-invariant (cf. Theorem 5.1.4).*

Example 5.1.20. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ given by the Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

Let $\beta \in \mathbb{F}_q^\times$, then the elliptic curve

$$E_1 : y^2 = x^3 + \beta^2 Ax + \beta^3 B$$

is a $\mathbb{F}_q$-twist of E. Indeed, taking $c \in \mathbb{F}_{q^2}$ such that $c = \sqrt{\beta}$ then $(x, y) \longmapsto (c^4 x, c^6 y)$ is an isomorphism from E to E_1 defined over $\mathbb{F}_{q^2}$. This twist is called a *quadratic twist.*

5.2 Supersingular elliptic curves

Let K be a field of characteristic $p > 0$ and E/K an elliptic curve. As mentioned in Section 5.1, the endomorphism ring of E is a torsion free $\mathbb{Z}$-module of rank $1, 2$ or 4. Namely, $\mathbb{Z}$, an order in an imaginary quadratic field or a maximal order in a quaternion algebra, respectively.

Definition 5.2.1. Let E/K be an elliptic curve, we say that E is *supersingular* if its endomorphism ring has rank 4.

There are further characterizations and interesting properties of supersingular elliptic curves (cf. [Sil09, Ch. III]).

Examples

1) If K is a field of characteristic 2 then every elliptic curve with a Weierstrass equation

$$y^2 + a_3 x = x^3 + a_4 x + a_6$$

is supersingular ([Was08, p. 122]).

2) If K is a field of characteristic 3 then every elliptic curve of the form

$$y^2 = x^3 + a_4 x + a_6$$

is supersingular ([Was08, p. 122]).

Supersingular elliptic curves will play an important role in our algorithm. We will need a test to know whether or not a given elliptic curve is supersingular.

Proposition 5.2.2. *Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of the prime number p and let $a = q + 1 - \#E(\mathbb{F}_q)$. Then E is supersingular if and only if $a \equiv 0 \pmod{p}$.*

For a proof of the proposition see for example [Was08, Prop. 4.31]. An important invariant in the theory of supersingular elliptic curves is the Hasse invariant which is defined as follows.

Definition 5.2.3. Let E be an elliptic curve over $\mathbb{F}_q$ defined by the equation $y^2 = f(x)$, where f is a polynomial in $\mathbb{F}_p[x]$ of degree 3. The *Hasse invariant* of E is defined to be the coefficient of x^{p-1} in the expansion of $f(x)^{\frac{(p-1)}{2}}$.

Remark 5.2.4. *In the literature it is common to define the Hasse invariant in terms of the differential associated to the elliptic curve (cf. [Kat77]).*

Lemma 5.2.5. *An elliptic curve E is supersingular if and only if its Hasse invariant is zero.*

5.3 Elliptic curves over $\mathbb{C}$ and Eisenstein series

In this section we follow very closely the book of Silverman [Sil09, Ch. VI].

Definition 5.3.1. Let $\Lambda \subset \mathbb{C}$ be a lattice, that is a discrete subgroup of $\mathbb{C}$ which contains a $\mathbb{R}$-basis for $\mathbb{C}$. An *elliptic function* (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ which satisfies

$$f(z + \omega) = f(z) \text{ for all } z \in \mathbb{C} \text{ and } \omega \in \Lambda.$$

The set of all elliptic functions for Λ forms a field, denoted by $\mathbb{C}(\Lambda)$.

Definition 5.3.2. Let $\Lambda \subset \mathbb{C}$ be a lattice. We define the *Weierstrass* $\wp_\Lambda$-function (relative to Λ) as

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda,\, \omega \neq 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

and also the *Eisenstein series* (for Λ) of weight $2k$ as

$$G_{2k}(\Lambda) = \sum_{\omega \neq 0 \in \Lambda} \omega^{-2k}.$$

It is customary to let $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

The Eisenstein series are absolutely convergent for all integers $k \geqslant 2$ and the series defining the Weierstrass $\wp_\Lambda$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$ (cf. [Sil09, Ch. VI, Thm. 3.1]).

The field $\mathbb{C}(\Lambda)$ is generated by the Weierstrass $\wp_\Lambda$-function and its derivative. These functions can be used to parametrize certain elliptic curve as we see in the following theorem (cf. [Sil09, Ch. VI, Prop. 3.6]).

Theorem 5.3.3. *Let $\Lambda \in \mathbb{C}$ be a lattice.*

a) The functions $\wp_\Lambda(z)$ and $\wp'_\Lambda(z)$ generate $\mathbb{C}(\Lambda)$, that is, $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.

b) The Weierstrass $\wp_\Lambda$-function and its derivative satisfy the identity

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda).$$

Further, the polynomial $f(x) = 4x^3 - g_2(\Lambda) - g_3(\Lambda)$ has distinct roots, so its discriminant

$$\Delta = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

is non-zero and therefore the equation

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

defines an elliptic curve over $\mathbb{C}$.

c) The map

$$\phi_\Lambda : \mathbb{C}/\Lambda \longrightarrow E_\Lambda(\mathbb{C}) \quad z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$$

is a complex analytic isomorphism of complex Lie groups.

d) Conversely, given an elliptic curve $E/\mathbb{C}$, there exists a lattice Λ, unique up to homothety, such that $E_\Lambda \cong E$.

Let E_1 and E_2 be elliptic curves over $\mathbb{C}$ corresponding to lattices Λ_1 and Λ_2, respectively. Then one can show that

$$\mathrm{Hom}(E_1, E_2) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\},$$

where the isogeny associated to α is given analytically by

$$\mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \quad z \longmapsto \alpha z.$$

We recall that two lattices Λ_1 and Λ_2 are homothetic if there exists $\alpha \in \mathbb{C}$ such that $\Lambda_1 = \alpha\Lambda_2$. Homothetic lattices correspond to isomorphic elliptic curves, so it is common in practice to replace the lattice $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ by $\Lambda_\tau := \tau\mathbb{Z} + \mathbb{Z}$ with $\tau = \omega_1/\omega_2 \in \mathfrak{H} := \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$, which is homothetic to Λ. Then for the lattice Λ_τ the definition of the Eisenstein series becomes

$$G_{2k}(\tau) := G_{2k}(\Lambda_\tau) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)=1}} \frac{1}{(m\tau + n)^{2k}}.$$

On the other hand, the fact that the lattice $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ does not change when we replace its basis $\{\omega_1, \omega_2\}$ by $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$ where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$ allows us to consider the modular group $\Gamma = SL_2(\mathbb{Z})$ and its action on $\mathfrak{H}$ in order to study isomorphism classes of elliptic curves.

Definition 5.3.4. Let k be an integer. A holomorphic function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ is called a *modular form of weight k with respect to the modular group* $\Gamma = SL_2(\mathbb{Z})$ if it satisfies the following conditions:

1) $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau + d)^k f(\tau)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$,

2) f has a Fourier expansion of the form

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n \tag{5.7}$$

where $q = e^{2\pi i\tau}$.

A modular form with respect to $\Gamma = SL_2(\mathbb{Z})$ is a *cusp form* if it satisfies in (5.7) the further condition that $a_0 = 0$.

Remark 5.3.5. *For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ we deduce*

$$f(\tau) = (-1)^k f(\tau).$$

So k must be even, otherwise $f(\tau) = 0$. In other words, there is no non-zero modular forms with respect to $\Gamma = SL_2(\mathbb{Z})$ of odd weight.

A typical example of modular forms is given by the Eisenstein series $G_k(\tau)$ defined above. The coefficients of $G_k(\tau)$ can be explicitly calculated as arithmetic functions on n. Namely, setting $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$, we have the following proposition [Kob84, Ch. III, p. 110].

Proposition 5.3.6. *Let k be an even integer greater than 2 and let $\tau \in \mathcal{H}$. Then the modular form $G_k(\tau)$ has q-expansion*

$$G_k(\tau) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right)$$

where $q = e^{2\pi i \tau}$ and the Bernoulli numbers B_k are defined by

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

It is convenient to define the normalized Eisenstein series

$$E_k(\tau) = \frac{1}{2\zeta(k)} G_k(\tau) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{5.8}$$

The series $E_k(\tau)$ is defined in this way in order to have rational coefficients. We have for example

$$E_4(\tau) = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n) q^n,$$
$$E_6(\tau) = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n) q^n,$$
$$E_8(\tau) = 1 + 480\sum_{n=1}^{\infty} \sigma_7(n) q^n.$$

Let $M_k(\Gamma)$ be the $\mathbb{C}$-vector space of modular forms with respect to $\Gamma = SL_2(\mathbb{Z})$ of weight k. We may use the standard notation M_k if the group Γ is clear from the context. It is clear that

$$M_k M_l \subset M_{k+l},$$

and so the direct sum

$$\bigoplus_{k=0}^{\infty} M_k$$

can be viewed as a graded algebra, whose structure is given by the next theorem.

Theorem 5.3.7. *Put $Q = E_4$ and $R = E_6$. The functions Q and R are algebraically independent and*

$$\bigoplus_{k=0}^{\infty} M_k = \mathbb{C}[Q, R].$$

One has for example

$$E_8 = Q^2, \quad E_{10} = QR, \quad E_{12} = \frac{441Q^3 + 250R^2}{691},$$

$$E_{14} = Q^2R \text{ and } \Delta = \frac{Q^3 - R^2}{1728}.$$

Corollary 5.3.8. *The dimension of M_k is given as follows:*

$$dim(M_k) = \begin{cases} [\frac{k}{12}], & \textit{if} \quad k \equiv 2 \pmod{12} \\ [\frac{k}{12}] + 1, & \textit{if} \quad k \equiv 0, 4, 6, 8, 10 \pmod{12}. \end{cases}$$

The dimension of M_k is then 1 for $k = 0, 4, 6, 8, 10$, with the basis $1, Q, R, Q^2, QR$, respectively.

From Theorem 5.3.7 follows that for k even there exists a unique polynomial $\varphi_k(X, Y) \in \mathbb{C}[X, Y]$ (actually in $\mathbb{Q}[X, Y]$) such that

$$\varphi_k(P, Q) = E_k. \tag{5.9}$$

One has for example

$$\begin{aligned} \varphi_4(X, Y) &= X, \\ \varphi_6(X, Y) &= Y, \\ \varphi_8(X, Y) &= X^2, \\ \varphi_{10}(X, Y) &= XY, \\ \varphi_{12}(X, Y) &= \frac{441X^3 + 250Y^2}{691}, \\ \varphi_{14}(X, Y) &= X^2Y, \end{aligned}$$

$$\varphi_{16}(X,Y) = \frac{X(1617X^3 + 2000Y^2)}{3617}.$$

5.4 Reduction modulo p of modular forms

In this section we closely closely the ideas introduced in [Ser73b]. Let p be a prime number greater than 3 and let v_p be the corresponding valuation of the field $\mathbb{Q}$. We can now define modular forms modulo p. Let us denote by $\mathfrak{o}$ the local ring of $\mathbb{Q}$ at p, that is, the ring of rational numbers with denominator prime to p, and let $\mathfrak{m}$ its maximal ideal.

Definition 5.4.1. Let

$$f = \sum_{n \geqslant 0} a_n q^n \in \mathbb{Q}[[q]]$$

be a formal power series with coefficients in $\mathbb{Q}$. We say that f is *p-integral* if $v_p(a_n) \geqslant 0$ (equivalently if $a_n \in \mathfrak{o}$) for all n .

Let $\tilde{a}_n$ denote the image of a_n in $\mathbb{F}_p = \mathfrak{o}/\mathfrak{m}$. Let f be a p-integral power series, then

$$\tilde{f} = \sum \tilde{a}_n q^n \in \mathbb{F}_p[[q]]$$

is called the *reduction of f modulo p.*

For a fixed integer k, consider the following set

$$\widetilde{M_k} := \left\{ \tilde{f} \;\mid\; f \text{ is a modular form of weight } k \text{ whose Fourier expansion is } p\text{-integral} \right\}.$$

Denote by $\widetilde{M}$ the union of the $\widetilde{M_k}$, which is a sub-algebra of $\mathbb{F}_p[[q]]$ and call it *the algebra of modular forms modulo p.*

Definition 5.4.2. A polynomial is called *isobaric* if all monomials appearing in the polynomial have the same weight according to some given weight function on the indeterminates.

Let f be a modular form of weight k, we know from Theorem 5.3.7 that f may be written as an isobaric polynomial in Q and R, that is

$$f = \sum c_{a,b} Q^a R^b$$

for some finite set (a,b) such that $4a + 6b = k$, *i.e.*, Q has weight 4 and R has weight 6.

Note that by equation (5.8) the denominators of the Eisenstein series are bounded, so we can normalize them to get integral coefficients and therefore p-integral for any prime p. By Theorem 5.3.7 it follows that $\widetilde{M_k}$ admits a $\mathbb{F}_p$-basis of monomials $\widetilde{Q}^a\widetilde{R}^b$, that is, $\widetilde{Q}$ and $\widetilde{R}$ generate the algebra $\widetilde{M}$. To describe the structure of $\widetilde{M}$ we only need to determine the ideal $\mathfrak{a} \subset \mathbb{F}_p[[X, Y]]$ of relations between $\widetilde{Q}$ and $\widetilde{R}$, *i.e.*, those polynomials F for which $F(\widetilde{Q}, \widetilde{R}) = 0$. This is the content of the following (cf. [SD75, Thm. 2])

Theorem 5.4.3. *Suppose that $p > 3$ is a prime. The ideal $\mathfrak{a}$ is a principal ideal generated by $A-1$ where $A \in \mathbb{F}_p[X, Y]$ is the isobaric polynomial of weight $p-1$ such that $A(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_{p-1}$. The polynomial $A(X, Y)$ has no repeated factor and $\widetilde{M}$ is naturally isomorphic to*

$$\mathbb{F}_p[X, Y]/(A-1)$$

which has a natural $\mathbb{Z}/(p-1)$-grading.

Examples

- For $p = 5$ one has $E_{p-1} = E_4 = Q$, so $A(X, Y) = X$. The ideal of relations among $\widetilde{Q}$ and $\widetilde{R}$ is generated by the relation $\widetilde{Q} = 1$. The algebra $\widetilde{M}$ is isomorphic to $\mathbb{F}_5[\widetilde{R}]$.
- For $p = 7$ one has $E_{p-1} = E_6 = R$. Analogous to the previous case $A(X, Y) = Y$ and $\widetilde{M} = \mathbb{F}_7[\widetilde{Q}]$.
- For $p = 11$ one has $E_{10} = QR$, the fundamental relation is $\widetilde{Q}\widetilde{R} = 1$, so that $A(X, Y) = XY$.
- For $p = 13$ one has $E_{12} \equiv 6Q^3 - 5R^2 \pmod{12}$, the fundamental relation is $6\widetilde{Q}^3 - 5\widetilde{R}^2 = 1$.

It is clear from Theorem 5.4.3 that A is a homogeneous polynomial of weight $(p-1)/2$, if X and Y have weight 2 and 3, respectively.

Proposition 5.4.4. *Let A be the polynomial of Theorem 5.4.3.*

1. *There exists a homogeneous polynomial F such that $A(X, Y) = F(X^3, Y^2)X^iY^j$ with $i, j \in \{0, 1\}$.*
2. *The exponents i and j depend on the congruence of $p-1$ modulo 12, namely*

a) $i = j = 0$ if and only if $p \equiv 1 \pmod{12}$.

b) $i = 1$ and $j = 0$ if and only if $p \equiv 5 \pmod{12}$.

c) $i = 0$ and $j = 1$ if and only if $p \equiv 7 \pmod{12}$.

d) $i = 1$ and $j = 1$ if and only if $p \equiv 11 \pmod{12}$.

Proof. Let A be the polynomial in $\mathbb{F}_p[X, Y]$ that generates the algebra $\widetilde{M}$ then the fact that $A(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_p$ and the graduation modulo p force A to be a pseudo-homogeneous polynomial of degree $(p-1)/2$ for X of weight 2 and Y of weight 3. Hence we can write A as

$$A(X, Y) = F(X^3, Y^2)X^iY^j \tag{5.10}$$

for $i, j \in \mathbb{N}$ and F a homogeneous polynomial of degree d. Then pseudo-degree (ps-deg) of A is $6d + 2i + 3j$ where $i \in \{0, 1, 2\}$ and $j \in \{0, 1\}$. We have six cases to consider.

1) If $i = j = 0$ then $A(X, Y) = F(X^3, Y^2)$ and ps-deg$(A) = 6d$, but ps-deg$(A) = (p-1)/2$ therefore $6d = (p-1)/2$. That is $p \equiv 1 \pmod{12}$ and 2. a) follows.

2) If $i = 1$ and $j = 0$ we have $A(X, Y) = F(X^3, Y^2)X$ then ps-deg$(A) = 6d + 2$. From ps-deg$(A) = (p-1)/2$ it follows that $6d + 2 = (p-1)/2$ and $d = (p-5)/12$, since d is an integer, $p \equiv 5 \pmod{12}$ and we have the assertion of 2. b).

3) If $i = 0$ and $j = 1$ we have $A(X, Y) = F(X^3, Y^2)Y$ then ps-deg$(A) = 6d + 3$. In view of ps-deg$(A) = (p-1)/2$ we get $d = (p-7)/12$ and thus $p \equiv 7 \pmod{12}$. So we have the claim of 2. c).

4) If $i = 1$ and $j = 1$ we get $A(X, Y) = F(X^3, Y^2)XY$ then ps-deg$(A) = 6d + 5$ as above, this implies that $p \equiv 11 \pmod{12}$ and 2. d) follows.

5) If $i = 2$ and $j = 0$ we have $A(X, Y) = F(X^3, Y^2)X^2$. Therefore ps-deg$(A) = 6d+4 = (p-1)/2$ implies that $d = (p-9)/12$ that is $3|p$ which is impossible since p is prime.

6) If $i = 2$ and $j = 1$ we have $A(X, Y) = F(X^3, Y^2)X^2Y$ and then ps-deg$(A) = 6d + 7$ which implies $3|p$ and since p is prime, this case is impossible.

□

Elliptic interpretation

Let $p \geqslant 5$ be a prime and E be an elliptic curve defined over $K := \mathbb{F}_p(Q, R)$ with equation

$$y^2 = 4x^3 - \frac{Q}{12}x - \frac{R}{216} \tag{5.11}$$

with Q and R regarded as indeterminates (compare the equation with (5.3)). As a result from the discussion in [SD75, pp. 21–24], the curve E has Hasse invariant $H(E) = \widetilde{A}(Q, R)$. Upon specializing (Q, R) the Hasse invariant H vanishes if and only if the corresponding elliptic curve is supersingular. In [Gor02] the author proves even more.

Proposition 5.4.5. *[Gor02, Prop. 5.3] The Hasse invariant is a modular form over $\mathbb{F}_p$ (of level) 1 and weight $p - 1$. Its q-expansion at the cusp is 1, hence H is equal to the reduction of E_{p-1} modulo p.*

Corollary 5.4.6. *The Hasse invariant does not have multiple factors.*

5.5 The Tate Curve

General references for the theory of Tate's analytic uniformization of elliptic curves are [Lan87, Ch. 15] and [Sil94, Ch. V]. We refer to them for more details and for proofs of cited results.

In the classical case, for the field of complex numbers, it is possible to represent the group of points on an elliptic curve over $\mathbb{C}$ as the quotient of the additive group of $\mathbb{C}$ by a discrete subgroup generated by two $\mathbb{R}$-linearly independent periods ω_1 and ω_2. One can absorb one of these periods passing from the additive group to the multiplicative group, by means of the exponential function and obtain a representation of the group of points of the elliptic curve as the quotient of the multiplicative group $\mathbb{C}^\times$ by a discrete subgroup generated by one multiplicative period namely, $t = e^{2\pi i\tau}$, where $\tau = \omega_2/\omega_1$. In $\mathbb{C}$, the explicit formulas giving this multiplicative representation are the well known Fourier expansions of the Weierstrass functions $\wp$, the Eisenstein series, etc.

Let K denote a field which is complete with respect to a discrete valuation v, and whose residue field is perfect of characteristic $p > 0$. Tate proved that the Fourier expansions of the Weierstrass functions $\wp$, suitable normalized, yield universal identities among power series that can be used to obtain a multiplicative representation for the group of rational points of certain elliptic curves over K (similar as in the classical case for the complex field).

The following statements can be found in [Roq70, Ch. III, pp. 23–33].

Theorem 5.5.1 (Tate). *Let K be a local field of arbitrary characteristic and let $\mathbf{q} \in K^\times$ with $0 < |\mathbf{q}| < 1$. Then the field of meromorphic $\mathbf{q}$-periodic functions on $\mathbb{G}_{m,K}$ is an elliptic function field $F(\mathbf{q})$, which means, finitely generated of transcendence degree 1 over K. More precisely $F(\mathbf{q}) = K(\wp, \wp')$ with*

$$\wp(u) = \sum_{n\in\mathbb{Z}} \frac{\mathbf{q}^n u}{(1-\mathbf{q}^n u)^2} - 2s_1 \quad \textit{and} \quad \wp'(u) = \sum_{n\in\mathbb{Z}} \frac{\mathbf{q}^{2n} u^2}{(1-\mathbf{q}^n u)^3} + s_1$$

where

$$s_k = \sum_{m\geqslant 1} \frac{m^k \mathbf{q}^m}{1-\mathbf{q}^m} \quad \textit{for } k \in \mathbb{N}.$$

The elliptic curve $E(\mathbf{q})$ associated to the elliptic function field $F(\mathbf{q})$ is given by the equation

$$\wp'^2 + \wp\wp' = \wp^3 + a_4(\mathbf{q})\wp + a_6(\mathbf{q}),$$

where $a_4(\mathbf{q}) = -5s_3$ and $a_6(\mathbf{q}) = \frac{1}{12}(5s_3 + 7s_5)$. Its j-invariant is

$$j(\mathbf{q}) = \frac{(1-48a_4(\mathbf{q}))^3}{\Delta} = \frac{1}{\mathbf{q}} + R(\mathbf{q})$$

where

$$R(\mathbf{q}) = 744 + 196884\mathbf{q} + ... \in \mathbb{Z}[[\mathbf{q}]] \textit{ and}$$
$$\Delta(\mathbf{q}) = a_4(\mathbf{q})^2 - a_6(\mathbf{q}) - 64a_4(\mathbf{q})^2 + 72a_4(\mathbf{q})a_6(\mathbf{q}) - 432a_6(\mathbf{q})^2.$$

To every $j \in K$ with $|j| > 1$ there is one and only one $\mathbf{q} \in K$ with $0 < |\mathbf{q}| < 1$ such that $j = j(\mathbf{q})$.
The classical well known product representation

$$\Delta(\mathbf{q}) = \mathbf{q} \prod_{n\geq 1} (1-\mathbf{q}^n)^{24}$$

holds also in the non-archimedean case for every characteristic.

The *Tate elliptic curve* (relative to $\mathbf{q}$) is the curve with the Weierstrass equation

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}). \tag{5.12}$$

Observe that since $a_6(\mathbf{q}) = \sum_{m\geqslant 1} \frac{7m^5+5m^3}{12} \frac{\mathbf{q}^m}{1-\mathbf{q}^n}$ and $7m^5 \equiv 5m^3 (\text{mod } 12)\ \forall m \in \mathbb{Z}$, the series $a_6(\mathbf{q})$ is also defined for $p = 2$ and $p = 3$.

Using the formulas above for the Weierstrass function and its derivative we obtain as in the classical case the v-adic analytic uniformization

$$\begin{array}{rccl} \phi : & \bar{K}^\times/\langle \mathbf{q} \rangle & \xrightarrow{\cong} & E_{\mathbf{q}}(\bar{K}) \\ & u & \longmapsto & \big(\wp(u), \wp'(u)\big). \end{array} \tag{5.13}$$

If $\text{char}(K) \neq 2, 3$, we can use the function $\wp + \frac{1}{12}$ and its derivative $\wp'$ as the generators of $F(\mathbf{q})$ over K. It is immediately verified that their defining relation is in Weierstrass normal form

$$\wp'^2 = \left(\wp + \frac{1}{12}\right)^3 - \frac{1}{4}g_2 \left(\wp + \frac{1}{12}\right) - \frac{1}{4}g_3$$

where the coefficients g_2 and g_3 are given by the classical $\mathbf{q}$-expansions

$$g_2 = \frac{1}{12} + 20s_3 \quad \text{and} \quad g_3 = -\frac{1}{216} + \frac{7}{3}s_5.$$

We call the corresponding elliptic curve

$$E_{Eis} : y^2 = 4x^3 - g_2x - g_3,$$

the curve in *Eisenstein form.* It is clear that it is isomorphic to the Tate curve (5.12). It is a straightforward calculation to get the following relation between the coefficients of the Tate curve and the curve in Eisenstein form

$$a_4 := a_4(\mathbf{q}) = \frac{g_2}{4} - \frac{1}{48} \quad \text{and} \quad a_6 := a_6(\mathbf{q}) = \frac{g_3}{4} + \frac{g_2}{4} - \frac{1}{1728}.$$

Consider the Eisenstein form $y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$, then the Hasse invariant H gives a relation between the coefficients g_2 and g_3. Taking $f(x) = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$ we can calculate H as the coefficient of x^{p-1} in the expansion of $f(x)^{\frac{(p-1)}{2}}$.

One has for example

$$\begin{aligned}
p = \ \ 5 &\Longrightarrow H_5 = g_2, \\
p = \ \ 7 &\Longrightarrow H_7 = g_3, \\
p = 11 &\Longrightarrow H_{11} = 11 g_2 g_3, \\
p = 13 &\Longrightarrow H_{13} = 8 g_3^2 + 6 g_2^3, \\
p = 17 &\Longrightarrow H_{17} = 8 g_2^4 + 10 g_2 g_3^2, \\
p = 19 &\Longrightarrow H_{19} = 7 g_3^3 + 11 g_2^3 g_3^2, \\
p = 23 &\Longrightarrow H_{23} = 13 g_2^4 g_3 + 9 g_2 g_3^3, \\
p = 29 &\Longrightarrow H_{29} = 4 g_2^7 + 18 g_2^4 g_3^2 + 8 g_2 g_3^4, \\
p = 31 &\Longrightarrow H_{31} = 2 g_2^6 g_3 + g_2^3 g_3^3 + 27 g_3^5.
\end{aligned}$$

5.6 Obtaining the Tate parameter

Let $N \in \mathbb{F}_q[T]$ be a polynomial of degree greater than 2 and $\varphi \in \underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ be a harmonic cocycle with rational Hecke eigenvalues. From Section 2.12 we know that there exists an elliptic curve E_φ defined over $\mathbb{F}_q(T)$ with conductor $N\infty$ associated with φ. This curve E_φ can be constructed as a Tate curve, that is there exists $\mathbf{q} \in \mathbb{F}_q((\pi))$ with $0 < |\mathbf{q}| < 1$ such that E_φ is in the isogeny class of

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}).$$

From Proposition 2.12.2, we know that $\mathbf{q}$ is a generator of the multiplicative subgroup

$$\{c_\varphi(\alpha) | \alpha \in \Gamma_0(N)\}$$

where $c_\varphi(\alpha)$ is the multiplicative integral

$$\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{t - \alpha z_0}{t - z_0}\, d\mu_\varphi(t)$$

defined in (3.9).

Now the first question is how to find $\alpha \in \Gamma$ such that $c_\varphi(\alpha) = \mathbf{q}$. Let $\{c_1, ...c_g\}$ be a basis for the homology of the quotient graph $\Gamma \setminus \mathcal{T}$. Let ω_i be a path in the tree $\mathcal{T}$ without backtracking such that ω_i is a lifting of the cycle c_i. Since the origin $v_{0,i}$ and the terminal $v_{1,i}$ of ω_i are Γ-equivalent, there exists a $\alpha_i \in \Gamma$ such that $\alpha_i v_{0,i} = v_{1,i}$. Consider the set $\mathcal{C} = \{\alpha_1, ..., \alpha_g\}$ with α_i as above, then from [Gek95, Cor. 3.19] we have that

$$\mathrm{val}(\mathbf{q}) = \min\{\mathrm{val}(c_\varphi(\alpha_i)) \ \mid \alpha_i \in \mathcal{C}\}. \tag{5.14}$$

Therefore, to obtain the Tate parameter we choose an integral with minimal valuation. In the appendix we will describe a procedure to find the minimal valuation without explicitly computing any integral. The algorithm to calculate the Tate parameter will be discussed in the Appendix B (cf. Algorithm 10), which can be calculated in polynomial time.

Theorem 5.6.1. *The Tate parameter* $\mathbf{q}$ *can be calculated up to accuracy* π^M *in time* $O(M^7)$*.*

We will probe this result in the appendix B (cf. Theorem B.2.1). This running time is strongly dominated by the running time for the algorithm to calculate the table. So after explain how calculate our table, we explain how to find the Tate parameter and we give the proof of this theorem.

5.7 Obtaining equations for the curves

Let $N \in \mathbb{F}_q[T]$ be a polynomial with $\deg(N) \geqslant 3$ and such that the space of new harmonic cocycles with rational Hecke-eigenvalues has dimension h. There exits h different isogeny classes of elliptic curves defined over $\mathbb{F}_q(T)$ with conductor $N\infty$.

For each one-dimensional rational eigenspace of $\underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ we need to find the Tate parameter associated to the corresponding rational eigencocycle φ. For this we use our algorithm to calculate the integral

$$\mathop{\times\!\!\!\!\!\!\int}_{\partial\Omega} \frac{t - \alpha z_0}{t - z_0}\, d\mu_\varphi(t)$$

for a suitable α obtained from (5.14).

Once we know the Tate parameter $\mathbf{q}$ up to accuracy π^M for some fixed integer $M > 1$, we need to compute the quantities s_3 and s_5 using the formula

$$s_k = \sum_{m\geqslant 1} \frac{m^k \mathbf{q}^m}{1-\mathbf{q}^m} = \sum_{m\geqslant 1} m^k \mathbf{q}^m \sum_{l\geqslant 0} \mathbf{q}^{ml} \quad \text{for } k \in \mathbb{N}. \tag{5.15}$$

Then we find the coefficients of the Tate curve given by $a_4(\mathbf{q}) = -s_3$ and $a_6(\mathbf{q}) = \frac{1}{12}(5s_3 + 7s_5)$. We carry out these calculations modulo π^{M+1} since we only know $\mathbf{q}$ up to accuracy π^M. Then the Tate equation is given by

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}). \tag{5.16}$$

However, in general, the quantities $a_4(\mathbf{q})$ and $a_6(\mathbf{q})$ are not rational and this analytic model does not allow us directly to find the isogeny class of the elliptic curve that we are looking for. In this section, we explain how to get equations defined over $\mathbb{F}_q(T)$ by choosing suitable models for the elliptic curves.

5.7.1 Elliptic curves in characteristic 2 and 3

We need to transform the Tate curve in one model defined over the rationals. For this we carry out in each characteristic an admissible change of variables to transform the Tate curve into a rational model depending only on one parameter.

In Characteristic 2

In this case we use the admissible change of variables

$$\begin{aligned} x &\longmapsto x, \\ y &\longmapsto y + x + a_4, \end{aligned}$$

then the Tate curve (5.16) is transformed into

$$E : y^2 + xy = x^3 + A_6$$

where the coefficients satisfy the relation $A_6 = a_6 + a_4^2$. A direct calculation shows that E has discriminant $\Delta = A_6$ and j-invariant $j = 1/A_6$.

In Characteristic 3

An admissible change of variables in characteristic 3 is given by

$$x \longmapsto x + a_4,$$
$$y \longmapsto y + a_4.$$

Then the Tate curve (5.16) is isomorphic to

$$E : y^2 + xy = x^3 + A_6$$

where $A_6 = a_6 + a_4^3 - a_4^2$, which has discriminant $\Delta = -A_6$ and j -invariant $j = 1/A_6$. In both cases, since the j-invariant of such elliptic curve is a rational function, it follows that A_6 is rational. So the elliptic curve is defined over $\mathbb{F}_q(T)$.

The next proposition plays an important role in our algorithm (cf. [Sch01, Prop. 1.3]) in the cases $p = 2, 3$.

Proposition 5.7.1. *Suppose $\mathbb{F}_q$ is a finite field of characteristic 2 or 3. Let E be an elliptic curve over $K = \mathbb{F}_q(T)$ with non-constant j-invariant $j(E)$. Write $j(E) = \frac{f(T)}{g(T)}$ with relatively prime $f(T)$ and $g(T)$ in $\mathbb{F}_q[T]$. Then*

a) the divisors of $f(T)$ are places of supersingular reduction, and

b) the divisors of $g(T)$ are places of bad reduction.

Proof. For *a*) we know that in characteristic 2 and 3, an elliptic curve is supersingular if and only if the j-invariant is zero. So let $\mathfrak{p}$ be a place that divides $f(T)$. Let $\widetilde{E}$ and $\tilde{j}$ the reduction of E and j modulo $\mathfrak{p}$, respectively. As $\mathfrak{p}$ divides $f(T)$ we have that $\tilde{j} = 0$ so $\widetilde{E}$ is a supersingular curve, that is $\mathfrak{p}$ is a supersingular place.

Since $j \neq 0$ we can take the usual normal forms for characteristic 2 and 3 (cf. [Sil09, Appendix A]) which have the advantage of describing an elliptic curve with an expression for the j-invariant relatively easy to manage.

An elliptic curve in characteristic 2 can be given by the Weierstrass model

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \tag{5.17}$$

which has discriminant $\Delta = a_6$ and j-invariant $j = 1/a_6$.

On the other hand in characteristic 3 an elliptic curve can be given by the normal model

$$E : y^2 = x^3 + a_2x^2 + a_6 \tag{5.18}$$

with discriminant $\Delta = -a_2^3a_6$ and j-invariant $j = -a_2^3/a_6$. Since the j-invariant of E is of the form $\frac{f(T)}{g(T)}$ we can write the equations of (5.17) and (5.18) as

$$E : y^2 + xy = x^3 + a_2x^2 + \frac{g(T)}{f(T)}$$

and

$$E : y^2 + xy = x^3 + a_2x^2 + 2a_2^3\frac{g(T)}{f(T)},$$

respectively. The model in characteristic 2 has discriminant $\frac{g(T)}{f(T)}$ and the one in characteristic 3 has discriminant $\frac{a_2^6g(T)}{f(T)}$.

Then for the proof of b), we can suppose without loss of generality that our elliptic curve has in each characteristic one of these models. From Tate's algorithm [Tat75] we know that E has a model defined over $\mathbb{F}_q[T]$ which is minimal at all finite places. This model is also isomorphic to E and its discriminant is divisible by $g(T)$. Let $\mathfrak{p}$ be a divisor of $g(T)$, then $\mathfrak{p}$ divides the discriminant, that is $\mathrm{val}_{\mathfrak{p}}(\Delta) > 0$. Hence $\mathfrak{p}$ is a bad place of E. □

A prime $\mathfrak{p}$ is a place of supersingular reduction if and only if the curve $\widetilde{E}$ is supersingular. By Proposition 5.2.2 $\widetilde{E}$ is supersingular if the corresponding Frobenious trace $t = q + 1 - \#\widetilde{E}(\mathbb{F}_q)$ is 0 modulo p. But t is also an eigenvalue for the Hecke operator $T_{\mathfrak{p}}$. Then if we are able to calculate from the harmonic cocycle a list of eigenvalues for primes of small degree, it is possible to have some candidates that divide the polynomial $f(T)$ of the proposition. On the other hand, what that polynomial $g(T)$ from last proposition concerns, places of bad reduction can be taken from the conductor which is also known. So we can use Proposition 5.7.1 to improve our approximation of A_6 to a rational function.

On the other hand, we know that $\mathrm{val}(j) = -\mathrm{val}(\mathbf{q})$, therefore we have that $\deg(g) - \deg(f) = -\mathrm{val}(\mathbf{q})$. Let us suppose that we have all the factors of f and g, so we can write them as

$$f(T) = \prod_{i=1}^{m} f_i^{t_i} \quad \text{and} \quad g(T) = \prod_{j=1}^{n} g_j^{r_j} \tag{5.19}$$

for t_i and r_j integers. Then we have

$$\sum_{j=1}^{n} r_j \deg g_j - \sum_{i=1}^{m} t_i \deg f_i = \mathrm{val}(A_6).$$

So we can try some m-tuples and n-tuples of t_i's and r_j's, respectively and take series of A_6 to get representation of A_6 as a rational function. Although in our examples we do not need to do this and in practice this is difficult to carry out since to calculate the supersingular places using the Hecke operator takes time.

At this point we have completed the first phase of the computation with the approximation of A_6 to a rational function. Next we need to see whether the elliptic curve

$$y^2 + xy = x^3 + A_6$$

has conductor $N\infty$. The computation of the conductor is performed using any Computer algebra system with this function available, in our case we use MAGMA.

If the conductor of E is not $N\infty$ then we need to carry out an appropriated change of variables to transform our elliptic curve into a form that allows us to find the right curve.

Remark 5.7.2. *So far, in characteristic* 2 *this has not happened in any of the examples known. That is, the model $E : y^2+xy = x^3+A_6$ seems to give always the right conductor,so the algorithm assumes this.*

In the following lines we describe the algorithm that allows us to find a rational representative in the isogeny class of the Tate curve in characteristic 2 and 3 with conductor $N\infty$.

Given a rational Hecke eigen function $\varphi \in \underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ where N is a polynomial with $\deg(N) \geqslant 3$, we want to find the elliptic curve associated with φ. The Algorithm 1 explains the procedure to get E from the Tate period $\mathbf{q}$.

Algorithm 1: `Curve2or3`

Input: The Tate parameter $\mathbf{q}$ up to accuracy of π^M and the Hecke eigen-cocycle φ.

Output: An elliptic curve in the isogeny class of the Tate curve associated to $\mathbf{q}$ or a message *"Accuracy too small, please increase M"*.

```
1:  Calculate the quantities $s_3$ and $s_5$ using the formula (5.15) and use them to calculate
    the coefficients of the Tate curve $a_4$ and $a_6$ up to accuracy $\pi^M$.
2:  calculate the quantity $A_6$:
      • if characteristic of $K$ is 2 then $A_6 = a_6 + a_4^2$,
      • if characteristic of $K$ is 3 then $A_6 = a_6 + a_4^3 - a_4^2$.
3:  use the algorithm of continued fractions to find the representation of $A_6$ as a rational
    function.
4:  for all place $f$ divisor of $N$ do
5:      if $f$ does not divide numerator of $A_6$ then
6:          Return "Accuracy too small, please increase M"
7:      end if
8:  end for
9:  define the elliptic curve $E : y^2 + xy = x^3 + A_6$
10: calculate the conductor of $E$ let say $c$
11: if $c = N\infty$ then
12:     Return $E$
13: end if
14: if characteristic $K = 3$ then
15:     for all places $f_i \mid c$ and $f_i \nmid N$, set $u^{-2} = (\prod_{f_i} f_i)$
16:     make the change of variables
            $x \longmapsto u^2 x,$
            $y \longmapsto u^3 y + u^2 x$
        to transform $E$ into $E_{\mathrm{n}} : y^2 = x^3 + a_2x^2 + a_6$ where $a_2 = u^{-2}$ and $a_6 = A_6 u^{-6}$
17: end if
18: Return $E$
```

Remark 5.7.3. *The Algorithm 1 finishes in step 6 if the accuracy M is too small and the series A_6 does not converge to a rational function. In the other case it continues and* *returns the curve E in step 12 if it is no necessary to carry out the change of variables or in step 18 after the change of variables.*

If char $K = 3$ and $j(E) \neq 0$ we use the change of variables $x \mapsto u^2x$ and $y \mapsto u^3y + u^2x$ to get the curve

$$E_{\mathrm{n}} := y^2 = x^3 + a_2x^2 + a_6 \quad \Delta(E_{\mathrm{n}}) = -a_2^3a_6, \;\; j(E_{\mathrm{n}}) = -a_2^3/a_6$$

for $u \in K^\times$ such that u^{-2} is divisible by all extra places appearing in the conductor of E. We claim that E_{n} has conductor $N\infty$. We cannot prove this, although we can give a heuristic argument as follows. From the change of variables we have that $\Delta(E_{\mathrm{n}}) = u^{-12}\Delta(E)$, and $a_2 = u^{-2}$ (cf. [Sil09, Table 1.2]). Since $j(E) = 1/A_6$, by Proposition 5.7.1, the denominator of A_6 is divisible only by supersingular places and since we can not eliminate places of bad reduction, we need u^{-12} to be the denominator of A_6. We have observed in many examples that the powers of the places that divide the denominator of A_6 is 6.

Let $\mathrm{Cond}(E_{\mathrm{n}})$ be the conductor of E_{n} and $\mathfrak{p}$ a place that divides u^{-12}, we have that $\mathrm{val}_{\mathfrak{p}}(\mathrm{Cond}(E_{\mathrm{n}})) = 0$ since $\mathfrak{p}$ does not divide $\Delta(E_{\mathrm{n}})$. Then $\mathrm{val}_{\mathfrak{p}}(\mathrm{Cond}(E_{\mathrm{n}})) = \mathrm{val}_{\mathfrak{p}}(\mathrm{Cond}(E_{\mathrm{Tate}}))$, where E_{Tate} is the Tate curve.

Example 5.7.4. Let $N = T^3 \in \mathbb{F}_2[T]$, from the quotient graph (see Figure 5.1), we can see that the dimension of the space of harmonic cocycles is 1. Therefore, the dimension of the space $\underline{H}_!^{new}(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)}$ is 1 and consequently there exists one $\mathbb{F}_q(T)$-isogeny class of elliptic curves with conductor $T^3\infty$.

With a partition, as the one described in the previous chapter, using the Algorithm 6 we calculate with accuracy up to $M = 85$ to find that

$$\mathbf{q} = \pi^4 + \pi^{36} + \pi^{68}.$$

Then using the formulas for $a_4(\mathbf{q})$ and $a_6(\mathbf{q})$ we get

$$a_4(\mathbf{q}) = a_6(\mathbf{q}) = \pi^4 + \pi^8 + \pi^{16} + \pi^{16} + \pi^{32} + \pi^{64}.$$

From the change of variables we have the relation $A_6 = a_6 + a_4^2$, so

$$\begin{aligned} A_6 &= (\pi^8 + \pi^{16} + \pi^{16} + \pi^{32} + \pi^{64}) + (\pi^4 + \pi^8 + \pi^{16} + \pi^{16} + \pi^{32} + \pi^{64}) \\ &= \pi^4 \\ &= 1/T^4. \end{aligned}$$

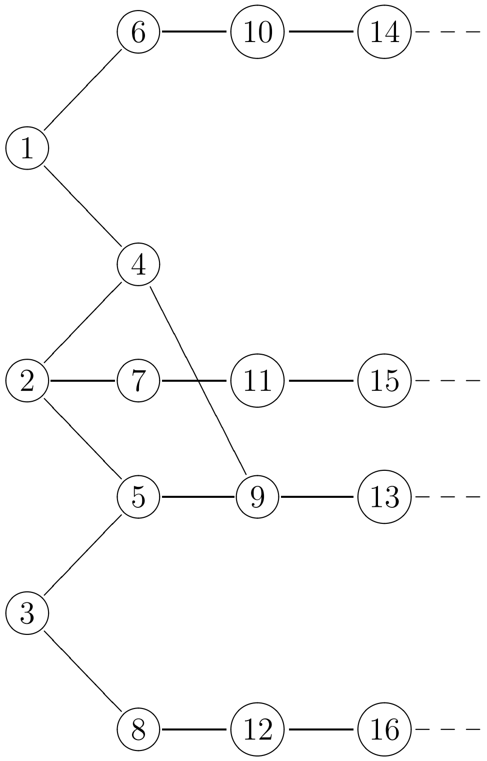


Figure 5.1: Quotient graph for $N = T^3$ over $\mathbb{F}_2$.

The desired elliptic curve is given by the equation $E : y^2+xy = x^3+\frac{1}{T^4}$ which has conductor $T^3\infty$, and split multiplicative reduction at ∞, as a routine application of Tate's algorithm [Tat75] shows.

Remark 5.7.5. *In [Pap01] Papikian finds the elliptic curve $y^2 + Txy = x^3 + T^2x$ which is isomorphic to E after the change of variables*

$$x \longmapsto T^2x,$$
$$y \longmapsto T^3y + T.$$

If $q = 2$, we can show using divisibility arguments and the definition of a_4 and a_6 that

$$a_4 = a_6 = \sum_{n\,\text{odd}\;n\leqslant 1} \frac{\mathbf{q}^n}{1-\mathbf{q}^n}.$$

Also from the change of variables, we have the relation $a_4^2 + a_6 = A_6$ where $A_6 \in \mathbb{F}_2(T)$. In other words, a_4 is a root of the polynomial $F(X) = X^2 + X + A_6 \in \mathbb{F}_2(T)[X]$. It is straightforward to check that if α is a root of F then $1 + \alpha$ is the other root.

Let us consider the rational function $A_6 = 1/T^4 = \pi^4$ and the polynomial $F(X) = X^2 + X + A_6 \in \mathbb{F}_2(T)[X]$. A direct calculation shows that $\alpha = \sum_{n \geqslant 2} \pi^{2^n}$ is a root of $F(X)$, hence, it is equal to a_4 since the other root of $F(X)$ has valuation 0. On the other hand the continued fraction expansion of α is the infinite periodic sequence

$$[1 + \pi^{-4}; \pi^{-4}, \pi^{-4}, ...].$$

Then by the Lagrange theorem for continued fractions $\alpha \notin \mathbb{F}_2(T)$ and is quadratic over $\mathbb{F}_2(T)$. In particular a_4 and a_6 are quadratic.

Once we know the rational function A_6, we can use the formula for a_4 and the polynomial $F(X) = X^2 + X + A_6 \in \mathbb{F}_2(T)[X]$ to arbitrarily increase the accuracy of $\mathbf{q}$. To do this, suppose that one knows $\mathbf{q}$ up to accuracy M, then make $\mathbf{q} = \mathbf{q} + b_{M+1}\pi^{M+1}$ where $b_{M+1} \in \mathbb{F}_2$ is an indeterminate. Plug in $\mathbf{q}$ in the formula for a_4 and use the polynomial $F(X)$ to find the value of b_{M+1}. With this procedure we can easily to compute $\mathbf{q}$ to an arbitrary high precision. For example:

$$\mathbf{q} = \pi^4 + \pi^{36} + \pi^{68} + \pi^{132} + \pi^{196} + \pi^{228} + \pi^{356} + \pi^{420} + \pi^{452} + O(\pi^{517}).$$

Example 5.7.6. Consider $N = T^3$ over $\mathbb{F}_3$. In this case $\dim H_1(\Gamma \backslash \mathcal{T}) = \dim \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} = 2$ which is the number of new forms. In terms of the standard basis they are $\varphi_1 = (1, 1)$ and $\varphi_2 = (1, -2)$. For each of them we obtain, using the Algorithm 6 (see Appendix B), the following Tate parameters (working with an accuracy of $M = 40$)

$$\begin{aligned} \mathbf{q_1} &= 2\pi^3 + 2\pi^{12} + \pi^{21} + 2\pi^{39}, \\ \mathbf{q_2} &= \pi^3 + 2\pi^{12} + 2\pi^{21} + \pi^{39}. \end{aligned}$$

Then applying the formulas for a_4 and a_6 we have for $\mathbf{q_1}$ up to accuracy $M = 40$

$$\begin{aligned} a_4(\mathbf{q_1}) &= 2\pi^3 + 2\pi^9 + 2\pi^{27}, \\ a_6(\mathbf{q_1}) &= \pi^3 + \pi^6 + \pi^9 + 2\pi^{12} + \pi^{18} + \pi^{27} + 2\pi^{30} + 2\pi^{36} \end{aligned}$$

and by the change of variables described above, we have $A_6 = a_6 + a_4^3 - a_4^2 = \pi^3$, so the corresponding rational elliptic curve is

$$E_1 : y^2 + xy = x^3 + 1/T^3.$$

It has conductor $T^3\infty$ and split multiplicative reduction at ∞.

Analogously, for $\mathbf{q}_2$ we have

$$\begin{aligned}
a_4(\mathbf{q_2}) &= \pi^3 + \pi^9 + \pi^{27},\\
a_6(\mathbf{q_2}) &= 2\pi^3 + \pi^6 + 2\pi^9 + 2\pi^{12} + \pi^{18} + 2\pi^{27} + 2\pi^{30} + 2\pi^{36}.
\end{aligned}$$

Performing the same calculations as above, we obtain the elliptic curve

$$E_2 : y^2 + xy = x^3 + 2/T^3.$$

Remark 5.7.7. *In [Sch01, Prop. 4.3], Schweizer found exactly the same elliptic curves, using other tools.*

Example 5.7.8. Consider now the polynomial $N = (T+2)(T^2+T+2)$. This example has a different flavor than the previous ones, since we do not get the curve immediately from the change of variables as above (in this case we have to apply step 16.b) of Algorithm 1). We need to make a further change of variables to find the curve with the right conductor.

In this case we have only one harmonic cocycle with rational eigenvalues, so it is also a new form. Working with accuracy of $M = 40$ and using our algorithm of integration, we find the Tate parameter

$$\begin{aligned}
\mathbf{q} = \pi^4 &+ \pi^5 + 2\pi^7 + 2\pi^9 + 2\pi^{10} + 2\pi^{11} + 2\pi^{14} + \pi^{15} + 2\pi^{17} + \pi^{18} +\\
&\pi^{19} + \pi^{21} + 2\pi^{22} + 2\pi^{23} + \pi^{25} + \pi^{27} + 2\pi^{28} + 2\pi^{29} + 2\pi^{32} +\\
&\pi^{33} + 2\pi^{34} + \pi^{35} + \pi^{36} + \pi^{37} + 2\pi^{38} + 2\pi^{39} + \pi^{40}.
\end{aligned}$$

Plugging in this value in the formulas for a_4 and a_6 we have that

$$\begin{aligned}
A_6 = 2\pi^4 &+ 2\pi^5 + \pi^7 + \pi^9 + \pi^{10} + \pi^{11} + \pi^{14} + 2\pi^{15} + 2\pi^{16} + 2\pi^{18} +\\
&2\pi^{19} + 2\pi^{20} + 2\pi^{23} + \pi^{24} + \pi^{25} + \pi^{27} + \pi^{28} + \pi^{29} + \pi^{32} + 2\pi^{33}\\
&+2\pi^{34} + 2\pi^{36} + 2\pi^{37} + 2\pi^{38}.
\end{aligned}$$

Applying continuous fractions it converges to

$$\begin{aligned}
A_6 &\sim \frac{2T^8 + 2T^7 + 2T^5 + T^4 + T^3 + 2T^2 + 2}{T^{12} + 2T^9 + T^6}\\
&= \frac{2(T+2)^4(T^2+T+2)^2}{T^6(T+1)^6}.
\end{aligned}$$

Then the elliptic curve

$$E : y^2 + xy = x^3 + \frac{2(T+2)^4(T^2+T+2)^2}{T^6(T+1)^6}$$

has conductor $T(T+1)(T+2)(T^2+T+2)\infty$, which is not $N\infty$. We need to "get rid of" the places T and $T+1$. To do this, we change our model of the curve to the standard one in characteristic 3,

$$E_{\text{norm}} : y^2 = x^3 + \hat{a}_2 x^2 + \hat{a}_6.$$

So the admissible change of variables from E to E_{norm} is given by

$$\begin{aligned} x &\longmapsto u^2 x, \\ y &\longmapsto u^3 y + u^2 x. \end{aligned}$$

With this change of variables we have that $u^2\hat{a}_2 = 1$ and $\hat{a}_6 = A_6\hat{a}_2^3$. Also, from the table given in [Sil09], we have that the discriminants of E and E_{norm} satisfy the relation $u^{12}\Delta_E = \Delta_{E_{\text{norm}}}$. So to get rid of the places T and $T+1$ we may take $u = \frac{1}{\sqrt{T(T+1)}}$, therefore $\hat{a}_2 = T(T+1)$ and $\hat{a}_6 = \frac{2(T+2)^4(T^2+T+2)^2}{T^3(T+1)^3}$. The new elliptic curve

$$E_{\text{norm}} : y^2 = x^3 + T(T+1)x^2 + \frac{2(T+2)^4(T^2+T+2)^2}{T^3(T+1)^3}$$

has the conductor $(T+2)(T^2+T+2)$ and split multiplicative reduction at ∞.

The following table gives some examples with the Tate parameter, the conductor N and the rational function A_6 in which we can see that the denominator has factors which are powers of 6.

Tate Parameter	Conductor	A_6
$2\pi^5+\pi^6+\pi^7+2\pi^{11}+\pi^{12}+\pi^{13}+2\pi^{20}+\pi^{21}+$ $\pi^{22}+2\pi^{23}+\pi^{24}+\pi^{25}+2\pi^{29}+\pi^{30}+$ $\pi^{31}+\pi^{32}+2\pi^{33}+2\pi^{34}+\pi^{35}+2\pi^{36}+2\pi^{37}+$ $\pi^{38}+2\pi^{39}+2\pi^{40}+O(\pi^{41})$	$T(T+2)(T^2+2T+2)$	$\frac{T^5(T^2+2T+2)}{(T^2+1)^6}$
$\pi^5+2\pi^7+\pi^8+2\pi^9+\pi^{11}+2\pi^{13}+\pi^{14}+2\pi^{15}+$ $\pi^{20}+2\pi^{22}+2\pi^{23}+2\pi^{24}+2\pi^{25}+\pi^{26}+2\pi^{27}+$ $\pi^{29}+2\pi^{31}+2\pi^{32}+2\pi^{33}+2\pi^{34}+2\pi^{36}+\pi^{37}+$ $\pi^{38}+\pi^{39}+\pi^{40}+O(\pi^{41})$	$T(T+2)(T^2+2T+2)$	$\frac{(T+2)^5(T^2+2T+2)}{(T^2+T+2)^6}$
$\pi^4+2\pi^5+\pi^7+2\pi^8+2\pi^{13}+\pi^{14}+\pi^{16}+2\pi^{17}+$ $2\pi^{22}+\pi^{23}+\pi^{25}+2\pi^{26}+2\pi^{28}+\pi^{29}+O(\pi^{36})$	$T^2(T+2)$	$\frac{T(T+2)}{(T+1)^6}$
$\pi^4+2\pi^5+\pi^7+\pi^9+2\pi^{10}+\pi^{11}+2\pi^{14}+$ $2\pi^{15}+\pi^{17}+\pi^{18}+2\pi^{19}+2\pi^{21}+2\pi^{22}+\pi^{23}+$ $2\pi^{25}+2\pi^{27}+2\pi^{28}+\pi^{29}+2\pi^{32}+2\pi^{33}+$ $2\pi^{34}+2\pi^{35}+O(\pi^{36})$	$(T+1)^2(T^2+2T+2)$	$\frac{(T+1)^4(T^2+2T+2)^2}{T^6(T+2)^6}$
$\pi^5+2\pi^7+\pi^8+2\pi^9+\pi^{11}+2\pi^{13}+\pi^{14}+2\pi^{15}+$ $\pi^{20}+2\pi^{22}+2\pi^{23}+2\pi^{24}+2\pi^{25}+\pi^{26}+2\pi^{27}+$ $\pi^{29}+2\pi^{31}+2\pi^{32}+2\pi^{33}+2\pi^{34}+2\pi^{36}+$ $\pi^{37}+\pi^{38}+\pi^{39}+\pi^{40}+O(\pi^{41})$	$(T+2)(T^2+2T+2)$	$\frac{(T+2)^5(T^2+2T+2)}{(T^2+T+2)^6}$

5.7.2 Elliptic curves over characteristic $p > 3$

In case $\mathrm{char}(K) \neq 2, 3$ it is more complicated to make a change of variables from the Tate curve to a model depending only on one parameter as the curve $y^2 + xy = x^3 + A_6$, used in characteristic 2 and 3. So we need to look for other model isomorphic to the Tate curve, in which we can claim rationality.

Let p be a prime greater than 3. Recall the definition of the Eisenstein series $E_4 = 1 + 240s_3(\mathbf{q})$ and $E_6 = 1 - 504s_5(\mathbf{q})$ and define also their normalization as $g_2 = \frac{1}{12}E_4$ and $g_3 = -\frac{1}{216}E_6$.

We consider now the following model for our elliptic curve

$$E_{Eis} : y^2 = 4x^3 - g_2x - g_3 \tag{5.20}$$

with the admissible change of variables

$$\begin{aligned} x &= x - \frac{1}{12}, \\ y &= y - \frac{1}{2}x + \frac{1}{24}. \end{aligned}$$

We can transform the Tate curve into the Eisenstein curve where the coefficients satisfy the known relations

$$\begin{aligned} -g_2 &= a_4 + \frac{1}{48} \\ -g_3 &= a_6 - \frac{1}{12}a_4 + \frac{1}{864}. \end{aligned}$$

From Theorem 5.4.3 we now deduce that there exists integers n_p and m_p such that $g_2^{n_p}$ and $g_3^{m_p}$ are rational and these integers depend on the class of p modulo 12 as follows.

Proposition 5.7.9. *Let $p > 3$ be a prime number and g_2 and g_3 the normalized Eisenstein series defined as above. Then $g_2^{n_p}, g_3^{m_p}$ are in $\mathbb{F}_p(T)$ where*

$$(n_p, m_p) = \begin{cases} (\frac{p-1}{4}, \frac{p-1}{6}) & \textit{if} \quad p \equiv 1 \pmod{12} \\ (\frac{p-1}{4}, \frac{p-1}{2}) & \textit{if} \quad p \equiv 5 \pmod{12} \\ (\frac{p-1}{2}, \frac{p-1}{6}) & \textit{if} \quad p \equiv 7 \pmod{12} \\ (\frac{p-1}{2}, \frac{p-1}{2}) & \textit{if} \quad p \equiv 11 \pmod{12}. \end{cases}$$

Proof. From Theorem 5.4.3 we have that there exists a polynomial $A(X, Y) \in \mathbb{F}_p[X, Y]$ such that $A(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_{p-1} = 1$ where $\widetilde{Q}$ and $\widetilde{R}$ are the reduction of the series E_4 and E_6 modulo p, respectively. Since g_2 and g_3 are the normalized series of E_4 and E_6 it is enough to prove the claims for $\widetilde{Q}$ and $\widetilde{R}$.

From Proposition 5.4.4 we have that A is a modular form of weight $(p-1)/2$ and we can write it as

$$A(X, Y) = F(X^3, Y^2)X^iY^j$$

where F is a homogeneous polynomial of degree d and A has pseudo degree $6d + 2i + 3j = (p-1)/2$. The exponents i and j depend on the congruence of $p-1$ modulo 12.

The elliptic curve (5.11) considered over $\mathbb{F}_p(\widetilde{Q}, \widetilde{R})$ has discriminant $\Delta = \frac{1}{1728}(\widetilde{Q}^3 - \widetilde{R^2})$ and j-invariant $j = \frac{1728\widetilde{Q}^3}{\Delta}$. Since j is a rational function it is easy to see that $\frac{\widetilde{Q}^3}{\widetilde{R}^2}$ is a rational function, that is, there exists a $f \in \mathbb{F}_p(T)$ such that $\frac{\widetilde{Q}^3}{\widetilde{R}^2} = f$.

Let us write

$$A(X,Y) = \sum_{l=0}^{d} X^{3l} X^{2(d-l)} X^i Y^j \alpha_l \tag{5.21}$$

for suitable $\alpha_l \in \mathbb{F}_p$. In view of $A(\widetilde{Q}, \widetilde{R}) = 1$ and $\widetilde{Q}^3 = f\widetilde{R}^2$ we have that

$$\begin{aligned} A(\widetilde{Q}, \widetilde{R}) &= \left(\sum_{l=0}^{d} \widetilde{Q}^{3l} \widetilde{R}^{2(d-l)} \alpha_l \right) \widetilde{Q}^i \widetilde{R}^j \\ &= \sum_{l=0}^{d} f^l \widetilde{R}^{2l} \widetilde{R}^{2d+j} \widetilde{R}^{-2l} \widetilde{Q}^i \alpha_l \\ &= \sum_{l=0}^{d} f^l \widetilde{R}^{2d+j} \widetilde{Q}^i \alpha_l \\ &= \left(\sum_{l=0}^{d} f^l \alpha_l \right) \widetilde{R}^{2d+j} \widetilde{Q}^i \\ &= 1. \end{aligned} \tag{5.22}$$

On the other hand, we have also that

$$\begin{aligned} A(\widetilde{Q}, \widetilde{R}) &= \left(\sum_{l=0}^{d} \widetilde{Q}^{3l} \widetilde{R}^{2(d-l)} \alpha_l \right) \widetilde{Q}^i \widetilde{R}^j \\ &= \sum_{l=0}^{d} \widetilde{Q}^{3l} \widetilde{Q}^{3d+i} f^{-(d-l)} \widetilde{Q}^{-3l} \widetilde{R}^j \alpha_l \\ &= \sum_{l=0}^{d} f^{-(d-l)} \widetilde{Q}^{3d+i} \widetilde{R}^j \alpha_l \\ &= \left(\sum_{l=0}^{d} f^{-(d-l)} \alpha_l \right) \widetilde{Q}^{3d+i} \widetilde{R}^j \\ &= 1. \end{aligned} \tag{5.23}$$

Then from (5.22) and (5.23) we have that $\widetilde{R}^{2d+j}\widetilde{Q}^i$ and $\widetilde{Q}^{3d+i}\widetilde{R}^j$ are rational functions for $i, j \in \{0, 1\}$.

1. If $p \equiv 1 \pmod{12}$ then from Proposition 5.4.4 $A(X,Y) = F(X^3, Y^2)$ that is, $i = j = 0$ then A has pseudo degree $6d = (p-1)/2$ and we have that $\widetilde{R}^{2d}$ and $\widetilde{Q}^{3d}$ are rational functions, hence $\widetilde{R}^{(p-1)/6}$ and $\widetilde{Q}^{(p-1)/4}$ are in $\mathbb{F}_p(T)$.

2. If $p \equiv 5 \pmod{12}$ we have in this case that $A(X,Y) = F(X^3, Y^2)X$ with pseudo-degree $6d + 2 = (p-1)/2$. Since $\widetilde{R}^{2d+j}\widetilde{Q}^i$ and $\widetilde{Q}^{3d+i}\widetilde{R}^j$ are rational functions then for $i = 1$ and $j = 0$ we get $\widetilde{R}^{2d}\widetilde{Q}$, $\widetilde{Q}^{3d+1} \in \mathbb{F}_p(T)$. Since $3d + 1 = (p-1)/4$, $\widetilde{Q}^{(p-1)/4} \in \mathbb{F}_p(T)$. On the other hand, $\widetilde{R}^{6d}\widetilde{Q^3}$ is also rational, replacing $\widetilde{Q}^3$ by $f\widetilde{R}^2$ we get that $\widetilde{R}^{6d+2}f \in \mathbb{F}_p(T)$ then $\widetilde{R}^{6d+2} = \widetilde{R}^{(p-1)/2}$ is rational.

3. If $p \equiv 7 \pmod{12}$ then $A(X,Y) = F(X^3, Y^2)Y$. In this case A has pseudo-degree $6d+3 = (p-1)/2$. We can proceed as above replacing i and j by 0 and 1, respectively. We have that $\widetilde{R}^{2d+1} = \widetilde{R}^{(p-1)/6}$ and $\widetilde{Q}^{3d}\widetilde{R}$ are rationals. Also $\widetilde{Q}^{6d}\widetilde{R}^2 = \left(\widetilde{Q}^{3d}\widetilde{R}\right)^2$ is rational. Then since $\widetilde{R}^2 = \widetilde{Q}^3 f^{-1}$ we have that $\widetilde{Q}^{6d+3}f^{-1} \in \mathbb{F}_p(T)$ which implies that $\widetilde{Q}^{6d+3} = \widetilde{Q}^{(p-1)/2} \in \mathbb{F}_p(T)$.

4. If $p \equiv 11 \pmod{12}$ then the polynomial A is $A(X,Y) = F(X^3, Y^2)XY$ with pseudo-degree $6d + 5 = (p-1)/2$ and therefore $\widetilde{R}^{2d+1}\widetilde{Q}$ and $\widetilde{Q}^{3d+1}\widetilde{R}$ are in $\mathbb{F}_p(T)$. In view of and $\widetilde{Q}^3 = f\widetilde{R}^2$ we have that $\widetilde{R}^{6d+3}\widetilde{R}^2 f$ is rational. Then $\widetilde{R}^{6d+5} = \widetilde{R}^{(p-1)/2} \in \mathbb{F}_p(T)$. Analogously, $\widetilde{Q}^{6d+2}\widetilde{Q}^3 f^{-1}$ is rational, which implies that $\widetilde{Q}^{(p-1)/2} \in \mathbb{F}_p(T)$.

□

Let us suppose that we have $g_2^{n_p} = \frac{f(T)}{g(T)}$ and $g_3^{m_p} = \frac{r(T)}{s(T)}$ for some polynomials $f(T), g(T), r(T), s(T) \in \mathbb{F}_p[T]$ (no necessarily monic cf. Example 5.7.15). Then we have that the curve E_{Eis} (5.20) is

$$y^2 = 4x^3 - \chi_{n_p}\left(\frac{f(T)}{g(T)}\right)^{1/n_p} x - \quad \xi_{m_p}\left(\frac{r(T)}{s(T)}\right)^{1/m_p}$$

where χ_{n_p} and ξ_{m_p} are n_p-th and m_p-th roots of the unity in $\mathbb{F}_p$, respectively, note that $n_p, m_p | p-1$, so that χ_{n_p} and χ_{n_p} indeed lie in $\mathbb{F}_p$. So the curve E_{Eis} is defined over a finite extension of $\mathbb{F}_p(T)$.

Let E be an elliptic curve over a field K of the form $Y^2 = X^3 + AX + C$ and $u \in K$ then the elliptic curve $E_u : Y^2 = X^3 + u^2AX + u^3B$ is a twist of E. Taking $u = 1/\sqrt{A}$ the curve E_u is $Y^2 = X^3 + X + \frac{B}{\sqrt[2]{A^3}}$.

When E is $E_{Eis} : y^2 = 4x^3 - g_2x - g_3$ we can carry out the twist as follows, let us suppose that $g_2^{n_p}$ and $g_3^{m_p}$ are as above, then taking $u^2 = \left(\frac{g(T)}{f(T)}\right)^{1/n_p}$ we get

$$
\begin{aligned}
y^2 &= 4x^3 - u^2\xi_{n_p}\left(\frac{f(T)}{g(T)}\right)^{1/n_p} x - u^3\chi_{m_p}\left(\frac{r(T)}{s(T)}\right)^{1/m_p} \rightsquigarrow \\
y^2 &= 4x^3 - \xi_{n_p}x - \quad \chi_{m_p}\left(\frac{r(T)}{s(T)}\right)^{1/m_p}\left(\frac{g(T)}{f(T)}\right)^{3/2n_p} .
\end{aligned}
$$

Remark 5.7.10. *This twisted elliptic curve may or not be defined over $\mathbb{F}_p(T)$, because the quantity $\left(\frac{r(T)}{s(T)}\right)^{1/m_p}\left(\frac{g(T)}{f(T)}\right)^{3/2n_p}$ is not always rational. However, by reviewing examples, heuristically we can say that after simplifications this expression becomes $F(T)G(T)^{1/2}$ for some rational functions $F(T)$ and $G(T)$. If $G(T)$ is not one, then we need to make another twist by taking $u = (G(T))^{-1/2}$. The resulting elliptic curve has always the right conductor.*

Algorithm 2: `Tatefor`$p > 3$

Input: The Tate parameter $\mathbf{q}$ up to accuracy of π^M.

Output: An elliptic curve in the isogeny class of the Tate curve associated to $\mathbf{q}$ or a message *"Accuracy too small, please increase M".*

```
Calculate the quantities $s_3$ and $s_5$ using the formula (5.15) and use them to calculate the coefficients of the Eisenstein curve $g_2$ and $g_3$ up to accuracy $\pi^M$.
set the quantities $n_p$ and $m_p$ as the exponents of $g_2$ and $g_3$, respectively. According to Proposition 5.7.9
use the algorithm of continued fractions to find the representation of $g_2^{n_p}$ and $g_3^{m_p}$ as a rational functions. Let say $g_2^{n_p} = \frac{f(T)}{g(T)}$ and $g_3^{m_p} = \frac{r(T)}{s(T)}$.
define two list $L_{n_p}$ and $L_{m_p}$ which contain the $n_p$-th and $m_p$-th roots of the unity in $\mathbb{F}_p$, respectively.
for $\xi_{n_p} \in L_{n_p}$ do
    for $\chi_{m_p} \in L_{m_p}$ do
        define the elliptic curve
            $$E : y^2 = 4x^3 - \xi_{n_p}x - \chi_{m_p}\left(\frac{r(T)}{s(T)}\right)^{1/m_p}\left(\frac{g(T)}{f(T)}\right)^{3/2n_p}$$
        .
        write $\left(\frac{r(T)}{s(T)}\right)^{1/m_p}\left(\frac{g(T)}{f(T)}\right)^{3/2n_p}$ as $F(T)G(T)^{1/2}$.    ▷ cf. Remark 5.7.10.
        if $G(T) \neq 1$ then
            set $u = (G(T))^{-1/2}$ and define the twisted curve
                $$E : y^2 = 4x^3 - \xi_{n_p}G(T)^{-1}x - \chi_{m_p}F(T)G(T)^{-1}$$
        end if
    end for
end for
calculate the conductor of $E$ let say $c$
if $c = N\infty$ then
    Return $E$
else
    Return "Accuracy too small, please increase M "    ▷ This message is printed if after considering all possible elliptic curves we do not get the right conductor.
```

```
end if
```

Remark 5.7.11. *If the prime p is a large prime then the numbers n_p and m_p are also big then one needs high accuracy to get convergence, in this cases it is better to consider other twist. Let $u = \frac{g_2}{g_3}$ then the twisted curve is*

$$y^2 = 4x^3 - u^2 g_2 x - u^3 g_3 \rightsquigarrow y^2 = 4x^3 - \frac{g_2^3}{g_3^2}x - \frac{g_2^3}{g_3^2}$$

since $\frac{g_2^3}{g_3^2}$ is a rational function, the curve is defined over K. The j-invariant of $y^2 = 4x^3 - Ax - A$ is $j = 1728\frac{A}{A-27}$. Solving for A shows that $j \in K$ if and only if $A \in K$. However the cost of this twist is that a lot of extra places may appear in the conductor, which one has later to get rid of. One can see, for instance Example 5.7.12 that the present form is not isogenous over K to the searched Weierstrass equation. It is only correct up to some unspecified quadratic twist.

Example 5.7.12. In characteristic 5.

With $p = 5$ consider the polynomial $N = T^2(T-1)$. The dimension of the space of harmonic cocycles is 4, then we have 4 isogeny classes. Let φ one of these harmonic cocycles with rational Hecke eigenvalues. In characteristic 5, we have that $E_4 = 1$ and $g_2 = 3$ and the Eisenstein form is

$$E_{Eis} : y^2 = 4x^3 + 2x - g_3.$$

Since $p-1$ is divisible by 4 and not by 6 then we have that $g_3^{(p-1)/2} \in \mathbb{F}_5(T)$. With an accuracy of $M = 70$ we get the Tate parameter

$$\begin{aligned}\mathbf{q} = \pi^2 &+ 2\pi^4 + \pi^5 + 4\pi^6 + 3\pi^8 + \pi^9 + 2\pi^{10} + 4\pi^{11} + 4\pi^{12} + 2\pi^{13} + \\ &4\pi^{14} + 3\pi^{15} + \pi^{16} + 2\pi^{17} + 3\pi^{19} + 4\pi^{20} + \pi^{21} + 2\pi^{22} + 2\pi^{23} + 3\pi^{24} + \\ &4\pi^{26} + 3\pi^{27} + 2\pi^{28} + 2\pi^{29} + 2\pi^{30} + 2\pi^{31} + 4\pi^{33} + 3\pi^{34} + \pi^{35} + 2\pi^{36} + \\ &4\pi^{37} + \pi^{39} + 3\pi^{40} + 2\pi^{41} + 2\pi^{42} + \pi^{43} + 2\pi^{44} + 4\pi^{45} + 3\pi^{46} + 4\pi^{47} + \\ &4\pi^{48} + 2\pi^{50} + \pi^{51} + 3\pi^{52} + \pi^{53} + 3\pi^{55} + 4\pi^{56} + 3\pi^{57} + 2\pi^{58} + 2\pi^{59} + \\ &2\pi^{60} + 2\pi^{61} + 4\pi^{62} + \pi^{64} + 3\pi^{65} + 2\pi^{66} + 3\pi^{67} + 4\pi^{68} + 4\pi^{69} + 4\pi^{70} + O(\pi^{71}).\end{aligned}$$

Plugging in this value in the equation of g_3 and applying the continuous fraction method we have that the series g_3^2 converges to the rational function $\frac{T(T+2)^2}{(T+3)^3}$. Using Algorithm 2 with $F(T) = \frac{T+2}{T+3}$ and $G(T) = \frac{T}{T+3}$, the equation for the elliptic curve E_{Eis} is

$$\begin{aligned} y^2 = 4x^3 + 2x - g_3 \rightsquigarrow y^2 &= x^3 + 2x - \xi_2 \frac{T+2}{T+3}\sqrt{\frac{T}{T+3}} \\ \rightsquigarrow y^2 &= x^3 + \frac{3T+4}{T}x + \frac{4T+3}{T} \end{aligned}$$

which has conductor $T^2(T-1)\infty$. To get the last equation we make a quadratic twist with $u = \sqrt{\frac{T+3}{T}}$ and $\xi_2 = 4$.

Remark 5.7.13. *In [Sch11] is given the elliptic curve $E_1 : y^2 = x^3 + 4T^2x^2 + 4T^3x$ as a representative of the isogeny class of E_{Eis}. They are isomorphic, namely the isomorphism is given by*

$$\begin{aligned} E_{Eis} &\longrightarrow E_1 \\ (x, y) &\mapsto (T^2x + 2T^2, T^3y). \end{aligned}$$

Example 5.7.14. In characteristic 7.

Let us consider the polynomial $N = T^3-2$ over $\mathbb{F}_7$. In this case we have that the dimension of the space of harmonic cocycles is 1 so there is only isogeny class. With an accuracy of $M = 60$ we find the value of the Tate parameter is

$$\begin{aligned} \mathbf{q} = 5\pi^3 &+ 4\pi^6 + p^9 + 6\pi^{12} + 2\pi^{15} + p^{18} + p^{21} + 2\pi^{24} \\ &+p^{27} + 3\pi^{30} + 5\pi^{33} + 2\pi^{36} + 5\pi^{39} + 5\pi^{42} + 5\pi^{45} + \\ &4\pi^{48} + 5\pi^{51} + 6\pi^{54} + 4\pi^{57} + 5\pi^{60} + O(\pi^{61}). \end{aligned}$$

When $p = 7$ we have that $g_3 = 6$ and also from the considerations of the modular forms modulo 7, we have that g_2^3 is a rational function. With the value of $\mathbf{q}$ and the formula for g_2 we have that

$$\begin{aligned} g_2 = 1 &+ 3\pi^3 + 3\pi^6 + \pi^9 + 2\pi^{12} + 5\pi^{15} + 3\pi^{18} + 4\pi^{21} + 5\pi^{24} + \\ &4\pi^{27} + \pi^{30} + 2\pi^{33} + 5\pi^{36} + 3\pi^{39} + 4\pi^{42} + 5\pi^{45} + \\ &4\pi^{48} + \pi^{51} + 2\pi^{54} + 5\pi^{57} + 3\pi^{60} + O(\pi^{61}) \end{aligned}$$

and g_2^3 converges to

$$\frac{(T^3+2)^3T^3}{(T^6+2T^3+2)^2}.$$

Then our model for the elliptic curve in the isogeny class is

$$\begin{aligned} y^2 = 4x^3 - g_2x + 1 &\rightsquigarrow y^2 = x^3 + \xi_3\sqrt[3]{\frac{(T^3+2)^3T^3}{(T^6+2T^3+2)^2}}\,x + 5 \\ &\rightsquigarrow y^2 = x^3 + T(T^3+2)x + 5(T^6+2T^3+3). \end{aligned}$$

We get the last equation by twisting with $u = \sqrt[3]{\frac{T^6+2T^3+2}{(T^3+2)^3T^3}}$ and using $\xi_3 = 1$.

Example 5.7.15. In characteristic 11.

Consider the polynomial $N = (T+8)(T+9)^2$ defined over $\mathbb{F}_{11}$, in this case there are 4 different isogeny classes, taking one the harmonic cocycles with rational Hecke eigenvalues and with accuracy $M = 40$ we have the following Tate parameter

$$\begin{aligned} \mathbf{q} = {} & 4\pi + 6\pi^2 + 4\pi^3 + 2\pi^4 + 4\pi^5 + 10\pi^6 + 9\pi^8 + 9\pi^9 + 10\pi^{10} + 8\pi^{11} + \\ & 7\pi^{12} + \pi^{13} + 7\pi^{14} + 10\pi^{15} + 10\pi^{16} + 2\pi^{17} + 9\pi^{18} + 6\pi^{19} + 9\pi^{20} + 6\pi^{21} + \\ & 6\pi^{22} + 7\pi^{24} + 8\pi^{25} + 3\pi^{26} + 2\pi^{27} + 4\pi^{28} + \pi^{29} + 4\pi^{30} + \pi^{31} + 4\pi^{32} + \\ & 4\pi^{33} + 9\pi^{34} + 9\pi^{35} + 8\pi^{36} + 6\pi^{37} + 3\pi^{38} + 10\pi^{39} + 4\pi^{40} + O(\pi^{41}). \end{aligned}$$

Using the relations of Serre and Swinnerton-Dyer, we have that g_2^5 and g_3^5 are rationals. Plugging in the value of $\mathbf{q}$ in the formulas for g_2 and g_3 we have that

$$\begin{aligned} g_2^5 = {} & 1 + 4\pi + 9\pi^2 + 8\pi^3 + 8\pi^4 + 2\pi^5 + 9\pi^6 + 7\pi^7 + 9\pi^9 + 6\pi^{10} + \\ & 3\pi^{11} + 5\pi^{12} + 3\pi^{13} + 10\pi^{14} + 10\pi^{15} + 8\pi^{16} + 3\pi^{17} + 6\pi^{18} + \\ & 3\pi^{20} + 2\pi^{21} + \pi^{22} + 9\pi^{23} + \pi^{24} + 7\pi^{25} + 7\pi^{26} + 10\pi^{27} + \pi^{28} + \\ & 2\pi^{29} + \pi^{31} + 8\pi^{32} + 4\pi^{33} + 3\pi^{34} + 4\pi^{35} + 6\pi^{36} + 6\pi^{37} + 7\pi^{38} + \\ & 4\pi^{39} + 8\pi^{40} + O(\pi^{41}) \end{aligned}$$

and

$$\begin{aligned} g_3^5 = {} & 10 + 4\pi + 4\pi^2 + 6\pi^4 + 2\pi^5 + 6\pi^6 + 5\pi^7 + 7\pi^8 + 8\pi^9 + 4\pi^{10} + \\ & 6\pi^{11} + 8\pi^{12} + 8\pi^{13} + \pi^{15} + 4\pi^{16} + \pi^{17} + 10\pi^{18} + 3\pi^{19} + 5\pi^{20} + \\ & 8\pi^{21} + \pi^{22} + 5\pi^{23} + 5\pi^{24} + 2\pi^{26} + 8\pi^{27} + 2\pi^{28} + 9\pi^{29} + 6\pi^{30} + \\ & 10\pi^{31} + 5\pi^{32} + 2\pi^{33} + 10\pi^{34} + 10\pi^{35} + 4\pi^{37} + 5\pi^{38} + 4\pi^{39} + 7\pi^{40} + O(\pi^{41}), \end{aligned}$$

which converge to $\frac{T^2+7T+4}{T^2+3T+5} = \frac{(T+9)^2}{(T+7)^2}$ and $\frac{10T^2+8T+6}{T^2+7T+4} = \frac{10(T+7)^2}{(T+9)^2}$, respectively. Taking $u^2 =$

$\sqrt[5]{\left(\frac{T+7}{T+9}\right)^2}$, $\xi_5 = 9$ and $\sqrt[5]{10} = 2$, the elliptic curve we are looking for is

$$y^2 = 4x^3 - g_2 x - g_3 \Longrightarrow y^2 = x^3 - \xi_5 \sqrt[5]{\frac{(T+9)^2}{(T+7)^2}} x - \sqrt[5]{\frac{10(T+7)^2}{(T+9)^2}}$$

$$\Longrightarrow y^2 = x^3 - \xi_5 x - 2\sqrt[5]{\left(\frac{T+7}{T+9}\right)^2} \sqrt[5]{\left(\frac{T+7}{T+9}\right)^3}$$

$$\Longrightarrow y^2 = x^3 + 6x + \frac{T+7}{T+9}$$

which has conductor $(T+8)(T+9)^2\infty$.

The other three isogeny classes are given by

$$\begin{aligned}
&E_2 : y^2 = x^3 + 6(T^4 + 6T^2 + 6T + 8)x + 10(T^2 + 2T + 6)(T^4 + 12T^3 + 6T + 9),\\
&E_3 : y^2 = x^3 + 9(T^2 + 11T + 9)x^2 + (T+12)^2(T^2 + 4T + 2),\\
&E_4 : y^2 = x^3 + (T+4)^2 x^2 + (T+2)(T+6)(T+10).
\end{aligned}$$

Example 5.7.16. In characteristic 13.

Consider the polynomial $N = T^3 + 11$ over $\mathbb{F}_{13}$. For this case there is only one harmonic cocycle with rational Hecke eigenvalues and with accuracy of $M = 40$ we have the following Tate parameter

$$\begin{aligned}
\mathbf{q} = {} & 2\pi^3 + 8\pi^6 + 9\pi^9 + \pi^{12} + 6\pi^{15} + 12\pi^{18} + 9\pi^{21} + 4\pi^{24} + 3\pi^{27} + \\
& 2\pi^{30} + 7\pi^{33} + 7\pi^{36} + 7\pi^{39} + O(\pi^{41}).
\end{aligned}$$

In this case we have that g_2^3 and g_3^2 are in $\mathbb{F}_{13}(T)$, then using the value of $\mathbf{q}$ and the formulas for g_2 and g_3 we have that

$$\begin{aligned}
g_2^3 = {} & 1 + 10\pi^3 + 2\pi^6 + 6\pi^9 + 6\pi^{12} + \pi^{15} + 7\pi^{18} + 11\pi^{21} + 3\pi^{24} + \\
& 7\pi^{27} + \pi^{30} + 12\pi^{36} + O(\pi^{41})
\end{aligned}$$

and

$$\begin{aligned}
g_3^2 = {} & 1 + 12\pi^3 + 5\pi^6 + 2\pi^9 + 2\pi^{12} + 9\pi^{15} + 11\pi^{18} + 8\pi^{21} + \pi^{24} + 11\pi^{27} + \\
& 9\pi^{30} + 4\pi^{36} + O(\pi^{41}).
\end{aligned}$$

Using continuous fractions we see that

$$g_2^3 \rightsquigarrow \frac{T^3(T^3+3)^3}{(T^6+2T^3+9)(T^6+10T+6)}$$

and

$$g_3^2 \rightsquigarrow \frac{(T^3+2)^2(T^3+10)^2}{(T^6+2T^3+9)(T^6+10T+6)}.$$

Using these values for g_2^3 and g_3^2, proceeding as in the examples above with $u^2 = \sqrt[3]{\frac{(T^6+2T^3+9)(T^6+10T+6)}{T^3(T^3+3)^3}}$ we have that

$$y^2 = 4x^3 - g_2x - g_3 \Longrightarrow y^2 = x^3 - \xi_3 x - (T^3+2)(T^3+10)\sqrt[2]{\frac{1}{T(T^3+3)}}$$

$$\Longrightarrow y^2 = x^3 + 3T(T+3)x + 3(T^3+2)(T^3+10).$$

We get the equation using the twist described in Algorithm 2 with $F(T) = (T^3+2)(T^3+10)$ and $G(T) = \frac{1}{T(T^3+3)}$.

A. Algorithms for the Quotient graph

In this appendix we shall provide the reader with some of the algorithms used in the thesis to deal with quotient graphs. In §2 we give a set of representatives for the edges of the quotient tree $\Gamma_0 \setminus \mathcal{T}$ where $\Gamma_0 = GL_2(A)$, and also give a routine, which we call `decom`, to calculate classes in $\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty$. In §3 we use the algorithm `decom` to lift a cycle in the quotient graph $\Gamma_0(N) \setminus \mathcal{T}$ to a path in $\mathcal{T}$. The algorithm `decom` gives a routine to solve the following problem: given two matrices $g_1, g_2 \in GL_2(K_\infty)$ which are in the same class in $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$, there exist $\gamma \in \Gamma_0(N)$ and $\kappa \in \mathcal{I}_\infty$ such that $g_1 = \gamma g_2 \kappa$. The algorithm that allows us to write such as decomposition is given in §4.

Also, we include a section that sets out the key definitions and results of computer arithmetic, which we need to give the running time of the main algorithms that allows us to calculate the Tate parameter.

A.1 Computational complexity of mathematical operations

The aim of this section is to give a brief summary of some fundamental definitions and results concerning computer arithmetic, algorithms for arithmetic in finite fields and polynomial rings. The intention is not to provide an implementation guide, instead, we state some complexity results that will be used later in the appendices of this thesis. More details of these subjects can be found in [vzGG13].

Since computers do not work on numbers but with data, so the very first issue is how to feed numbers as a data into a computer. Data are stored in pieces called *words.* Current machines use either 32 or 64-bit words; in this thesis we assume that we have a 64-bit processor. Integers are represented as a sequence of binary words. We think of an algorithm as a sequence of word operations. The *analysis of running time* of an algorithm (or just *running time*) quantifies the amount of time taken by the algorithm to run as a function of the length of the string representing the input. We can think of the running time as the number of statements executed by the program or as the length of time taken to run the program on some standard computer. It is common to estimate their complexity in the asymptotic sense, *i.e.*, estimating the complexity function for arbitrarily large input, so we introduce the following definition.

Definition A.1.1. Let f and g be two functions defined on some subset of the real numbers. One writes

$$f(x) = O(g(x)) \text{ as } x \to \infty$$

if and only if there exists a positive real number C and a real number x_0 such that

$$|f(x)| \leq \ C|g(x)| \text{ for all } x \geq x_0.$$

Let R be a commutative ring with 1. Operations like add or multiply may correspond to many bit or word operations. As a general rule, we will consider the number of arithmetic operations (additions and multiplications) in the ring R, (divisions, if R is a field) used by an algorithm. The other operations such as index calculations or memory accesses, tend to be of the same order of magnitude. These are usually performed with machine instructions on single words (for example move a pointer in an array, etc), and their cost becomes negligible when the arithmetic quantities are large. The next result can be found in [vzGG13, Cor. 4.7].

Lemma A.1.2. *Let $q = p^n$ with p a prime number and $n \geqslant 1$. One arithmetic operation, that is, addition, multiplication, or division, over $\mathbb{F}_q$ can be done using $O(n^2)$ word operations, where $n = \lfloor \log_2(q)/64 \rfloor + 1$.*

Let $R[x]$ be the polynomial ring with coefficients in R. The basic algorithms for addition, subtraction, multiplication, and division of polynomials are quite straightforward adaptations of the corresponding algorithms for integers. In fact, because of the lack of "carry overs" these algorithms are actually much simpler in the polynomial case. We have the following easy result.

Lemma A.1.3. *Let f and g be arbitrary polynomials in $R[x]$ of degree n and m, respectively.*

1. *We can compute $f + g$ with $O(n + m)$ operations in R.*

2. *We can compute fg with $O(nm)$ operations in R.*

3. *If $g \neq 0$ and the leading coefficient of g is a unit in R, we can compute $q, r \in R[x]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$ with $O(\deg(g)\deg(q))$ operations in R.*

Remark A.1.4. *Throughout the book [vzGG13], the authors discuss four algorithms to do fast multiplication of polynomials, the classical one, Karatsuba ([*Ibid., §*8.1]), Fast Fourier Transform (FFT) ([*Ibid., §*8.2]) and Shönhage & Strassen ([*Ibid., §*8.3]. Due to the variety of multiplication algorithms, we introduce the following definition.*

Definition A.1.5. Let R be a commutative ring with 1. We call a function $M : \mathbb{N} \longrightarrow \mathbb{R}_{>0}$ a *multiplication time for* $R[x]$ if polynomials in $R[x]$ of degree lest than n can be multiplied using at most $M(n)$ operations in R.

The following table summarizes the multiplication times for the algorithms mentioned above.

Algorithm	$M(n)$
Classical	$2n^2$
Karatsuba	$O(n^{1.59})$
FFT	$O(n\log(n))$
Shönhage & Strassen	$O(n\log(n)\log(\log(n)))$

A.2 Representatives for the edges of $\Gamma_0 \setminus \mathcal{T}$

In the first part of this section, we recall some definitions, in order to fix the notation. We define the *Iwahori subgroup* of $GL_2(K_\infty)$ as

$$\mathcal{I} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(O_\infty) \;\middle|\; c \equiv 0 \pmod{\pi} \right\}. \tag{A.1}$$

We denote by $\mathcal{I}_\infty = \mathcal{I}K_\infty^\times$. Analogously, $\mathcal{K}$ and $\mathcal{K}_\infty$ denote the groups $GL_2(O_\infty)$ and $GL_2(O_\infty)K_\infty^\times$, respectively.

In the rest of this appendix, we denote by Γ_0 the group $GL_2(A)$ and by $\Gamma_0(N)$ the subgroup of Γ_0 consisting of matrices which are upper triangular modulo N, where N is a polynomial in $A = \mathbb{F}_q[T]$.

The Bruhat-Tits tree for $GL_2(K_\infty)$ is denoted by $\mathcal{T}$ (cf. §2.4), while the quotients $\Gamma_0 \setminus \mathcal{T}$ and $\Gamma_0(N) \setminus \mathcal{T}$ are denoted by $\mathcal{G}_1$ and $\mathcal{G}_N$, respectively. We use also the notation $\mathcal{G}_{N,M}$ for the quotient graph $\mathcal{G}_N$ with the cusps up to level M.

The classes in $GL_2(K_\infty)/\mathcal{I}_\infty$ will be denoted by $[\cdot]_1$ and the classes in $GL_2(K_\infty)/\mathcal{K}_\infty$ by $[\cdot]_0$. Also the classes of edges and vertices in the double quotient $\Gamma_0 \setminus \mathcal{T}$ are denoted by $[\![\cdot]\!]_1$ and $[\![\cdot]\!]_0$, respectively. In the case of the quotient graph by the subgroup $\Gamma_0(N)$ we add the subindex N.

The edges and vertices of a graph $\mathcal{G}$ will be denoted by $Y(\mathcal{G})$ and $X(\mathcal{G})$, respectively.

Notation: Let H be a subgroup of a group G. We say that $\mathcal{S} = \{s_1, s_2, ...\} \subseteq G$ is a set of representatives for the quotient $H \setminus G$ if for all $g \in G$, there exist $h \in H$ and a unique $s_i \in \mathcal{S}$ such that $g = hs_i$. Analogously for H_1 and H_2 subgroups of G, we say that $\mathcal{S}$ is a set of representatives for the double quotient $H_1 \setminus G/H_2$ if for all $g \in G$, there exist $h_1 \in H_1$, $h_2 \in H_2$ and a unique $s_i \in \mathcal{S}$ such that $g = h_1 s_i h_2$.

We know that $\mathcal{G}_1$ is isomorphic to the subgraph in $\mathcal{T}$ whose vertices are $\{[k, 0]\}_{k \geqslant 0}$ (cf. Lemma 2.4.4 for the definition). The following theorem (cf. [Ser03, p. 87]) gives a set of representatives for the vertices of $\mathcal{G}_1$.

Proposition A.2.1. *A set of representatives for* $\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty$ *is given by*

$$\left\{ \Lambda_n = \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix} \quad \textit{for} \quad n \geqslant 0 \right\}.$$

That is, given $g \in GL_2(K_\infty)$ *there exist a unique* $n \geqslant 0$*,* $\gamma \in \Gamma_0$ *and* $\alpha \in \mathcal{K}_\infty$ *such that*

$$g = \gamma \Lambda_n \alpha.$$

Notation: Let $g \in GL_2(K_\infty)$, we say that the vertex represented by g has "level" n if $g \in [\![\Lambda_n]\!]_0$.

In [But07, Lemma 18] one can find a constructive proof of Proposition A.2.1. There, the author explains how to decompose any $g \in GL_2(K_\infty)$ as $g = \gamma \Lambda_n \alpha$. So in this appendix we assume that we already have an algorithm that allows us to write such decomposition.

Before giving a set of representatives for the edges of $\mathcal{G}_1$ we need to define some functions and sets that will be useful in this section. Let us define first the function *origin* as follows

$$\begin{aligned} o_1 := \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty &\longrightarrow \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty \,. \\ [\![g]\!]_1 &\longmapsto o_1([\![g]\!]_1) = [\![g]\!]_0 \end{aligned} \tag{A.2}$$

That is, given $g \in GL_2(K_\infty)$ we define the origin of the class $\Gamma_0 g \mathcal{I}_\infty$ to be the vertex represented by $\Gamma_0 g \mathcal{K}_\infty$. The function o_1 is surjective and is not injective. So it is important to describe the fibers of classes in $\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty$.

Let $g \in GL_2(K_\infty)$ then

$$o_1^{-1}\left(\Gamma_0 g \mathcal{K}_\infty\right) = \left\{\Gamma_0 h \mathcal{I}_\infty \mid \Gamma_0 h \mathcal{K}_\infty = \Gamma_0 g \mathcal{K}_\infty\right\}.$$

Let $g_1, g_2 \in GL_2(K_\infty)$ such that $\Gamma_0 g_1 \mathcal{K}_\infty = \Gamma_0 g_2 \mathcal{K}_\infty$ and $\Gamma_0 g_1 \mathcal{I}_\infty \neq \Gamma_0 g_2 \mathcal{I}_\infty$. That is, g_1 and g_2 represent different edges with the same origin, then $g_1 \in \Gamma_0 g_2 \mathcal{K}_\infty$ and $g_1 \notin \Gamma_0 g_2 \mathcal{I}_\infty$. Hence in order to understand how many classes there are in $o_1^{-1}\left(\Gamma_0 g \mathcal{K}_\infty\right)$ we need to study the number of orbits of Γ_0 in $g_2 \mathcal{K}_\infty/\mathcal{I}_\infty$, where Γ_0 acts $g_2 \mathcal{K}_\infty/\mathcal{I}_\infty$ via left matrix multiplication.

A straightforward calculation shows that there is a 1-1 correspondence between $\mathcal{K}_\infty/\mathcal{I}_\infty = \mathcal{K}/\mathcal{I}$ and $\mathbb{P}^1(\mathbb{F}_q)$ given by

$$\begin{aligned} \mathcal{K}/\mathcal{I} &\longrightarrow \mathbb{P}^1(\mathbb{F}_q). \\ \left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right)\mathcal{I} &\longmapsto (a \pmod{\pi} : c \pmod{\pi}). \end{aligned}$$

Hence a set of representatives for $\mathcal{K}/\mathcal{I}$ is

$$\mathcal{R} = \left\{ \left(\begin{array}{cc} s & 1 \\ 1 & 0 \end{array} \right) \middle| \, s \in \mathbb{F}_q \right\} \bigcup \left\{ \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \right\}.$$

Proposition A.2.2. *Let $g \in GL_2(K_\infty)$.*

1. *If $g = \mathbb{I}_2$ then $\#\Gamma_0 \setminus \mathcal{K}_\infty/\mathcal{I}_\infty = 1$. That is, Γ_0 acts transitively on $\mathcal{K}_\infty/\mathcal{I}_\infty$.*
2. *If $g \notin [\![\mathbb{I}_2]\!]_1$ then $\#\Gamma_0 \setminus g\mathcal{K}_\infty/\mathcal{I}_\infty = 2$ and $\Gamma_0 \setminus g\mathcal{K}_\infty/\mathcal{I}_\infty = \{\Gamma_0 g \mathcal{I}_\infty, \Gamma_0 g s_1 \mathcal{I}_\infty\}$ where $s_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

Proof. 1. Let $\left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right)$ be an element of $\mathcal{R}$, for a $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_0$ we have

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} s & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha s + \beta & \alpha \\ \gamma s + \delta & \gamma \end{pmatrix}. \tag{A.3}$$

From (A.3) we see that $\mathbb{I}_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is an element of this orbit since $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -s \end{smallmatrix}\right) \in \Gamma_0$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -s \end{smallmatrix}\right)\left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then the orbit of $\mathbb{I}_2$ intersect all orbits of $\left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for all $s \in \mathbb{F}_q$. Hence there exists only one orbit and $\#\Gamma_0 \setminus \mathcal{K}_\infty/\mathcal{I}_\infty = 1$.

2. If $g \notin [\![\mathbb{I}_2]\!]$, without loss of generality (Prop. A.2.1) we may consider $g = \left(\begin{smallmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for some $n \geqslant 1$, that is,

$$\begin{aligned} g &= \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix}\begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix} \\ &= \Lambda_n \begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix}. \end{aligned}$$

First note that for $s, s' \in \mathbb{F}_q$ with $s \neq s'$ the orbits of $\left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and of $\left(\begin{smallmatrix} s' & 1 \\ 1 & 0 \end{smallmatrix}\right)$ intersect each other, indeed, let $\gamma = \left(\begin{smallmatrix} 1 & T^n(s'-s) \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0$, then γ verifies

$$\begin{pmatrix} 1 & T^n(s'-s) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} sT^n & T^n \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} s'T^n & T^n \\ 1 & 0 \end{pmatrix}.$$

On the other hand, for all $s \in \mathbb{F}_q$ the orbit of $\mathbb{I}_2$ does not intersect the orbit of $\left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right)$. It is enough to prove that $\Gamma_0 g_0^{(n)} \mathcal{I}_\infty \neq \Gamma_0 g_0^{(n)} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \mathcal{I}_\infty$. Suppose to the contrary that they are equal, then we have

$$\begin{aligned} \Gamma_0 g_0^{(n)} \mathcal{I}_\infty = \Gamma_0 g_0^{(n)} s_1 \mathcal{I}_\infty &\iff s_1 \in g_0^{(n)^{-1}} \Gamma_0 g_0^{(n)} \mathcal{I}_\infty \\ &\iff g_0^{(n)^{-1}} \Gamma_0 g_0^{(n)} \cap \mathcal{I}_\infty s_1 \neq \emptyset. \end{aligned}$$

Let $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \rho \end{smallmatrix}\right)$ in Γ_0 then we have

$$g_0^{(n)^{-1}} \begin{pmatrix} \alpha & \beta \\ \gamma & \rho \end{pmatrix} g_0^{(n)} = \begin{pmatrix} \alpha & \beta T^{-n} \\ \gamma T^n & \rho \end{pmatrix}. \tag{A.4}$$

On the other hand, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathcal{I}_\infty$ we have

$$\begin{aligned}\begin{pmatrix} a & b \\ c & d \end{pmatrix} s_1 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} b & a \\ d & c \end{pmatrix}. \end{aligned} \tag{A.5}$$

Then from equations (A.4) and (A.5) we have $d = \gamma T^n$. But $d \in \mathcal{O}_\infty$ and $\mathrm{val}(\gamma T^n) \geqslant n \geqslant 1$ since $n > 0$, and we get a contradiction. The claim follows.

□

Remark A.2.3. *From Proposition A.2.2 we have*

a) The fiber $o_1^{-1}([\![\mathbb{I}_2]\!]_0)$ has only one element. That is, there is only one edge with origin $[\![\mathbb{I}_2]\!]_0$.

b) If $g \neq \mathbb{I}_2$ there are exactly two edges with origin $[\![g]\!]_0$, namely, the class $[\![g]\!]_1$ and $[\![gs_1]\!]_1$ where $s_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

The following is a portion of the graph $\Gamma_0 \setminus \mathcal{T}$.

$$\begin{tikzcd}
{[\![\Lambda_0]\!]_0} \arrow[r, bend left, "g_0^{(0)}"] & {[\![\Lambda_1]\!]_0} \arrow[l, bend left, "g_0^{(-1)}"] \arrow[r, bend left, "g_0^{(1)}"] & {[\![\Lambda_2]\!]_0} \arrow[l, bend left, "g_0^{(-2)}"] \arrow[r, bend left, "g_0^{(2)}"] & {[\![\Lambda_3]\!]_0} \arrow[l, bend left, "g_0^{(-3)}"] \arrow[r, bend left, "g_0^{(3)}"] & \cdots \arrow[l, bend left, "g_0^{(-4)}"]
\end{tikzcd}$$

Corollary A.2.4. *The set*

$$\mathcal{R}_{\Gamma_0} = \left\{ \begin{pmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{pmatrix} \middle| \, n \geqslant 0 \right\} \bigcup \left\{ \begin{pmatrix} 0 & \pi^n \\ 1 & 0 \end{pmatrix} \middle| \, n < 0 \right\} \tag{A.6}$$

is a set of representatives for the edges of $\Gamma_0 \setminus \mathcal{T}$.

Let us denote the elements of $\mathcal{R}_{\Gamma_0}$ by $g_0^{(n)}$, i.e., *$g_0^{(n)} = \left(\begin{smallmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for $n \geqslant 0$ and $g_0^{(n)} = \left(\begin{smallmatrix} 0 & \pi^n \\ 1 & 0 \end{smallmatrix}\right)$ for $n < 0$. Then given $g \in GL_2(K_\infty)$ there exist $n \in \mathbb{Z}$, $\gamma \in \Gamma_0$ and $\kappa \in \mathcal{I}_\infty$ such that $g = \gamma g_0^{(n)} \kappa$.*

Proof. From Proposition A.2.1 we have that the matrix $\Lambda_n = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi^n \end{smallmatrix}\right)$ for $n \geqslant 0$, is a representative for the vertices of $X(\mathcal{G}_1)$.

If $n = 0$ then $\Lambda_0 = g_0^{(0)}$ is the unique element in $o_1^{-1}([\![\mathbb{I}_2]\!]_0)$.

If $n \geqslant 1$ we have

$$\begin{aligned} g_0^{(n)} &= \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix} \begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix} \\ &= \Lambda_n \begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix}. \end{aligned}$$

Also we have the equality

$$\begin{aligned} g_0^{(-n)} &= \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix} \\ &= \Lambda_n s_1 \begin{pmatrix} \pi^{-n} & 0 \\ 0 & \pi^{-n} \end{pmatrix}. \end{aligned} \tag{A.7}$$

Then, by Proposition A.2.2, $g_0^{(n)}$ and $g_0^{(-n)}$ are representatives for the two edges with origin $[\![\Lambda_n]\!]_0$ □

Remark A.2.5. *Given a g in $GL_2(K_\infty)$ we can use the algorithm from [But07] to decompose g as $g = \gamma\Lambda_n\alpha$ for some $n \geqslant 0$, $\gamma \in \Gamma_0$ and $\alpha \in \mathcal{K}_\infty$. From Proposition A.2.2 we see that $g \in [\![g_0^n]\!]_1$ if and only if $\alpha \in \mathcal{I}_\infty$.*

We explain now how to decompose an element $g \in GL_2(K_\infty)$ as $g = \gamma g_0^{(n)}\kappa$ for some $n \in \mathbb{Z}$, $\gamma \in \Gamma_0$ and $\kappa \in \mathcal{I}_\infty$.

Let us consider the class of g in $\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty$ then

$$g = \gamma\Lambda_m\alpha$$

where $\gamma \in \Gamma_0$, $\alpha \in \mathcal{K}_\infty$, $\Lambda_m = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi^m \end{smallmatrix}\right)$ and $m \geqslant 0$. Write $\alpha = r\iota'$ for $\iota \in \mathcal{I}_\infty$ and $r \in \mathcal{R}$ as above (cf. A.2.2) and $\Lambda_m = g_0^{(m)} \left(\begin{smallmatrix} \pi^m & 0 \\ 0 & \pi^m \end{smallmatrix}\right)$. Then $g = \gamma g_0^{(m)} r\iota$ for a unique $m \geqslant 0$ and $\iota = \iota' \left(\begin{smallmatrix} \pi^m & 0 \\ 0 & \pi^m \end{smallmatrix}\right)$.

Case 1 If $r = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ then we are done.

Case 2 If $m = 0$, then $g_0^{(m)} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\gamma r \in \Gamma_0$and we are done.

Case 3 If $m \geqslant 1$ we may assume that $r = \left(\begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for some $s \in \mathbb{F}_q$. Then we have

$$\begin{aligned}
\gamma \begin{pmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s & 1 \\ 1 & 0 \end{pmatrix} \iota &= \gamma \begin{pmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \iota \\
&= \gamma \begin{pmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pi^{n} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pi^{-n} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \iota \\
&= \gamma \begin{pmatrix} 1 & sT^n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \pi^{-n} \\ 1 & 0 \end{pmatrix} \iota \\
&= \gamma \begin{pmatrix} 1 & sT^n \\ 0 & 1 \end{pmatrix} g_0^{(-m)} \iota
\end{aligned}$$

The previous discussion is easily transformed into an algorithm which allows us to find the corresponding decomposition of g in the quotient $\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty$.

Algorithm 3: `decom`

Input: A matrix $g \in GL_2(K_\infty)$.
Output: A list $\mathcal{D} = [n, \gamma, \kappa]$ such that $g = \gamma g_0^{(n)} \kappa$ with $\gamma \in \Gamma_0$ and $\kappa \in \mathcal{I}_\infty$.

```
Write $g$ as $g = \gamma \Lambda_n \alpha$ for $\gamma \in \Gamma_0$ and $\alpha \in \mathcal{K}_\infty$        ▷ cf.[But07, Lemma 18]
if $\alpha \in \mathcal{I}_\infty$ then
    define $\mathcal{D} = [n, \gamma, \alpha]$
else
    if $n = 0$ then
        search $c \in \mathbb{F}_q$ such that $\left(\begin{smallmatrix} c & 1 \\ 1 & 0 \end{smallmatrix}\right) \alpha \in \mathcal{I}_\infty$
        define $\mathcal{D} = [n, \gamma \left(\begin{smallmatrix} 0 & 1 \\ 1 & -c \end{smallmatrix}\right), \left(\begin{smallmatrix} c & 1 \\ 1 & 0 \end{smallmatrix}\right) \alpha]$
        if $n = 1$ then
            search $c \in \mathbb{F}_q$ such that $\left(\begin{smallmatrix} c & 1 \\ 1 & 0 \end{smallmatrix}\right) \alpha \in \mathcal{I}_\infty$
            define $\mathcal{D} = [-1, \gamma \left(\begin{smallmatrix} 0 & 1 \\ 1 & -c \end{smallmatrix}\right), \delta \left(\begin{smallmatrix} c & 1 \\ 1 & 0 \end{smallmatrix}\right) \alpha \delta^{-1}]$
        end if
        if $n > 1$ then
            write $g$ as $g\delta = \gamma \Lambda_{n-1} \alpha$
            define $\mathcal{D} = [-n, \gamma, \delta \alpha \delta^{-1} \left(\begin{smallmatrix} \pi^{n-1} & 0 \\ 0 & \pi^{n-1} \end{smallmatrix}\right)]$
        end if
    end if
end if
```

```
Return $\mathcal{D}$
```

The function origin (A.2) allows us to define another function called *terminus*, as follows

$$\begin{aligned} t_1 : \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty &\longrightarrow \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty \\ [\![g]\!]_1 &\longmapsto t_1([\![g]\!]_1) = o_1([\![g\delta]\!]_1) \end{aligned}$$

where the matrix δ is the non trivial element in the quotient class of $\mathcal{N}/\mathcal{I}$, with $\mathcal{N}$ is the normalizer of $\mathcal{I}$ in $GL_2(K_\infty)$.

We conclude this section by giving some diagrams that are very useful to describe some of the algorithms that are consequence of Algorithm 3. Let us consider first

$$\begin{tikzcd}
GL_2(K_\infty)/\mathcal{I}_\infty = Y(\mathcal{T}) \arrow[r, "o"] \arrow[d, "pr_Y"'] & GL_2(K_\infty)/\mathcal{K}_\infty = X(\mathcal{T}) \arrow[d, "pr_X"] \\
\Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty = Y(\mathcal{G}_1) \arrow[r, "o_1"'] & \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty = X(\mathcal{G}_1).
\end{tikzcd}$$

Where the maps pr_Y and pr_X are the projections in the quotient graph of edges and vertices, respectively. They are defined as follows

$$\begin{aligned} pr_Y : GL_2(K_\infty)/\mathcal{I}_\infty &\longrightarrow \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{I}_\infty \\ [g]_1 &\longmapsto [\![g]\!]_1 \end{aligned}$$

and

$$\begin{aligned} pr_X : GL_2(K_\infty)/\mathcal{K}_\infty &\longrightarrow \Gamma_0 \setminus GL_2(K_\infty)/\mathcal{K}_\infty \ . \\ [g]_0 &\longmapsto [\![g]\!]_0 \end{aligned}$$

It is straightforward to verify that

$$pr_X(o([g]_1)) = o_1(pr_Y([g]_1)). \tag{A.8}$$

From §2.8 we have that the quotient graph by the congruence subgroup $\Gamma_0(N)$ for $N \in \mathbb{F}_q[T]$, is a covering of the tree $\mathcal{G}_1$. The functions origin and terminus are also well defined here

$$\begin{aligned} o_N : \Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty &\longrightarrow \Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{K}_\infty \\ [\![g]\!]_{1,N} &\longmapsto [\![g]\!]_{0,N} \end{aligned}$$

and

$$t_N(\llbracket g \rrbracket_{1,N}) = o_N(\llbracket g\delta \rrbracket_{1,N}).$$

We also have well defined projection maps from $\mathcal{T}$ to $\Gamma_0(N) \setminus \mathcal{T}$ as follows

$$\begin{tikzcd}
GL_2(K_\infty)/\mathcal{I}_\infty = Y(\mathcal{T}) \arrow[r, "o"] \arrow[d, "pr_{Y_N}"'] & GL_2(K_\infty)/\mathcal{K}_\infty = X(\mathcal{T}) \arrow[d, "pr_{X_N}"] \\
\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty = Y(\Gamma_0(N) \setminus \mathcal{T}) \arrow[r, "o_{1,N}"'] & \Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{K}_\infty = X(\Gamma_0(N) \setminus \mathcal{T}),
\end{tikzcd}$$

with the maps pr_{Y_N} and pr_{X_N} defined as

$$\begin{aligned} pr_{Y_N} : GL_2(K_\infty)/\mathcal{I}_\infty &\longrightarrow \Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty \\ [g]_1 &\longmapsto \llbracket g \rrbracket_{1,N} \end{aligned}$$

and

$$\begin{aligned} pr_{X_N} : GL_2(K_\infty)/\mathcal{K}_\infty &\longrightarrow \Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{K}_\infty \\ [g]_0 &\longmapsto \llbracket g \rrbracket_{0,N}. \end{aligned}$$

A set of representatives for $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$

We can not define a canonical set of representatives for the double quotient $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$. However, after fixing a set $\mathcal{S}_N$ of representatives for $\Gamma_0(N) \setminus \Gamma_0$, we may use the fact that $\Gamma_0(N) \setminus \mathcal{T}$ is a covering of $\mathcal{G}_1$ to give a non-canonical set of representatives for the edges of $\Gamma_0(N) \setminus \mathcal{T}$.

Since Γ_0 is discrete in $GL_2(K_\infty)$, the stabilizers in Γ_0 of edges or vertices are finite. More specifically, define

$$\mathrm{B}_0 = GL_2(\mathbb{F}_q)$$

and for $n \geqslant 1$

$$\mathrm{B}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| \, a, c \in \mathbb{F}_q^\times, b \in \mathbb{F}_q[T] \text{ with } \deg(f) \leqslant n \right\}. \tag{A.9}$$

Then for $n \geqslant 0$, B_n is the stabilizer in Γ_0 of the vertex represented by Λ_n in $\mathcal{T}$. Analogously $\mathrm{B}_n \cap \mathrm{B}_{n+1}$ is the stabilizer in Γ_0 of the edge with origin $[\Lambda_n]_0$ and terminal $[\Lambda_{n+1}]_0$ (cf. [Ser03, Prop. 3, p. 87]). Note that $\mathrm{B}_n \cap \mathrm{B}_{n+1} = \mathrm{B}_n$ for $n \geqslant 1$ and $\mathrm{B}_0 \cap \mathrm{B}_1$ is the set of upper triangular matrices with entries in $\mathbb{F}_q$.

Let $\mathcal{S}_N = \{s_1, ..., s_r\}$ be a set of representatives for $\Gamma_0(N) \setminus \Gamma_0$. Then given $\gamma \in \Gamma_0$ there exits a $\beta \in \Gamma_0(N)$ and a unique $s_i \in \mathcal{S}_N$ such that $\gamma = \beta s_i$.

In [But07] there is a method to calculate $\mathcal{S}_N$ (cf. [*Ibid.*, Lemma 1.22]), actually we also have the following correspondence (cf. [*Ibid.*, Cor. 1.23]).

Proposition A.2.6. *Let $N \in \mathbb{F}_q[T]$. Then $\Gamma_0(N) \setminus \Gamma_0 \cong \mathbb{P}^1(\mathbb{F}_q[T]/N)$.*

Once the set $\mathcal{S}_N$ is fixed, every $g \in GL_2(K_\infty)$ can be written as

$$\begin{aligned} g &= \gamma g_0^{(n)} \kappa \quad \gamma \in \Gamma_0 \text{ and } \kappa \in \mathcal{I}_\infty \\ &= \beta s_i g_0^{(n)} \kappa. \end{aligned}$$

Therefore, given $s_i, s_j \in \mathcal{S}_N$ two matrices such that $[\![s_i g_0^{(n)}]\!]_{1,N} = [\![s_j g_0^{(n)}]\!]_{1,N}$ then there exists $b \in \mathrm{B}_n$ such that $s_i b s_j^{-1} \in \Gamma_0(N)$. So, for each class in $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$ representing an edge e, we choose one representative s_e of $\mathcal{S}_N$ and consider the subset $\widetilde{\mathcal{S}}_N \subset \mathcal{S}_N$ consisting of a representative for each $e \in \mathcal{G}_{N,M}$. This set $\widetilde{\mathcal{S}}_N$ allows us to define a set of representatives for $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$ as

$$\mathcal{R}_N := \{ s_e g_0^{(n)} \mid s_e \in \widetilde{\mathcal{S}}_N \text{ and } g_0^{(n)} \in \mathcal{R}_{\Gamma_0} \}. \tag{A.10}$$

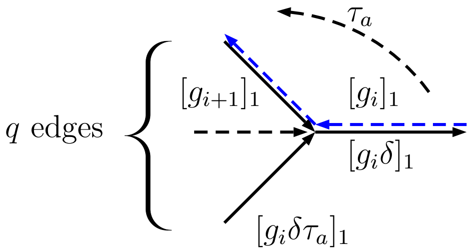
A.3 Lifting cycles to $\mathcal{T}$

The Algorithm 3 may be used to lift a cycle in $\Gamma_0(N) \backslash \mathcal{T}$ to a path in $\mathcal{T}$ without backtracking. Let $\mathcal{C} = \{\tilde{e}_0, ..., \tilde{e}_{h-1}\}$ be a cycle in $\mathcal{G}_N$ such that $t_{1,N}(\tilde{e}_{h-1}) = o_{1,N}(\tilde{e}_0)$ and $t_{1,N}(\tilde{e}_i) = o_{1,N}(\tilde{e}_{i+1})$. Then there exists a sequence of consecutive edges $\{e_0, e_1 ..., e_{h-1}\}$ in $\mathcal{T}$ such that $o(e_0)$ is $\Gamma_0(N)$-equivalent with $t(e_{h-1})$ and $pr_{Y_N}(e_i) = \tilde{e}_i$ for all i in $\{0, 1, ..., h-1\}$.

It is enough to see how to lift two consecutive edges in the cycle $\mathcal{C}$ to two consecutive edges on the tree $\mathcal{T}$. Let us suppose that $g_i \in GL_2(K_\infty)$ with $[\![g_i]\!]_{1,N} = \tilde{e}_i$ and $e_i \in \mathcal{T}$ is a lifting of $\tilde{e}_i$. We want to find a matrix $g_{i+1} \in GL_2(K_\infty)$ such that it lifts $\tilde{e}_{i+1}$ to an edge $e_{i+1} \in \mathcal{T}$ with $t(e_i) = o(e_{i+1})$.

Claim: The matrix $g_{i+1} = g_i \delta \tau_a \delta$ for some $a \in \mathbb{F}_q$ were $\delta = \left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right)$ and $\tau_a = \left(\begin{smallmatrix} \pi & a \\ 0 & 1 \end{smallmatrix}\right)$.

We have that $t([g_i]_1) = o([g_i\delta]_1)$ and multiplication by τ_a, gives on the tree $\mathcal{T}$ all the edges whose terminal is the vertex $o([g_i\delta]_1)$ (see figure, the blue edges corresponds to the wanted path)



that is $o([g_i\delta]_1) = t([g_i\delta\tau_a]_1)$, by definition of the function origin and terminal we have

$$t([g_i]_1) = o([g_i\delta\tau_a\delta]_1).$$

Hence the q edges with origin $t(e_i)$ are given by $[g_i\delta\tau_a\delta]_1$ for all $a \in \mathbb{F}_q$. So one of these edges project to $\tilde{e}_{i+1}$ or equivalently $pr_{Y_N}([g_i\delta\tau_a\delta]_1) = \tilde{e}_{i+1}$, which proves the claim.

We can summarize the previous discussion with the following algorithm.

Algorithm 4: `FindPath`

Input: A list $\mathcal{C} = [g_0, g_1, ..., g_{r-1}]$ of length r of matrices in $GL_2(K_\infty)$ representing a cycle in $\Gamma_0(N) \setminus \mathcal{T}$, that is, $t_N([\![g_i]\!]_{1,N}) = o_N([\![g_{i+1}]\!]_{1,N})$ for all $i \in \{0, ...r-2\}$ and $t_N([\![g_{r-1}]\!]_{1,N}) = o_N([\![g_0]\!]_{1,N})$.

Output: A list $\mathcal{P} = [h_0, h_1, ..., h_{r-1}]$ of length r of matrices in $GL_2(K_\infty)$ representing a path in $\mathcal{T}$ and such that $o([h_0]_1)$ is $\Gamma_0(N)$-equivalent to $t([h_{r-1}]_1)$.

```
Make a list $L$ with the elements of the finite field $\mathbb{F}_q$
set $\mathcal{P} = [g_0]$
for $i$ from 1 to $r-1$ do
    let $n = \#\mathcal{P}$ and set $g_{\text{aux}} = \mathcal{P}[n]$        ▷ $g_{aux}$ is the last element of $\mathcal{P}$
    bool←false
    $k \leftarrow 1$
    while bool=false do
        $a \leftarrow L[k]$
        set $h_{\text{aux}} = g_{\text{aux}}\delta\tau_a\delta$
```

```
            if $pr_{1,N}([h_{\text{aux}}]_1) = g_{i+1}$ then
                bool $\leftarrow$ true
            end if
            $k \leftarrow k + 1$
        end while
        append $h_{\text{aux}}$ to $\mathcal{P}$
    end for
    Return $\mathcal{P}$
```

A.4 Finding the representative

In many algorithms, it is necessary to work with elements in $GL_2(K_\infty)$ which belong to the same class in $\Gamma_0(N)\backslash GL_2(K_\infty)/\mathcal{I}_\infty$. So given two different matrices g_1 and g_2 in $GL_2(K_\infty)$ such that $\llbracket g_1 \rrbracket_{1,N} = \llbracket g_2 \rrbracket_{1,N}$, we want to find $\gamma \in \Gamma_0(N)$ and $\kappa \in \mathcal{I}_\infty$ such that $g_1 = \gamma g_2 \kappa$. Using Algorithm 3 we can give an efficient method to write such decomposition. We present first the following result as a trivial corollary of Proposition A.2.4. Nevertheless we give a constructive proof which gives Algorithm `FindTheRep`.

Corollary A.4.1. *Let $g_1, g_2 \in GL_2(K_\infty)$. Suppose that $\llbracket g_1 \rrbracket_{1,N} = \llbracket g_2 \rrbracket_{1,N}$. Then there is an algorithm to find $\gamma \in \Gamma_0(N)$ and $\kappa \in \mathcal{I}_\infty$ such that $g_1 = \gamma g_2 \kappa$.*

Proof. Let $g_1, g_2 \in GL_2(K_\infty)$ be two matrices $\Gamma_0(N)$-equivalent. Then g_1 and g_2 are in the same class in $GL_2(A)\backslash GL_2(K_\infty)/\mathcal{I}_\infty$, therefore there exist $s_1, s_2 \in GL_2(A)$ and $\kappa_1, \kappa_2 \in \mathcal{I}_\infty$ such that

$$g_1 = s_1 g_0^{(n)} \kappa_1,$$
$$g_2 = s_2 g_0^{(n)} \kappa_2$$

where $g_0^{(n)}$ is the representative for the quotient $GL_2(A)\backslash GL_(K_\infty)/\mathcal{I}_\infty$ described in Proposition A.2.4.

Since g_1 and g_2 are $\Gamma_0(N)$-equivalent we have

$$\begin{aligned}\Gamma_0(N)s_1g_0^{(n)}\mathcal{I}_\infty = \Gamma_0(N)s_2g_0^{(n)}\mathcal{I}_\infty &\iff s_1g_0^{(n)} \in \Gamma_0(N)s_2g_0^{(n)}\mathcal{I}_\infty \\ &\iff \mathbb{I}_2 \in s_1^{-1}\Gamma_0(N)s_2g_0^{(n)}\mathcal{I}_\infty(g_0^{(n)})^{-1} \\ &\iff s_1^{-1}\Gamma_0(N)s_2 \cap g_0^{(n)}\mathcal{I}_\infty(g_0^{(n)})^{-1} \neq \emptyset \\ &\iff s_1^{-1}\Gamma_0(N)s_2 \cap \Big(\Gamma_0 \cap g_0^{(n)}\mathcal{I}_\infty(g_0^{(n)})^{-1}\Big) \neq \emptyset.\end{aligned}$$

An easy calculation shows that

$$\Gamma_0 \cap g_0^{(n)}\mathcal{I}_\infty(g_0^{(n)})^{-1} = B_n,$$

where B_n is the set defined in (A.9). Then there exists a $b \in B_n$ and $\gamma \in \Gamma_0(N)$ such that $s_1^{-1}\gamma s_2 = b$. A direct calculation shows that setting

$$\kappa = \kappa_2^{-1}(g_0^{(n)})^{-1}b^{-1}g_0^{(n)}\kappa_1$$

satisfy $g_1 = \gamma g_2 \kappa$. We only need to verify that κ is an element of $\mathcal{I}_\infty$. Indeed κ_2^{-1} and κ_1 are in $\mathcal{I}_\infty$, and since $b \in g_0^{(n)}\mathcal{I}_\infty(g_0^{(n)})^{-1}$ we have $(g_0^{(n)})^{-1}b^{-1}g_0^{(n)} \in \mathcal{I}_\infty$.

□

Algorithm 5: `FindTheRep`

Input: Two matrices g_1 and g_2 in $GL_2(K_\infty)$ that are $\Gamma_0(N)$-equivalent.

Output: Two Matrices $\gamma \in \Gamma_0(N)$ and $\kappa \in \mathcal{I}_\infty$ such that $g_1 = \gamma g_2 \kappa$.

```
Use Algorithm 3 to write
        $g_1 = s_1 g_0^{(n)} \kappa_1$
        $g_2 = s_2 g_0^{(n)} \kappa_2$
calculate the stabilizer B$_n$
bool ← false
$i$ ← 1
while bool=false do
    $b$ ← $B_n[i]$
    **if** $s_1 b s_2^{-1} \in \Gamma_0(N)$ **then**
        bool $\leftarrow$ true
    **end if**
    $i \leftarrow i + 1$
**end while**
**Return**
```

$$\gamma = s_1 b s_2^{-1} \text{ and}$$
$$\kappa = \kappa_2^{-1}(g_0^{(n)})^{-1} b^{-1} g_0^{(n)} \kappa_1.$$

B. Algorithms for the table

In this appendix we describe the main algorithms that we use in the calculation of the table and the integral. The first section deals with the implementation of the Hecke operator U_∞, the algorithm that allows us to build up the table and the one that we use to decompose functions in $\mathcal{F}_I$ as a product of elements in the pseudo-basis $\mathcal{B}_M$.

In the second section we give the algorithm to calculate the valuation of the integral and the one to lift a path in the tree $\mathcal{T}$ to a path in Ω. Finally we explain how to calculate the Tate parameter and give a proof of Theorem 5.6.1.

B.1 Algorithms for the calculation of the table

The Hecke Operator U_∞

We recall the definition of the Hecke operator

$$(U_\infty \phi)(\gamma)(f(t)) := \prod_{a \in \mathbb{F}_q} \phi(\gamma \tau_a) f(\pi t + a)$$

for $\phi \in \mathcal{S}$, $f \in \mathcal{F}_I$ and $\gamma \in \Gamma \setminus PGL_2(K_\infty)$.

A crucial fact that helps us to calculate U_∞ quickly is the $\mathcal{I}_\infty$-equivariance. As we already explained in Chapter 4, it is enough to calculate the values of U_∞ in a set of representatives $\mathcal{R}_N$ of the edges of the quotient $\Gamma_0(N) \setminus GL_2(K_\infty)/\mathcal{I}_\infty$ up to some level M.

Therefore for each $\gamma_{\text{rep}} \in \mathcal{R}_N$

$$(U_\infty \phi)(\gamma_{\text{rep}})(1 + \xi^\delta \pi^i t^j) := \prod_{a \in \mathbb{F}_q} \phi(\gamma_{\text{rep}} \tau_a)(1 + \xi^\delta \pi^i (\pi t + a)^j). \tag{B.1}$$

From the definition of the operator U_∞, we have that for each $a \in \mathbb{F}_q$, we need to find the edge of $\mathcal{G}_{N,M}$ corresponding to $\gamma_{\text{rep}}\tau_a$. However, we only know the values of ϕ in elements of $\mathcal{R}_N$. Via Algorithm 5, we find the corresponding representative of $\gamma_{\text{rep}}\tau_a$ in $\mathcal{R}_N$ as follows: we consider $\gamma_{\text{rep}}\tau_a$ as an element of $GL_2(K_\infty)/\mathcal{I}_\infty$ and use the projection function pr_{Y_N} to find $g_a \in GL_2(K_\infty)$ such that

$$\begin{aligned}[\![g_a]\!]_1 &= [\![\gamma_{\text{rep}}\tau_a]\!]_1 \\ &= [\![\hat{\gamma}_{\text{rep}}]\!]_1\end{aligned}$$

for some $\hat{\gamma}_{\text{rep}} \in \mathcal{R}_N$. Then using Algorithm 5, we can find $\gamma \in \Gamma_0(N)$ and $\kappa \in \mathcal{I}_\infty$ such that

$$\gamma_{\text{rep}}\tau_a = \gamma\hat{\gamma}_{\text{rep}}\kappa.$$

Plugging in this in equation (B.4) we get

$$\begin{aligned}(U_\infty\phi)\,(\gamma_{\text{rep}})(1+\xi^\delta\pi^i t^j) &= \prod_{a\in\mathbb{F}_q}\phi\,(\gamma_{\text{rep}}\tau_a)\,(1+\xi^\delta\pi^i(\pi t+a)^j) \\ &= \prod_{a\in\mathbb{F}_q}\phi\,(\gamma\hat{\gamma}_{\text{rep}}\kappa)\,(1+\xi^\delta\pi^i(\pi t+a)^j) \\ &= \prod_{a\in\mathbb{F}_q}\phi\,(\hat{\gamma}_{\text{rep}})\,(\kappa * (1+\xi^\delta\pi^i(\pi t+a)^j)).\end{aligned}$$

In the last equality we use the $\Gamma_0(N)$-invariance of the function ϕ, Lemma 4.3.7 and the action defined in (4.6). From the preceding discussion we see that for a fixed $\gamma_{\text{rep}} \in \mathcal{R}_N$ in order to evaluate $\phi(\gamma_{\text{rep}})(f_{ij})$ for $f_{ij} \in \mathcal{B}_M$ we need to calculate $\gamma_{\text{rep}}\tau_a$ in many instances.

Remark B.1.1. *We save time by precalculating the decomposition $\gamma_{rep}\tau_a = \gamma\hat{\gamma}_{rep}\kappa$ for all $a \in \mathbb{F}_q$ and $\gamma_{rep} \in \mathcal{R}_N$. So for each γ_{rep} we store in the data structure of the quotient graph $\mathcal{G}_{N,M}$ the list $[\gamma_{rep}, a, \hat{\gamma}_{rep}, \kappa]$ (called* "signature"*) to indicate that $\gamma_{rep}\tau_a = \gamma\hat{\gamma}_{rep}\kappa$ for all $a \in \mathbb{F}_q$.*

Therefore the computation of the operator U_∞ breaks up in two parts. The first one is carried out with the quotient graph $\mathcal{G}_{N,M}$ and consists in the elaboration of the list with the signatures $[\gamma_{\text{rep}}, a, \hat{\gamma}_{\text{rep}}, \kappa]$ and the second one takes place during the calculation of the table and reduces to read the signatures from a list.

Observe that the calculation of the operator U_∞ does not depend on the harmonic cocycle explicitly.

The table

Let $\varphi \in \underline{H}_!^{new}(\mathcal{T},\mathbb{Z})^{\Gamma_0(N)}$, as we have seen in §3.1.1, the harmonic cocycle φ gives rise to a measure μ_φ on $\mathcal{M}_0(\mathbb{P}^1(O_\infty),\mathbb{Z})^\Gamma$. The objective of this subsection is explain how to calculate the table that allows us to evaluate any integral of the form

$$\mathop{\times\!\!\!\!\!\!\int}_{O_\infty} f \, d\mu_\varphi$$

for $f \in \mathcal{F}_I$ with accuracy up to π^M, where M is an integer $\geqslant 1$.

In §4.3 we explained already how to fill out this table, however, the construction given there is slightly different from the actual implementation. Since this is the main algorithm of the whole work, we think it is worthy to explain the actual implementation.

Let us recall some facts and definitions from §4.3. Let $M \geqslant 1$ be an integer, the associated pseudo-basis is (cf. Lemma 4.3.1)

$$\mathcal{B}_M := \{1+\xi^\delta\pi^i t^j \;|(i,j)\in\mathcal{F}_I, i\leq M,\ \delta=0,...,d-1\}$$

with d the degree of the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$.

A straightforward calculation shows that the cardinality of $\mathcal{B}_M$ is

$$d\left(\frac{(M+1)(M+2)}{2}-1\right)=\frac{d}{2}(M^2+3M).$$

For each $\gamma_{\text{rep}} \in \mathcal{R}_N$ we want to calculate

$$\Phi_{\mu_\varphi}(\gamma_{\text{rep}})(1+\xi^\delta\pi^i t^j) = \mathop{\times\!\!\!\!\!\!\int}_{O_\infty} (1+\xi^\delta\pi^i t^j)\; d(\gamma_{\text{rep}}^{-1} * \mu_\varphi). \tag{B.2}$$

As we discussed in §4.3, for each $\gamma_{\text{rep}} \in \mathcal{R}_N$ and a fixed δ_0 we have to calculate $\frac{1}{2}(M^2+3M)$ integrals, hence to each γ_{rep} we attach d “triangular matrices” $\mathbb{T}_{\gamma_{\text{rep}},\delta}$ for varying δ) whose entries are the integrals of the form (B.2) (for functions f of $\mathcal{B}_{M,\delta}$ (cf. (4.10)). For the implementation we condense all these matrices in one matrix $\mathbb{T}$ of size $\#\mathcal{R}_N \times \#\mathcal{B}_M$.

First order the pseudo-basis $\mathcal{B}_M$ increasingly, according to the order relation defined in §4.3. Observe that the constants correspond to the functions of $\mathcal{B}_M$ with $j=0$. There are exactly Md constants and their integrals are located in the first Md columns of the matrix

$\mathbb{T}$. The algorithm consists of two stages. In the first stage we calculate the values of the function $\Phi_{\mu_\varphi}(\gamma_{\text{rep}})$ at the constants, this can be made very quickly using the formula

$$\Phi_{\mu_\varphi}(\gamma_{\text{rep}})(1+\xi^\delta\pi^i) = \left(1+\xi^\delta\pi^i\right)^{\varphi(\gamma_{\text{rep}}e_0)}. \tag{B.3}$$

In the second stage, we calculate the value of the integral at the non-constant functions, starting from the smallest one in $\mathcal{B}_M$. Note that we start with functions of the form $1+\xi^\delta\pi^M t^j$ for $\delta \in \{0,...,d-1\}$ an j from 0 to M. In each case the resulting functions after applying the U_∞ operator factorize as a product of constants, and the value of the integral is already known. After this is done for all representatives in $\mathcal{R}_N$, we proceed to apply U_∞ to functions of the form $1+\xi^\delta\pi^{M-1}t^j$, then the exponents of π increase in 1. So the new factors appearing are either constants or of the form $1+\xi^\delta\pi^M t^j$. In each case we know the integral.

Continuing in this fashion, we apply the U_∞ operator to each element of $\mathcal{B}_M$ as many times as necessary, until we get the integral to the wanted precision (cf. §4.3).

Let us suppose that we want to calculate $U_\infty(\phi)(\gamma_{\text{rep}})(1+\xi^\delta\pi^i t^j)$ and suppose that γ_{rep} represents an edge of level l over a cusp of $\mathcal{G}_{N,M}$. Then by definition of the U_∞ we have

$$\left(U_\infty\phi\right)(\gamma_{\text{rep}})(1+\xi^\delta\pi^i t^j) := \prod_{a\in\mathbb{F}_q}\phi\left(\gamma_{\text{rep}}\tau_a\right)(1+\xi^\delta\pi^i(\pi t+a)^j). \tag{B.4}$$

So after applying the operator U_∞ we need to calculate over the edges given by $\gamma_{\text{rep}}\tau_a$ of level $l-1$ at a function f with $\text{val}_\pi(t) = i+1$. Observe that each time that we apply the operator U_∞ we move over the cusp in direction the compact part of $\mathcal{G}_{N,M}$. The integral is 1 if after applying successively the operator U_∞ we are still over the cusp and the valuation in π of the function is M, this happens if and only if

$$i+l \geqslant \deg(N)+M.$$

Remark B.1.2. *We use the previous inequality to rule out in the calculation of the table the functions and edges for which we know a priori that the integral is* 1.

Algorithm 6: `TheTable`

Input: The data structure $\mathcal{G}_{N,M}$ corresponding to the quotient graph $\Gamma_0(N)\backslash\mathcal{T}$ up to level M. A harmonic cocycle φ with rational Hecke eigenvalues. This is actually a list with all the values of φ at the edges of $\mathcal{G}_{N,M}$.

Output: A matrix $\mathbb{T}$ with entries in $1+\pi\mathbb{F}_{q^2}[\![\pi]\!]$ with all the values of the integrals of functions in $\mathcal{B}_M$. (The entries of $\mathbb{T}$ are elements in $1+\pi\mathbb{F}_{q^2}[\![\pi]\!]$ modulo π^M).

```
Set $\mathcal{R}_N$ to be the list of representatives of the edges of the graph $\Gamma_0(N)\backslash\mathcal{T}$ up to depth $M$
initialize a matrix $\mathbb{T}$ of ones of size $n \times m$, where $n = \#\mathcal{R}_N$ and $m = \#\mathcal{B}_M$
for $s$ from 1 to $n$ do
    for $k$ from 1 to $Md$ do                                   ▷ the constants are the last $Md$ entries
        $\mathbb{T}[s][k] \leftarrow \mathcal{B}_M[k]^{\varphi(\mathcal{R}_N[s]e_0)}$          ▷ Here we fill the entries corresponding to the constants.
    end for
end for
for $s$ from 1 to $n$ do
    for $k$ from $Md+1$ to $m$ do
        $f \leftarrow \mathcal{B}_M[k]$
        set $\gamma_{\text{rep}} \leftarrow \mathcal{R}_N[s]$
        set level($\gamma_{\text{rep}}$) the level of the edge given by $\gamma_{\text{rep}}$          ▷ apply Algorithm 3
        set $ii = \text{val}_\pi(f-1)$
        if $ii + \text{level}(\gamma_{\text{rep}}) - \deg(N) < M$ then          ▷ cf. Remark B.1.2
            set $I \leftarrow 1$
            for $a \in \mathbb{F}_q$ do                          ▷ we start to apply the $U_\infty$ operator
                read from $\mathcal{G}_{N,M}$ the signature $[\gamma_{\text{rep}}, a, \hat{\gamma}_{\text{rep}}, \kappa]$
                $s_0 \leftarrow$ Position $(\mathcal{R}_N, \hat{\gamma}_{\text{rep}})$
                $f \leftarrow f\langle\tau_a\kappa^{-1}\rangle$
                set a list $\mathcal{L}_f$ with the factors of $f$          ▷ apply Algorithm 7
                for $l$ in $\mathcal{L}_f$ do
                    $k_0 \leftarrow$ Position $(\mathcal{B}_M, l[1])$
                    $I \leftarrow I \times \mathbb{T}[s_0][k_0]^{l[2]}$          ▷ the value $\mathbb{T}[s_0][k_0]$ is known
                end for
```

```
25:             end for
26:             $\mathbb{T}[s][k] \leftarrow I$
27:         end if
28:     end for
29: end for
30: Return $\mathbb{T}$
```

Remark B.1.3. *1. Note that after filling the columns that correspond to the constants, we continue filling the table $\mathbb{T}$ from the "left to the right". In the step 16 we apply the Hecke operator U_∞. So if we are in the column j-th we only need values of the integral already stored in other columns on the left.*

2. We do not need to give in the input the integer M since the basis $\mathcal{B}_M$ is stored in the data structure of $\mathcal{G}_{N,M}$.

Let us suppose that there are h elements in $\underline{H}_!^{new}(\mathcal{T},\mathbb{Z})^{\Gamma_0(N)}$ with rational Hecke eigenvalues. In this case there are h isogeny classes of the given conductor $N\infty$. To find these classes we need to calculate h integrals and therefore h tables. We save time if we make all the tables simultaneously as follows.

Let us assume that $\underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(N)}$ has dimension $g \geqslant h$. Let $\mathcal{B} := \{\psi_1, ..., \psi_g\}$ be its standard basis as defined in §2.9. Let also $\{\varphi_1, ..., \varphi_h\}$ be the set of harmonic cocycles with rational Hecke eigenvalues, then

$$\varphi = \sum_{j=1}^{g} c_{ij}\psi_j \text{ for } c_{ij} \in \mathbb{Z}.$$

Since the integral is multiplicative, we have

$$\begin{aligned} c_{\varphi_i}(\gamma) &= {\times}\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu_{\varphi_i}(t) \\ &= \prod_{j=1}^{g} \left({\times}\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu_{\psi_j}(t) \right)^{c_j}. \end{aligned}$$

So we can make tables for all the ψ's instead of calculate many tables for each harmonic cocycle with rational Hecke eigenvalues. The reason is that for each entry of the table we need to calculate the operator U_∞ and it does not depend on the harmonic cocycle explicitly.

For the implementation we take Algorithm 6 we need to initialize g matrices of 1's instead of only one and modify the steps 3-7 to calculate the values for the integral at the constant at all the elements in the standard basis instead of doing it only for φ.

Analysis for the algorithm `TheTable`

For the cost analysis of the algorithm to calculate the table, we need to consider separately two loops. The first one is the loop to calculate the integral at the constants and the second one is the part in which we apply the operator U_∞.

Before starting with the analysis for the running time of Algorithm 6, we need a bound for the number of edges of the quotient graph $\mathcal{G}_{N,M}$. We know that $\#\mathcal{G}_{N,M} = \#\mathcal{C}_N + \#\mathcal{SP}_N$, where $\mathcal{C}_N$ and $\mathcal{SP}_N$ are the compact part and the cusps of $\mathcal{G}_{N,M}$, respectively.

Unfortunately there is no easy formula for the compact part. However we can use the fact that the quotient graph $\mathcal{G}_{N,M}$ is a covering of $\mathcal{G}_1$ to estimate the number of edges in the compact part as $\#\mathcal{S}_N \deg(N)$, where $\mathcal{S}_N$ is a set of representatives for $\Gamma_0(N) \setminus \Gamma_0$. From [Non01, p. 68] we have that if $N = \prod_{i=1}^{s} f_{l_i}^{r_i}$ with f_{l_i} a prime polynomial of degree l_i then

$$\#\mathcal{S}_N = \prod_{i=1}^{s} q^{l_i(r_i-1)}(q^{l_i}+1)$$

and

$$\#\mathcal{SP}_N = 2^s + \frac{\kappa(N) - 2^s}{q-1}$$

where $\kappa(N) := \prod_{i=1}^{s} \left(q^{l_i\lfloor (r_i-1)/2)\rfloor} + q^{l_i\lfloor r_i/2)\rfloor}\right)$. Then $\#\mathcal{S}_N$ is a polynomial in q of degree $\deg(N)$. A bound for $\#\mathcal{C}_N$ is $2^s q^{\deg(N)} \deg(N)$ and for $\#\mathcal{SP}_N$ is $q^{\deg(N)/2}2^s$. Therefore the number of edges in $\mathcal{G}(N, M)$ is bounded by

$$2^s q^{\deg(N)} \deg(N) + 2^s M q^{\deg(N)/2}. \tag{B.5}$$

For the first loop (steps 3-7), note that we are exponentiating polynomials in π of the form $1 + \xi^s\pi^i$ for $1 \leqslant i \leqslant M$ and this can be done via binomial expansion $(1+\xi^s\pi^i)^k = \sum_{l=0}^{k} \binom{k}{l}(\xi^s)^l\pi^{il}$ and using the fact that we are working modulo π^{M+1}, so that is suffices to compute for l in the range $0, ..., \frac{M}{i}$ is bounded by M/i. Summing over the two loops the number of operations is bounded by

$$n \sum_{\delta=0}^{d-1} \sum_{i=1}^{M} M/i \leqslant ndM(1 + \log M)$$

using that $\sum_{i=1}^{M} 1/i \leqslant 1 + \log M$ and where $n = \#\mathcal{G}_{N,M}$. Hence the cost for all iterations of the loop is

$$2^s Md \left(1 + \log M\right) \left(q^{\deg(N)} \deg(N) + 2^s M q^{\deg(N)/2}\right). \tag{B.6}$$

Examining the second loop shows that the number of operations inside it, depends on the condition "if" (step 14) and the "for" loop in step 16. So we need to count the number of edges in $\mathcal{G}_{N,M}$ and functions in $\mathcal{B}_M$ that satisfy the inequality $i + \text{level}(\gamma_{\text{rep}}) - \deg(N) < M$. Let us first to consider some particular cases. If $i = M$ then the inequality becomes $\text{level}(\gamma_{\text{rep}}) < \deg(N)$, then there are $\#\mathcal{C}_N Md$ edges and functions that verify the condition in step 14.

If $i = M - 1$ then we have $\text{level}(\gamma_{\text{rep}}) - 1 < \deg(N)$, in this case there are $(\#\mathcal{C}_N + \#\mathcal{SP}_N)(M - 1)d$ edges and functions that satisfy the inequality. We can see here that for $i = M - k$ the inequality becomes $\text{level}(\gamma_{\text{rep}}) - k < \deg(N)$ then there are $(\#\mathcal{C}_N + k\#\mathcal{SP}_N)(M - k)d$. Therefore we can have that the number of edges and functions that verify the condition in step 14 is

$$\#\mathcal{C}_N Md + ... + \left(\#\mathcal{C}_N + k\#\mathcal{SP}_N\right)(M - k)d + ... + (\#\mathcal{C}_N + (M - 1)\#\mathcal{SP}_N)d.$$

A straightforward calculation shows that the last expression simplifies to

$$d\left(\frac{\#\mathcal{C}_N}{2}(M^2 + M) + \frac{\#\mathcal{SP}_N}{6}(M^3 - M)\right). \tag{B.7}$$

The loop that starts in step 16 is executed q times and it includes the function to factorize which has a cost of $5M^4$ (see the analysis for Algorithm 7). Hence the cost for all iterations of the second loop is $\left(5dqM^4\left(\frac{\#\mathcal{C}_N}{2}(M^2 + M) + \frac{\#\mathcal{SP}_N}{6}(M^3 - M)\right)\right)$. Which is also a bound for the cost of the algorithm, since the total of operations in the algorithm is the sum of the costs in the two loops but the dominant cost of the algorithm is the second loop. We may summarize the previous discussion in the following proposition.

Proposition B.1.4. *The Algorithm 6 can be performed using no more that*

$$\frac{5}{6}dM^7 2^s q^{\frac{n}{2}+1} + \frac{5}{2}2^s dM^6 q^{n+1} n + \frac{1}{2}d\left(5q^{n+1}2^s n - \frac{5}{3}2^s q^{\frac{n}{2}+1}\right)M^5$$

operations, where n is the degree of N.

Factorization

We now consider the problem of factorizing functions in $\mathcal{F}_I$. In Chapter 4 we stated the following lemma, here we give a constructive straightforward proof that will lead us to the algorithm of factorization.

Lemma B.1.5. *Given any function $f \in \mathcal{F}_I$ and any integer $M \geqslant 1$, then there exists a finite set of indices $J \subseteq I$ and $m_{ij\delta} \in \{1, 2, ..., p-1\}$ such that*

$$f \equiv \prod_{(i,j)\in J} (1 + \xi^\delta \pi^i t^j)^{m_{ij\delta}} \pmod{\pi^{M+1}}$$

where $\xi \in \mathbb{F}_{q^2}$ is a primitive element for the extension over $\mathbb{F}_p$, $\delta \in \{0, ..., d-1\}$ with d the degree of the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$. The representation is unique modulo p powers of $f_{ij\delta} = 1 + \xi^\delta \pi^i t^j$, so the set

$$\mathcal{B}_M := \{1 + \xi^\delta \pi^i t^j \mid (i,j) \in \mathcal{F}_I, i \leq M,\ \delta = 0, ..., d-1\}.$$

is what we call a multiplicative pseudo-basis.

Proof. For $f = \sum_{(i,j)\in I} a_{ij}\pi^i t^j \in \mathbb{F}_{q^2}[\![t]\!][\![\pi]\!]$ we set

$$\mathrm{val}_\pi(f) = \min\{i \geqslant 0 \mid \exists j \geqslant 0 \text{ such that } a_{ij} \neq 0\}$$

(with $\min\varnothing = \infty$) and for $i \geqslant 0$ we define $f[\pi^i] := \sum_j a_{ij}t^j$, furthermore for $g \in \mathbb{F}_{q^2}[\![t]\!]$, val_t denotes the usual valuation in t.

Let $f = 1 + \sum_{(i,j)} a_{ij}\pi^i t^j$ in $\mathcal{F}_I$, let $i_0 = \mathrm{val}_\pi(f-1)$ and $j_0 = \mathrm{val}_t(f[\pi^{i_0}])$. Then we can write f as

$$f = 1 + a_{i_0 j_0}\pi^{i_0}t^{j_0} + \sum_{(i,j)\neq(i_0,j_0)\in I} a_{ij}\pi^i t^j.$$

Note that since $\{1, \xi, \xi^2, ..., \xi^{d-1}\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$ we have $a_{i_0 j_0} = \sum_{s=0}^{d-1} b_s \xi^s$ for $b_s \in \mathbb{F}_p$. Using this, a straightforward calculation shows that

$$\begin{aligned}\prod_{s=0}^{d-1}(1+\xi^s\pi^{i_0}t^{j_0})^{b_s} &= \prod_{s=0}^{d-1}\sum_{k=0}^{b_s}\binom{b_s}{k}(\xi^s)^k(\pi^{i_0}t^{j_0})^k \\ &= \prod_{s=0}^{d-1}(1+\xi^s b_s \pi^{i_0}t^{j_0} + O(\pi^{i_0+1})) \\ &= 1 + \left(\sum_{s=0}^{d-1} b_s\xi^s\right)\pi^{i_0}t^{j_0} + O(\pi^{i_0+1}) \\ &\equiv 1 + a_{i_0j_0}\pi^{i_0}t^{j_0} \pmod{\pi^{i_0+1}}.\end{aligned} \tag{B.8}$$

Set $f_{i_0j_0} = \prod_{s=0}^{d-1}(1+\xi^s\pi^{i_0}t^{j_0})^{b_s} \in \mathcal{F}_I$. Dividing f by $f_{i_0j_0}$ and reducing modulo π^{M+1} we get

$$\begin{aligned} f_0 &= f/f_{i_0j_0} \\ &= (f_{i_0j_0} + (f - f_{i_0j_0})/f_{i_0j_0}) \\ &= 1 + (f - f_{i_0j_0})f_{i_0j_0}^{-1} \\ &= 1 + \sum_{j>j_0} b_{i_0j}\pi^{i_0}t^j + \sum_{\substack{i>i_0 \\ j\geqslant j_0}} a_{ij}\pi^i t^j \end{aligned}$$

I.e., $\mathrm{val}_\pi(f_0 - 1) \geqslant i_0$ and $\mathrm{val}_t(f_0[\pi^{i_0}]) > j_0$. Note that the factors $1 + \xi^s\pi^{i_0}t^{j_0}$ of $f_{i_0j_0}$ are elements of the pseudo-basis $\mathcal{B}_M$.

Continuing in this fashion, since the function $f_0 \in \mathcal{F}_I$, we can construct a sequence $f_k \in \mathcal{F}_I$ with $(1+M)\mathrm{val}_\pi(f_k - 1) + \mathrm{val}_t(f_k[\pi^{\mathrm{val}_\pi(f_k-1)}])$ strictly increasing and then the procedure finishes after a finitely number of divisions since we are working modulo π^{M+1}. Defining J to be the set consisting of indices (i_k, j_k) such that $i_k = \mathrm{val}_\pi(f_k - 1)$ and $j_k = \mathrm{val}_t(f_k[\pi^{i_k}])$ coming from the step k, we have that

$$f \equiv \prod_{(i,j)\in J}\ \prod_{\delta\in\{0,\ldots,d-1\}} (1+\xi^\delta\pi^i t^j)^{m_{ij\delta}} \pmod{\pi^{M+1}}$$

which follows by construction and equality (B.8). □

Remark B.1.6. *Note that the factorization of a function $f \in \mathcal{B}_M$ is not unique. Let $f_{ij} = 1 + \xi^\delta\pi^i t^j \in \mathcal{B}_M$ be a factor of a function f with $q^2 | \gcd(i,j)$ then it admit other representation as a product of elements of $\mathcal{B}_M$, namely the q^2-th roots of f_{ij}.*

We conclude with Algorithm 7 which is basically a transcription of the proof of Lemma B.1.5.

ALGORITHM 7: `factorize`

Input: A function f in $\mathcal{F}_I$ and an integer M.

Output: A list $\mathcal{L}$ consisting of pairs $[f_{ij}, e_{ij}]$ with $f_{ij} \in \mathcal{B}_M$, $e_{ij} > 0$ and $(i,j) \in J \subset I$ such that $f \equiv \prod_{f_{ij} \in \mathcal{L}} f_{ij}^{f_{ij}} \pmod{\pi^{M+1}}$.

```
1:  Initialize $\mathcal{L} = [\,]$
2:  define $f_{\text{aux}} = f \pmod{\pi^{M+1}}$
3:  **while** $f_{\text{aux}} \neq 1$ **do**
4:      $i_0 \leftarrow \text{val}_\pi(f_{\text{aux}} - 1)$
5:      $j_0 \leftarrow \text{val}_t(\text{coefficient}(i_0, f_{\text{aux}} - 1))$
6:      write $f_{\text{aux}} = 1 + a_{i_0 j_0}\pi^{i_0}t^{j_0} + \sum_{(i,j) \neq (i_0,j_0) \in I} a_{ij}\pi^i t^j$
7:      write $a_{i_0 j_0} = \sum_{s=0}^{d-1} b_s \xi^s$ with $b_s \in \mathbb{F}_p$
8:      set $z = \pi^{i_0}t^{j_0}$                    ▷ *we change the variable since $i_0$ and $j_0$ are fixed*
9:      set $f_{i_0 j_0} = \prod_{s=0}^{d-1}(1 + \xi^s z)^{b_s}$            ▷ *use the binomial expansion*
10:     compute $g = f_{i_0 j_0}^{-1}$           ▷ *We make the change of variables again $z$ by $\pi^{i_0}t^{j_0}$*
11:     $f_{\text{aux}} \leftarrow f_{\text{aux}} g$
12:     append to $\mathcal{L}$ all the pairs $[1 + \xi^s \pi^{i_0}t^{j_0}, b_s]$ from the factorization of $f_{i_0 j_0}$ (step 9)
13: **end while**
14: **Return** $\mathcal{L}$
```

Analysis for the algorithm `factorize`

A closer look to the algorithm shows that in order to find the running time, it is enough to find a bound for the number of iterations of the while-loop (step 3-step 13) in the worst case, which occurs when the function f is divisible by all the elements of the pseudo-basis $\mathcal{B}_M$. A straightforward calculation shows that $\#\mathcal{B}_M = \frac{d}{2}(M^2 + 3M)$.

Step 7 can be done in $O(d)$ and its cost is negligible since d is constant and M is larger than d. In step 9 we calculate the product $f_{i_0 j_0} = \prod_{s=0}^{d-1}(1 + \xi^s \pi^{i_0}t^{j_0})^{b_s}$ with $1 \leqslant b_s < p$, therefore since $\pi^{i_0}t^{j_0}$ is fixed, we can make the substitution $\pi^{i_0}t^{j_0}$ by z, before to carry out the exponentiation, then we get $(1+\xi^s z)^{b_s}$ so we can use the binomial expansion to obtain $\sum_{l=0}^{b_s}\binom{b_s}{l}(\xi^s)^l z^l$. Since $b_s < p$ we have that this exponentiation can be performed in at most p operations, we need to express $(\xi^s)^l$ in the basis $1, ..., \xi^{d-1}$ over $\mathbb{F}_p$. On the other hand, after exponentiating we get d polynomials of degree at most p in the new variable z and multiplying them cost at most $(d-1)pM$ because any partial product has at most M terms. Hence the cost for the step 9 is pdM.

In step 10 we invert $f_{i_0j_0}$, again using the auxiliary variable $z = \pi^{i_0}t^{j_0}$. Let $e = \lfloor M/i_0 \rfloor$ then

$$\begin{aligned} g = f_{i_0j_0}^{-1} &= \prod_{\delta=0}^{d-1}(1+\xi^\delta z)^{-b_s} \\ &= \prod_{\delta=0}^{d-1}\sum_{l=0}^{e}(\xi^\delta)^l\binom{-b_s}{l}z^l \\ &\equiv \prod_{\delta=0}^{d-1}\left(\sum_{l=0}^{e}(-\xi^\delta)^l\binom{b_s+l-1}{l}z^l\right) \quad (\text{mod } z^e). \end{aligned}$$

The cost to set up each factor is e, we then carry out $d-1$ multiplications modulo z^e, *i.e.,* the cost here is $(d-1)(e+1)^2$. In total the cost is atmost $d(e^2+3e+1)$.

To compute $f_{aux}g$, observe that f_{aux} has at most M^2 terms and g has $e+1$ terms. So the cost for the steps 7-13 is at most

$$dpM + d(e^2+3e+1) + (e+1)M^2. \tag{B.9}$$

We need to sum this over all $(i,j) \in I$ to obtain the bound C for the number of operations.

$$\begin{aligned} C &= \sum_{i=1}^{M}\left(\sum_{j=0}^{i} dpM + d\left(\frac{M^2}{i^2}+\frac{3M}{i}+1\right)d + \left(\frac{M}{i}+1\right)M^2\right) \\ &= \sum_{i=1}^{M}\left(\sum_{j=0}^{i}(dpM+d+M^2) + \left(\frac{M^2d}{i^2}+\frac{3Md}{i}+\frac{M^3}{i}\right)\right) \\ &= \sum_{i=1}^{M}(dpM+d+M^2)(i+1) + \left(\frac{M^2d}{i^2}+\frac{3Md}{i}+\frac{M^3}{i}\right)(i+1) \\ &= (dpM+d+M^2)\frac{M^2+3M}{2} + \sum_{i=1}^{M}\left(\frac{M^2d}{i^2}+\frac{3Md}{i}+\frac{M^3}{i}\right)(i+1) \end{aligned}$$

We know from calculus that the harmonic series diverges and $\sum_{i=1}^{M} \frac{1}{i} < 1 + \log N$. Also the series $\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$, then $\sum_{i=1}^{M} \frac{1}{i^2} < 2$. Let us suppose also that $dp < M$ and $M > 6$ then $4 + \log M < M$. Therefore we have

$$\begin{aligned}
C &< \frac{3}{2}M^4 + dp\left(\frac{1}{2}M^3 + \frac{3}{2}M^2\right) + \frac{3}{2}M^3 + \frac{13}{2}dM^2 + (1+\log M)(dM^2 + 3dM + M^3) \\
&< \frac{3}{2}M^4 + M\left(\frac{1}{2}M^3 + \frac{3}{2}M^2\right) + \frac{3}{2}M^3 + \frac{13}{2}dM^2 + (1+\log M)(dM^2 + 3dM + M^3) \\
&= 2M^4 + (4+\log M)(M^3 + dM^2 + 3dM) + \frac{5}{2}dM^2 - \frac{15}{2}dM \\
&< 2M^4 + M(M^3 + dM^2 + 3dM) + \frac{5}{2}dM^2 - \frac{15}{2}dM \\
&= 3M^4 + d\left(M^3 + \frac{11}{2}dM^2 - \frac{15}{2}M\right) \\
&< 4M^4 + \frac{11}{2}M^3 - \frac{15}{2}M^2 \text{ (since } d < M) \\
&< 5M^4
\end{aligned}$$

Proposition B.1.7. *Suppose that $M > 6$ and $dp < M$ then a bound for the running time of the Algorithm 7 is $5M^4$.*

B.2 Algorithms for the calculation of the integral

Valuation of the integral

To obtain the Tate parameter associated to an harmonic cocycle φ we need to calculate the integral

$$c_\varphi(\gamma) = \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu_\varphi(t)$$

where γ is an element of $\Gamma_0(N)$ associated to a cycle c of the quotient graph $\Gamma_0(N) \setminus \mathcal{T}$ (see §4.4.3). As we mentioned in §5.6 if $\mathcal{C} = \{c_1, ...c_g\}$ is a basis for the homology of the quotient graph $\Gamma \setminus \mathcal{T}$ then to each $c_i \in \mathcal{C}$ there is associated a matrix $\gamma_i \in \Gamma$, let us call by abuse of notation $\mathcal{C}$ the set of all γ_i's. Then

$$\operatorname{val}(\mathbf{q}) = \min\{\operatorname{val}(c_\varphi(\gamma_i)) \ \mid \gamma_i \in \mathcal{C}\}.$$

Let us consider a cycle c in the quotient tree and $v_0, v_1, ..., v_r$ be a path in $\mathcal{T}$ that lifts c. This sequence of the vertices induces a sequence $z_0, ..., z_r$ in Ω such that $\lambda(z_i) = v_i$, then

$$\begin{aligned} c_\varphi(\gamma) &= \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t} \, d\mu_\varphi(t) && \text{(B.10)} \\ &= \times\!\!\!\!\!\!\int_{\partial\Omega} \prod_{i=0}^{r-1} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t) \\ &= \prod_{i=0}^{r-1} \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t). \end{aligned}$$

We can use this decomposition to know the valuation of the integral, namely,

$$\begin{aligned} \operatorname{val}\left(\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t} \, d\mu_\varphi(t) \right) &= \operatorname{val}\left(\times\!\!\!\!\!\!\int_{\partial\Omega} \prod_{i=0}^{r-1} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t) \right) \\ &= \operatorname{val}\left(\prod_{i=0}^{r-1} \times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t) \right) \\ &= \sum_{i=0}^{r-1} \operatorname{val}\left(\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t) \right). && \text{(B.11)} \end{aligned}$$

Therefore we need to calculate the valuation of

$$\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t).$$

We have

$$\begin{aligned} \operatorname{val}\left(\times\!\!\!\!\!\!\int_{\partial\Omega} \frac{z_i - t}{z_{i+1} - t} \, d\mu_\varphi(t) \right) &= \operatorname{val}\left(\varinjlim_{\alpha} \prod_{U \in \mathcal{C}_\alpha} \left(\frac{z_i - t}{z_{i+1} - t} \right)^{\mu_\varphi(U)} \right) \\ &= \varinjlim_{\alpha} \operatorname{val}\left(\prod_{U \in \mathcal{C}_\alpha} \left(\frac{z_i - t}{z_{i+1} - t} \right)^{\mu_\varphi(U)} \right) \\ &= \varinjlim_{\alpha} \sum_{U \in \mathcal{C}_\alpha} \mu_\varphi(U) \operatorname{val}\left(\frac{z_i - t}{z_{i+1} - t} \right) && \text{(B.12)} \\ &= \varinjlim_{\alpha} \sum_{U \in \mathcal{C}_\alpha} \mu_\varphi(U) && \text{(B.13)} \\ &= \mu(U_{e_i}) \\ &= \varphi(e_i) \end{aligned}$$

where e_i is the edge with origin v_i. The equality from (B.12) to (B.13) follows from the fact that z_i and z_{i+1} are the liftings of consecutive vertices and the point t belongs to one of the open sets in the partition determined by e_i, which implies val $\left(\frac{z_i-t}{z_{i+1}-t}\right) = 1$. Using the last equality and the equation (B.11) we have that

$$\mathrm{val}\left(\rlap{\times}\int_{\partial\Omega} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu_{\varphi}(t)\right) = \sum_{e_i} \varphi(e_i)$$

where e_i runs over the cycle c.

Summarizing we have that the valuation of the Tate parameter is given by

$$\mathrm{val}(\mathbf{q}) = \min\left\{\sum_{e\in c_i} \varphi(e) \ \mid c_i \in \mathcal{C}\right\}.$$

So to calculate the Tate parameter, we choose the γ that lifts the cycle with the minimal valuation. One can obtain this result applying the equation (1.3) from [GEK97].

Lifting vertices to Ω

Let c be the cycle that gives the minimal valuation of the integral for a given harmonic cocycle φ and let $\mathcal{P} = \{w_0, w_1, ..., w_r\}$ be the lifting of the vertices of c to the tree $\mathcal{T}$ to consecutive vertices and such that v_0 and v_r are $\Gamma_0(N)$-equivalent. That is, there exists $\gamma \in \Gamma_0(N)$ and $\alpha \in \mathcal{K}_\infty$ such that $w_0 = \gamma w_r \alpha$ (they represent vertices not edges).

From the discussion above, we need an algorithm to find the sequence $z_0, ..., z_r \in \Omega$. This can be done using the $GL_2(K_\infty)$-equivariance of the reduction map $\lambda : \Omega \longrightarrow \mathcal{T}$ (cf. §2.6) as follows.

Let v_0 be standard vertex in $\mathcal{T}$, we know that the standard affinoid is defined to be

$$\lambda^{-1}(v_0) = \left\{z \in C_\infty^\times \mid |z| \le 1, \quad |z - c| \ge 1 \quad \forall c \in \mathbb{F}_q\right\}.$$

Let $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ then $\xi \in \lambda^{-1}(v_0)$.

Since the translates of the affinoid $\lambda^{-1}(v_0)$ by $GL_2(K_\infty)$ cover Ω and two translates are either identical, disjoint or intersect each other, we can get any affinoid by translating the standard one. Equivalently, given a vertex $v \in \mathcal{T}$ with $v \ne v_0$, to get a element in $\lambda^{-1}(v)$ it is enough to find a $g \in GL_2(K_\infty)$ such that $[v]_0 = [gv_0]_0$. Then we have that $g\langle\xi\rangle \in \lambda^{-1}(v)$.

There is no loss of generality in assuming that the matrices w_i are in normal form. Let say that $w_0 = \left(\begin{smallmatrix}\pi^k & u\\ 0 & 1\end{smallmatrix}\right)$ for some $k \geqslant 0$. Then we have that

$$z_0 = \pi^k \xi + u \in \lambda^{-1}(w_0). \tag{B.14}$$

Since we can go from w_i to the next vertex w_{i+1} by multiplying by an appropriate element $g_i \in GL_2(K_\infty)$, we may define $z_{i+1} = g_i\langle z_i\rangle$, *i.e.*, the action of g_i in z_i by Möbious transformations.

On the other hand, to calculate our integral we use the equality $z_r = \gamma z_0$, however, on the tree we have $[v_r]_0 = [\gamma v_0]_0$, so the elements g_i are required so, that its product is γ. The following algorithm allows us to find the sequence of the g_i's with such property.

Algorithm 8: `TransitionGammas`

Input: A list $\mathcal{P} = [w_0, w_1, ..., w_r]$ of matrices in $GL_2(K_\infty)$ representing consecutive vertices in $\mathcal{T}$ and such that w_0 and w_r are $\Gamma_0(N)$-equivalent.

Output: A list $\mathcal{L}$ consisting of matrices $g_i \in GL_2(K_\infty)$ such that $[g_i w_i]_0 = [w_{i+1}]_0$ and the product of the g_i's is in $\Gamma_0(N)$.

```
Write $w_r = \gamma w_0 \alpha$ with $\gamma \in \Gamma_0(N)$ and $\alpha \in \mathcal{K}_\infty$. (Use Algorithm 4)
make a loop to define the list
    $\mathcal{L} = [w_1 w_r^{-1}\gamma, w_2 w_1^{-1}, w_3 w_2^{-1}, ..., w_{r-1} w_{r-2}^{-1}, w_r w_{r-1}^{-1}]$
Return $\mathcal{L}$
```

A direct calculation shows that the product of the elements in $\mathcal{L}$ is actually γ. Also the condition

$$[g_i w_i]_0 = [w_{i+1}]_0$$

is verified. Using Algorithm 8 we can now lift the vertices of a given path to a sequence of z_i's in Ω.

Algorithm 9: `LiftToOmega`

Input: A list $\mathcal{P} = [w_0, w_1, ..., w_r]$ of matrices in $GL_2(K_\infty)$ representing consecutive vertices and such that w_0 and w_r are $\Gamma_0(N)$-equivalent.

Output: A list $\mathcal{Z}$ consisting of different elements in Ω lifting the vertices of $\mathcal{P}$.

```
Use Algorithm 8 to produce the list $\mathcal{S} = [g_0, g_1, ..., g_{r-1}]$
initialize $\mathcal{Z} = [z_0 = w_0\langle\xi\rangle]$          ▷ We lift $w_0$ as in (B.14)
for $i$ from 2 to $r$ do
    append to $\mathcal{Z}$ the element $g_{i-1}\langle\mathcal{Z}[i-1]\rangle$          ▷ $\langle\cdot\rangle$ is the action by Möbius
transformation.
end for
Return $\mathcal{Z}$
```

The integral

In Chapter 4 we saw how to carry out the change of variables, and we explained how we can integrate over an edge e determined by the adjacent vertices v and v'. Using the partition induced by Lemma 4.4.1, we can break up the integral

$$\fint_{\partial\Omega} \frac{t-z}{t-z'}\, d\mu_\varphi(t)$$

where z and z' are liftings to Ω of v and v', respectively. For the change of variables we also supposed that $v = [k, u]$ and $v' = [k+1, u+a_0\pi^k]$ for some $a_0 \in \mathbb{F}_q$, respectively. From Lemma 2.4.5 we have that all the neighbors of v different from v' are given by $[k+1, u+a\pi^k]$ for $a \in \mathbb{F}_q \setminus a_0$ and $[k, u \mod \pi^{k-1}O_\infty]$, which is the only one that can not be obtained form v multiplying by τ_a. The neighbors of v' are of the form $[k+2, u+a_0\pi^k+b\pi^{k+1}]$ with $b \in \mathbb{F}_q$.

Notation: All the neighbors of the vertices v and v' different from $[k, u \mod \pi^{k-1}O_\infty]$ are called *the neighbors of zero*, while $[k, u \mod \pi^{k-1}O_\infty]$ is called the *neighbor of infinity.*

Algorithm 10: `IntegrateOverEdge`

Input: An edge e in $\mathcal{G}_{N,M}$ given by the vertices $v = [k, u]$ and $v' = [k+1, u+a_0\pi^k]$. A pair $[z, z']$ of elements in Ω over $o(e)$ and $t(e)$, respectively. A harmonic cocycle φ. The data structure $\mathcal{G}_{N,M}$ of the quotient graph $\Gamma_0(N) \setminus \mathcal{T}$. The table $\mathbb{T}$ with the values of the integral at the functions of $\mathcal{B}_M$.

Output: The integral

$$\oint_{\partial\Omega} \frac{t-z}{t-z'}\, d\mu_\varphi(t)$$

over the edge e. That is, using the partition of $\partial\Omega$ induced by e, up to precision π^M.

```
Set a list $\mathcal{L} = [\,]$
set a list $\mathcal{N}$ with all neighbors of zero    ▷ we have an auxiliary routine to do that
set $h_0 = [k, u \mod \pi^{k-1} O_\infty]$    ▷ the neighbor of infinity
for all $h \in \mathcal{N}$ do
    $\gamma \leftarrow h$    ▷ for the change of variable (cf. equation (3.4))
    $w \leftarrow h[1][2]$
    set $f_\mathrm{n} = 1 - \left(\frac{h[1][1]}{z-w}\right) t$ and $f_\mathrm{d} = 1 - \left(\frac{h[1][1]}{z'-w}\right) t$    ▷ $f_n$ and $f_d$ are the numerator and the denominator, respectively cf. §4.4.3
    $C_\mathrm{n} = z - w$ and $C_\mathrm{d} = z' - w$    ▷ these are the constants
    append to $\mathcal{L}$ the list $[f_\mathrm{n}, f_\mathrm{d}, C_\mathrm{n}, C_\mathrm{d}, \gamma]$
end for
set $u = h_0[1][2]$
if $k \neq 0$ then
    set $f_\mathrm{n} = 1 - \left(\frac{z-u}{\pi^{k-1}}\right) t$ and $f_\mathrm{d} = 1 - \left(\frac{z'-u}{\pi^{k-1}}\right) t$
    set $\gamma = \left(\begin{smallmatrix} T^{k-1} & u \\ 1 & 0 \end{smallmatrix}\right)$
    append to $\mathcal{L}$ the list $[f_\mathrm{n}, f_\mathrm{d}, 1, 1, \gamma]$
end if
if $k = 0$ then
    set $f_\mathrm{n} = 1 - \pi z t$ and $f_\mathrm{d} = 1 - \pi z' t$
    set $\gamma = \left(\begin{smallmatrix} 0 & T \\ 1 & 0 \end{smallmatrix}\right)$
    append to $\mathcal{L}$ the list $[f_\mathrm{n}, f_\mathrm{d}, 1, 1, \gamma]$
end if
$I = 1$ and $C = 1$
for $l$ in $\mathcal{L}$ do
    $\gamma = l[5]$ and find $\gamma_\mathrm{rep}$, the representative of the edge given by $\gamma$ and write $\gamma = \beta\gamma_\mathrm{rep}\kappa$    ▷ use Algorithm 5
    set $h_\mathrm{n} = l[1]\langle\kappa^{-1}\rangle$ and $h_\mathrm{d} = l[2]\langle\kappa^{-1}\rangle$
    define $I_\mathrm{n}$ to be the integral over $O_\infty$ of $h_\mathrm{n}$    ▷ use Algorithm 11
    define $I_{\mathrm{d}}$ to be the integral over $O_\infty$ of $h_{\mathrm{d}}$
    $I \leftarrow I \times \left(\frac{l[3]}{l[4]}\right)^{\varphi(\gamma_{\mathrm{rep}} e_0)} \frac{I_{\mathrm{n}}}{I_{\mathrm{d}}}$
end for
Return $I$
```

In the previous algorithm, we use an auxiliary routine to calculate the integral of a function $f \in \mathcal{F}_I$. The implementation is an easy routine and we only give the algorithm without further explanation.

Algorithm 11: `Integrate over` O_∞

Input: A function $f \in \mathcal{B}_M$. A matrix γ_{rep} a representative for the edges of $\mathcal{G}_{N,M}$. The data structure $\mathcal{G}_{N,M}$ of the quotient graph. The table $\mathbb{T}$ with the values of the integral at the functions of $\mathcal{B}_M$.

Output: The integral of f over O_∞ up to accuracy π^M that is,

$$\fint_{O_\infty} f \, d\mu_\varphi. \tag{B.15}$$

.

```
Set $\mathcal{B}_M$ the pseudo basis for $\mathcal{F}_I$
Int= 1
set $k$ to be the position in $\mathcal{R}_N$ of $\gamma_{\mathrm{rep}}$ ▷ The set $\mathcal{R}_N$ is a list which is already stored in the data structure of $\mathcal{G}_{N,M}$
run Algorithm 7 to set a list $\mathcal{L}$ of factors of $f$ with multiplicities
for $l$ in $\mathcal{L}$ do
    set $s$ to be the position in $\mathcal{B}_M$ of $l[2]$
    Int ← Int × $\mathbb{T}[k][s]^{l[2]}$
end for
Return Int
```

Analysis for the algorithm `Integrate over` $\mathcal{O}_\infty$

A similar analysis as in Algorithm 7 shows that the worst case occurs when the function f factorizes as a product of all elements in $\mathcal{B}_M$, then the list $\mathcal{L}$ has $\frac{d}{2}(M^2+3M)$ elements. So we only need to calculate the cost of the step 7. Each entry of the table $\mathbb{T}$ is an element of the ring $1+\pi\mathbb{F}_{q^2}[\![\pi]\!]$ and the exponent $l[2]$ satisfies $1 \leqslant l[2] \leqslant p-1$ then using the powering algorithm (cf. [Coh93, Algorithm 1.2.1]) and one of the algorithms for fast multiplication allows to calculate the step 7 in $O(\log(p+1)M^2)$ operations, therefore the running time of the algorithm is $O(M^4)$.

Analysis for the algorithm `IntegrateOverEdge`

We ignore the cost for the steps 1-21 since most of them are assignments or operations whose cost is $O(1)$. Therefore we only consider the cost of the operations in the last loop. In steps 26 and 27 we calculate the integral of the functions h_{n} and h_{d}, respectively, we know that the running time for Algorithm 11 is $O(M^4)$. In step 28 we calculate three products so we need to consider the analysis separately. Note that the constants $l[3]$ and $l[4]$ do not depend on the size of M but on the path where we are integrating, so the cost of calculating $\left(\frac{l[3]}{l[4]}\right)^{\varphi(\gamma_{\text{rep}}e_0)}$ may be considered small (or even constant) compared with big values of M. The product $I \times \frac{I_{\text{n}}}{I_{\text{d}}}$ can be carried out using fast multiplication in time $O(M)$, since they are polynomials of degree at most M (cf. Remark A.1.4). Therefore, adding up the costs for the steps 26, 27 and 28 we get that the algorithm takes time $O(M^4)$.

Theorem B.2.1. *The Tate parameter* $\mathbf{q}$ *can be calculated up to accuracy* π^M *in time* $O(M^7)$.

Proof. In order to find the Tate parameter we need to calculate the table an after the integral using Algorithms 6 and 10, respectively. The dominant cost of Algorithm 6 gives the running time for the calculation of $\mathbf{q}$, which is $O(M^7)$. □

Remark B.2.2. *Most of the computer algebra systems use a combination of the fast algorithms for multiplications or quotients of polynomials mentioned in Remark A.1.4 and they take* $M(n) \in 63.43n\log n\log\log n + O(n\log n)$. *However in most of the cases we can not compute with* M *bigger than this constant, this is the reason we use for the analysis of the complexity the classical algorithm for multiplication.*

C. Tables

C.1 Preliminaries

In this appendix we give some tables for the isogeny classes in characteristic 3 and 5 and conductor of degrees three and four in each case. In characteristic 2 there are already (using other methods) tables for conductor of small degree (cf. [Gek97],[Sch01],[Sch99] and [Sch00]). Since applying the transformation $T \mapsto T + a$ for a in $\mathbb{F}_q^{\times}$ we can transform any curve with bad reduction at the place $T - a$ to have bad reduction at the place T, we only consider in the tables conductors which are divisible by T and the those that are primes.

Each table have three columns, the first one is for the conductor, which is given by the factors of a polynomial N in $\mathbb{F}_q[T]$, we omit the ∞ place, since we know that it appears in the conductor with exponent 1. The second column is for the corresponding elliptic curve and the last one for the traces. All the traces have length 8, which correspond to the first 8 prime polynomials relatively prime to N. We consider the list of primes ordered lexicographically.

Remark C.1.1. *1. As we already mentioned there are no elliptic curves with split multiplicative reduction at ∞ with conducto $N\infty$ and degree of N less than* 2.

2. Over $\mathbb{F}_3$ and $\mathbb{F}_5$ there are not elliptic curves with prime conductor of degree 3.

C.2 Table for degree 3 over $\mathbb{F}_3$

Table C.1: Isogeny classes for degree 3 over $\mathbb{F}_3$

Conductor	**Curve**	**Trace**
T,T^2+2	Y^2=X^3+(T^2+2)X^2+(2T^8+T^6+2T^4)/(T^6+2)	[0,0,2,2,−8,−8,8,−4]
T,T+1,T+2	Y^2=X^3+(T^2+2T+2)X^2+(2T^4+2T^3+T^2+T)/(T^6+2T^3+2)	[2,2,−6,−4,−4,4,4,−4]
	Y^2=X^3+(T^2+T+2)X^2+(2T^4+T^3+T^2+2T)/(T^6+T^3+2)	[2,−6,2,−4,−4,4,−4,4]
	Y^2=X^3+(T^2+1)X^2+(2T^4+T^2)/(T^6+1)	[−6,2,2,−4,−4,−4,4,4]
T^2,T+1	Y^2+XY=X^3+(2T^3+2)/T^9	[−2,−2,−2,4,4,−8,4,−2]
	Y^2=X^3+(T^2+2T)X^2+(2T^5+2T^4)/(T^3+2)	[0,2,2,−2,4,4,−4,−8]
T^2,T+2	Y^2+XY=X^3+(2T^3+1)/T^9	[−2,−2,4,−2,−8,4,4,4]
	Y^2=X^3+(T^2+T)X^2+(2T^5+T^4)/(T^3+1)	[0,2,−2,2,4,4,4,−4]
T^2+2T+2,T	Y^2=X^3+(T^2+1)X^2+(T^7+2T^6+2T^5)/(T^6+1)	[−1,−1,0,5,8,−7,8,−2]
T^2+T+2,T	Y^2=X^3+(T^2+1)X^2+(2T^7+T^6+T^5)/(T^6+1)	[−1,−1,0,5,−7,8,−7,−2]

C.3 Table for degree 4 over $\mathbb{F}_3$

Table C.2: Isogeny classes for degree 3 over $\mathbb{F}_3$

Conductor	**Curve**	**Trace**
T,T^3+2T^2+T+1	Y^2=X^3+(T^2+2T+2)X^2+(T^5+2T^4+T^3+T^2)/(T^6+2T^3+2)	[−2,−1,−1,−1,0,−1,−4,−8]
T,T^3+2T^2+1	Y^2+XY=X^3+(T^7+2T^6+T^4)/(T^{12}+T^9+T^3+1)	[−3,−2,−2,−5,1,−5,−8,7]
T^2,T+1,T+2	Y^2+XY=X^3+(2T^2+1)/T^6	[−2,−2,−2,4,4,−8,4,4]
T^2,T^2+1	Y^2+XY=X^3+(2T^2+2)/T^6	[−2,−2,−2,−2,−2,−2,−2,4]
	Y^2=X^3+(T^2+T)X^2+(2T^7+2T^5)/(T^3+1)	[0,2,4,−4,4,−2,−2,8]
	Y^2=X^3+(T^2+2T)X^2+(2T^7+2T^5)/(T^3+2)	[2,0,−4,4,−2,4,−4,4]
T^4	Y^2+XY=X^3+1/T^6	[−2,−2,−5,1,1,4,4,−2]
	Y^2+XY=X^3+2/T^6	[1,1,−2,1,1,7,7,4]
T^2,T^2+T+2	Y^2=X^3+(T^2+2T)X^2+(2T^2+2T+1)/(T^3+2)	[−1,−3,2,−5,1,−2,−1,−2]
	Y^2+XY=X^3+(2T^6+2T^3+1)/T^9	[1,1,−2,1,7,−2,−5,10]
	Y^2=X^3+(T^2+T)X^2+(2T^6+2T^5+T^4)/(T^3+1)	[−3,−1,−4,−1,−5,−8,1,2]
	Y^2=X^3+(T^2+2T)X^2+(2T^5+2T^4+T^3)/(T^3+2)	[2,0,2,−2,−2,−2,8,−2]
T^2,(T+2)^2	Y^2=X^3+1)X^2+2T/(T^3+2)	[−2,4,−2,−2,4,−8,−8,4]
	Y^2=X^3+1)X^2+(2T+1)/T^3	[−2,−2,4,−2,−8,4,4,4]
T^3,T+1	Y^2=X^3+(T^2+2T)X^2+(2T^4+T^3+2T^2)/(T^3+2)	[−3,−1,−4,−2,−2,1,−1,7]
	Y^2+XY=X^3+(2T^6+T^3+2)/T^9	[1,−5,4,−2,−2,1,7,−5]
	Y^2+XY=X^3+(T^3+1)/T^9	[1,4,−5,−2,−2,10,−2,4]

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(T^2{+}2T)X^2{+}(T^7{+}2T^6{+}T^5{+}T^4{+}2T^3{+}T^2)/(T^3{+}2)$	[3,−4,−1,−2,10,−2,2,4]
T^2,$T^2{+}2T{+}2$	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}(2T^5{+}T^4{+}T^3)/(T^3{+}1)$	[0,2,2,−2,−2,−2,4,8]
	$Y^2{=}X^3{+}(T^2{+}2T)X^2{+}(T^6{+}2T^5{+}2T^4)/(T^3{+}2)$	[−1,−3,−4,−1,−8,−5,−4,−2]
	$Y^2{+}XY{=}X^3{+}(T^6{+}2T^3{+}2)/T^9$	[1,1,−2,1,−2,7,4,−8]
	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}(T^2{+}2T{+}2)/(T^3{+}1)$	[−3,−1,2,−5,−2,1,−8,−4]
	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}(T^8{+}2T^7{+}2T^6)/(T^3{+}1)$	[3,−1,−4,1,4,1,−8,2]
T^2,$(T{+}1)^2$	$Y^2{=}X^3{+}1)X^2{+}2T/(T^3{+}1)$	[−2,4,−2,−2,−8,4,4,−2]
	$Y^2{=}X^3{+}1)X^2{+}(2T{+}2)/T^3$	[−2,−2,−2,4,4,−8,4,−2]
T,$T^3{+}2T{+}2$	$Y^2{=}X^3{+}(T^2{+}2T{+}2)X^2{+}(T^4{+}2T^2{+}2T)/(T^6{+}2T^3{+}2)$	[−2,−1,2,−1,−3,−7,1,1]
	$Y^2{+}XY{=}X^3{+}(T^8{+}2T^6{+}2T^5)/(T^{12}{+}2T^9{+}2T^3{+}1)$	[−2,−3,−2,−5,1,7,−5,−5]
T^3,$T{+}2$	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}(T^4{+}T^3{+}T^2)/(T^3{+}1)$	[−3,−1,−2,−4,1,−2,−2,−10]
	$Y^2{+}XY{=}X^3{+}(T^6{+}T^3{+}1)/T^9$	[1,−5,−2,4,1,−2,−2,−2]
	$Y^2{+}XY{=}X^3{+}(T^3{+}2)/T^9$	[1,4,−2,−5,10,−2,7,−2]
	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}(T^7{+}T^6{+}T^5{+}2T^4{+}2T^3{+}2T^2)/(T^3{+}1)$	[3,−4,−2,−1,−2,10,1,2]
T,$T{+}1$,$T^2{+}2T{+}2$	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(2T^6{+}2T^5{+}2T^4{+}T^2)/(T^6{+}T^3{+}2)$	[−2,−4,0,−10,8,4,−4,−8]
	$Y^2{+}XY{=}X^3{+}(2T^8{+}2T^6{+}2T^3{+}T^2)/(T^{12}{+}2T^9{+}2T^3{+}1)$	[0,−2,−2,−8,4,4,4,4]
	$Y^2{=}X^3{+}(T^2{+}1)X^2{+}2T^2(T{+}1)^6(T^2{+}2T{+}2)/(T^6{+}1)$	[2,0,−4,2,8,−4,4,−8]
T,$(T{+}2)^3$	$Y^2{=}X^3{+}(T^2{+}T)X^2{+}2T^5/(T^4{+}2T^3{+}T{+}2)$	[3,2,1,−4,−2,1,−2,−1]
	$Y^2{+}XY{=}X^3{+}2T^6/(T^9{+}2)$	[1,−2,−5,4,−2,1,10,7]
	$Y^2{+}XY{=}X^3{+}(T^3/(T^9{+}2)$	[1,−2,4,−5,−2,10,1,−2]
T,$(T{+}1)^2$,$T{+}2$	$Y^2{+}XY{=}X^3{+}(2T^2{+}T)/(T^6{+}2T^3{+}1)$	[−2,−2,−2,4,4,4,4,−8]
T,$T^3{+}T^2{+}T{+}2$	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(2T^5{+}2T^4{+}2T^3{+}T^2)/(T^6{+}T^3{+}2)$	[−1,−2,−1,0,−1,−4,−1,7]
T,$T^3{+}2T^2{+}2T{+}2$	$Y^2{=}X^3{+}(T^2{+}2T{+}2)X^2{+}(T^{10}{+}2T^9{+}2T^8{+}2T^7)/(T^6{+}2T^3{+}2)$	[1,2,−1,−1,0,8,−7,1]
T,$T{+}2$,$T^2{+}1$	$Y^2{=}X^3{+}(T^2{+}2T{+}2)X^2{+}(2T^6{+}2T^5{+}T^4{+}2T^3{+}2T^2)/(T^6{+}2T^3{+}2)$	[−2,−4,0,−10,8,−8,4,−4]
	$Y^2{+}XY{=}X^3{+}(2T^8{+}2T^7{+}T^6{+}2T^5{+}2T^4)/(T^{12}{+}T^9{+}T^3{+}1)$	[0,−2,−2,−8,4,4,4,4]
	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(2T^{10}{+}2T^9{+}T^8{+}2T^7{+}2T^6)/(T^6{+}T^3{+}2)$	[2,0,−4,2,8,−8,−4,4]
T,$T{+}1$,$T^2{+}T{+}2$	$Y^2{+}XY{=}X^3{+}(2T^4{+}T^3{+}T)/(T^{12}{+}2T^9{+}2T^3{+}1)$	[0,−2,−2,4,4,4,4,−8]
	$Y^2{=}X^3{+}(T^2{+}1)X^2{+}(2T^8{+}T^7{+}T^6{+}T^5{+}T^3{+}2T^2{+}2T)/(T^6{+}1)$	[2,0,−4,−4,−4,8,4,10]
	$Y^2{=}X^3{+}(T^2{+}2T{+}2)X^2{+}(2T^8{+}2T^6{+}T^4{+}2T^3)/(T^6{+}2T^3{+}2)$	[2,−4,0,−4,−4,−8,4,2]
T,$T^3{+}2T{+}1$	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(T^4{+}2T^2{+}T)/(T^6{+}T^3{+}2)$	[−1,−2,2,−3,−1,−7,−8,−7]
	$Y^2{+}XY{=}X^3{+}(T^8{+}2T^6{+}T^5)/(T^{12}{+}T^9{+}T^3{+}1)$	[−3,−2,−2,1,−5,7,−8,7]
T,$T{+}2$,$T^2{+}T{+}2$	$Y^2{=}X^3{+}(T^2{+}2T{+}2)X^2{+}(2T^6{+}T^5{+}2T^4{+}T^2)/(T^6{+}2T^3{+}2)$	[−2,−4,0,8,−10,4,−2,−4]
	$Y^2{+}XY{=}X^3{+}(2T^8{+}2T^6{+}T^3{+}T^2)/(T^{12}{+}T^9{+}T^3{+}1)$	[0,−2,−2,4,−8,4,−8,4]
	$Y^2{=}X^3{+}(T^2{+}1)X^2{+}2T^2(T{+}2)^6(T^2{+}T{+}2)/(T^6{+}1)$	[2,0,−4,8,2,−4,10,4]
T,$(T{+}1)^3$	$Y^2{=}X^3{+}(T^2{+}2T)X^2{+}T^5/(T^4{+}T^3{+}2T{+}2)$	[3,2,−4,1,1,−2,−10,4]
	$Y^2{+}XY{=}X^3{+}(T^3/(T^9{+}1)$	[1,−2,−5,4,10,−2,−2,−5]
	$Y^2{+}XY{=}X^3{+}(T^6/(T^9{+}1)$	[1,−2,4,−5,1,−2,−2,4]
	$Y^2{=}X^3{+}(T^2{+}2T)X^2{+}T^8/(T^4{+}T^3{+}2T{+}2)$	[−3,2,−1,4,−2,10,2,7]
T,$T^3{+}T^2{+}2T{+}1$	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(T^{10}{+}T^9{+}2T^8{+}T^7)/(T^6{+}T^3{+}2)$	[2,1,−1,0,−1,−7,8,4]
T,$T{+}1$,$T^2{+}1$	$Y^2{=}X^3{+}(T^2{+}T{+}2)X^2{+}(2T^6{+}T^5{+}T^4{+}T^3{+}2T^2)/(T^6{+}T^3{+}2)$	[−2,0,−4,8,−10,−2,−4,4]

Continued on next page

Conductor	Curve	Trace
	$Y^2+XY=X^3+(2T^8+T^7+T^6+T^5+2T^4)/(T^{12}+2T^9+2T^3+1)$	$[0,-2,-2,4,-8,-8,4,4]$
	$Y^2=X^3+(T^2+2T+2)X^2+(2T^{10}+T^9+T^8+T^7+2T^6)/(T^6+2T^3+2)$	$[2,-4,0,8,2,10,4,-4]$
$T,T+2,T^2+2T+2$	$Y^2+XY=X^3+(2T^4+2T^3+2T)/(T^{12}+T^9+T^3+1)$	$[0,-2,-2,4,4,-8,4,4]$
	$Y^2=X^3+(T^2+1)X^2+(2T^8+2T^7+T^6+2T^5+2T^3+2T^2+T)/(T^6+1)$	$[2,0,-4,-4,-4,2,-8,4]$
	$Y^2=X^3+(T^2+T+2)X^2+(2T^8+2T^6+T^4+T^3)/(T^6+T^3+2)$	$[2,-4,0,-4,-4,10,8,4]$
$T,T+1,(T+2)^2$	$Y^2+XY=X^3+(2T^2+2T)/(T^6+T^3+1)$	$[-2,-2,-2,4,4,4,-8,4]$

C.4 Table for degree 3 over $\mathbb{F}_5$

Table C.3: Isogeny classes for degree 3 over $\mathbb{F}_5$

Conductor	Curve	Trace
$T,T+2,T+3$	$Y^2=X^3+(3T^4+3T^2+3)X+T^6+2T^5+T^4+2T^3+4T^2+2T+4$	$[-2,-2,-6,-6,10,2,2,-6]$
	$Y^2=X^3+(3T^4+2T^3+3T+2)X+T^6+4T^5+2T^4+T^3+3T^2+3T+3$	$[0,0,2,2,2,-4,8,2]$
	$Y^2=X^3+(3T^4+3T^3+2T+2)X+T^6+T^5+2T^4+4T^3+3T^2+2T+3$	$[0,0,2,2,-10,8,-4,2]$
$T,(T+1)^2$	$Y^2=X^3+(3T^4+T^3+4T+2)X+T^6+T^5+2T^4+3T^3+2T^2+4T+3$	$[3,-3,0,-4,-4,-7,2,8]$
	$Y^2=X^3+(3T^4+T^3+4T+2)X+T^6+2T^5+T+2$	$[-2,2,0,6,6,-2,2,-2]$
	$Y^2=X^3+(3T^4+2T^3+3T^2+2T+3)X+T^6+4T^5+T+4$	$[1,1,-4,-4,-4,1,6,-4]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+4T+3)X+T^6+T^5+4T^4+T^2+4T+4$	$[-2,-2,2,2,2,10,-6,2]$
$T,(T+4)^2$	$Y^2=X^3+(3T^4+T^3+2T^2+T+3)X+T^6+2T^5+2T^4+T^3+3T+1$	$[2,-2,-2,2,2,6,2,-6]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+3T+3)X+T^6+T^5+4T+4$	$[-4,1,1,-4,-4,6,-4,6]$
	$Y^2=X^3+(3T^4+4T^3+T+2)X+T^6+3T^5+4T+2$	$[0,2,-2,6,6,-8,-2,2]$
	$Y^2=X^3+(3T^4+4T^3+T+2)X+T^6+4T^5+2T^4+2T^3+2T^2+T+3$	$[0,-3,3,-4,-4,2,8,2]$
T,T^2+2	$Y^2=X^3+(3T^4+T^2+2)X+T^6+T^2+3$	$[2,-2,-2,2,-6,2,-6,10]$
T,T^2+T+2	$Y^2=X^3+(3T^4+4T^3+2T^2+3T+2)X+T^6+T^5+3T^4+T^3+3T+3$	$[0,0,-3,3,-10,8,-1,-1]$
$T,T+3,T+4$	$Y^2=X^3+(3T^4+2T^3+T^2+4T+2)X+T^6+2T^5+3T^4+T^3+2T^2+T+2$	$[0,0,-4,2,8,-10,2,8]$
	$Y^2=X^3+(3T^4+3T^3+4T+3)X+T^6+4T^4+3T^3+T^2+3T+4$	$[-2,-2,2,10,2,10,-6,2]$
	$Y^2=X^3+(3T^4+4T^3+2T+3)X+T^6+T^5+3T^4+T+1$	$[0,0,8,-10,-4,2,2,-4]$
$T,T+1,T+2$	$Y^2=X^3+(3T^4+T^3+3T+3)X+T^6+4T^5+3T^4+4T+1$	$[0,0,8,-10,2,8,2,2]$
	$Y^2=X^3+(3T^4+2T^3+T+3)X+T^6+4T^4+2T^3+T^2+2T+4$	$[-2,-2,2,10,-6,2,-6,-6]$
	$Y^2=X^3+(3T^4+3T^3+T^2+T+2)X+T^6+3T^5+3T^4+4T^3+2T^2+4T+2$	$[0,0,-4,2,2,-4,2,2]$
T,T^2+4T+2	$Y^2=X^3+(3T^4+T^3+2T^2+2T+2)X+T^6+4T^5+3T^4+4T^3+2T+3$	$[3,-3,0,0,-10,8,8,-1]$
T,T^2+3	$Y^2=X^3+(3T^4+4T^2+2)X+T^6+T^2+2$	$[-2,2,2,-2,-6,2,10,-6]$
$T,T+2,T+4$	$Y^2=X^3+(3T^4+T^3+4T^2+3T+2)X+T^6+T^5+2T^4+2T^3+2T^2+3T+3$	$[0,0,2,-4,8,2,-4,2]$
	$Y^2=X^3+(3T^4+2T^3+4T+3)X+T^6+3T^5+2T^4+3T+4$	$[0,0,-10,8,-4,2,8,2]$
	$Y^2=X^3+(3T^4+4T^3+3T+3)X+T^6+T^4+T^3+T^2+4T+1$	$[-2,-2,10,2,2,-6,2,-6]$
T,T^2+2T+3	$Y^2=X^3+(3T^4+3T^3+3T^2+4T+2)X+T^6+2T^5+2T^4+3T^3+T+2$	$[-3,0,3,0,8,-10,8,-1]$
T,T^2+3T+3	$Y^2=X^3+(3T^4+2T^3+3T^2+T+2)X+T^6+3T^5+2T^4+2T^3+4T+2$	$[0,3,0,-3,8,-10,-1,-1]$

Continued on next page

Conductor	Curve	Trace
$T,T+1,T+3$	$Y^2=X^3+(3T^4+T^3+2T+3)X+T^6+T^4+4T^3+T^2+T+1$	$[-2,-2,10,2,-6,-6,10,2]$
	$Y^2=X^3+(3T^4+3T^3+T+3)X+T^6+2T^5+2T^4+2T+4$	$[0,0,-10,8,2,2,2,-4]$
	$Y^2=X^3+(3T^4+4T^3+4T^2+2T+2)X+T^6+4T^5+2T^4+3T^3+2T^2+2T+3$	$[0,0,2,-4,2,2,-10,8]$
$T,T+1,T+4$	$Y^2=X^3+(3T^4+2T^2+3)X+T^6+T^5+4T^4+4T^3+4T^2+T+1$	$[-2,-2,-6,-6,-6,2,2,10]$
	$Y^2=X^3+(3T^4+T^3+T+2)X+T^6+2T^5+3T^4+2T^3+3T^2+4T+2$	$[0,0,2,2,2,8,8,-10]$
$T,(T+3)^2$	$Y^2=X^3+(3T^4+T^3+2T^2+4T+3)X+T^6+2T^5+3T+1$	$[1,-4,1,-4,-4,1,-4,-4]$
	$Y^2=X^3+(3T^4+2T^3+3T^2+3T+3)X+T^6+3T^5+T^4+T^2+2T+1$	$[-2,2,-2,2,2,-2,2,2]$
	$Y^2=X^3+(3T^4+3T^3+3T+2)X+T^6+T^5+3T+3$	$[-2,0,2,6,6,4,-2,-2]$
	$Y^2=X^3+(3T^4+3T^3+3T+2)X+T^6+3T^5+3T^4+T^3+2T^2+2T+2$	$[3,0,-3,-4,-4,-1,8,8]$
$T,(T+2)^2$	$Y^2=X^3+(3T^4+2T^3+2T+2)X+T^6+4T^5+2T+3$	$[2,0,-2,6,6,4,2,2]$
	$Y^2=X^3+(3T^4+2T^3+2T+2)X+T^6+2T^5+3T^4+4T^3+2T^2+3T+2$	$[-3,0,3,-4,-4,-1,2,2]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+2T+3)X+T^6+T^5+3T^4+2T^3+4T+4$	$[-2,2,-2,2,2,-2,-6,-6]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+T+3)X+T^6+3T^5+2T+1$	$[1,-4,1,-4,-4,1,6,6]$
$T^2,T+1$	$Y^2=X^3+(3T^4)X+T^6+2T^5$	$[-4,1,1,-4,1,1,6,-4]$
	$Y^2=X^3+(3T^4+T^3)X+T^6+2T^4$	$[0,-3,3,8,-1,-7,2,-4]$
	$Y^2=X^3+(3T^4+T^3)X+T^6+4T^5$	$[0,2,-2,-2,4,-2,2,6]$
	$Y^2=X^3+(3T^4+3T^3+3T^2)X+T^6+4T^4+T^3$	$[2,-2,-2,2,-2,10,-6,2]$
$T^2,T+2$	$Y^2=X^3+(3T^4)X+T^6+4T^5$	$[1,1,-4,1,-4,-4,6,6]$
	$Y^2=X^3+(3T^4+T^3+2T^2)X+T^6+T^4+3T^3$	$[-2,-2,2,-2,2,2,6,-6]$
	$Y^2=X^3+(3T^4+2T^3)X+T^6+3T^4$	$[-3,3,0,-1,8,8,2,2]$
	$Y^2=X^3+(3T^4+2T^3)X+T^6+3T^5$	$[2,-2,0,4,-2,-2,-8,2]$
$T^2,T+3$	$Y^2=X^3+(3T^4)X+T^6+T^5$	$[-4,1,1,1,-4,-4,-4,1]$
	$Y^2=X^3+(3T^4+3T^3)X+T^6+3T^4$	$[0,3,-3,-1,8,-4,-4,-1]$
	$Y^2=X^3+(3T^4+3T^3)X+T^6+2T^5$	$[0,-2,2,4,-2,6,6,4]$
	$Y^2=X^3+(3T^4+4T^3+2T^2)X+T^6+T^4+2T^3$	$[2,-2,-2,-2,2,2,2,-2]$
$T^2,T+4$	$Y^2=X^3+(3T^4)X+T^6+3T^5$	$[1,1,-4,-4,1,6,1,6]$
	$Y^2=X^3+(3T^4+2T^3+3T^2)X+T^6+4T^4+4T^3$	$[-2,-2,2,2,-2,-6,-2,6]$
	$Y^2=X^3+(3T^4+4T^3)X+T^6+2T^4$	$[3,-3,0,8,-1,2,-1,2]$
	$Y^2=X^3+(3T^4+4T^3)X+T^6+T^5$	$[-2,2,0,-2,4,2,4,-8]$

C.5 Table for non-primes of degree 4 over $\mathbb{F}_5$

Table C.4: Isogeny classes for non-primes of degree 4 over $\mathbb{F}_5$

Conductor	Curve	Trace
$T,T+1,T^2+4T+2$	$Y^2=X^3+(3T^4+3T^2+T+2)X+T^6+2T^5+2T^4+T^3+4T+2$	$[0,3,3,-1,2,2,2,-7]$
	$Y^2=X^3+(3T^4+2T^3+2)X+T^6+T^5+T^4+T^3+2T^2+3T+2$	$[-2,-3,-1,7,-4,-8,2,-3]$
	$Y^2=X^3+(3T^4+2T^3+T^2+2T+2)X+T^6+T^5+4T^4+2T^3+4T^2+2T+3$	$[-2,-2,0,8,6,2,-8,4]$

Continued on next page

Conductor	**Curve**	**Trace**
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}3)X{+}T^6{+}2T^5{+}2T^4{+}3T^3{+}2T^2{+}4$	$[-4,-1,-3,-7,-6,2,-2,7]$
$T,T{+}4,T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}T{+}2)X{+}T^6{+}T^4{+}T^3{+}2T^2{+}4T{+}2$	$[-2,-2,-2,-6,2,-2,2,-6]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}4T{+}3)X{+}T^6{+}3T^5{+}2T^4{+}2T^3{+}2T^2{+}2T{+}1$	$[-1,-2,-3,-2,-2,-2,1,1]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}T{+}2)X{+}T^6{+}T^5{+}4T^2{+}4T{+}2$	$[2,1,3,1,1,-5,-2,-2]$
$T,(T{+}2)^2,T{+}3$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3T{+}2)X{+}T^6{+}2T^4{+}4T^3{+}T{+}3$	$[-3,-1,6,-6,3,-8,-4,3]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3T{+}2)X{+}T^6{+}4T^5{+}4T^3{+}2T^2{+}2T{+}2$	$[2,4,6,-6,-2,2,-4,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T{+}3)X{+}T^6{+}4T^4{+}2T^3{+}T^2{+}4$	$[2,2,2,2,-2,-2,-2,-6]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}2T^3{+}2T^2{+}2T{+}4$	$[-3,-3,2,2,-7,8,8,-1]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3T{+}2)X{+}T^6{+}T^5{+}2T^4{+}4T^3{+}T^2{+}2T{+}3$	$[4,0,-6,-6,6,-4,4,-6]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}2)X{+}T^6{+}3T^5{+}2T^3{+}4T^2{+}2$	$[1,3,-6,6,3,-4,-8,3]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}2)X{+}T^6{+}4T^5{+}T^4{+}3T^3{+}3T{+}3$	$[-4,-2,-6,6,-2,-4,2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}T{+}2)X{+}T^6{+}T^5{+}2T^4{+}2T^3{+}4T^2{+}3T{+}2$	$[0,-4,-6,-6,-6,4,-4,-6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}T{+}3)X{+}T^6{+}T^5{+}2T^4{+}T^3{+}3T^2{+}T{+}4$	$[1,1,6,6,1,-4,-4,-9]$
$T,T^3{+}4T^2{+}T{+}2$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}T{+}3)X{+}T^6{+}3T^5{+}2T^2{+}3T{+}4$	$[0,0,0,3,-1,-1,-4,-7]$
$T,T{+}2,(T{+}4)^2$	$Y^2{=}X^3{+},3T^4{+}3T^2{+}2T{+}2)X{+}T^6{+}2T^5{+}4T^4{+}4T^3{+}4T^2{+}3T{+}2$	$[2,2,-2,-2,-2,-6,6,-10]$
	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}2T{+}2)X{+}T^6{+}4T^5{+}3T^4{+}T^3{+}T^2{+}2T{+}3$	$[-3,-3,-7,8,8,-1,-4,-10]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3)X{+}T^6{+}3T^5{+}2T^4{+}3T^2{+}1$	$[0,4,6,-4,4,-6,4,6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}T{+}3)X{+}T^6{+}2T^3{+}T^2{+}2T{+}4$	$[3,1,3,-4,-8,3,-8,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}T{+}3)X{+}T^6{+}T^5{+}T^4{+}T^3{+}2T^2{+}3T{+}1$	$[-2,-4,-2,-4,2,-2,-8,4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}4T{+}2)X{+}T^6{+}3T^5{+}2T^4{+}3T^3{+}4T^2{+}4T{+}3$	$[-4,0,-6,4,-4,-6,-4,6]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}3T^5{+}2T^4{+}2T^3{+}2T^2{+}T{+}4$	$[1,1,1,-4,-4,-9,-4,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2)X{+}T^6{+}T^5{+}4T^3{+}T^2{+}3$	$[4,2,-2,2,-4,-2,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2)X{+}T^6{+}2T^5{+}2T^4{+}2T^2{+}3$	$[-1,-3,3,-8,-4,3,8,-6]$
$T,T{+}1,T^2{+}2$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}4T{+}2)X{+}T^6{+}2T^5{+}T^4{+}T^3{+}4T{+}3$	$[1,2,3,-7,-8,9,-4,7]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3)X{+}T^6{+}T^5{+}3T^4{+}1$	$[-3,-4,-1,3,2,-3,-6,-7]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}3T{+}4$	$[-3,0,-3,-1,2,-1,2,-1]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}T^4{+}T^2{+}4T{+}1$	$[0,2,2,6,2,-6,6,8]$
$T,T^3{+}2T^2{+}2T{+}2$	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}4T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}3T{+}4$	$[3,0,0,0,-1,-1,-1,2]$
$T,T^3{+}3T^2{+}2T{+}2$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}4T{+}3)X{+}T^6{+}3T^5{+}2T^4{+}3T{+}4$	$[-3,3,0,3,-1,8,2,-4]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}2T^3{+}T{+}1$	$[-3,-3,0,-1,9,-4,2,-8]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}3T^2{+}4T{+}1$	$[0,-2,-1,-4,-3,4,3,2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}2)X{+}T^6{+}3T^5{+}T^4{+}4T^3{+}3T^2{+}3$	$[-2,0,3,4,3,-2,-9,-8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}4T^5{+}3T^4{+}4T^3{+}2T^2{+}3T{+}4$	$[-3,1,-4,-1,-3,-8,-6,8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}3T{+}2)X{+}T^6{+}2T^5{+}T^4{+}T^2{+}2T{+}2$	$[-1,1,-2,-3,-1,-2,6,-4]$
$T,T{+}3,T^2{+}3T{+}4$	$Y^2{=}X^3{+}(3T^4{+}T^2{+}2T{+}2)X{+}T^6{+}2T^5{+}T^4{+}T^2{+}3T{+}2$	$[-2,0,-4,-2,-8,-8,4,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}T^5{+}T^4{+}2T^3{+}4T{+}1$	$[0,-2,-4,-8,4,-2,-8,4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T{+}3)X{+}T^6{+}3T^5{+}T^4{+}4T^3{+}4T^2{+}3T{+}4$	$[2,-2,2,-2,-2,-6,6,6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}T^5{+}3T^3{+}T^2{+}4T{+}1$	$[-4,-2,0,4,-8,-2,4,-8]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}2)X{+}T^6{+}T^5{+}4T^4{+}4T^2{+}2$	$[4,0,2,-8,-2,4,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}2T^3{+}4T^2{+}2T{+}4$	$[2,2,-2,6,-6,6,-6,-2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}4T{+}2)X{+}T^6{+}2T^5{+}2T^3{+}4T^2{+}4T{+}3$	$[-2,-4,0,-2,4,4,-8,-2]$

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}4T{+}2)X{+}T^6{+}2T^5{+}4T^4{+}3T^3{+}4T{+}3$	$[0,4,2,4,-2,-8,-2,-8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}2T{+}3)X{+}T^6{+}T^4{+}3T^3{+}2T^2{+}4T{+}4$	$[-2,2,2,-6,6,-2,-2,-6]$
$T,T{+}1,T^2{+}T{+}2$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2T{+}2)X{+}T^6{+}3T^5{+}2T^4{+}2T{+}3$	$[-1,-3,-2,1,1,3,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}4T{+}3)X{+}T^6{+}3T^5{+}2T^4{+}3T^3{+}2T^2{+}2T{+}1$	$[-2,-3,-1,-2,-2,3,1,1]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}T{+}2)X{+}T^6{+}3T^5{+}3T^4{+}T^3{+}T^2{+}T{+}3$	$[2,2,2,2,-6,-6,2,-6]$
$T,T{+}2,T^2{+}T{+}1$	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}3T{+}2)X{+}T^6{+}T^4{+}2T^3{+}2T^2{+}4T{+}3$	$[-2,-2,0,-8,4,-6,-8,2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}3T{+}3)X{+}T^6{+}4T^4{+}4T^3{+}T{+}4$	$[-3,-2,-1,-4,-3,1,2,-8]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}3T{+}1$	$[-1,-4,-3,-8,7,3,-2,2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}T{+}2)X{+}T^6{+}3T^5{+}3T^4{+}T^3{+}4T^2{+}4T{+}2$	$[3,0,3,-4,-7,-1,2,2]$
$T,T{+}4,T^2{+}3$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3T{+}3)X{+}T^6{+}3T^2{+}4T{+}1$	$[-1,-3,-4,3,-2,-6,-3,-7]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}2T^2{+}3T{+}4$	$[-3,-3,0,-1,2,2,-1,-1]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}T{+}3)X{+}T^6{+}T^4{+}3T^3{+}2T^2{+}2T{+}4$	$[2,0,2,6,-8,6,-6,8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}2T{+}2)X{+}T^6{+}2T^5{+}3T^3{+}2T^2{+}T{+}2$	$[-3,-1,-2,-7,2,-4,9,7]$
$T,T^3{+}4T{+}2$	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3)X{+}T^6{+}4T^5{+}T^4{+}4T^3{+}1$	$[-4,-1,0,-2,8,2,-2,-2]$
$T,T{+}2,T^2{+}4T{+}1$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}4T{+}2)X{+}T^6{+}3T^5{+}2T^2{+}T{+}2$	$[-3,0,-3,-7,-4,2,2,-1]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}3)X{+}T^6{+}T^5{+}4T^3{+}T^2{+}4$	$[-1,-2,-3,-3,-4,-4,2,1]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}2)X{+}T^6{+}2T^5{+}4T^4{+}T^3{+}2T^2{+}2$	$[0,2,2,4,-8,6,-8,-6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}2T^5{+}3T^2{+}2T{+}1$	$[-3,-4,-1,7,-8,-6,-2,3]$
$T,T{+}1,T{+}3,T{+}4$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3T{+}3)X{+}T^6{+}T^5{+}4T^4{+}T^3{+}4T^2{+}4T{+}4$	$[2,-2,-6,-2,-6,2,-2,2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}4T{+}2)X{+}T^6{+}T^4{+}4T{+}3$	$[2,-2,2,-6,-2,2,2,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3)X{+}T^6{+}3T^5{+}4T^4{+}T^3{+}2T^2{+}1$	$[2,-6,-2,2,2,-6,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}2T{+}3)X{+}T^6{+}T^4{+}T^3{+}4T^2{+}4$	$[2,2,2,2,-2,-2,-6,-2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}T{+}2)X{+}T^6{+}2T^5{+}2T^4{+}T^3{+}2T^2{+}2T{+}3$	$[-2,2,-2,-2,2,-2,2,2]$
$T,T^3{+}4T^2{+}4T{+}2$	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}4T{+}2)X{+}T^6{+}T^4{+}2T^3{+}2T^2{+}4T{+}2$	$[-4,0,-3,2,-2,3,5,-4]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}4T^3{+}2T^2{+}4T{+}4$	$[-1,1,-4,-3,-8,-3,-1,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}3)X{+}T^6{+}3T^5{+}3T^2{+}3T{+}4$	$[3,3,0,-3,8,-1,-1,-4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}T^5{+}3T^4{+}3T^2{+}2T{+}1$	$[-4,-2,-1,0,4,-3,-7,4]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}4T{+}2)X{+}T^6{+}4T^5{+}3T^4{+}3T^2{+}4T{+}3$	$[3,-1,2,1,-2,-1,7,2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}4T^5{+}3T^3{+}3T^2{+}2T{+}1$	$[-1,-3,0,-3,-4,9,7,-6]$
$T,T{+}2,T^2{+}3T{+}4$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}3T{+}2)X{+}T^6{+}3T^5{+}3T^4{+}2T{+}2$	$[-2,-3,-1,4,-5,1,-2,-5]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}4T{+}3)X{+}T^6{+}2T^5{+}4T^4{+}T^2{+}2T{+}4$	$[-2,-2,-2,6,6,2,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}T{+}2)X{+}T^6{+}4T^5{+}4T^2{+}T{+}3$	$[1,3,2,-5,4,-2,-5,-2]$
$T,T{+}3,(T{+}4)^2$	$Y^2{=}X^3{+},3T^4{+}4T^2{+}3)X{+}T^6{+}4T^5{+}2T^3{+}4T^2{+}4$	$[0,4,-4,6,4,-6,-6,-4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}T{+}2)X{+}T^6{+}2T^4{+}4T^3{+}4T^2{+}T{+}3$	$[-4,-2,2,-2,-4,-2,-6,-8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}T{+}2)X{+}T^6{+}4T^4{+}4T^2{+}4T{+}2$	$[1,3,-8,3,-4,3,-6,-8]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}2T^4{+}T^2{+}4T{+}4$	$[-2,-4,-4,-2,2,-2,6,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}4T^4{+}3T^3{+}4$	$[3,1,-4,3,-8,3,6,8]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3T{+}2)X{+}T^6{+}4T^5{+}3T^3{+}T^2{+}3T{+}3$	$[4,0,4,-6,-4,6,-6,4]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}2)X{+}T^6{+}T^5{+}4T^4{+}T^2{+}T{+}2$	$[-2,-2,-2,-2,-2,-2,2,6]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}2)X{+}T^6{+}4T^5{+}2T^2{+}3$	$[3,3,8,-7,8,-7,2,-4]$

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}4T^5{+}3T^4{+}3T^3{+}3T^2{+}2T{+}4$	$[1,1,-4,1,-4,1,6,-4]$
$T,T^3{+}2T^2{+}3$	$Y^2{=}X^3{+}(3T^4{+}3T{+}3)X{+}T^6{+}4T^3{+}T^2{+}4T{+}1$	$[-4,0,-1,-2,2,8,-2,-1]$
$T,T{+}1,T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}3T{+}2)X{+}T^6{+}4T^5{+}T^4{+}3T^3{+}3T^2{+}3T{+}3$	$[3,2,1,-4,7,-8,9,-7]$
	$Y^2{=}X^3{+}(3T^4{+}T^2{+}4T{+}3)X{+}T^6{+}3T^4{+}2T^3{+}3T^2{+}3T{+}4$	$[-1,-4,-3,-6,-7,2,-3,3]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}3T{+}2)X{+}T^6{+}4T^5{+}T^4{+}4T^3{+}2T^2{+}3T{+}3$	$[2,2,0,6,8,2,-6,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}2)X{+}T^6{+}3T^5{+}3T^4{+}2T^3{+}3T^2{+}2$	$[-3,0,-3,2,-1,2,-1,-1]$
$T,T{+}4,T^2{+}T{+}2$	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}4T{+}2)X{+}T^6{+}3T^5{+}2T^4{+}4T^3{+}T{+}2$	$[3,3,0,-1,2,-1,-1,-1]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3)X{+}T^6{+}3T^5{+}2T^4{+}2T^3{+}2T^2{+}4$	$[-3,-1,-4,-7,-6,3,-3,3]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2)X{+}T^6{+}4T^5{+}T^4{+}4T^3{+}2T^2{+}2T{+}2$	$[-1,-3,-2,7,-4,1,9,-7]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}3T{+}2)X{+}T^6{+}4T^5{+}4T^4{+}3T^3{+}4T^2{+}3T{+}3$	$[0,-2,-2,8,6,-6,-6,6]$
$T,T^3{+}T^2{+}T{+}3$	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}4T{+}3)X{+}T^6{+}2T^5{+}2T^2{+}2T{+}4$	$[3,0,0,0,-1,-1,-1,2]$
$T,T{+}2,(T{+}3)^2$	$Y^2{=}X^3{+},3T^4{+}4T^2{+}2T{+}2)X{+}T^6{+}2T^4{+}T^3{+}4T{+}3$	$[-1,-3,6,-6,3,-8,8,-6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}2T{+}2)X{+}T^6{+}T^5{+}T^3{+}2T^2{+}3T{+}2$	$[4,2,6,-6,-2,-8,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2{+}4T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}4T^3{+}3T^2{+}4T{+}4$	$[1,1,6,6,1,-4,-4,6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}2)X{+}T^6{+}T^5{+}T^4{+}2T^3{+}2T{+}3$	$[-2,-4,-6,6,-2,-2,-8,4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}2)X{+}T^6{+}2T^5{+}3T^3{+}4T^2{+}2$	$[3,1,-6,6,3,8,-8,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}4T{+}2)X{+}T^6{+}4T^5{+}2T^4{+}3T^3{+}4T^2{+}2T{+}2$	$[-4,0,-6,-6,6,4,-4,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T{+}3)X{+}T^6{+}4T^4{+}3T^3{+}T^2{+}4$	$[2,2,2,2,-2,6,6,-10]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}3T^3{+}2T^2{+}3T{+}4$	$[-3,-3,2,2,-7,-4,-4,-10]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2T{+}2)X{+}T^6{+}4T^5{+}2T^4{+}T^3{+}T^2{+}3T{+}3$	$[0,4,-6,-6,-6,-4,4,6]$
$T,T{+}1,T^2{+}3T{+}3$	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}4T{+}2)X{+}T^6{+}4T^5{+}4T^2{+}T{+}2$	$[3,1,2,1,1,3,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}T{+}3)X{+}T^6{+}2T^5{+}2T^4{+}3T^3{+}2T^2{+}3T{+}1$	$[-3,-2,-1,-2,-2,3,-5,-5]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}4T{+}2)X{+}T^6{+}T^4{+}4T^3{+}2T^2{+}T{+}2$	$[-2,-2,-2,-6,2,-6,-2,6]$
$T,(T{+}1)^2,T{+}3$	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}3T{+}2)X{+}T^6{+}2T^5{+}3T^4{+}2T^2{+}2T{+}3$	$[2,2,-2,-2,2,2,-2,6]$
	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}3T{+}2)X{+}T^6{+}T^5{+}3T^4{+}4T^3{+}T^2{+}3T{+}3$	$[-3,-3,-7,8,2,2,-7,-4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3)X{+}T^6{+}2T^5{+}2T^4{+}3T^2{+}1$	$[4,0,6,-4,-6,-6,-6,-4]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2)X{+}T^6{+}3T^5{+}2T^4{+}2T^2{+}3$	$[-3,-1,3,-8,6,-6,3,-8]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2)X{+}T^6{+}4T^5{+}T^3{+}T^2{+}3$	$[2,4,-2,2,6,-6,-2,-8]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}2T^5{+}2T^4{+}3T^3{+}2T^2{+}4T{+}4$	$[1,1,1,-4,6,6,1,-4]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}4T{+}3)X{+}T^6{+}3T^3{+}T^2{+}3T{+}4$	$[1,3,3,-4,-6,6,3,8]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2{+}4T{+}3)X{+}T^6{+}4T^5{+}T^4{+}4T^3{+}2T^2{+}2T{+}1$	$[-4,-2,-2,-4,-6,6,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}T{+}2)X{+}T^6{+}2T^5{+}2T^4{+}2T^3{+}4T^2{+}T{+}3$	$[0,-4,-6,4,-6,-6,6,4]$
$T,T^3{+}2T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}T{+}3)X{+}T^6{+}2T^5{+}2T^4{+}2T{+}4$	$[3,0,3,-3,-1,8,-1,-7]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2)X{+}T^6{+}2T^5{+}T^4{+}T^3{+}3T^2{+}3$	$[4,3,0,-2,3,-2,5,9]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}T{+}3)X{+}T^6{+}T^5{+}3T^4{+}T^3{+}2T^2{+}2T{+}4$	$[-1,-4,1,-3,-3,-8,-1,3]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T{+}2)X{+}T^6{+}3T^5{+}T^4{+}T^2{+}3T{+}2$	$[-3,-2,1,-1,-1,-2,7,1]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}3T^2{+}T{+}1$	$[-4,-1,-2,0,-3,4,-7,-9]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}3T^3{+}4T{+}1$	$[-1,0,-3,-3,9,-4,7,-1]$
$T,T^3{+}3T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}2T{+}4$	$[0,0,0,3,-1,-1,-4,8]$
$T,T{+}4,T^2{+}2$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}T^4{+}T^2{+}T{+}1$	$[2,2,0,6,-8,-8,-6,4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}2T{+}4$	$[-3,0,-3,-1,2,-4,-1,-7]$

Continued on next page

Conductor	Curve	Trace
	$Y^2=X^3+(3T^4+3T^3+3T^2+T+2)X+T^6+3T^5+T^4+4T^3+T+3$	[3,2,1,−7,2,−4,1,−3]
	$Y^2=X^3+(3T^4+3T^3+4T^2+3)X+T^6+4T^5+3T^4+1$	[−1,−4,−3,3,−2,−8,3,7]
$T,T+1,T^2+3$	$Y^2=X^3+(3T^4+4T^2+2T+3)X+T^6+3T^2+T+1$	[−4,−3,−1,3,2,3,−8,7]
	$Y^2=X^3+(3T^4+T^3+2T^2+3T+2)X+T^6+3T^5+2T^3+2T^2+4T+2$	[−2,−1,−3,−7,−8,1,−4,−3]
	$Y^2=X^3+(3T^4+3T^3+3T^2+4T+3)X+T^6+T^4+2T^3+2T^2+3T+4$	[2,0,2,6,2,−6,−8,4]
	$Y^2=X^3+(3T^4+4T^3+3T^2+3T+3)X+T^6+2T^5+2T^2+2T+4$	[0,−3,−3,−1,2,−1,−4,−7]
$T,T+3,T^2+4T+1$	$Y^2=X^3+(3T^4+2T^2+2T+2)X+T^6+T^4+3T^3+2T^2+T+3$	[0,−2,−2,−8,4,6,8,6]
	$Y^2=X^3+(3T^4+3T^2+2T+3)X+T^6+4T^4+T^3+4T+4$	[−1,−2,−3,−4,−3,−4,7,−7]
	$Y^2=X^3+(3T^4+T^3+4T^2+4T+2)X+T^6+2T^5+3T^4+4T^3+4T^2+T+2$	[3,0,3,−4,−7,2,−1,−1]
	$Y^2=X^3+(3T^4+4T^3+3T^2+4T+3)X+T^6+2T^5+3T^4+2T+1$	[−3,−4,−1,−8,7,−6,−7,3]
$T,T+4,T^2+4T+2$	$Y^2=X^3+(3T^4+4T^3+T^2+T+3)X+T^6+2T^5+2T^4+2T^3+2T^2+3T+1$	[−1,−3,−2,−2,−2,−2,−5,−5]
	$Y^2=X^3+(3T^4+4T^3+T^2+3T+2)X+T^6+2T^5+2T^4+3T+3$	[−2,−3,−1,1,1,−5,4,−2]
	$Y^2=X^3+(3T^4+4T^3+4T^2+4T+2)X+T^6+2T^5+3T^4+4T^3+T^2+4T+3$	[2,2,2,2,−6,−2,6,−2]
$T,T+2,T^2+2T+4$	$Y^2=X^3+(3T^4+T^2+3T+2)X+T^6+3T^5+T^4+T^2+2T+2$	[−4,0,−2,−2,−8,4,−2,−2]
	$Y^2=X^3+(3T^4+T^3+2T^2+T+2)X+T^6+3T^5+3T^3+4T^2+T+3$	[0,−4,−2,−2,4,−8,−2,6]
	$Y^2=X^3+(3T^4+T^3+3T^2+T+2)X+T^6+3T^5+4T^4+2T^3+T+3$	[2,4,0,4,−2,4,6,−2]
	$Y^2=X^3+(3T^4+T^3+4T^2+3T+3)X+T^6+T^4+2T^3+2T^2+T+4$	[2,2,−2,−6,6,6,−6,2]
	$Y^2=X^3+(3T^4+2T^3+4T^2+4T+3)X+T^6+T^5+2T^4+3T^3+4T^2+3T+4$	[−2,2,2,6,−6,−2,2,−6]
	$Y^2=X^3+(3T^4+3T^3+2T+3)X+T^6+T^5+T^3+T+4$	[2,−2,2,−2,−2,−6,2,2]
	$Y^2=X^3+(3T^4+3T^3+3T^2+T+3)X+T^6+4T^5+2T^3+T^2+T+1$	[0,−2,−4,4,−8,−2,−2,6]
	$Y^2=X^3+(3T^4+3T^3+4T^2+2)X+T^6+4T^5+4T^4+4T^2+2$	[2,0,4,−8,−2,−8,−2,−2]
	$Y^2=X^3+(3T^4+4T^3+3T^2+2T+3)X+T^6+4T^5+T^4+3T^3+T+1$	[−4,−2,0,−8,4,−2,6,−2]
T,T^3+4T+3	$Y^2=X^3+(3T^4+2T^3+3)X+T^6+T^5+T^4+T^3+1$	[−2,0,−1,−4,8,2,−9,4]
T,T^3+T^2+4T+3	$Y^2=X^3+(3T^4+2T^2+T+2)X+T^6+T^4+3T^3+2T^2+T+2$	[2,−3,0,−4,−2,3,−9,−2]
	$Y^2=X^3+(3T^4+2T^3+T^2+T+2)X+T^6+T^5+3T^4+3T^2+T+3$	[1,2,−1,3,−2,−1,6,−8]
	$Y^2=X^3+(3T^4+2T^3+3T^2+T+3)X+T^6+T^5+2T^3+3T^2+3T+1$	[−3,0,−3,−1,−4,9,2,6]
	$Y^2=X^3+(3T^4+3T^3+3T^2+T+3)X+T^6+4T^5+3T^4+3T^2+3T+1$	[0,−1,−2,−4,4,−3,3,−2]
	$Y^2=X^3+(3T^4+4T^3+3T^2+4T+3)X+T^6+2T^5+3T^4+T^3+2T^2+T+4$	[−3,−4,1,−1,−8,−3,−6,−2]
	$Y^2=X^3+(3T^4+4T^3+4T^2+3)X+T^6+2T^5+3T^2+2T+4$	[−3,0,3,3,8,−1,2,−4]
$T,T+1,T+2,T+4$	$Y^2=X^3+(3T^4+4T^2+2T+3)X+T^6+T^5+T^4+3T^2+T+1$	[2,−2,−6,2,−2,2,2,2]
	$Y^2=X^3+(3T^4+T^3+2T^2+4T+2)X+T^6+3T^5+2T^4+4T^3+2T^2+3T+3$	[−2,2,−2,−6,−6,2,−2,−2]
	$Y^2=X^3+(3T^4+2T^3+2T^2+3T+3)X+T^6+T^4+4T^3+4T^2+4$	[2,2,2,2,−2,−2,−6,−2]
	$Y^2=X^3+(3T^4+3T^3+4T^2+3)X+T^6+T^5+T^4+4T^3+T^2+4T+4$	[2,−6,−2,−2,2,−2,2,−6]
	$Y^2=X^3+(3T^4+4T^3+3T^2+T+2)X+T^6+T^4+T+3$	[2,−2,2,−2,2,−6,−2,2]
$T,T+3,T^2+T+1$	$Y^2=X^3+(3T^4+T^3+3T^2+T+3)X+T^6+3T^5+3T^2+3T+1$	[−1,−4,−3,7,−8,3,−7,−3]
	$Y^2=X^3+(3T^4+2T^3+3T^2+2)X+T^6+3T^5+4T^4+4T^3+2T^2+2$	[2,2,0,4,−8,6,8,−6]
	$Y^2=X^3+(3T^4+3T^3+3T^2+3)X+T^6+4T^5+T^3+T^2+4$	[−3,−2,−1,−3,−4,−7,7,9]
	$Y^2=X^3+(3T^4+4T^3+T^2+T+2)X+T^6+2T^5+2T^2+4T+2$	[−3,0,−3,−7,−4,−1,−1,−1]
$T,T+4,T^2+T+1$	$Y^2=X^3+(3T^4+T^3+3T^2+3T+2)X+T^6+3T^5+4T^2+2T+2$	[3,1,2,4,−5,−2,−5,−2]
	$Y^2=X^3+(3T^4+2T^3+2T^2+2T+3)X+T^6+3T^5+2T^4+T^3+2T^2+3T+1$	[−2,−2,−2,6,6,−6,−2,2]

Continued on next page

Conductor	**Curve**	**Trace**
	$Y^2=X^3+(3T^4+2T^3+2T^2+4T+2)X+T^6+T^5+2T^4+4T+3$	$[-3,-2,-1,-5,4,1,-2,1]$
$T,T+2,T^2+4T+2$	$Y^2=X^3+(3T^4+4T+2)X+T^6+3T^5+4T^4+4T^3+3T^2+T+2$	$[2,1,3,7,-4,-4,2,9]$
	$Y^2=X^3+(3T^4+4T^2+2T+3)X+T^6+2T^4+T^3+3T^2+T+1$	$[-4,-3,-1,-7,-6,-8,-2,-3]$
	$Y^2=X^3+(3T^4+T^3+T^2+4T+2)X+T^6+3T^5+4T^4+2T^3+2T^2+T+2$	$[2,0,2,8,6,-8,-8,-6]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+2)X+T^6+T^5+2T^4+T^3+3T^2+3$	$[0,-3,-3,-1,2,-4,2,-1]$
$T,T+1,(T+3)^2$	$Y^2=X^3+,3T^4+T^2+3)X+T^6+3T^5+T^3+4T^2+1$	$[0,4,6,-4,6,-6,-6,4]$
	$Y^2=X^3+(3T^4+T^2+3T+2)X+T^6+T^4+4T^2+3T+3$	$[1,3,3,-8,-6,3,3,-4]$
	$Y^2=X^3+(3T^4+T^2+3T+2)X+T^6+3T^4+2T^3+4T^2+2T+2$	$[-4,-2,-2,2,4,-2,-2,-4]$
	$Y^2=X^3+(3T^4+T^3+2T^2+4T+3)X+T^6+3T^5+2T^4+4T^3+3T^2+4T+1$	$[1,1,1,-4,6,-9,1,-4]$
	$Y^2=X^3+(3T^4+T^3+3T^2+2)X+T^6+2T^5+T^4+T^2+2T+3$	$[-2,-2,-2,-2,-10,-6,-2,-2]$
	$Y^2=X^3+(3T^4+T^3+3T^2+2)X+T^6+3T^5+2T^2+2$	$[3,3,-7,8,-10,-1,-7,8]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+T+3)X+T^6+T^5+T^4+4T^3+1$	$[3,1,3,-4,-6,3,3,-8]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+T+3)X+T^6+T^5+3T^4+T^2+3T+1$	$[-2,-4,-2,-4,4,-2,-2,2]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+4T+2)X+T^6+3T^5+4T^3+T^2+T+2$	$[4,0,-6,4,6,-6,6,-4]$
T,T^3+4T^2+4	$Y^2=X^3+(3T^4+4T+3)X+T^6+2T^3+T^2+3T+4$	$[-1,-4,-2,0,8,2,-7,-2]$
T,T^3+T+4	$Y^2=X^3+(3T^4+4T^3+3)X+T^6+2T^5+4T^4+3T^3+4$	$[-1,-2,-4,0,2,8,-7,1]$
T,T^3+2T^2+T+4	$Y^2=X^3+(3T^4+3T^2+3T+2)X+T^6+4T^4+4T^3+2T^2+2T+3$	$[0,2,-4,-3,3,-2,2,-8]$
	$Y^2=X^3+(3T^4+T^3+2T^2+3T+3)X+T^6+3T^5+2T^4+3T^2+T+4$	$[-2,0,-4,-1,-3,4,8,2]$
	$Y^2=X^3+(3T^4+3T^3+T^2+3)X+T^6+4T^5+3T^2+4T+1$	$[3,-3,3,0,-1,8,-4,-4]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+2T+3)X+T^6+4T^5+2T^4+3T^3+2T^2+2T+1$	$[1,-3,-1,-4,-3,-8,2,8]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+3T+3)X+T^6+2T^5+T^3+3T^2+T+4$	$[-3,-3,-1,0,9,-4,-6,-8]$
	$Y^2=X^3+(3T^4+4T^3+4T^2+3T+2)X+T^6+2T^5+2T^4+3T^2+2T+2$	$[-1,1,3,2,-1,-2,-4,-4]$
$T,T+1,T^2+2T+4$	$Y^2=X^3+(3T^4+T^3+2T^2+3)X+T^6+3T^5+3T^3+T^2+1$	$[-3,-1,-2,-4,-3,-8,1,-7]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+3T+3)X+T^6+T^5+3T^2+T+4$	$[-1,-3,-4,-8,7,2,3,3]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+3T+2)X+T^6+4T^5+2T^2+3T+3$	$[-3,-3,0,-4,-7,2,-1,-1]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+2)X+T^6+T^5+T^4+2T^3+2T^2+3$	$[2,0,2,-8,4,2,-6,6]$
$T,T+2,T+3,T+4$	$Y^2=X^3+(3T^4+T^2+T+3)X+T^6+2T^5+4T^4+3T^2+2T+4$	$[2,-6,-2,-2,2,-2,2,-6]$
	$Y^2=X^3+(3T^4+T^3+T^2+3)X+T^6+2T^5+4T^4+2T^3+T^2+3T+1$	$[2,-2,-6,-2,-6,2,-2,2]$
	$Y^2=X^3+(3T^4+2T^3+3T^2+2T+2)X+T^6+T^5+2T^4+3T^3+T^2+2T+3$	$[-2,-2,2,2,-2,-6,-6,2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+3T+2)X+T^6+4T^4+2T+2$	$[2,2,-2,2,2,2,-2,-2]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+4T+3)X+T^6+4T^4+2T^3+4T^2+1$	$[2,2,2,-6,-2,-2,2,-2]$
$T,T+3,T^2+3T+3$	$Y^2=X^3+(3T^4+3T^3+T^2+2T+2)X+T^6+4T^5+T^4+T^3+4T^2+4T+3$	$[2,2,2,-6,2,-6,2,6]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+3T+3)X+T^6+4T^5+3T^4+T^3+2T^2+T+4$	$[-2,-1,-3,-2,-2,1,1,-5]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+4T+2)X+T^6+4T^5+3T^4+T+2$	$[-1,-2,-3,1,1,-2,-2,4]$
$T,T+2,T^2+2$	$Y^2=X^3+(3T^4+T^2+T+3)X+T^6+3T^2+2T+4$	$[-3,-1,-4,3,-7,-3,3,2]$
	$Y^2=X^3+(3T^4+T^3+2T^2+2T+3)X+T^6+4T^4+T^3+2T^2+T+1$	$[0,2,2,6,8,-6,-6,2]$
	$Y^2=X^3+(3T^4+2T^3+3T^2+4T+2)X+T^6+T^5+T^3+2T^2+3T+3$	$[-1,-3,-2,-7,7,9,1,-8]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+4T+3)X+T^6+4T^5+2T^2+4T+1$	$[-3,-3,0,-1,-1,-1,-1,2]$
$T,T+4,T^2+4T+1$	$Y^2=X^3+(3T^4+4T^2+4T+2)X+T^6+T^5+4T^4+T^2+4T+3$	$[0,-4,-2,-8,-2,6,-2,-2]$
	$Y^2=X^3+(3T^4+T^3+T+3)X+T^6+2T^5+3T^3+2T+1$	$[-2,2,2,-2,-2,-6,6,2]$
	$Y^2=X^3+(3T^4+T^3+T^2+2)X+T^6+3T^5+T^4+4T^2+3$	$[0,2,4,-2,-8,6,4,-2]$

Continued on next page

Conductor	**Curve**	**Trace**
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2{+}3T{+}3)X{+}T^6{+}3T^5{+}T^3{+}T^2{+}2T{+}4$	$[-2,0,-4,-8,4,-2,-8,-2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}4T{+}3)X{+}T^6{+}4T^4{+}T^3{+}2T^2{+}2T{+}1$	$[2,2,-2,6,-6,2,-6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}3T{+}2)X{+}T^6{+}T^5{+}T^4{+}T^3{+}2T{+}2$	$[4,2,0,-2,4,-2,-8,6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}3T{+}2)X{+}T^6{+}T^5{+}4T^3{+}4T^2{+}2T{+}2$	$[-4,0,-2,4,-2,-2,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}T{+}3)X{+}T^6{+}3T^5{+}4T^4{+}4T^3{+}2T{+}4$	$[-2,-4,0,4,-8,-2,4,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2T{+}3)X{+}T^6{+}2T^5{+}T^4{+}3T^3{+}3T{+}4$	$[2,-2,2,-6,6,2,-2,2]$
$T{,}T{+}1{,}T^2{+}3T{+}4$	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}T{+}3)X{+}T^6{+}T^4{+}3T^3{+}3T{+}1$	$[-1,-3,-2,-3,-4,-8,2,7]$
	$Y^2{=}X^3{+}(3T^4{+}3T^2{+}T{+}2)X{+}T^6{+}4T^4{+}4T^3{+}2T^2{+}2T{+}2$	$[0,-2,-2,4,-8,2,-8,8]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}2T{+}2)X{+}T^6{+}4T^5{+}2T^4{+}2T^3{+}4T^2{+}2T{+}3$	$[3,3,0,-7,-4,2,2,-1]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}2T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}4T{+}4$	$[-3,-1,-4,7,-8,2,-2,-7]$
$T{,}T{+}1{,}(T{+}2)^2$	$Y^2{=}X^3{+}{,}3T^4{+}T^2{+}3)X{+}T^6{+}4T^5{+}3T^4{+}3T^2{+}4$	$[0,4,-4,6,6,4,-6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}4T{+}2)X{+}T^6{+}2T^5{+}2T^4{+}2T^3{+}T^2{+}T{+}2$	$[-3,-3,8,-7,-10,-4,2,2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}4T{+}2)X{+}T^6{+}T^5{+}T^4{+}3T^3{+}4T^2{+}4T{+}3$	$[2,2,-2,-2,-10,6,2,2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3T{+}2)X{+}T^6{+}4T^5{+}3T^4{+}T^3{+}4T^2{+}2T{+}2$	$[-4,0,4,-6,6,-4,-6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T{+}3)X{+}T^6{+}4T^3{+}T^2{+}T{+}1$	$[3,1,-4,3,-6,-8,6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}4T^4{+}2T^3{+}2T^2{+}4T{+}4$	$[-2,-4,-4,-2,4,-8,6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}2)X{+}T^6{+}3T^5{+}3T^3{+}T^2{+}2$	$[4,2,2,-2,4,-2,-6,6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}2)X{+}T^6{+}T^5{+}3T^4{+}2T^2{+}2$	$[-1,-3,-8,3,-6,8,-6,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}T{+}3)X{+}T^6{+}4T^5{+}3T^4{+}4T^3{+}2T^2{+}3T{+}1$	$[1,1,-4,1,6,-4,6,6]$
$T{,}T^3{+}T^2{+}3T{+}4$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}4T{+}1$	$[0,0,3,0,-1,-1,2,-7]$
$T{,}T{+}3{,}T^2{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3)X{+}T^6{+}3T^5{+}2T^4{+}4$	$[-3,-1,-4,3,-7,-6,-8,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2{+}3T{+}2)X{+}T^6{+}T^5{+}4T^4{+}2T^3{+}2T{+}2$	$[1,3,2,-7,7,-4,-4,2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}T{+}3)X{+}T^6{+}T^5{+}4T^4{+}T^2{+}2T{+}4$	$[0,2,2,6,8,6,-8,-8]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2{+}3T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}4T{+}1$	$[-3,-3,0,-1,-1,2,-4,2]$
$T{,}T^3{+}4T^2{+}3T{+}4$	$Y^2{=}X^3{+}(3T^4{+}T^2{+}3T{+}3)X{+}T^6{+}4T^5{+}3T^4{+}4T{+}1$	$[3,3,-3,0,8,-1,-4,-4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2{+}T{+}2)X{+}T^6{+}T^5{+}4T^4{+}T^2{+}T{+}3$	$[1,-3,-1,-2,-2,-1,-4,2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}2)X{+}T^6{+}4T^5{+}4T^4{+}3T^3{+}3T^2{+}2$	$[0,4,-2,3,-2,3,2,-4]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}2T^4{+}3T^3{+}2T^2{+}4T{+}1$	$[1,-1,-3,-4,-8,-3,2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}3T^2{+}2T{+}4$	$[-2,-4,0,-1,4,-3,8,4]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2{+}4T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}4T^3{+}3T{+}4$	$[-3,-1,-3,0,-4,9,-6,-6]$
$T{,}T{+}3{,}T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}2T^2{+}2T{+}2)X{+}T^6{+}T^5{+}3T^4{+}2T^3{+}2T{+}3$	$[0,3,3,2,-1,-4,-7,-1]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2)X{+}T^6{+}3T^5{+}4T^4{+}2T^3{+}2T^2{+}4T{+}3$	$[-2,-1,-3,-4,7,-4,-3,1]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}4T{+}2)X{+}T^6{+}3T^5{+}T^4{+}4T^3{+}4T^2{+}T{+}2$	$[-2,0,-2,6,8,-8,4,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3)X{+}T^6{+}T^5{+}3T^4{+}T^3{+}2T^2{+}1$	$[-4,-3,-1,-6,-7,-8,7,3]$
$T{,}(T{+}1)^2{,}T{+}4$	$Y^2{=}X^3{+}(3T^4{+}T^2{+}T{+}2)X{+}T^6{+}2T^5{+}3T^3{+}2T^2{+}T{+}3$	$[4,2,-6,6,-2,-4,-8,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^2{+}T{+}2)X{+}T^6{+}3T^4{+}3T^3{+}3T{+}2$	$[-1,-3,-6,6,3,-4,-8,3]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}3T^5{+}3T^4{+}2T^3{+}3T^2{+}3T{+}1$	$[1,1,6,6,-9,-4,-4,1]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T{+}3)X{+}T^6{+}T^4{+}4T^3{+}T^2{+}1$	$[2,2,2,2,-6,-2,6,-2]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T{+}3)X{+}T^6{+}T^5{+}2T^4{+}4T^3{+}2T^2{+}T{+}1$	$[-3,-3,2,2,-1,8,-4,-7]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}T{+}2)X{+}T^6{+}3T^5{+}3T^4{+}3T^3{+}T^2{+}T{+}2$	$[0,4,-6,-6,-6,4,-4,-6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2T{+}2)X{+}T^6{+}3T^5{+}3T^4{+}4T^3{+}4T^2{+}4T{+}3$	$[-4,0,-6,-6,-6,-4,4,6]$

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}2)X{+}T^6{+}2T^5{+}4T^4{+}T^3{+}4T{+}2$	[−2,−4,6,−6,−2,2,−2,−2]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}2)X{+}T^6{+}4T^5{+}4T^3{+}4T^2{+}3$	[3,1,6,−6,3,−8,8,3]
$T,T^3{+}2T^2{+}4T{+}4$	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}2T{+}3)X{+}T^6{+}4T^5{+}2T^2{+}4T{+}1$	[0,3,0,0,−1,−1,2,2]
$T,T{+}2,T^2{+}T{+}2$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}2T{+}2)X{+}T^6{+}3T^5{+}4T^2{+}2T{+}3$	[1,2,3,1,1,−2,−2,3]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}2T{+}2)X{+}T^6{+}4T^4{+}2T^3{+}2T^2{+}2T{+}3$	[−2,−2,−2,2,−6,−6,−2,−6]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2{+}3T{+}3)X{+}T^6{+}4T^5{+}3T^4{+}4T^3{+}2T^2{+}T{+}4$	[−2,−1,−3,−2,−2,1,−5,3]
$T^2,T{+}2,T{+}3$	$Y^2{=}X^3{+}(3T^4)X{+}T^6{+}2T^4$	[1,1,6,−9,1,−4,−4,6]
	$Y^2{=}X^3{+}(3T^4{+}T^2)X{+}T^6{+}2T^2$	[3,3,−10,−1,−7,8,−4,2]
	$Y^2{=}X^3{+}(3T^4{+}T^2)X{+}T^6{+}T^5{+}T^4{+}2T^3$	[−2,−2,−10,−6,−2,−2,6,2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2)X{+}T^6{+}4T^3$	[0,4,6,−6,6,−4,−4,−6]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2T)X{+}T^6{+}3T^5{+}T^4{+}2T^3{+}3T^2{+}2T$	[1,3,−6,3,3,−8,−8,−6]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2{+}2T)X{+}T^6{+}3T^5{+}3T^4{+}4T^3{+}3T^2$	[−4,−2,4,−2,−2,2,−8,−6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2)X{+}T^6{+}T^3$	[4,0,6,−6,−6,4,4,−6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}3T)X{+}T^6{+}2T^5{+}T^4{+}3T^3{+}3T^2{+}3T$	[3,1,−6,3,3,−4,8,6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}3T)X{+}T^6{+}2T^5{+}3T^4{+}T^3{+}3T^2$	[−2,−4,4,−2,−2,−4,−2,6]
$T^2,T^2{+}T{+}1$	$Y^2{=}X^3{+}(3T^4{+}3T^2)X{+}T^6{+}4T^5{+}4T^4{+}T^3$	[2,0,0,2,4,−4,−2,−8]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T)X{+}T^6{+}3T^5{+}4T^4{+}T^3{+}2T$	[−2,−2,−1,−1,4,−4,7,2]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2)X{+}T^6{+}4T^5{+}T^4{+}4T^3$	[−2,−2,2,−4,−8,8,−2,−4]
	$Y^2{=}X^3{+}(3T^4{+}3T^3)X{+}T^6{+}4T^5{+}4T^4$	[0,−2,−1,−3,4,−2,1,4]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T^2)X{+}T^6{+}4T^5{+}T^3$	[−2,0,−4,0,2,2,−6,2]
$T^2,(T{+}1)^2$	$Y^2{=}X^3{+},3T^4{+}2T^2)X{+}T^6{+}3T^5{+}3T^3$	[−3,−3,0,−4,4,−7,2,8]
	$Y^2{=}X^3{+}(3T^4{+}2T^2)X{+}T^6{+}4T^5{+}2T^3$	[2,2,0,6,−6,−2,2,−2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2)X{+}T^6{+}4T^4{+}2T^3{+}2T^2$	[4,1,−1,−4,−1,1,6,−4]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2)X{+}T^6{+}T^5{+}4T^4{+}4T^3$	[−1,1,4,−4,4,1,6,−4]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T)X{+}T^6{+}3T^5{+}2T^3{+}T^2{+}2T$	[0,−3,−3,8,1,−7,2,−4]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T)X{+}T^6{+}2T^5{+}3T^3{+}4T^2$	[0,2,2,−2,−4,−2,2,6]
	$Y^2{=}X^3{+}(3T^4{+}3T^3)X{+}T^6{+}T^5$	[3,−1,2,4,8,1,−4,−6]
	$Y^2{=}X^3{+}(3T^4{+}3T^3)X{+}T^6{+}2T^5{+}T^4$	[−2,−1,−3,−6,3,1,−4,4]
	$Y^2{=}X^3{+}(3T^4{+}3T^3)X{+}T^6{+}4T^5{+}3T^4$	[−2,4,2,−1,−7,1,−9,−1]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}3T)X{+}T^6{+}T$	[2,−1,3,−6,−3,1,−4,4]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}3T)X{+}T^6{+}4T^5{+}T^4{+}4T^3{+}T^2$	[−3,−1,−2,4,−8,1,−4,−6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}3T)X{+}T^6{+}2T^5{+}3T^4{+}2T^3{+}3T^2{+}3T$	[2,4,−2,−1,7,1,−9,−1]
$T^2,(T{+}4)^2$	$Y^2{=}X^3{+},3T^4{+}2T^2)X{+}T^6{+}2T^5{+}2T^3$	[0,−3,−3,−4,4,−2,−8,−2]
	$Y^2{=}X^3{+}(3T^4{+}2T^2)X{+}T^6{+}T^5{+}3T^3$	[0,2,2,6,−6,8,2,−2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T)X{+}T^6{+}4T$	[3,−1,2,−6,−3,2,−7,−2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T)X{+}T^6{+}T^5{+}T^4{+}T^3{+}T^2$	[−2,−1,−3,4,−8,2,−2,−2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2T)X{+}T^6{+}3T^5{+}3T^4{+}3T^3{+}3T^2{+}2T$	[−2,4,2,−1,7,−3,−2,3]
	$Y^2{=}X^3{+}(3T^4{+}2T^3)X{+}T^6{+}3T^5{+}T^4$	[−3,−1,−2,−6,3,−2,7,2]
	$Y^2{=}X^3{+}(3T^4{+}2T^3)X{+}T^6{+}T^5{+}3T^4$	[2,4,−2,−1,−7,3,2,−3]
	$Y^2{=}X^3{+}(3T^4{+}2T^3)X{+}T^6{+}4T^5$	[2,−1,3,4,8,−2,2,2]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}4T)X{+}T^6{+}2T^5{+}3T^3{+}T^2{+}3T$	[−3,−3,0,8,1,−2,1,−2]

Continued on next page

Conductor	**Curve**	**Trace**
	$Y^2=X^3+(3T^4+3T^3+4T)X+T^6+3T^5+2T^3+4T^2$	$[2,2,0,-2,-4,-2,-4,8]$
	$Y^2=X^3+(3T^4+4T^3+3T^2)X+T^6+4T^4+3T^3+2T^2$	$[-1,1,4,-4,-1,-6,-1,-6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2)X+T^6+4T^5+4T^4+T^3$	$[4,1,-1,-4,4,-6,4,-6]$
T^2,T^2+4T+1	$Y^2=X^3+(3T^4+3T^2)X+T^6+T^5+4T^4+4T^3$	$[2,0,0,2,4,-4,6,8]$
	$Y^2=X^3+(3T^4+2T^3)X+T^6+T^5+4T^4$	$[-3,-1,-2,0,4,-2,3,-8]$
	$Y^2=X^3+(3T^4+2T^3+4T^2)X+T^6+T^5+4T^3$	$[0,-4,0,-2,2,2,2,-6]$
	$Y^2=X^3+(3T^4+3T^3+3T^2)X+T^6+T^5+T^4+T^3$	$[-4,2,-2,-2,-8,8,-10,4]$
	$Y^2=X^3+(3T^4+4T^3+2T)X+T^6+2T^5+4T^4+4T^3+3T$	$[-1,-1,-2,-2,4,-4,-1,4]$
T^2,T^2+2	$Y^2=X^3+(3T^4)X+T^6+4T^4$	$[-4,1,1,-4,-9,-4,6,1]$
	$Y^2=X^3+(3T^4+2T^2)X+T^6+3T^2$	$[0,-3,-3,0,-1,8,2,-7]$
	$Y^2=X^3+(3T^4+2T^2)X+T^6+3T^4$	$[0,2,2,0,-6,-2,2,-2]$
	$Y^2=X^3+(3T^4+2T^3)X+T^6+T^5+2T^4$	$[2,-1,3,0,3,-2,-8,-3]$
	$Y^2=X^3+(3T^4+3T^3)X+T^6+4T^5+2T^4$	$[0,3,-1,2,3,-4,6,9]$
T^2,T^2+T+2	$Y^2=X^3+(3T^4+T^3+T)X+T^6+3T^5+4T^4+4T^2$	$[-3,1,-4,0,9,4,-3,-1]$
	$Y^2=X^3+(3T^4+T^3+2T^2)X+T^6+4T^4+2T^3$	$[3,1,-2,2,3,-8,-3,9]$
	$Y^2=X^3+(3T^4+T^3+3T^2)X+T^6+2T^5+2T^4+4T^3$	$[0,4,1,-1,6,4,-9,-9]$
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+T^5+2T^4+2T^3$	$[-4,0,-1,-1,-6,-4,-1,1]$
	$Y^2=X^3+(3T^4+3T^3)X+T^6$	$[0,-2,-1,-3,-6,-2,-9,-1]$
	$Y^2=X^3+(3T^4+3T^3)X+T^6+4T^5+4T^4+3T^3$	$[0,-2,4,2,-6,-2,6,-6]$
	$Y^2=X^3+(3T^4+3T^3+3T^2)X+T^6+4T^5+4T^3$	$[1,-3,-2,-2,-3,8,5,7]$
	$Y^2=X^3+(3T^4+4T^3)X+T^6+4T^5$	$[3,-3,0,4,3,4,-3,-3]$
T^2,$T+3$,$T+4$	$Y^2=X^3+(3T^4)X+T^6+2T^5+3T^4$	$[1,1,-4,1,-4,1,6,-4]$
	$Y^2=X^3+(3T^4+T^3+3T^2)X+T^6+2T^5+3T^4+T^3$	$[0,4,-4,-6,-4,6,6,4]$
	$Y^2=X^3+(3T^4+T^3+4T^2)X+T^6+2T^4+T^3+2T^2$	$[-3,-3,-4,-7,8,-7,-10,-4]$
	$Y^2=X^3+(3T^4+T^3+4T^2)X+T^6+2T^5+2T^4+4T^3$	$[2,2,6,-2,-2,-2,-10,6]$
	$Y^2=X^3+(3T^4+2T^3+2T)X+T^6+T^5+4T^4+T^2$	$[-2,-4,-2,-2,-4,-2,4,-8]$
	$Y^2=X^3+(3T^4+2T^3+2T)X+T^6+3T^5+4T^3+2T^2+3T$	$[3,1,8,3,-4,3,-6,-8]$
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+2T^5+3T^4+2T^3$	$[-4,0,4,6,4,-6,6,-4]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+2T)X+T^6+T^5+3T^3+3T^2$	$[4,2,-8,-2,2,-2,4,-2]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+2T)X+T^6+4T^5+3T^4+T^3+4T^2+4T$	$[-1,-3,-8,3,-8,3,-6,8]$
T^2,$T+1$,$T+2$	$Y^2=X^3+(3T^4)X+T^6+3T^5+3T^4$	$[1,1,-4,1,-9,-4,6,6]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+3T)X+T^6+4T^5+2T^3+3T^2$	$[2,4,-8,-2,-2,-4,-6,6]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+3T)X+T^6+T^5+3T^4+4T^3+4T^2+T$	$[-3,-1,-8,3,3,-4,-6,6]$
	$Y^2=X^3+(3T^4+3T^3+3T)X+T^6+2T^5+T^3+2T^2+2T$	$[1,3,8,3,3,-8,6,-6]$
	$Y^2=X^3+(3T^4+3T^3+3T)X+T^6+4T^5+4T^4+T^2$	$[-4,-2,-2,-2,-2,2,6,-6]$
	$Y^2=X^3+(3T^4+3T^3+2T^2)X+T^6+3T^5+3T^4+3T^3$	$[0,-4,4,6,-6,-4,-6,-6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2)X+T^6+3T^5+3T^4+4T^3$	$[4,0,-4,-6,-6,4,-6,-6]$
	$Y^2=X^3+(3T^4+4T^3+4T^2)X+T^6+2T^4+4T^3+2T^2$	$[-3,-3,-4,-7,-1,8,2,2]$
	$Y^2=X^3+(3T^4+4T^3+4T^2)X+T^6+T^5+T^4$	$[2,2,6,-2,-6,-2,2,2]$
T^2,T^2+4T+2	$Y^2=X^3+(3T^4+T^3)X+T^6+T^5$	$[4,0,-3,3,3,4,-2,2]$
	$Y^2=X^3+(3T^4+2T^3)X+T^6$	$[-3,-1,-2,0,-6,-2,-2,7]$

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(3T^4{+}2T^3)X{+}T^6{+}T^5{+}4T^4{+}2T^3$	[2,4,−2,0,−6,−2,−2,2]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2)X{+}T^6{+}T^5{+}T^3$	[−2,−2,−3,1,−3,8,4,−2]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2)X{+}T^6{+}4T^5{+}2T^4{+}3T^3$	[−1,−1,0,−4,−6,−4,4,1]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T)X{+}T^6{+}2T^5{+}4T^4{+}4T^2$	[0,−4,1,−3,9,4,−2,−2]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2)X{+}T^6{+}4T^4{+}3T^3$	[2,−2,1,3,3,−8,−8,2]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2)X{+}T^6{+}3T^5{+}2T^4{+}T^3$	[−1,1,4,0,6,4,4,−1]
T^2,$T^2{+}3$	$Y^2{=}X^3{+}(3T^4)X{+}T^6{+}T^4$	[1,−4,−4,1,−9,−4,1,6]
	$Y^2{=}X^3{+}(3T^4{+}3T^2)X{+}T^6{+}3T^2$	[−3,0,0,−3,−1,−4,−7,2]
	$Y^2{=}X^3{+}(3T^4{+}3T^2)X{+}T^6{+}2T^4$	[2,0,0,2,−6,6,−2,2]
	$Y^2{=}X^3{+}(3T^4{+}T^3)X{+}T^6{+}3T^5{+}3T^4$	[−1,0,2,3,3,−2,−3,6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3)X{+}T^6{+}2T^5{+}3T^4$	[3,2,0,−1,3,2,9,−8]
T^2,$T{+}2$,$T{+}4$	$Y^2{=}X^3{+}(3T^4)X{+}T^6{+}T^5{+}2T^4$	[1,1,1,−4,−4,6,−4,−9]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T)X{+}T^6{+}3T^5{+}T^4{+}T^2$	[−4,−2,−2,−2,−8,4,2,−2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T)X{+}T^6{+}4T^5{+}3T^3{+}2T^2{+}4T$	[1,3,3,8,−8,−6,−8,3]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2)X{+}T^6{+}T^5{+}2T^4{+}4T^3$	[0,−4,6,4,−4,6,−4,−6]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2)X{+}T^6{+}3T^4{+}2T^3{+}2T^2$	[−3,−3,−7,−4,−4,−10,8,−1]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}T^2)X{+}T^6{+}T^5{+}3T^4{+}3T^3$	[2,2,−2,6,6,−10,−2,−6]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2)X{+}T^6{+}T^5{+}2T^4{+}2T^3$	[4,0,−6,−4,4,6,4,−6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}4T)X{+}T^6{+}2T^5{+}2T^4{+}2T^3{+}4T^2{+}2T$	[−3,−1,3,−8,8,−6,−4,3]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}4T)X{+}T^6{+}3T^5{+}T^3{+}3T^2$	[2,4,−2,−8,−2,4,−4,−2]
T^2,$T^2{+}2T{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3)X{+}T^6$	[−1,0,−3,−2,−2,−6,−2,7]
	$Y^2{=}X^3{+}(3T^4{+}T^3)X{+}T^6{+}3T^5{+}T^4{+}4T^3$	[4,0,2,−2,−2,−6,−2,2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2)X{+}T^6{+}3T^5{+}2T^3$	[−2,1,−2,−3,8,−3,−8,−9]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T)X{+}T^6{+}T^5{+}T^4{+}4T^2$	[−4,−3,0,1,4,9,−8,−5]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2)X{+}T^6{+}4T^5{+}3T^4{+}2T^3$	[1,0,−1,4,4,6,4,−1]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2)X{+}T^6{+}T^4{+}T^3$	[−2,3,2,1,−8,3,4,−7]
	$Y^2{=}X^3{+}(3T^4{+}3T^3)X{+}T^6{+}3T^5$	[0,3,4,−3,4,3,−4,1]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2)X{+}T^6{+}2T^5{+}3T^4{+}T^3$	[−1,−4,−1,0,−4,−6,4,9]
T^2,$T^2{+}3T{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}3T^2)X{+}T^6{+}3T^5{+}3T^4{+}4T^3$	[0,−1,−4,−1,−4,−6,−9,1]
	$Y^2{=}X^3{+}(3T^4{+}2T^3)X{+}T^6{+}2T^5$	[−3,4,3,0,4,3,−7,−3]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T)X{+}T^6{+}4T^5{+}T^4{+}4T^2$	[1,0,−3,−4,4,9,1,−1]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}2T^2)X{+}T^6{+}T^5{+}3T^4{+}3T^3$	[4,−1,0,1,4,6,−1,−9]
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2)X{+}T^6{+}T^4{+}4T^3$	[1,2,3,−2,−8,3,5,9]
	$Y^2{=}X^3{+}(3T^4{+}4T^3)X{+}T^6$	[−2,−3,0,−1,−2,−6,7,−1]
	$Y^2{=}X^3{+}(3T^4{+}4T^3)X{+}T^6{+}2T^5{+}T^4{+}T^3$	[−2,2,0,4,−2,−6,2,−6]
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}2T^2)X{+}T^6{+}2T^5{+}3T^3$	[−3,−2,1,−2,8,−3,−3,7]
T^2,$T{+}1$,$T{+}3$	$Y^2{=}X^3{+}(3T^4)X{+}T^6{+}4T^5{+}2T^4$	[1,1,1,−4,6,6,1,−4]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}T)X{+}T^6{+}2T^5{+}4T^3{+}3T^2$	[4,2,−2,−8,6,−6,−2,2]
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}T)X{+}T^6{+}3T^5{+}2T^4{+}3T^3{+}4T^2{+}3T$	[−1,−3,3,−8,6,−6,3,−8]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2)X{+}T^6{+}3T^4{+}3T^3{+}2T^2$	[−3,−3,−7,−4,2,2,−7,8]
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}T^2)X{+}T^6{+}3T^5{+}4T^4$	[2,2,−2,6,2,2,−2,−2]

Continued on next page

Conductor	Curve	Trace
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+4T^5+2T^4+3T^3$	[0,4,−6,−4,−6,−6,6,−4]
	$Y^2=X^3+(3T^4+4T^3+T)X+T^6+T^5+2T^3+2T^2+T$	[3,1,3,8,−6,6,3,−4]
	$Y^2=X^3+(3T^4+4T^3+T)X+T^6+2T^5+T^4+T^2$	[−2,−4,−2,−2,−6,6,−2,−4]
	$Y^2=X^3+(3T^4+4T^3+3T^2)X+T^6+4T^5+2T^4+T^3$	[−4,0,6,4,−6,−6,−6,4]
T^2,$T+1$,$T+4$	$Y^2=X^3+(3T^4)X+T^6+3T^4$	[1,1,−9,6,6,−4,−4,1]
	$Y^2=X^3+(3T^4+4T^2)X+T^6+2T^2$	[3,3,−1,−10,2,−4,8,−7]
	$Y^2=X^3+(3T^4+4T^2)X+T^6+2T^5+4T^4+T^3$	[−2,−2,−6,−10,2,6,−2,−2]
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+2T^3$	[0,4,−6,6,−6,4,−4,6]
	$Y^2=X^3+(3T^4+2T^3+2T^2+T)X+T^6+T^5+2T^4+2T^3+3T^2$	[−4,−2,−2,4,6,−2,2,−2]
	$Y^2=X^3+(3T^4+2T^3+2T^2+T)X+T^6+T^5+4T^4+T^3+3T^2+4T$	[1,3,3,−6,6,8,−8,3]
	$Y^2=X^3+(3T^4+3T^3+2T^2)X+T^6+3T^3$	[4,0,−6,6,−6,−4,4,−6]
	$Y^2=X^3+(3T^4+3T^3+2T^2+4T)X+T^6+4T^5+2T^4+3T^3+3T^2$	[−2,−4,−2,4,−6,−8,−4,−2]
	$Y^2=X^3+(3T^4+3T^3+2T^2+4T)X+T^6+4T^5+4T^4+4T^3+3T^2+T$	[3,1,3,−6,−6,−8,−4,3]
T^2,$(T+3)^2$	$Y^2=X^3+,3T^4+3T^2)X+T^6+2T^5+4T^3$	[2,0,2,−6,6,−4,−2,2]
	$Y^2=X^3+(3T^4+3T^2)X+T^6+4T^5+T^3$	[−3,0,−3,4,−4,1,8,−8]
	$Y^2=X^3+(3T^4+T^3+2T)X+T^6+T^5+T^3+4T^2$	[0,2,2,−4,−2,−6,6,−4]
	$Y^2=X^3+(3T^4+T^3+2T)X+T^6+4T^5+4T^3+T^2+T$	[0,−3,−3,1,8,4,−4,1]
	$Y^2=X^3+(3T^4+2T^3+T^2+T)X+T^6+3T$	[2,3,−1,−3,−6,8,4,−7]
	$Y^2=X^3+(3T^4+2T^3+T^2+T)X+T^6+T^5+2T^4+4T^3+3T^2+4T$	[2,−2,4,7,−1,−7,−1,−2]
	$Y^2=X^3+(3T^4+2T^3+T^2+T)X+T^6+2T^5+4T^4+3T^3+T^2$	[−3,−2,−1,−8,4,3,−6,−2]
	$Y^2=X^3+(3T^4+3T^3+2T^2)X+T^6+T^4+4T^3+2T^2$	[4,−1,1,−1,−4,4,−4,−1]
	$Y^2=X^3+(3T^4+3T^3+2T^2)X+T^6+3T^5+T^4+3T^3$	[−1,4,1,4,−4,−1,−4,4]
	$Y^2=X^3+(3T^4+4T^3)X+T^6+T^5+4T^4$	[−2,−3,−1,3,−6,−8,4,7]
	$Y^2=X^3+(3T^4+4T^3)X+T^6+2T^5+2T^4$	[−2,2,4,−7,−1,7,−1,2]
	$Y^2=X^3+(3T^4+4T^3)X+T^6+3T^5$	[3,2,−1,8,4,−3,−6,2]
T^2,T^2+2T+4	$Y^2=X^3+(3T^4+2T^2)X+T^6+3T^5+T^4+3T^3$	[0,2,2,0,−4,4,−2,2]
	$Y^2=X^3+(3T^4+T^3)X+T^6+3T^5+T^4$	[−1,0,−3,−2,−2,4,−2,7]
	$Y^2=X^3+(3T^4+T^3+T^2)X+T^6+3T^5+3T^3$	[−4,−2,0,0,2,2,6,−2]
	$Y^2=X^3+(3T^4+2T^3+4T)X+T^6+T^5+T^4+3T^3+4T$	[−1,−2,−1,−2,−4,4,−4,−7]
	$Y^2=X^3+(3T^4+4T^3+2T^2)X+T^6+3T^5+4T^4+2T^3$	[2,−2,−4,−2,8,−8,2,2]
T^2,T^2+3T+4	$Y^2=X^3+(3T^4+2T^2)X+T^6+2T^5+T^4+2T^3$	[0,2,2,0,−4,4,−2,−8]
	$Y^2=X^3+(3T^4+T^3+2T^2)X+T^6+2T^5+4T^4+3T^3$	[−2,−4,−2,2,8,−8,2,−4]
	$Y^2=X^3+(3T^4+3T^3+T)X+T^6+4T^5+T^4+2T^3+T$	[−2,−1,−2,−1,−4,4,2,2]
	$Y^2=X^3+(3T^4+4T^3)X+T^6+2T^5+T^4$	[−2,−3,0,−1,−2,4,−8,4]
	$Y^2=X^3+(3T^4+4T^3+T^2)X+T^6+2T^5+2T^3$	[0,0,−2,−4,2,2,−2,2]
T^2,$(T+2)^2$	$Y^2=X^3+,3T^4+3T^2)X+T^6+3T^5+T^3$	[2,0,2,−6,6,−4,−2,2]
	$Y^2=X^3+(3T^4+3T^2)X+T^6+T^5+4T^3$	[−3,0,−3,4,−4,1,−2,2]
	$Y^2=X^3+(3T^4+T^3)X+T^6+2T^5$	[−1,2,3,8,4,−7,2,−4]
	$Y^2=X^3+(3T^4+T^3)X+T^6+3T^5+2T^4$	[4,2,−2,−7,−1,−2,−3,−9]
	$Y^2=X^3+(3T^4+T^3)X+T^6+4T^5+4T^4$	[−1,−3,−2,3,−6,−2,2,−4]
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+T^4+T^3+2T^2$	[1,−1,4,−1,−4,4,−6,6]

Continued on next page

Conductor	Curve	Trace
	$Y^2=X^3+(3T^4+2T^3+2T^2)X+T^6+2T^5+T^4+2T^3$	$[1,4,-1,4,-4,-1,-6,6]$
	$Y^2=X^3+(3T^4+3T^3+T^2+4T)X+T^6+2T$	$[-1,3,2,-3,-6,2,-2,-4]$
	$Y^2=X^3+(3T^4+3T^3+T^2+4T)X+T^6+3T^5+4T^4+2T^3+T^2$	$[-1,-2,-3,-8,4,7,-2,-4]$
	$Y^2=X^3+(3T^4+3T^3+T^2+4T)X+T^6+4T^5+2T^4+T^3+3T^2+T$	$[4,-2,2,7,-1,2,3,-9]$
	$Y^2=X^3+(3T^4+4T^3+3T)X+T^6+T^5+T^3+T^2+4T$	$[-3,-3,0,1,8,-8,-2,2]$
	$Y^2=X^3+(3T^4+4T^3+3T)X+T^6+4T^5+4T^3+4T^2$	$[2,2,0,-4,-2,2,8,2]$
$T,T+1,T^2+4T+1$	$Y^2=X^3+(3T^4+3T^3+2T^2+T+2)X+T^6+4T^5+2T^4+T+3$	$[-1,-2,-3,-5,4,3,-5,-2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+3T+3)X+T^6+T^5+T^4+T^2+T+1$	$[-2,-2,-2,6,6,-6,-2,-6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+2T+2)X+T^6+2T^5+4T^2+3T+2$	$[2,1,3,4,-5,3,-2,1]$
T,T^3+T^2+1	$Y^2=X^3+(3T^4+T+3)X+T^6+3T^3+T^2+2T+4$	$[0,-2,-4,-1,8,2,2,4]$
$T,(T+2)^2,T+4$	$Y^2=X^3+(3T^4+T^2+3)X+T^6+2T^5+4T^3+4T^2+1$	$[4,0,6,-4,-4,-6,4,-6]$
	$Y^2=X^3+(3T^4+T^2+2T+2)X+T^6+T^4+4T^2+2T+3$	$[3,1,3,-8,-8,-6,8,6]$
	$Y^2=X^3+(3T^4+T^2+2T+2)X+T^6+3T^4+3T^3+4T^2+3T+2$	$[-2,-4,-2,2,-8,-6,-2,6]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+T+2)X+T^6+2T^5+T^3+T^2+4T+2$	$[0,4,-6,4,4,-6,-4,-6]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+4T+3)X+T^6+4T^5+T^4+T^3+1$	$[1,3,3,-4,8,6,-8,-6]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+4T+3)X+T^6+4T^5+3T^4+T^2+2T+1$	$[-4,-2,-2,-4,-2,6,-8,-6]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+T+3)X+T^6+2T^5+2T^4+T^3+3T^2+T+1$	$[1,1,1,-4,-4,6,-4,6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+2)X+T^6+T^5+T^4+T^3+2T^2+2$	$[-2,-2,-2,-2,6,2,6,2]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+2)X+T^6+2T^5+2T^2+2$	$[3,3,-7,8,-4,2,-4,2]$
$T,T+3,T^2+T+2$	$Y^2=X^3+(3T^4+T+2)X+T^6+2T^5+4T^4+T^3+3T^2+4T+2$	$[3,1,2,7,-4,-7,-3,1]$
	$Y^2=X^3+(3T^4+4T^2+3T+3)X+T^6+2T^4+4T^3+3T^2+4T+1$	$[-1,-3,-4,-7,-6,3,7,3]$
	$Y^2=X^3+(3T^4+2T^3+3T^2+2)X+T^6+4T^5+2T^4+4T^3+3T^2+3$	$[-3,-3,0,-1,2,-1,-7,-1]$
	$Y^2=X^3+(3T^4+4T^3+T^2+T+2)X+T^6+2T^5+4T^4+3T^3+2T^2+4T+2$	$[2,0,2,8,6,6,4,-6]$
T,T^3+T+1	$Y^2=X^3+(3T^4+T^3+3)X+T^6+3T^5+4T^4+2T^3+4$	$[0,-4,-2,-1,2,8,2,-1]$
$T,T+1,T+2,T+3$	$Y^2=X^3+(3T^4+T^2+4T+3)X+T^6+2T^5+T^4+3T^3+4T^2+3T+1$	$[2,-6,-2,2,2,-6,-2,-2]$
	$Y^2=X^3+(3T^4+T^3+3T^2+T+3)X+T^6+4T^4+3T^3+4T^2+1$	$[2,2,2,-6,-2,-2,2,-2]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+2T+2)X+T^6+4T^4+3T+2$	$[2,2,-2,-2,-6,-2,-6,2]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+3T+2)X+T^6+4T^5+2T^4+2T^3+T^2+3T+3$	$[-2,-2,2,-2,2,2,-2,-6]$
	$Y^2=X^3+(3T^4+4T^3+T^2+3)X+T^6+T^5+T^4+3T^3+2T^2+4$	$[2,-2,-6,2,-2,2,2,2]$
$T,T+4,T^2+3T+4$	$Y^2=X^3+(3T^4+T^3+2T^2+2)X+T^6+4T^5+T^4+3T^3+2T^2+3$	$[2,0,2,-8,4,-6,8,-8]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+2T+2)X+T^6+T^5+2T^2+2T+3$	$[0,-3,-3,-4,-7,-1,-1,2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+2T+3)X+T^6+4T^5+3T^2+4T+4$	$[-4,-3,-1,-8,7,-3,-7,-2]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+3)X+T^6+2T^5+2T^3+T^2+1$	$[-2,-1,-3,-4,-3,9,7,2]$
T,T^3+3T^2+T+1	$Y^2=X^3+(3T^4+3T^2+2T+2)X+T^6+4T^4+T^3+2T^2+3T+3$	$[-3,-4,2,0,3,-2,-2,9]$
	$Y^2=X^3+(3T^4+T^3+2T^2+2T+3)X+T^6+3T^5+4T^3+3T^2+4T+4$	$[0,-1,-3,-3,9,-4,-2,-1]$
	$Y^2=X^3+(3T^4+T^3+4T^2+2T+2)X+T^6+3T^5+2T^4+3T^2+3T+2$	$[2,3,1,-1,-1,-2,2,1]$
	$Y^2=X^3+(3T^4+2T^3+T^2+3)X+T^6+T^5+3T^2+T+1$	$[0,3,-3,3,-1,8,8,-7]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+3T+3)X+T^6+T^5+2T^4+2T^3+2T^2+3T+1$	$[-4,-1,-3,1,-3,-8,2,3]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+2T+3)X+T^6+2T^5+2T^4+3T^2+4T+4$	$[-1,-4,0,-2,-3,4,-4,-9]$
$T,T+4,T^2+2T+4$	$Y^2=X^3+(3T^4+2T^2+4T+3)X+T^6+T^4+2T^3+2T+1$	$[-2,-3,-1,-3,-4,9,-7,1]$
	$Y^2=X^3+(3T^4+3T^2+4T+2)X+T^6+4T^4+T^3+2T^2+3T+2$	$[-2,-2,0,4,-8,-6,6,-6]$

Continued on next page

Conductor	**Curve**	**Trace**
	$Y^2=X^3+(3T^4+2T^3+2T^2+3T+3)X+T^6+T^5+2T^4+T+4$	$[-4,-1,-3,7,-8,-3,3,3]$
	$Y^2=X^3+(3T^4+3T^3+T^2+3T+2)X+T^6+T^5+2T^4+3T^3+4T^2+3T+3$	$[0,3,3,-7,-4,-1,-1,-1]$
$T,T+1,T^2+T+1$	$Y^2=X^3+(3T^4+4T^2+T+2)X+T^6+4T^5+4T^4+T^2+T+3$	$[-2,-4,0,-8,-2,-2,4,-8]$
	$Y^2=X^3+(3T^4+T^3+T^2+3T+3)X+T^6+3T^5+T^4+2T^3+2T+4$	$[2,-2,2,-6,6,-6,-6,6]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+4T+3)X+T^6+2T^5+4T^4+T^3+3T+4$	$[0,-4,-2,4,-8,-2,-8,-2]$
	$Y^2=X^3+(3T^4+3T^3+T^2+T+3)X+T^6+4T^4+4T^3+2T^2+3T+1$	$[-2,2,2,6,-6,2,-2,-2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+2T+2)X+T^6+4T^5+T^4+4T^3+3T+2$	$[0,2,4,-2,4,-2,-2,-8]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+2T+2)X+T^6+4T^5+T^3+4T^2+3T+2$	$[-2,0,-4,4,-2,6,-8,4]$
	$Y^2=X^3+(3T^4+4T^3+4T+3)X+T^6+T^5+4T^4+2T^3+4T^2+T+1$	$[2,2,-2,-2,-2,2,6,-6]$
	$Y^2=X^3+(3T^4+4T^3+T^2+2)X+T^6+2T^5+T^4+4T^2+3$	$[4,2,0,-2,-8,-2,-2,4]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+2T+3)X+T^6+2T^5+4T^3+T^2+3T+4$	$[-4,0,-2,-8,4,6,4,-2]$
$T,T+3,T^2+2$	$Y^2=X^3+(3T^4+T^2+4T+3)X+T^6+3T^2+3T+4$	$[-4,-1,-3,3,7,-8,-6,-2]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+T+3)X+T^6+T^5+2T^2+T+1$	$[0,-3,-3,-1,-7,-4,2,2]$
	$Y^2=X^3+(3T^4+3T^3+3T^2+T+2)X+T^6+4T^5+4T^3+2T^2+2T+3$	$[-2,-3,-1,-7,-3,-4,-4,2]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+3T+3)X+T^6+4T^4+4T^3+2T^2+4T+1$	$[2,2,0,6,4,-8,6,-8]$
$T,T+2,T^2+2T+3$	$Y^2=X^3+(3T^4+2T^3+T^2+3T+2)X+T^6+T^5+T^4+4T^3+4T^2+T+3$	$[2,2,2,-6,2,6,-2,-6]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+T+2)X+T^6+T^5+3T^4+4T+2$	$[-3,-2,-1,1,1,-5,-2,3]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+2T+3)X+T^6+T^5+3T^4+4T^3+2T^2+4T+4$	$[-3,-1,-2,-2,-2,4,-5,3]$
$T,(T+3)^2,T+4$	$Y^2=X^3+(3T^4+T^2+3)X+T^6+T^5+3T^4+3T^2+4$	$[4,0,-4,6,-4,-6,-6,4]$
	$Y^2=X^3+(3T^4+2T^2+T+2)X+T^6+3T^5+2T^4+3T^3+T^2+4T+2$	$[-3,-3,8,-7,-4,-7,-1,8]$
	$Y^2=X^3+(3T^4+2T^2+T+2)X+T^6+T^5+2T^4+2T^2+T+2$	$[2,2,-2,-2,6,-2,-6,-2]$
	$Y^2=X^3+(3T^4+T^3+2T^2+4T+3)X+T^6+T^5+3T^4+T^3+2T^2+2T+1$	$[1,1,-4,1,-4,1,-9,-4]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+2)X+T^6+2T^5+2T^3+T^2+2$	$[2,4,2,-2,-8,-2,-2,-4]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+2)X+T^6+4T^5+3T^4+2T^2+2$	$[-3,-1,-8,3,-8,3,3,-4]$
	$Y^2=X^3+(3T^4+4T^3+T^2+2T+2)X+T^6+T^5+3T^4+4T^3+4T^2+3T+2$	$[0,-4,4,-6,4,6,-6,-4]$
	$Y^2=X^3+(3T^4+4T^3+4T^2+3T+3)X+T^6+T^3+T^2+4T+1$	$[1,3,-4,3,8,3,3,-8]$
	$Y^2=X^3+(3T^4+4T^3+4T^2+3T+3)X+T^6+2T^5+4T^4+3T^3+2T^2+T+4$	$[-4,-2,-4,-2,-2,-2,-2,2]$
T,T^3+T^2+3T+1	$Y^2=X^3+(3T^4+T^2+2T+3)X+T^6+T^5+3T^4+T+1$	$[0,-3,3,3,8,-1,8,-4]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+T+3)X+T^6+T^5+2T^4+T^3+2T+4$	$[0,-3,-1,-3,-4,9,-2,6]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+4T+3)X+T^6+T^5+2T^4+3T^2+3T+4$	$[-1,0,-4,-2,4,-3,-4,-2]$
	$Y^2=X^3+(3T^4+3T^3+T^2+4T+2)X+T^6+4T^5+4T^4+T^2+4T+3$	$[-2,-1,-3,1,-2,-1,2,-8]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+2)X+T^6+T^5+4T^4+2T^3+3T^2+2$	$[3,-2,4,0,-2,3,-2,-2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+2T+3)X+T^6+3T^5+2T^4+2T^3+2T^2+T+1$	$[-4,-3,-1,1,-8,-3,2,-2]$
$T,T+2,T^2+3$	$Y^2=X^3+(3T^4+T^3+2T^2+2T+3)X+T^6+T^5+2T^4+T+1$	$[0,-3,-3,-1,-7,-1,-1,2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+4T+3)X+T^6+4T^5+4T^4+T^2+3T+4$	$[2,2,0,6,4,-6,-6,2]$
	$Y^2=X^3+(3T^4+4T^3+T^2+3)X+T^6+2T^5+2T^4+4$	$[-4,-1,-3,3,7,3,-3,2]$
	$Y^2=X^3+(3T^4+4T^3+2T^2+2T+2)X+T^6+4T^5+4T^4+3T^3+3T+2$	$[2,3,1,-7,-3,1,9,-8]$
T,T^3+4T^2+3T+1	$Y^2=X^3+(3T^4+3T^3+4T^2+2T+3)X+T^6+T^5+2T^4+T+1$	$[0,3,0,0,-1,-1,2,2]$
$T,T+2,T^2+3T+3$	$Y^2=X^3+(3T^4+2T^2+3T+2)X+T^6+4T^5+3T^4+3T^3+3T+3$	$[3,3,0,2,-1,-1,-1,2]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+3)X+T^6+4T^5+3T^4+4T^3+2T^2+1$	$[-1,-3,-4,-6,-7,3,-3,-2]$
	$Y^2=X^3+(3T^4+4T^3+2)X+T^6+2T^5+4T^4+3T^3+2T^2+T+3$	$[-3,-1,-2,-4,7,-7,9,2]$

Continued on next page

Conductor	Curve	Trace
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}4T^2{+}T{+}2)X{+}T^6{+}2T^5{+}T^4{+}T^3{+}4T^2{+}4T{+}2$	$[-2,0,-2,6,8,6,-6,-8]$
$T,T{+}3,T^2{+}4T{+}2$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}2T{+}3)X{+}T^6{+}T^5{+}3T^4{+}T^3{+}2T^2{+}4T{+}4$	$[-3,-1,-2,-2,-2,4,-5,1]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3T{+}2)X{+}T^6{+}4T^4{+}3T^3{+}2T^2{+}3T{+}3$	$[-2,-2,-2,2,-6,6,6,2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}3T{+}2)X{+}T^6{+}2T^5{+}4T^2{+}3T{+}3$	$[3,2,1,1,1,-5,4,-2]$
$T,T^3{+}3T^2{+}4T{+}1$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}3T{+}3)X{+}T^6{+}T^5{+}2T^2{+}T{+}1$	$[0,0,3,0,-1,-1,2,8]$
$T,T{+}1,(T{+}4)^2$	$Y^2{=}X^3{+},3T^4{+}T^2{+}4T{+}2)X{+}T^6{+}3T^5{+}2T^3{+}2T^2{+}4T{+}3$	$[2,4,-6,6,4,-2,2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^2{+}4T{+}2)X{+}T^6{+}3T^4{+}2T^3{+}2T{+}2$	$[-3,-1,-6,6,-6,8,-8,3]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}T^2{+}3T{+}2)X{+}T^6{+}2T^5{+}3T^4{+}T^3{+}4T^2{+}T{+}3$	$[0,-4,-6,-6,6,-4,4,-6]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2)X{+}T^6{+}T^5{+}T^3{+}4T^2{+}3$	$[1,3,6,-6,-6,-8,-4,3]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}4T^2{+}2)X{+}T^6{+}3T^5{+}4T^4{+}4T^3{+}T{+}2$	$[-4,-2,6,-6,4,-8,-4,-2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T{+}3)X{+}T^6{+}T^4{+}T^3{+}T^2{+}1$	$[2,2,2,2,-10,6,-2,-2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T{+}3)X{+}T^6{+}4T^5{+}2T^4{+}T^3{+}2T^2{+}4T{+}1$	$[-3,-3,2,2,-10,-4,8,-7]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}4T{+}2)X{+}T^6{+}2T^5{+}3T^4{+}2T^3{+}T^2{+}4T{+}2$	$[4,0,-6,-6,6,4,-4,6]$
	$Y^2{=}X^3{+}(3T^4{+}3T^3{+}3T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}3T^4{+}3T^3{+}3T^2{+}2T{+}1$	$[1,1,6,6,6,-4,-4,1]$
$T,T{+}3,T^2{+}2T{+}4$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}4T{+}2)X{+}T^6{+}T^5{+}4T^2{+}4T{+}3$	$[2,3,1,-5,4,1,1,-2]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}T{+}3)X{+}T^6{+}T^5{+}3T^4{+}3T^3{+}2T^2{+}T{+}4$	$[-2,-2,-2,6,6,2,-6,-6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}3T^2{+}2T{+}2)X{+}T^6{+}2T^5{+}3T^4{+}3T{+}2$	$[-1,-3,-2,4,-5,-2,-2,1]$
$T,T{+}4,T^2{+}3T{+}3$	$Y^2{=}X^3{+}(3T^4{+}2T{+}2)X{+}T^6{+}T^5{+}T^4{+}2T^3{+}3T^2{+}2T{+}3$	$[1,2,3,-4,7,1,-3,2]$
	$Y^2{=}X^3{+}(3T^4{+}T^2{+}T{+}3)X{+}T^6{+}3T^4{+}3T^3{+}3T^2{+}2T{+}4$	$[-3,-4,-1,-6,-7,3,7,-2]$
	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2{+}2)X{+}T^6{+}2T^5{+}3T^4{+}3T^3{+}3T^2{+}2$	$[-3,0,-3,2,-1,-1,-7,2]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}4T^2{+}2T{+}2)X{+}T^6{+}T^5{+}T^4{+}T^3{+}2T^2{+}2T{+}3$	$[0,2,2,6,8,-6,4,-8]$
$T,T^3{+}3T^2{+}2$	$Y^2{=}X^3{+}(3T^4{+}2T{+}3)X{+}T^6{+}T^3{+}T^2{+}T{+}1$	$[-2,-1,0,-4,2,8,-9,1]$
$T,(T{+}1)^2,T{+}2$	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}3)X{+}T^6{+}T^5{+}3T^3{+}4T^2{+}4$	$[4,0,-4,6,-6,4,-6,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}4T{+}2)X{+}T^6{+}2T^4{+}T^3{+}4T^2{+}4T{+}3$	$[-2,-4,2,-2,6,-2,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^2{+}4T{+}2)X{+}T^6{+}4T^4{+}4T^2{+}T{+}2$	$[3,1,-8,3,6,8,3,-6]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}2)X{+}T^6{+}T^5{+}2T^2{+}3$	$[3,3,8,-7,2,-4,-1,-10]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}2T^2{+}2)X{+}T^6{+}3T^5{+}4T^4{+}2T^3{+}2T^2{+}3$	$[-2,-2,-2,-2,2,6,-6,-10]$
	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}2T{+}3)X{+}T^6{+}T^5{+}3T^4{+}2T^3{+}3T^2{+}3T{+}4$	$[1,1,-4,1,6,-4,-9,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}2T{+}2)X{+}T^6{+}T^5{+}2T^3{+}T^2{+}2T{+}3$	$[0,4,4,-6,-6,-4,-6,6]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}2T^4{+}T^2{+}T{+}4$	$[-4,-2,-4,-2,-6,-8,-2,4]$
	$Y^2{=}X^3{+}(3T^4{+}4T^3{+}T^2{+}3T{+}3)X{+}T^6{+}2T^5{+}4T^4{+}2T^3{+}4$	$[1,3,-4,3,-6,-8,3,-6]$

C.6 Table for primes of degree 4 over $\mathbb{F}_5$

Table C.5: Isogeny classes for primes of degree 4 over $\mathbb{F}_5$

Conductor	Curve	Trace
$T^4{+}2T^3{+}4T^2{+}3T{+}3$	$Y^2{=}X^3{+}(3T^4{+}T^3{+}2T^2{+}4T)X{+}T^6{+}3T^5{+}3T^2{+}T{+}1$	$[0,0,0,4,0,-2,6,-6]$
$T^4{+}4T^3{+}T^2{+}4T{+}3$	$Y^2{=}X^3{+}(3T^4{+}2T^3{+}3T^2{+}2T)X{+}T^6{+}T^5{+}3T^2{+}2T{+}4$	$[0,4,0,0,0,6,-2,-2]$

Continued on next page

Conductor	**Curve**	**Trace**
T^4+2	$Y^2=X^3+(3T^4+2)X+T^6+3T^2$	$[4,0,0,0,0,-6,-6,-2]$
T^4+T^2+2	$Y^2=X^3+(3T^4+3T^2)X+T^6+4T^4+4T^2+3$	$[0,2,0,0,2,-6,6,6]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+2T)X+T^6+T^5+3T^4+T^3+3T^2+2$	$[0,1,-2,-2,-3,6,-3,3]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+3T)X+T^6+4T^5+3T^4+4T^3+3T^2+2$	$[0,-3,-2,-2,1,6,-3,3]$
$T^4+2T^3+T^2+2$	$Y^2=X^3+(3T^4+T^3+3T^2+2)X+T^6+3T^5+3T^4+T^3+3T^2+3T$	$[4,4,-2,0,-2,-2,-2,-10]$
$T^4+3T^3+T^2+2$	$Y^2=X^3+(3T^4+4T^3+3T^2+2)X+T^6+2T^5+3T^4+4T^3+3T^2+2T$	$[4,-2,0,-2,4,-2,-2,6]$
T^4+4T^2+2	$Y^2=X^3+(3T^4+2T^2)X+T^6+T^4+4T^2+2$	$[0,0,2,2,0,6,-6,-2]$
	$Y^2=X^3+(3T^4+T^3+T^2+4T)X+T^6+3T^5+2T^4+2T^3+3T^2+3$	$[0,-2,-3,1,-2,-3,6,4]$
	$Y^2=X^3+(3T^4+4T^3+T^2+T)X+T^6+2T^5+2T^4+3T^3+3T^2+3$	$[0,-2,1,-3,-2,-3,6,-4]$
$T^4+T^3+4T^2+2$	$Y^2=X^3+(3T^4+3T^3+2T^2+2)X+T^6+4T^5+2T^4+2T^3+3T^2+4T$	$[4,-2,-2,4,0,-2,-2,-2]$
$T^4+4T^3+4T^2+2$	$Y^2=X^3+(3T^4+2T^3+2T^2+2)X+T^6+T^5+2T^4+3T^3+3T^2+T$	$[4,0,4,-2,-2,-2,-2,2]$
T^4+3T^3+T+2	$Y^2=X^3+(3T^4+T^3+3T^2+3T+4)X+T^6+3T^5+3T^4+T^2+2T+1$	$[-2,-3,0,1,-2,3,-4,-7]$
	$Y^2=X^3+(3T^4+2T^3+4T^2+T+4)X+T^6+T^5+3T^4+3T^3+4T^2+3T+1$	$[-2,1,0,-3,-2,3,4,1]$
	$Y^2=X^3+(3T^4+4T^3+3T)X+T^6+2T^5+4T^4+2T^3+T+2$	$[0,2,0,2,0,6,-2,2]$
T^4+4T^3+2T+2	$Y^2=X^3+(3T^4+T^3+T^2+2T+4)X+T^6+3T^5+2T^4+T^3+4T^2+4T+4$	$[-2,0,-2,1,-3,4,3,4]$
	$Y^2=X^3+(3T^4+2T^3+T)X+T^6+T^5+T^4+4T^3+3T+3$	$[0,0,0,2,2,-2,6,-2]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+T+4)X+T^6+4T^5+2T^4+T^2+T+4$	$[-2,0,-2,-3,1,-4,3,-4]$
T^4+T^3+3T+2	$Y^2=X^3+(3T^4+2T^3+2T^2+4T+4)X+T^6+T^5+2T^4+T^2+4T+4$	$[-2,1,-3,-2,0,-4,3,4]$
	$Y^2=X^3+(3T^4+3T^3+4T)X+T^6+4T^5+T^4+T^3+2T+3$	$[0,2,2,0,0,-2,6,-2]$
	$Y^2=X^3+(3T^4+4T^3+T^2+3T+4)X+T^6+2T^5+2T^4+4T^3+4T^2+T+4$	$[-2,-3,1,-2,0,4,3,-4]$
T^4+2T^3+4T+2	$Y^2=X^3+(3T^4+T^3+2T)X+T^6+3T^5+4T^4+3T^3+4T+2$	$[0,0,2,0,2,6,-2,-6]$
	$Y^2=X^3+(3T^4+3T^3+4T^2+4T+4)X+T^6+4T^5+3T^4+2T^3+4T^2+2T+1$	$[-2,-2,-3,0,1,3,4,6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+2T+4)X+T^6+2T^5+3T^4+T^2+3T+1$	$[-2,-2,1,0,-3,3,-4,6]$
$T^4+T^3+T^2+T+4$	$Y^2=X^3+(3T^4+3T^3+3T^2+3T+1)X+T^6+4T^5+2T^2+3$	$[2,2,2,2,-4,-2,6,-2]$
$T^4+4T^3+2T^2+T+4$	$Y^2=X^3+(3T^4+T^2+2T+3)X+T^6+3T^4+T^3+3T^2+T+2$	$[1,0,-3,-2,-2,-7,4,3]$
	$Y^2=X^3+(3T^4+2T^3+T^2+3T+1)X+T^6+T^5+4T^4+T^3+3T^2+2$	$[2,0,2,0,0,2,-2,6]$
	$Y^2=X^3+(3T^4+4T^3+3T^2+3T+1)X+T^6+2T^5+3T^4+3T^3+4T^2+2T+1$	$[-3,0,1,-2,-2,1,-4,3]$
$T^4+2T^3+2T^2+T+1$	$Y^2=X^3+(3T^4+T^3+T^2+3T+4)X+T^6+3T^5+2T^4+4T^3+4T^2+1$	$[-2,-2,4,0,4,2,6,-6]$
$T^4+2T^3+3T^2+2T+4$	$Y^2=X^3+(3T^4+4T^2+4T+3)X+T^6+2T^4+2T^3+3T^2+3T+3$	$[1,-3,-2,0,-2,4,-7,-3]$
	$Y^2=X^3+(3T^4+T^3+4T^2+T+1)X+T^6+3T^5+T^4+2T^3+3T^2+3$	$[2,2,0,0,0,-2,2,6]$
	$Y^2=X^3+(3T^4+2T^3+2T^2+T+1)X+T^6+T^5+2T^4+T^3+4T^2+T+4$	$[-3,1,-2,0,-2,-4,1,-3]$
$T^4+3T^3+4T^2+2T+4$	$Y^2=X^3+(3T^4+4T^3+2T^2+T+1)X+T^6+2T^5+2T^2+2$	$[2,2,-4,2,2,6,-2,-2]$
$T^4+T^3+3T^2+2T+1$	$Y^2=X^3+(3T^4+3T^3+4T^2+T+4)X+T^6+4T^5+3T^4+3T^3+4T^2+4$	$[-2,4,4,-2,0,6,2,6]$
$T^4+3T^3+3T^2+3T+4$	$Y^2=X^3+(3T^4+4T^2+T+3)X+T^6+2T^4+3T^3+3T^2+2T+3$	$[1,-2,0,-2,-3,4,-7,4]$
	$Y^2=X^3+(3T^4+3T^3+2T^2+4T+1)X+T^6+4T^5+2T^4+4T^3+4T^2+4T+4$	$[-3,-2,0,-2,1,-4,1,-4]$
	$Y^2=X^3+(3T^4+4T^3+4T^2+4T+1)X+T^6+2T^5+T^4+3T^3+3T^2+3$	$[2,0,0,0,2,-2,2,-2]$
$T^4+2T^3+4T^2+3T+4$	$Y^2=X^3+(3T^4+T^3+2T^2+4T+1)X+T^6+3T^5+2T^2+2$	$[2,2,2,-4,2,6,-2,-10]$
$T^4+4T^3+T^2+4T+4$	$Y^2=X^3+(3T^4+2T^3+3T^2+2T+1)X+T^6+T^5+2T^2+3$	$[2,-4,2,2,2,-2,6,6]$
$T^4+T^3+2T^2+4T+4$	$Y^2=X^3+(3T^4+T^2+3T+3)X+T^6+3T^4+4T^3+3T^2+4T+2$	$[1,-2,-2,-3,0,-7,4,1]$
	$Y^2=X^3+(3T^4+T^3+3T^2+2T+1)X+T^6+3T^5+3T^4+2T^3+4T^2+3T+1$	$[-3,-2,-2,1,0,1,-4,-7]$

Continued on next page

Conductor	Curve	Trace
	$Y^2=X^3+(3T^4+3T^3+T^2+2T+1)X+T^6+4T^5+4T^4+4T^3+3T^2+2$	[2,0,0,2,0,2,−2,2]
$T^4+4T^3+3T^2+3T+1$	$Y^2=X^3+(3T^4+2T^3+4T^2+4T+4)X+T^6+T^5+3T^4+2T^3+4T^2+4$	[−2,0,−2,4,4,6,2,−2]
T^4+3	$Y^2=X^3+(3T^4+3)X+T^6+2T^2$	[−4,2,2,2,2,−10,−10,6]
T^4+2T^2+3	$Y^2=X^3+(3T^4+T^2)X+T^6+3T^4+T^2+4$	[0,−2,4,4,−2,−10,−6,−2]
T^4+3T^2+3	$Y^2=X^3+(3T^4+4T^2)X+T^6+2T^4+T^2+1$	[0,4,−2,−2,4,−6,−10,2]
$T^4+3T^3+2T^2+4T+1$	$Y^2=X^3+(3T^4+4T^3+T^2+2T+4)X+T^6+2T^5+2T^4+T^3+4T^2+1$	[−2,4,0,4,−2,2,6,−2]
$T^4+T^3+T^2+T+3$	$Y^2=X^3+(3T^4+3T^3+3T^2+3T)X+T^6+4T^5+3T^2+3T+4$	[0,0,0,0,4,6,−2,6]
$T^4+3T^3+4T^2+2T+3$	$Y^2=X^3+(3T^4+4T^3+2T^2+T)X+T^6+2T^5+3T^2+4T+1$	[0,0,4,0,0,−2,6,6]

C.7 Table for primes of degree 5 over $\mathbb{F}_5$

Table C.6: Isogeny classes for primes of degree 5 over $\mathbb{F}_5$

Conductor	Curve	Trace
$T^5+2T^4+3T^2+3T$	$Y^2=X^3+(3T^4+2T^3+4T^2+T+3X)+T^6+T^5+3T^4+3T^3+T^2+3T+1$	[−1,−2,0,1,−2,−4,−1,−2]
T^5+T^4+2T+2	$Y^2=X^3+(3T^4+4T^3+4T+3X)+T^6+2T^5+4T^4+2T^3+4T^2+T+2$	[1,−3,2,−2,−2,−2,−4,7]
T^5+3T^4+2T+2	$Y^2=X^3+(3T^4+2T^2X)+T^6+T^5+3T^4+2T^3+T^2+4T+4$	[0,0,−3,−3,0,−4,−1,8]
T^5+4T^4+2T+2	$Y^2=X^3+(3T^4+T^3+3T^2+3T+1X)+T^6+3T^5+3T^4+3T^3+T^2+4T$	[2,−4,0,2,−6,−6,−8,2]
$T^5+2T^4+T^3+2T^2+1$	$Y^2=X^3+(3T^4+4T^3+3T^2+4T+1X)+T^6+2T^5+3T^4+T^3+T^2+2T+4$	[−3,−2,−3,−3,0,−6,2,−2]
$T^5+T^4+T^3+2T+2$	$Y^2=X^3+(3T^4+T^3+2T^2+T+3X)+T^6+3T^5+T^3+T^2+2T$	[−4,−3,−2,−2,0,2,2,1]
T^5+2T^3+2T+2	$Y^2=X^3+(3T^4+4T^3+3T^2+3T+1X)+T^6+2T^5+3T^4+T^3+2T^2+T$	[2,0,−2,−2,6,−4,−2,−6]
$T^5+T^4+2T^3+2T+2$	$Y^2=X^3+(3T^4+2T^3+2T^2+4T+3X)+T^6+T^5+2T^4+3T^2+T+2$	[1,−1,0,−2,−1,7,−4,−2]
$T^5+3T^4+3T^3+3T^2+3T$	$Y^2=X^3+(3T^4+3T^3+3T^2+4T+3X)+T^6+4T^5+4T^4+3T^3+3T^2+2T+1$	[4,2,0,2,−4,−6,2,2]
$T^5+4T^4+2T^3+2T+2$	$Y^2=X^3+(3T^4+4T^3X)+T^6+2T^5+4T^4+3T^3+T^2+T+2$	[0,3,−3,0,−1,8,−6,−3]

References

[AB04] Montserrat Alsina and Pilar Bayer. *Quaternion orders, quadratic forms, and Shimura curves*, volume 22 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2004. 38

[BC91] J.F. Boutot and H. Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld. Number 196-197, pages 7, 45–158 (1992). 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). 2, 38

[BD98] Massimo Bertolini and Henri Darmon. Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization. *Invent. Math.*, 131(3):453–491, 1998. 2, 3, 42

[Bos09] Siegfried Bosch. *Lineare Algebra.* Springer, Berlin, Heidelberg, 4. berarb. aufl. 2008 edition, 2009. 14

[BCDT] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001. 2

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 6

[But12] Ralf Butenuth. *Quaternionic Drinfeld modular forms.* PhD thesis, 2012. Thesis (Ph.D.)-Heidelberg University(Germany). 12

[But07] Ralf Butenuth. Ein Algorithmus zum Berechnen von Hecke-Operatoren auf Drinfeldschen Modulformen. Master's thesis, University Duisburg-Essen, August 2007. 116, 120, 121, 124

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin-New York, 4th printing edition edition, 1993. 148

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. 2, 36, 37, 38, 45

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. 36, 38, 41

[DP06] Henri Darmon and Robert Pollack. Efficient calculation of Stark-Heegner points via overconvergent modular symbols. *Israel J. Math.*, 153:319–354, 2006. 45

[Dri74] V. G. Drinfeld. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974. ii, 1

[FvdP81] Jean Fresnel and Marius van der Put. *Géométrie analytique rigide et applications*, volume 18 of *Progress in Mathematics*. Birkhäuser, Boston, Mass., 1981. 10

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013. 113, 114, 115

[Gek86] Ernst-Ulrich Gekeler. *Drinfel′d modular curves*, volume 1231 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1986. 19

[Gek95] Ernst-Ulrich Gekeler. Analytical construction of Weil curves over function fields. *J. Théor. Nombres Bordeaux*, 7(1):27–49, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). 29, 91

[Gek97] Ernst-Ulrich Gekeler. Jacquet-Langlands theory over K and relations with elliptic curves. In *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 224–257. World Sci. Publ., River Edge, NJ, 1997. 19

[GEK97] Erns-Ulrich-Gekeler. On the drinfeld discriminant function. *Compositio Mathematica*, 106:181–202, 4 1997. 143

[Gek99] Ernst-Ulrich Gekeler. Lectures on Drinfeld modular forms. CICMA Lecture Notes, 1999. 18

[GN95] Ernst-Ulrich Gekeler and Udo Nonnengardt. Fundamental domains of some arithmetic groups over function fields. *Internat. J. Math.*, 6(5):689–708, 1995.

[Gel75] Stephen S. Gelbart. *Automorphic forms on adèle groups*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975. Annals of Mathematics Studies, No. 83. 27

[GI63] O. Goldman and N. Iwahori. The space of p-adic norms. *Acta Math.*, 109:137–177, 1963. 17

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole. 87

[GR96] Ernst-Ulrich. Gekeler and M. Reversat. Jacobians of Drinfeld modular curves. *J. Reine Angew. Math.*, 476:27–93, 1996. ii, 3, 5, 7, 15, 18, 24, 25, 26, 28, 29, 31

[Gek97] Ernst-Ulrich Gekeler. Highly ramified pencils of elliptic curves in characteristic 2. *Duke Math. J.*, 89(1):95–107, 07 1997. 149

[Gre06] Matthew Greenberg. *Heegner points and rigid analytic modular forms*. PhD thesis, 2006. Thesis (Ph.D.)-McGill University (Canada). 2, 42, 43, 45

[GvdP80] Lothar Gerritzen and Marius van der Put. *Schottky groups and Mumford curves*, volume 817 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980. 39, 42

[GMS] Xavier Guitart, Marc Masdeu, Mehmet Haluk Sengun, Uniformization of modular elliptic curves via p-adic periods. *arXiv:1501.02936*, 2015. 3

[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970. 28

[Kat77] Nicholas M. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977. 79

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984. 43, 82

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate. 87

[Lon02] Ignazio Longhi. Non-Archimedean integration and elliptic curves over function fields. *J. Number Theory*, 94(2):375–404, 2002. ii, 3, 31, 32, 34

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954. 75

[Non01] Udo Nonnengardt. Arithmetisch definierte Graphen über Rationalen Funktionenkörpern. Master's thesis, Saarland University, 2001. 19, 20, 21, 22, 23, 24, 135

[Pál06] Ambrus Pál. Proof of an exceptional zero conjecture for elliptic curves over function fields. *Math. Z.*, 254(3):461–483, 2006. 31

[Pap01] M Papikian. Heegner point computations over function fields. In Arizona winter School, 2001. http://www.math.psu.edu/papikian/Research/Heegner.pdf 98

[PS11] Robert Pollack and Glenn Stevens. Overconvergent modular symbols and p-adic L-functions. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(1):1–42, 2011. 2, 42, 43

[Roq70] Peter Roquette. *Analytic theory of elliptic functions over local fields.* Hamburger Mathematische Einzelschriften (N.F.), Heft 1. Vandenhoeck & Ruprecht, Göttingen, 1970. 29, 88

[Sch84] P. Schneider. Rigid-analytic L-transforms. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 216–230. Springer, Berlin, 1984. 34

[Sch01] Andreas Schweizer. On elliptic curves over function fields of characteristic two. *J. Number Theory*, 87(1):31–53, 2001. 93, 100, 149

[Sch11] Andreas Schweizer. Strong Weil curves over $\mathbb{F}_q(T)$ with small conductor. *J. Number Theory*, 131(2):285–299, 2011. 109

[Sch99] Andreas Schweizer. On elliptic curves in characteristic 2 with wild additive reduction. *Acta Arithmetica*, 91(2):171–180, 1999. 149

[Sch00] Andreas Schweizer. Extremal elliptic surfaces in characteristic 2 and 3. *Manuscripta mathematica*, 102(4):505–521, 2000. 149

[SD75] H. P. F. Swinnerton Dyer. Correction to: "On l-adic representations and congruences for coefficients of modular forms" (Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55, Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973). In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 149. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975. 85, 87

[Ser73a] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser73b] Jean-Pierre Serre. Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. In *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, pages 319–338. Lecture Notes in Math., Vol. 317. Springer, Berlin, 1973. 84

[Ser03] Jean-Pierre Serre. *Trees*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation. 11, 19, 20, 22, 116, 124

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 42, 87

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 35, 37, 69, 73, 78, 79, 80, 93, 97, 101

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975. 94, 98

[Tei91] Jeremy T. Teitelbaum. The Poisson kernel for Drinfeld modular curves. *J. Amer. Math. Soc.*, 4(3):491–511, 1991. 31, 34

[VdP82] Marius Van der Put. Les fonctions theta d'une courbe de Mumford. *Groupe de travail d'analyse ultramtrique*, 9(1):1–12, 1981-1982. 25

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980. 38

[Voi] John Voight. The arithmetic of quaternion algebras. In Preparation. 38

[Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography. 78, 79