CODE CONSTRUCTION ON MODULAR CURVES

A DISSERTATION SUBMITTED TO
THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By
Orhun Kara
August, 2003

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Alexander Klyachko (Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Serguei Stepanov

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Hurşit Önsiper

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Alexander Shumovsky

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Assoc. Prof. Dr. Sinan Sertöz

Approved for the Institute of Engineering and Science:

Prof. Dr. Mehmet B. Baray
Director of the Institute

ABSTRACT

CODE CONSTRUCTION ON MODULAR CURVES

Orhun Kara
Ph.D. in Mathematics
Supervisor: Prof. Dr. Alexander Klyachko
August, 2003

In this thesis, we have introduced two approaches on code construction on modular curves and stated the problems step by step. Moreover, we have given solutions of some problems in road map of code construction.

One of the approaches uses mostly geometric and algebraic tools. This approach studies local invariants of the plane model $\overline{Z_0(\ell)}$ of the modular curve $Y_0(\ell)$ given by the modular equation Φ_ℓ in affine coordinates. The approach is based on describing the hyperplane of regular differentials of $\overline{Z_0(\ell)}$ vanishing at a given $\mathbb{F}_{p^2}$ rational point. As constructing a basis for the regular differentials of $\overline{Z_0(\ell)}$, we need to investigate its singularities. We have described the singularities of $\overline{Z_0(\ell)}$ for prime ℓ in both characteristic 0 and positive characteristic. We have shown that all singularities of of the affine part, $Z_0(\ell)$, are self intersections. These self intersections are all simple nodes in characteristic 0 whereas the order of contact of any two smooth branches passing though a singular point may be arbitrarily large in characteristic $p > 3$ where $p \neq \ell$. Moreover the self intersections in characteristic zero are double.

Indeed, structure of singularities of the affine curve $Z_0(\ell)$ essentially depends on two types of elliptic curves: The singularities corresponding to ordinary elliptic curves and the singularities corresponding to supersingular elliptic curves. The singularities corresponding to ordinary elliptic curves are all double points even though they are not necessarily simple nodes as in the case of characteristic 0. The singularities corresponding to supersingular elliptic curves are the most complicated ones and it may happen that there are more then two smooth branches passing though such kind of a singular point. We have computed the order of contact of any two smooth branches passing though a singular point both for ordinary case and for supersingular case.

We have also proved that two points of $\overline{Z_0(\ell)}$ at ∞ are cusps for odd prime ℓ which are analytically equivalent to the cusp of 0, given by the equation $x^\ell = y^{\ell-1}$. These two cusps are permuted by Atkin-Lehner involution. The multiplicity of singularity of each cusp is $\frac{(\ell-1)(\ell-2)}{2}$. This result is valid in any characteristic $p \neq 2, 3$.

The second approach is based on describing the Goppa codes on modular curve $Y(\ell)$ as $PSL_2(\mathbb{F}_\ell)$ module. The main problem in this approach is investigating the structure of a group code as $PSL_2(\mathbb{F}_\ell)$ module. We propose a way of computing the characters of representations of a group code by using the localization formula. Moreover, we give an example of computing the characters of the code which associated to a canonical divisor on $Y(\ell)$.

Keywords: Modular curve, elliptic curve, Goppa codes, isogeny, endomorphism ring, singularity, self intersection, supersingular elliptic curve, reduction, lifting, cusp, representations, characters.

ÖZET

MODÜLER EĞRİLER ÜZERİNDE KOD İNŞASI

Orhun Kara
Matematik Bölümü, Doktora
Tez Yöneticisi: Prof. Dr. Alexander Klyachko
Ağustos, 2003

Bu tezde, modüler eğriler üzerinde hata düzeltme kodlarının inşası hakkında iki yaklaşım sunduk ve problemleri ifade ettik. Ayrıca bu problemlerden bazılarının çözümlerini verdik.

Yaklaşımlardan birisi çoğunlukla cebirsel ve geometrik araçları kullanmaktadır. Bu yaklaşım, $Y_0(\ell)$ modüler eğrisinin düzlemdeki modeli olan $\overline{Z_0(\ell)}$'in bölgesel değişmezleri üzerinde aritmetik yapmaya dayanır. $\overline{Z_0(\ell)}$'in herhangi bir $\mathbb{F}_{p^2}$ rasyonel noktasında sıfırlanan diferansiyellerin betimlenmesi temel alınmıştır. Bu differansiyellerin kümesini oluşturabilmek için, $\overline{Z_0(\ell)}$'nin tekilliklerini betimlemek gerekmektedir. $\overline{Z_0(\ell)}$'nin tekilliklerini, $\overline{Z_0(\ell)}$ hem karekteristiği 0 olan cisimdeyken hem de karekteristiği $p > 3$ olan cisimdeyken ayrı ayrı betimledik. Tekillikleri analiz ederken ℓ'in p'den farklı bir asal sayı olduğunu kabül ettik. Ayrıca kaç tane tekillik olduğunu hesapladık.

$Z_0(\ell)$'in tekilliklerin yapısı iki tür eliptik eğriye bağlıdır: Sıradan eliptik eğrilerden gelen tekillikler ve süpertekil eliptik eğrilerden gelen tekillikler. Sıradan eliptik eğrilerden gelen tekilliklerin hepsi de çift noktadırlar. Süpertekil eliptik eğrilerden gelen tekillikler ise en karmaşık olanlardır ve bu şekilde bir tekillikten geçen ikiden fazla düzenli dallanma olabilir. Biz hem sıradan eliptik eğrilerden gelen tekillikler için ve hem de süpertekil eliptik eğrilerden gelen tekillikler için bu tekilliklerden gecen herhangi iki düzenli dallanmanın kontak mertebesini hesapladık.

Ayrıca $\overline{Z_\ell}$'in sonsuzda bulunan iki noktasının da kasp türü tekillikler olduğunu ve bu tekilliklerin $x^\ell = y^{\ell-1}$ eğrisinin 0'daki tekilliğine analitik olarak denk olduğunu ispatladık.

Diğer yaklaşım modüler eğriler üzerinde hata düzeltme kodlarını $PS_2(\mathbb{F}_\ell)$ modülü olarak betimlemeye dayanmaktadır. Bu yaklaşımda ana problem grup kodlarının yapılarını $PS_2(\mathbb{F}_\ell)$ modül olarak ifade etmektir. Biz modüler eğriler üzerindeki grup kodlarının karakterlerini hesaplamak için yöreselleştirme formülünü kullanan bir metod önerdik. Ayrıca kanonik diferansiyele denk gelen grup kodunun karakterlerini hesapladık.

Anahtar sözcükler: Modüler eğri, elliptik eğri, Goppa kodları, isogeni, endomorfizma halkası, tekillik, kendiyle kesişme, süpertekil elliptik eğri, indirgeme, kaydırma, kasp, temsiller, karakterler.

Acknowledgement

I would like to express my special thanks and gratitude to my supervisor Prof. Alexander Klyachko for his excellent guidance and patience.

I would like to thank to Prof. Önsiper, Prof. Sertöz, Prof. Shumovsky and Prof. Stepanov for reading and commenting on the thesis.

I am grateful to all my professors both in Bilkent University and in METU who have been taught me both mathematical approaching and mathematical explaining. I would like to thank Prof. Serge Vladuţ for accepting me to work together and Prof. Gilles Lachaud for his helps during my studies at IML in Luminy.

I would like to express my special thanks to all my friends and colleague in UEKAE, particularly Alparslan Babaoğlu and Murat Apohan for their support and vast tolerance.

I would like to thank my wife for her endless support and love and also my little daughter for driving me to reveal my childhood and loading me with positive energy and natural motivation to fresh my curiosity.

To my cute little daughter...

Contents

Chapter 1

Introduction

1.1 Motivation

A linear code C over a finite field $\mathbb{F}_q$ is a linear subspace of the vector space $\mathbb{F}_q^n = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$. The Hamming weight of a vector $x \in \mathbb{F}_q^n$ is the number of nonzero coordinates of x. Then, the minimum distance d of a code C is defined as the minimum of Hamming weights of the nonzero vectors of C. The parameters of C is given as $[n, k, d]_q$ where n is the block length and k is the dimension of C. Moreover, an $[n, k, d]_q$ code has two more parameters, its *information rate* and its *relative minimum distance*. The former is $R = \frac{k}{n}$ and indicates how much information a code vector carries. The latter one is $\delta = \frac{d}{n}$ and measures the error correction ability of the code. Roughly speaking, a good $[n, k, d]_q$ code should have large relative minimum distance $\delta = d/n$ and information rate $R = k/n$.

Let us define the set

$$V_q = \{(\delta, R) \in [0, 1] \times [0, 1] : \exists \text{ an } [n, k, d]_q \text{ code with } \frac{d}{n} = \delta, \frac{k}{n} = R\}$$

and denote the limit points of V_q as U_q. The function $\alpha_q(\delta)$ defined as

$$\alpha_q(\delta) = \sup\{R : (\delta, R) \in U_q\}$$

indicates the maximum possible information rate among those of all very long codes with relative minimum distance δ. However, $\alpha_q(\delta)$ is unknown. Even,

there is only few information derived about it so far. It is one of the main problems of coding theory to discover $\alpha_q(\delta)$. A very common approach for providing information about $\alpha_q(\delta)$ is constructing upper and lower bounds for it. One of the most important lower bounds is Gilbert-Varshamov bound, given as

$$\alpha_q(\delta) \geq 1 - H_q(\delta) \tag{1.1}$$

where H_q is the q-ary entropy function

$$H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), H(0) := 0.$$

The Gilbert-Varshamov bound could not been improved until the algebraic-geometric codes were introduced. Goppa has proposed a brilliant way of code construction on algebraic curves in [GO 1]. It turns out that some Goppa codes on curves with a lot of rational points have pretty nice parameters. More explicitly, when a family $\mathcal{X}$ of curves X_α over $\mathbb{F}_q$ attains the Drinfeld-Vladuţ bound given as

$$\limsup_{g_{X_\alpha}\to\infty} \frac{|X_\alpha(\mathbb{F}_q)|}{g_{X_\alpha}} \leq \sqrt{q} - 1$$

where g_{X_α} is genus of the curve X_α and $|X_\alpha(\mathbb{F}_q)|$ is the cardinality of $\mathbb{F}_q$ rational points of X_α, then the parameters of the corresponding Goppa codes lie on the line $R = 1 - \delta - 1/(\sqrt{(}q) - 1)$. This line is obviously better than the Gilbert Varshamov bound in the interval (δ_1, δ_2) where δ_1 and δ_2 are intersection points of $1 - H_q(\delta)$ and $1 - \delta - 1/(\sqrt{(}q) - 1)$. Due to this crucial development, the algebraic geometric codes attaining the Drinfeld - Vladuţ bound have attracted the attention of coding theory world. It is known at least three constructions of such curves: Classical modular curves, Drinfeld modular curves (see [TS-VLA] for these two curves) and Garcia-Stichtenoth tower of Artin-Schreier extensions (see [GA-STI]).

In this work, we are interested in classical modular curves. The modular curve $X_0(N)$ is the moduli space of elliptic curves E with cyclic subgroup of order N. Equivalently, $X_0(N)$ is moduli space of triples (E, E', ϕ) where $\phi : E \longmapsto E'$ is a cyclic isogeny of degree N between elliptic curves E and E'. Similarly, the modular curve $X(N)$ is moduli space of the pairs (E, α_N), E is an elliptic curve

and α_N is a structure of level N with determinant $\det \alpha_N = 1$. In [DE-RA], Deligne and Rapoport have proved that the projective closures $Y_0(N)$ and $Y(N)$ of modular curves $X_0(N)$ and $X(N)$ respectively have good (smooth) reduction over any prime ideal not dividing N. In particular, the modular curve $Y_0(N)$ is defined over $\mathbb{Q}$. That is, for any prime p not dividing N, there exists a good reduction of $Y_0(N)$ modulo p. So, we can still consider the modular curves in positive characteristics as moduli spaces of elliptic curves with some special structures. If E is a supersingular elliptic curve, an elliptic curve with noncommutative endomorphism ring, then its j invariant, $j(E)$, is in $\mathbb{F}_{p^2}$ and the point represented by the pair (E, N) is an $\mathbb{F}_{p^2}$ rational point of $X_0(N)$. Similarly, the the point (E, α_N) is an $\mathbb{F}_{p^2}$ rational point of $X(N)$. The number of supersingular elliptic curves is enough large so that the curves $Y_0(N)$ and $Y(N)$ over $\mathbb{F}_{p^2}$ reach the Drinfeld-Vladuţ bound for $(N, p) = 1$.

It has been pointed out that the Goppa codes on modular curves have the best known asymptotic parameters so far. However, it is difficult to construct codes on modular curves efficiently. The modular curves have nice analytic description as a quotient space of the action of some specific subgroups of $PSL_2(\mathbb{Z})$ on upper half plane, $\mathbb{H}$, of the complex numbers $\mathbb{C}$ for characteristic 0. Unfortunately, these curves have no known such beautiful description as algebraic objects which causes difficulties in code construction.

1.2 What is Done in This Thesis

We have introduced two approaches on code construction on modular curves and stated the progress in one of them. One of the approaches is geometric approach. It is due to Klyachko (cf. [KLY]) and the other one is called group theoretic approach. This approach is due to Vladuţ and Tsfasman (cf. [TS-VLA]). We consider the modular curves $Y_0(\ell)$ and $Y(\ell)$ over a finite field of characteristic p where ℓ is also a prime different then p. We give a brief introduction to both approaches in chapter 4. The group theoretical approach considers the codes on modular curves $Y(\ell)$ as group modules and tries to describe them not as

vector spaces but as group modules or in special cases, as group ideals. The group $PSL(2,\mathbb{Z}/\ell\mathbb{Z})$ acts on the Goppa codes constructed on $Y(\ell)$. The action is permuting the coordinates of vectors of the code. So, the codes can be considered as group codes.

1.2.1 Geometric Approach

The geometric approach studies local invariants of the plane model $\overline{Z_0(\ell)}$ of the modular curve $Y_0(\ell)$ given by the modular equation Φ_ℓ. The approach is based on describing the hyperplane of regular differentials of $\overline{Z_0(\ell)}$ vanishing at a given $\mathbb{F}_{p^2}$ rational point. Unfortunately the plane model $\overline{Z_0(\ell)}$ is highly singular curve. So, the elements of the hyperplane must vanish at singular points also.

We embed $Y_0(\ell)$ into $\mathbb{P}(\Omega)$ where $\Omega = \Omega[Y_0(\ell)]$ is the space of regular differentials of $Y_0(\ell)$. It is really an embedding of $Y_0(\ell)$ for $\ell \geq 71$ since it is not hyperelliptic for the case $\ell \geq 71$ (see [OGG]). Then Goppa codes are configurations of rational points on $\mathbb{P}(\Omega)$. The code construction can be viewed in two steps: First step is finding a basis for the space $\Omega[Y_0(\ell)]$ and last step is describing the hyperplanes of $\Omega[Y_0(\ell)]$ whose elements vanish at rational points. Let Ω^* be the dual space of Ω. Consider

$$Y_0(\ell) \longrightarrow \mathbb{P}(\Omega^*)$$

$$x \mapsto \Omega_x = \{w \in \Omega : w(x) = 0\}.$$

Any configuration of the points Ω_x in $\mathbb{P}(\Omega^*)$ which does not lie in a hyperplane in $\mathbb{P}(\Omega^*)$ gives a Goppa code on the modular curve $Y_0(\ell)$ for a set of $\mathbb{F}_q$ rational points x. So, we should find a description of regular differentials that vanish at a given rational point $x \in Y_0(\ell)(\mathbb{F}_q)$.

We make use of a singular plane model of $Y_0(\ell)$ to construct its regular differentials. The curve $Y_0(\ell)$ has singular plane model $\overline{Z_0(\ell)}$ coming from projection

$$\pi : Y_0(\ell) \to \mathbb{P}^2 \tag{1.2}$$

given in affine coordinates by $\rho \mapsto (j(E), j(E'))$ where $\rho : E \to E'$ is a cyclic isogeny of degree ℓ between elliptic curves E and E' . One can define the affine

part, $Z_0(\ell)$, explicitly by classical modular equation

$$Z_0(\ell) : \Phi_\ell(X, Y) = 0. \tag{1.3}$$

Let $X \subset \mathbb{P}^2$ be a curve given by $F(x, y, z) = 0$ of degree d. If X is smooth then the regular differentials are of the form

$$\omega = P\frac{xdy - ydx}{F_z} = P\frac{xdz - zdx}{F_y} = P\frac{zdy - ydz}{F_x} \tag{1.4}$$

where $P = P(x, y, z)$ is a homogeneous polynomial of degree $d - 3$. We follow this approach to construct regular differentials. However, the projective plane model $\overline{Z_0(\ell)}$ is a singular curve. But the differentials on a singular plane curve are still of the form given in equation 1.4. We should impose some additional local conditions on the polynomial P at singular points. So, constructing the regular differentials on $\overline{Z_0(\ell)}$ as in the form 1.4, we should first describe the singularities of $\overline{Z_0(\ell)}$.

1.2.2 Singularities of Modular Curve

We have described the singularities of $\overline{Z_0(\ell)}$ for prime ℓ in both characteristic 0 and positive characteristic in one section in chapter 5. We have shown that both in positive characteristic $p > 3$ for $(p, \ell) = 1$ and in characteristic 0, the map

$$\pi : X_0(\ell) \longmapsto \mathbb{A}^2$$

$$(E, E', \phi) \longmapsto (j(E), j(E')) \tag{1.5}$$

is immersion. That is, the differential, $d\pi$, is injective. So, π is local embedding of nonsingular branches. Hence, all singularities of $Z_0(\ell)$ are self intersections. We have also proved that two points of $\overline{Z_0(\ell)}$ at ∞ in projective space are cusps for odd prime ℓ which are analytically equivalent to the cusp of 0, given by the equation $x^\ell = y^{\ell-1}$ (see Proposition 5.2.2). These two cusps are permuted by Atkin-Lehner involution. The multiplicity of singularity of each cusp is $\frac{(\ell-1)(\ell-2)}{2}$. This result is valid in any characteristic $p \neq 2, 3$ (see [KLY-KA]) .

1.2.2.1 The Case of Characteristic 0

The modular curve $X_0(\ell)$ has a useful analytic interpretation as the quotient space $\mathbb{H}/\Gamma_0(\ell)$ where $\mathbb{H}$ is upper half plane, $\{z \in \mathbb{C} : \text{im}z > 0\}$ and

$$\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) : c \equiv 0 \bmod \ell \right\}.$$

We have used this interpretation to calculate the genus of projective closure $Y_0(\ell)$ of $X_0(\ell)$ by using Hurwitz genus formula:

$$g(Y_0(\ell)) = \frac{\ell+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{\ell}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{\ell}\right)\right) \tag{1.6}$$

where Legendre symbols are given by

$$\left(\frac{-1}{\ell}\right) = \begin{cases} 0 & \text{if } \ell = 2, \\ 1 & \text{if } \ell \equiv 1 \bmod 4, \\ -1 & \text{if } \ell \equiv 3 \bmod 4 \end{cases}$$

and

$$\left(\frac{-3}{\ell}\right) = \begin{cases} 0 & \text{if } \ell = 3, \\ 1 & \text{if } \ell \equiv 1 \bmod 3, \\ -1 & \text{if } \ell \equiv 2 \text{ mo d } 3. \end{cases}$$

We have described the singularities of the plane projective curve $\overline{Z_0(\ell)}$. First, we have investigated that all singularities of the affine part, $Z_0(\ell)$, are double points. Such self intersection comes from existence of two cyclic isogenies $\sigma, \rho : E \longmapsto E'$ of degree ℓ, which are not equivalent modulo automorphism of E and E'. That is, $\sigma \neq \epsilon'\rho\epsilon$ where $\epsilon \in \text{Aut}(E)$ and $\epsilon' \in \text{Aut}(E')$. Then, the triples (E, E', σ) and (E, E', ρ) represent two different points on $X_0(\ell)$ whereas their projections, $(j(E), j(E'))$ is a single point on $Z_0(\ell)$ which is a singularity. It turns out that there exists at most two such nonequivalent isogenies of degree ℓ and hence all self intersections are double (see theorem 5.2.4).

We have described self intersections explicitly. In two different parameterization in a neighborhood of a point of $Z_0(\ell)$ we get two different tangent vectors.

That is, singularities of $Z_0(\ell)$ in characteristic 0 are not just double self intersections, they are exactly simple nodes (normal self intersections, see proposition 5.2.3).

The following theorem describes the singularities of $Z_0(\ell)$ in characteristic 0. This theorem is combination of theorem 5.2.4 and proposition 5.2.3.

Theorem 1.2.1 *There exists a one to one correspondence between self intersections of the curve $Z_0(\ell)$ over $\mathbb{C}$ and the elliptic curves E having complex multiplication $\alpha : E \longmapsto E$ such that*

i) $N(\alpha) = \alpha\overline{\alpha} = \ell^2$ and

ii) $\frac{\alpha}{\ell}$ is not root of unity.

Moreover, all self intersections are simple nodes.

Using the theorem above, we can relate number of singularities of $Z_0(\ell)$ with Hurwitz class number

$$H(-D) = \sum \frac{2}{|\mathrm{Aut}Q|}$$

where summation is over equivalence classes of binary integer quadratic forms $Q = ax^2 + bxy + cy^2,\ \ a, b, c \in \mathbb{Z}$, of discriminant $-D = b^2 - 4ac$. The quadratic form $x^2 + y^2$ is counted with weight $\frac{1}{2}$ and the quadratic form $x^2 + xy + y^2$ is counted with weight $\frac{1}{3}$. All other quadratic forms in other equivalent classes are counted with weight 1. Then, number of nodes is given as:

Theorem 1.2.2 *Number of simple nodes of $Z_0(\ell)$ is*

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2 - 4\ell^2).$$

As explained above the projective closure, $\overline{Z_0(\ell)}$, has additional two singular points at ∞, which are cusps analytically equivalent to that of $x^\ell = y^{\ell-1}$ (see proposition 5.2.2). The multiplicity of this cusp is $\frac{(\ell-1)(\ell-2)}{2}$. As a corollary, we

get an independent proof of Hurwitz class number formula by comparing two genus formulas for $Y_0(\ell)$. One of them is calculated by Hurwitz genus formula, given in 1.6 independent from the projective plane model , $\overline{Z_0(\ell)}$, and the other one is calculated from the projective plane model, $\overline{Z_0(\ell)}$, by Plücker genus formula including singularities of $\overline{Z_0(\ell)}$. The independent proof of Hurwitz class number formula confirms all the statements for the characteristic 0 case:

Corollary 1.2.1

$$\sum_{t=-2\ell}^{2\ell} H(\ell^2 - 4t^2) = 2\ell^2 + \ell$$

where we define $H(0) = \frac{-1}{12}$.

1.2.2.2 The Case of Positive Characteristic

First of all, since the canonical projection $\pi : X_0(\ell) \longmapsto \mathbb{A}^2$ is immersion in any characteristic $p \neq 2, 3$; we get

Proposition 1.2.1 *The singularities of* $Z_0(\ell)$ *in positive characteristic* $p > 3$ *are just multiple self intersections.*

In positive characteristic also, the singularities of $Z_0(\ell)$ are the points $(j(E), j(E'))$ where there exists at least two cyclic isogenies $\sigma, \rho : E \longmapsto E'$ of degree ℓ and those two isogenies σ, ρ are not equivalent modulo automorphisms of E and E'.

The new results for positive characteristic case can be viewed in two parts:

i) The singularities corresponding to ordinary elliptic curves in positive characteristic. An ordinary elliptic curve defined over a finite field is an elliptic curve whose endomorphism ring is an order in an imaginary quadratic field.

ii) The singularities corresponding to supersingular elliptic curves. Recall that a supersingular elliptic curve is an elliptic curve in positive characteristic p, which

has no element of order p. In difference with ordinary elliptic curves, endomorphism ring of a supersingular curve is an order in quaternion algebra. In addition, there are finitely many supersingular elliptic curves in positive characteristic p and all of them are defined over $\mathbb{F}_{p^2}$.

Structure of singularities of the affine curve $Z_0(\ell)$ essentially depends on these two types of elliptic curves.

It turns out that in the ordinary case, the multiplicity of a self intersection is a power of characteristic p, which is given by the following:

Theorem 1.2.3 *Let $Z_0(\ell)$ be the plane model of $X_0(\ell)$ in characteristic $p > 3$, $(p, \ell) = 1$. Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\sigma, \quad \rho \in \ Hom(E, E')$ of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in \ End(E)$ where $\widehat{\rho}$ is the dual of ρ. Assume p splits in $\mathbb{Q}(\alpha)$. Then the singularity at $(j(E), j(E'))$ has multiplicity p^r where p^r is p part of the conductor of $\mathbb{Z}[\alpha]$. That is, if $f = p^r c_0$ where $c_0 \not\equiv 0 \ mod\ p$ then multiplicity is p^r.*

As in characteristic 0 the number of self intersections of multiplicity p^r can be calculated via Hurwitz class function:

Corollary 1.2.2 *The number of self intersections of multiplicity p^r corresponding to ordinary elliptic curves is*

$$\sum_{0<t<2\ell, t\neq\ell}{}' H(t^2 - 4\ell^2)$$

where summation is taken over those t for which $t^2 - 4\ell^2 = -p^{2r}D$; $\left(\frac{-D}{p}\right) = 1$.

If we sum number of all self intersections with multiplicities corresponding to ordinary elliptic curves, we get:

Corollary 1.2.3 *Sum of the multiplicities of all self intersections of $Z_0(\ell)$ corresponding to ordinary elliptic curves is*

$$\sum_{t^2-4\ell^2=p-adic\ square, 0<t<2\ell, t\neq\ell} H(t^2-4\ell^2).$$

We know that also in positive characteristic two cusps of $\overline{Z_0(\ell)}$ at ∞ are singular with multiplicities $\frac{(\ell-1)(\ell-2)}{2}$. The modular curve $Y_0(\ell)$ has the same genus given in 1.6 in positive characteristic also since it has a good reduction. Therefore, we compare two genus formulas for $Y_0(\ell)$ and as a corollary we get:

Corollary 1.2.4 *Sum of the multiplicities of all self intersections corresponding to supersingular elliptic curves is*

$$\sum_{t^2-4\ell^2\neq p-adic\ square, 0<t<2\ell, t\neq\ell} H(t^2-4\ell^2).$$

The second part is about the singularities corresponding to supersingular elliptic curve. The statement of this part describes those singularities:

Theorem 1.2.4 *Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\rho, \sigma \in Hom(E, E')$, of degree ℓ. Assume E is supersingular. Let $\alpha = \widehat{\rho}\sigma \in End(E)$ where $\widehat{\rho}$ is the dual isogeny of ρ. If p^r is the p part of the conductor of $\mathbb{Z}[\alpha]$ then the multiplicity of intersection of these two branches is*

i) $2 + 2p + \cdots + 2p^{r-1} + p^r$ if p is prime in $\mathbb{Q}(\alpha)$, and

ii) $2 + 2p + \cdots + 2p^{r-1} + 2p^r$ if p is ramified in $\mathbb{Q}(\alpha)$.

1.2.3 Algebraic Geometric Codes with Automorphisms

Let X be a smooth projective algebraic curve over a finite field $\mathbb{F}_q$ and G be an arbitrary subgroup of the automorphism group of X. Assume D is a G invariant

$\mathbb{F}_q$ rational divisor. Then the vector spaces $H^0(X, \mathcal{L}_D) = L(D)$ and $H^1(X, \mathcal{L}_D) = \Omega(D)$ are G modules where $\mathcal{L}_D$ is the line bundle associated to the divisor D. The Goppa code on X associated to D is the realization of the space $H^0(Y(\ell), \mathcal{L}_D)$ in a coordinate system of a vector space over $\mathbb{F}_q$ defined by $\mathbb{F}_q$ rational points of X. This construction corresponds to $L(D)$ construction of functions. Similarly, the space $H^1(X, \mathcal{L}_D)$ corresponds to $\Omega(D)$ construction of differential forms (we refer to first chapter for both Ω and L constructions). The Goppa codes corresponding to $H^0(X, \mathcal{L}_D) = L(D)$ and $H^1(X, \mathcal{L}_D) = \Omega(D)$ are G modules as group codes over $\mathbb{F}_q$. The notion of group codes is given in section 4.3. The main problem in this approach is investigating the structure of a group code on X as G module.

Problem: Evaluate the action of G on the Goppa code $C = L(D)$ over $\mathbb{F}_q$.

This problem is introduced in [TS-VLA] for the case of modular curves. Let the characteristic of the field $\mathbb{F}_q$ be p. We assume that p is coprime to the order of the group G. In this case, we can consider the representations of codes in characteristic 0. Because, the reduction modulo p of an irreducible G representation over a number field remains irreducible if p is coprime to the order of the group G. In this thesis, we propose a way of computing the characters of representations of a group code by using the localization formula for the modular curve $Y(\ell)$.

The localization formula has several forms associated to several applications. We refer to [HEJ] for extended applications. However, the most convenient form for our use can be found in [TH]. In general, the formula is as follows. Let V be a smooth projective algebraic variety and $g : V \to V$ be an automorphism of V having isolated fixed points, V^g. Let E be a g bundle on V with action $g : E \to E$ compatible with the action $g : V \to V$. Let $\mathcal{E}$ be the sheaf of local sections of E. Then we have the formula (cf. [TH])

Theorem 1.2.5

$$tr(g : H^*(V, \mathcal{E})) := \sum_{d=0}^{dimV} (-1)^d tr(g : H^d(V, \mathcal{E})) = \sum_{x \in V^g} \frac{tr(g : E_x)}{det(1 - g^{-1} : T_x)} \quad (1.7)$$

where T_x is the tangent space at x and E_x is the fiber of vector bundle over x.

We apply the localization formula to calculate the characters of group codes

on the modular curve $Y(\ell)$. Let us assume that $g \in PSL_2(\mathbb{F}_\ell)$ has isolated fixed points and $Y(\ell)^g$ is the set of these fixed points. Let D be a g invariant divisor and $\mathcal{L}_D$ be the line bundle associated with D. The quantity $tr(g : L_x)$ is the trace of g on the linear space L_x, fiber of the linear bundle over x, and $tr(g : T_x^*)$ is the trace of g on the dual of the tangent space T_x. The action of g on both spaces L_x and T_x^* is multiplication by some root of unity since these spaces are of dimension 1. The action of g on L_x is multiplication by a complex number, say ζ_x and the action of g on the dual space T_x^* is also multiplication by a complex number say η_x. In our case, the localization formula can be given as

$$\begin{aligned} tr(g : H^0(Y(\ell), \mathcal{L}_D)) - tr(g : H^1(Y(\ell), \mathcal{L}_D)) &= \sum_{x \in Y(\ell)^g} \frac{tr(g : L_x)}{1 - tr(g : T_x^*)} \\ &= \sum_{x \in Y(\ell)^g} \frac{\zeta_x}{1 - \eta_x}. \end{aligned} \tag{1.8}$$

Moreover, we give an example by considering the canonical divisor and we have described the characters of the corresponding modular code. It turns out that the multiplicities of irreducible components of code C depends on the class number $h(-\ell)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$. The characters of group elements having nontrivial fixed points on the regular differentials Ω are given. Let s, h and e_1^+ be the generators of the stabilizers of the elliptic points of order 2, 3 and the point ∞ of $Y(1)$ respectively. e_ω^+ is an element of the group generated by e_1^+ in $PSL_2(\mathbb{F}_\ell)$ and not conjugate to e_1^+ in $PSL_2(\mathbb{F}_\ell)$. Then the traces of these elements are given as

Theorem 1.2.6

$$tr(s : \Omega) = 1 - \frac{1}{4}(\ell - \left(\frac{-1}{\ell}\right)),$$

$$tr(h : \Omega) = 1 - \frac{1}{3}(\ell - \left(\frac{-3}{\ell}\right)),$$

$$tr(e_1^+ : \Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \ mod\ 4, \\ \frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \ mod\ 4 \end{cases} \tag{1.9}$$

and

$$tr(e_\varepsilon^+ : \Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \ mod\ 4, \\ -\frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \ mod\ 4 \end{cases} \tag{1.10}$$

where $\ell > 3$ is a prime, $h(-\ell)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-\ell})$ and $\left(\frac{*}{\ell}\right)$ is the Legendre symbol.

All the other group elements which are not conjugate any of h, s, e_1^+ and e_ϵ^+ have trace equal to 1.

We calculated the multiplicities of the irreducible representations in Ω. The multiplicities are given in the following:

Theorem 1.2.7 *Let $\chi = \chi_\rho$ be the character of a nontrivial irreducible representation ρ of $SL_2(\ell)$ which is trivial at -1. The multiplicity m_χ of ρ in Ω is given as*

$$m_\chi = \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) + \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] \qquad (1.11)$$

when $\ell \equiv 1 \bmod 4$ and

$$\begin{aligned} m_\chi &= \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) \\ &+ \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] + \frac{1}{2\ell}h(-\ell)\sqrt{(}-\ell)[\bar{\chi}(e_1^+) - \bar{\chi}(e_\epsilon^+)] \end{aligned} \qquad (1.12)$$

when $\ell \equiv 3 \bmod 4$. Here $\bar{\chi}$ is the complex conjugation of χ and $h(-\ell)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

The multiplicity is 0 for trivial representation.

We further make a discussion on how to calculate the characters of the code space associated to arbitrary $PSL_2(\mathbb{F}_\ell)$ invariant divisor.

1.3 List of Notation:

$X_0(N)$: The affine modular curve which is moduli space of triples (E, E', ϕ) where $\phi : E \longmapsto E'$ is a cyclic isogeny of degree N between elliptic curves E and E'

$Y_0(N)$: Projective Closure of $X_0(N)$

$Z_0(N) = \pi(X_0(N))$: Affine plane model of $X_0(N)$

$\overline{Z_0(N)}$: Projective closure of $Z_0(N)$

$X(N)$: The modular curve which is moduli space of the pairs (E, α_N), E is an elliptic curve and α_N is a structure of level N with determinant $\det \alpha_N = 1$

$Y(N)$: Projective closure of $X(N)$

$\Phi_N(X, Y)$: Modular polynomial of level N.

$\mathbb{F}_q$: Finite field of order q.

$SL(2, \mathbb{Z}/N\mathbb{Z})$: The set of 2 by 2 matrices of determinant 1, whose entries are elements of the ring $\mathbb{Z}/N\mathbb{Z}$

$SL_2(\mathbb{F}_\ell)$: The set of 2 by 2 matrices of determinant 1, whose entries are elements of the finite field $\mathbb{F}_\ell$.

$PSL(2, \mathbb{Z}/N\mathbb{Z})$: The quotient group of $SL(2, \mathbb{Z}/N\mathbb{Z})$ by its center

$GL(2, \mathbb{Z}/N\mathbb{Z})$: The set of 2 by 2 nonsingular matrices whose entries are elements of the ring $\mathbb{Z}/N\mathbb{Z}$

$\mathbb{C}$: Complex numbers

$\mathbb{H}$: Upper half plane of complex numbers

$\mathbb{R}$: Real numbers

$\mathbb{Z}$: Rational integers

$\mathbb{Q}$: Rational numbers

$[n, k, d]_q$: Code over $\mathbb{F}_q$ with parameters n, k, d

$(X, \mathcal{P}, D)_\Omega$: Goppa code on the curve X with parameters $\mathcal{P}, D$ associated to Ω construction.

$(X, \mathcal{P}, D)_L$: Goppa code on the curve X with parameters $\mathcal{P}, D$ associated to L construction.

$[G : S]$: Index of subgroup S in G

H_q: Entropy function

Chapter 2

Algebraic Geometric Codes

In this chapter, we have explained the importance of curves with many rational points in coding theory. Under some conditions, the asymptotic parameters of Goppa codes constructed on curves with maximum number of rational points are known to be the best so far. We have introduced the linear codes and explained about their parameters. By a code, we always mean a linear code. In the second section, we give an example of Goppa construction on curves and evaluate the performance of the parameters of Geometric Goppa codes in the last section.

2.1 Linear Codes, Parameters

A linear error correcting block code or simply a linear code C over a finite field $\mathbb{F}_q$ is a linear subspace of the vector space $\mathbb{F}_q^n = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$. Any element $x \in C$ is called a *code word*. By abuse of terminology, we always mean linear code by code. Let us introduce a metric on $\mathbb{F}_q^n$ as

$$d(x, y) = \#\{i : x_i \neq y_i\}$$

where $x = (x_1, ..., x_n)$ and $y = (y_1, ...y_n) \in \mathbb{F}_q^n$. This metric is called as *Hamming Distance*. The Hamming Weight of a vector $x \in \mathbb{F}_q^n$ is its Hamming distance to the origin and denoted by $||x||$.

Let us define the minimum Hamming weight of nonzero code words:

$$d = \min_{x \in C, x \neq 0} ||x||.$$

The parameter d is called the minimum distance of the code C. Then the parameters of a code C is given as $[n, k, d]_q$ where n is the block length and k is the dimension of C.

An $[n, k, d]_q$ code has two more parameters, its *information rate* and its *relative minimum distance*. The former is $R = \frac{k}{n}$ and indicates how much information a code word carries. The latter one is $\delta = \frac{d}{n}$ and measures the error correction ability of the code.

Any matrix whose rows form a basis for an $[n, k, d]_q$ linear code C is called a *generator matrix* of C. The encoding process is an injective linear transformation

$$\phi : \mathbb{F}^k \longrightarrow \mathbb{F}_q^n$$

whose image is C. If G is a generator matrix then

$$\phi : \mathbb{F}^k \longrightarrow \mathbb{F}_q^n$$

$$x \mapsto x \cdot G$$

is an example of encoding process. Then, each vector in $\mathbb{F}_q^k$ is encoded to a code word in $\mathbb{F}_q^n$. Let us assume that these code words are transmitted via a noisy channel where some of the coordinates of code words may be changed. On the other edge of the channel, we may receive some distorted vectors $x' \in \mathbb{F}_q^n$. If the number of distorted coordinates of a code word x is not more than the integer part of $\frac{d-1}{2}$ then we can recover x from x' by searching the closest code word of C to x' which is uniquely given as x. This process is called decoding and explains the role of notion of minimum distance of a code. If there are more than $\frac{d-1}{2}$ distorted coordinates then the closest code word to the distorted vector x' will not be x. In this case the decoding process fails and this case is called as incorrect decoding.

2.1.1 Asymptotically Good Codes

Roughly interpreting, a good $[n, k, d]_q$ code should have large relative minimum distance $\delta = d/n$ and information rate $R = k/n$. Let us define the set

$$V_q = \{(\delta, R) \in [0,1] \times [0,1] : \exists \text{ an } [n,k,d]_q \text{ code with } \frac{d}{n} = \delta, \frac{k}{n} = R\}.$$

It is well known by Shannon's channel coding theorem that (see [SHA]) for any noisy channel there exist codes for which the probability of incorrect decoding of a received code word is as small as we want. Such good codes have very large block lengths. Therefore, we should be interested in relative minimum distances and information rates of codes of large block lengths. So, let us take the limit points of V_q and denote U_q as the set of these limit points. That is, $(\delta, R) \in U_q$ if and only if there exists an infinite sequence of distinct $[n_i, k_i, d_i]_q$ codes with $\delta_i = \frac{d_i}{n_i}$, different from δ $\forall i$, $R_i = \frac{k_i}{n_i}$, different from R $\forall i$ such that

$$\lim_{i \to \infty} (\delta_i, R_i) = (\delta, R).$$

For $(\delta, R) \in U_q$, if both δ and R are nonzero then the family of codes having parameters (δ_i, R_i) tending to (δ, R) are called asymptotically good codes. Let

$$\alpha_q(\delta) = \sup\{R : (\delta, R) \in U_q\}.$$

That is, $\alpha_q(\delta)$ is the maximum possible information rate among those of all very long codes with relative minimum distance δ.

The function $\alpha_q(\delta)$ is unknown. Even, there is only few information derived about it so far. It is one of the main problems of coding theory to discover $\alpha_q(\delta)$. A powerful result by Aoaltonen (see [AAL]) states that $\alpha_q(\delta)$ is a continuous decreasing function which vanishes on the interval $(\frac{q-1}{q}, 1)$. A very common approach for providing information about $\alpha_q(\delta)$ is to find upper and lower bounds for it. The lower bounds are all constructive and obtained by introducing an example of family of codes. one of the most important lower bound is Gilbert-Varshamov bound which is given as

$$\alpha_q(\delta) \geq 1 - H_q(\delta) \tag{2.1}$$

where H_q is the q-ary entropy function

$$H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), H(0) := 0.$$

This bound was not improved until the algebraic-geometric codes were introduced. Tsfasman, Vladuţ and Zink have been given an example of codes constructed on classical modular curves whose parameters lie on the line $R = 1-\delta-1/(\sqrt{(}q)-1)$ when $q \geq 49$ is a square of a prime (cf. [TS-VLA-ZI]). This line is obviously better than the Gilbert Varshamov bound in the interval (δ_1, δ_2) where δ_1 and δ_2 are intersection points of $1-H_q(\delta)$ and $1-\delta-1/(\sqrt{(}q)-1)$. Due to this crucial development, the algebraic geometric codes have attracted the attention of coding theory world.

2.2 Goppa Codes on Curves

Let X be a projective smooth curve of genus g defined over $\mathbb{F}_q$ and $\mathcal{P} = \{P_1, ..., P_n\} \subseteq X(\mathbb{F}_q)$, $|\mathcal{P}| = n$, $D \in Div(X)$ is a $\mathbb{F}_q$ rational divisor. Let $suppD \cap \mathcal{P} = \emptyset$ and $D_o = P_1 + \cdots + P_n \in Div(X)$. Assume $\deg D = a > 2g-2$. Consider the space of rational differential forms

$$\Omega(D_o - D) = \{\omega \in \Omega(X)^* : div(\omega) + D_0 - D \geq 0\} \cup \{0\}.$$

If ω is defined over $\mathbb{F}_q$ then for a point $P \in X(\mathbb{F}_q)$ we have the residue $Res_P(\omega) \in \mathbb{F}_q$. The map

$$Res_{\mathcal{P}} : \Omega(D_o - D) \longrightarrow \mathbb{F}_q^n$$

$$Res_{\mathcal{P}} : \omega \mapsto (Res_{P_1}(\omega), ..., Res_{P_n}(\omega))$$

defines a code $C = Res_{\mathcal{P}}(\Omega(D_o - D))$. We call this algebraic geometric construction a Geometric Goppa construction, or simply a Goppa construction on curves (see [GO 1] or [GO 2]). We denote $C = (X, \mathcal{P}, D)_\Omega$. The following statement explains the parameters of such construction:

Proposition 2.2.1 *Let X be a smooth projective curve of genus g defined over $\mathbb{F}_q$ and C be a $(X, \mathcal{P}, D)_\Omega$ construction. Assume $suppD \cap \mathcal{P} = \emptyset$ and $degD = a >$*

$2g-2$. *Then parameters of* C *are given as*

$$k \geq n - a + g - 1$$

$$d \geq a - 2g + 2$$

Proof: Let us define the divisor $D_o = P_1 + \cdots + P_n \in Div(X)$. Let K be a canonical divisor on X. Then the space $\Omega(D_o - D) = \{\omega \in \Omega(X)^* : div(\omega)+D_0-D \geq 0\}\cup\{0\}$ is isomorphic to the space of functions $L(D_o+K-D) = \{f \in \overline{\mathbb{F}_q}(X)^* : div(f) + D_o + K - D \geq 0\} \cup \{0\}$. By Riemann Roch theorem the dimension of $L(D_o + K - D)$ is at least $n - a + g - 1$. On the other hand $\deg D = a > 2g-2$ and hence any nonzero $\omega \in \Omega(D_o - D)$ has overall more than $2g-2$ zeros counted with multiplicities outside the support of the divisor D_o. So, ω must have some simple poles on some points $P_1, ..., P_n$. Therefore the residue map

$$Res_{\mathcal{P}} : \Omega(D_o - D) \longrightarrow \mathbb{F}_q^n$$

$$Res_{\mathcal{P}} : \omega \mapsto (Res_{P_1}(\omega), ..., Res_{P_n}(\omega))$$

is embedding. Hence the dimension of C is at least $n - a + g - 1$. Similarly any nonzero $\omega \in \Omega(D_o - D)$ must have at least $a - 2g + 2$ poles outside the support of D. So, the minimum distance d is at least $a - 2g + 2$

QED

The construction above is known as the Ω construction. It is based on some space of differentials. There is another type of construction, L construction, which is essentially equivalent to Ω construction. This one is based on some spaces of rational functions of curves. Let X be a projective smooth curve of genus g defined over $\mathbb{F}_q$ and $\mathcal{P} = \{P_1, ..., P_n\} \subseteq X(\mathbb{F}_q)$, $|\mathcal{P}| = n$, $D \in Div(X)$ is a $\mathbb{F}_q$ rational divisor. Let $supp D \cap \mathcal{P} = \emptyset$.

The L construction is as follows. Consider the map

$$Ev_{\mathcal{P}} : L(D) \longrightarrow \mathbb{F}_q^n,$$

$$Ev_{\mathcal{P}} : f \mapsto (f(P_1), ..., f(P_n))$$

where the space $L(D)$ is given as

$$L(D) = \{f \in \bar{\mathbb{F}}_q(X)^* : div(f) + D \geq 0\} \cup \{0\}.$$

Then, we get a code $C = Ev_{\mathcal{P}}(L(D))$. This construction is known as L construction and the code C is denoted as $C = (X, \mathcal{P}, D)_L$.

2.2.0.1 Linear codes as projective systems

A linear $[n, k, d]_q$ nondegenerate code C is a configuration $\mathcal{P}$ of points of a projective space $\mathbb{P}(V)$ where V is a vector space of dimension k over $\mathbb{F}_q$. A configuration is a finite unordered family in a projective space. Then, $|\mathcal{P}| = n$ and $d = n - \max|\mathcal{P} \cap H|$ where the maximum being taken over all projective hyperplanes $H \subset \mathbb{P}(V)$. Let V^* be the dual space of V. Consider the map $\varphi : V^* \to \mathbb{F}_q^n$ defined by $\varphi(f) = (f(P_1), ..., f(P_n))$ where $f \in V^*$ and P_i's are points of $\mathcal{P}$. Then the code C is, as a linear space, the image of φ in $\mathbb{F}_q^n$.

Geometric Goppa codes have a natural interpretation as a configuration in a projective space. Let X be a variety. Assume that there is an embedding $X \subseteq \mathbb{P}^k$. Let $\mathcal{P}$ be a configuration whose points are in $X(\mathbb{F}_q)$ such that $|\mathcal{P}| > k$. Assume that $\mathcal{P}$ does not lie in a hyperplane. Then the configuration $\mathcal{P}$ is a Goppa $[n, k, d]_q$ code on X.

2.3 Drinfeld-Vladuţ Bound

In the previous section, we have seen an example of code construction on curves. If X is a smooth projective curve of genus g defined over $\mathbb{F}_q$ then any Goppa code on X will have dimension greater then or equal to $n - a + g - 1$ and and minimum distance greater then or equal to $a - 2g + 2$ where a is an integer bigger then the dimension of regular differential forms on X and n is the number of $\mathbb{F}_q$ rational points of X. The critical bounds $n - a + g - 1$ and $a - 2g + 2$ are called the designed dimension and the designed minimum distance respectively. If we have the family of curves of same genus, say g and the family of Goppa codes

constructed on this family of curves, it is evident that the designed dimension increases when the number of rational points of curves in the family increases whereas the designed minimum distance remains unchanged. So, the best Goppa code on curves of same genus g is the code constructed on a curve having maximal number of $\mathbb{F}_q$ rational points. The crucial question is whether such best Goppa codes have parameters lying above the Gilbert-Varshamov bound. The answer is yes. So, there exists Goppa codes having better parameters than the codes lying on Gilbert-Varshamov bound.

So, curves over a field $\mathbb{F}_q$ that have big number of rational points have great importance in coding theory. For a given family of the curves X_α over $\mathbb{F}_q$ we have the Drinfeld-Vladuţ bound:

Theorem 2.3.1 [VLA-DR] *Let X_α be smooth curves of genus g_{X_α} over the finite field $\mathbb{F}_q$. Then*

$$\limsup_{g_{X_\alpha}\to\infty} \frac{|X_\alpha(\mathbb{F}_q)|}{g_{X_\alpha}} \leq \sqrt{q} - 1.$$

It is one of the main research area in coding theory to search for the family of curves X_α over a finite field $\mathbb{F}_q$ such that $\frac{|X_\alpha(\mathbb{F}_q)|}{g_{X_\alpha}}$ is very close to the Drinfeld-Vladuţ bound for very large genus g_{X_α} since the Goppa codes on such family of curves having plenty of rational points over $\mathbb{F}_q$, have nice parameters. Indeed, the best family of curves are those which achieves the Drinfeld-Vladuţ bound. It has been a difficult problem to construct such family of curves. For a square order q, the bound is sharp. It is known three constructions of such family of curves attaining Drinfeld - Vladuţ bound: Classical modular curves, Drinfeld modular curves (see [TS-VLA] for these two curves) and the tower of Artin-Schreier extensions (see [GA-STI]). It is still unknown whether Drinfeld - Vladuţ bound is sharp for nonsquare order q.

Corollary 2.3.1 *Let X_α be smooth curves of genus g_{X_α} over the finite field $\mathbb{F}_q$ attaining the Drinfeld-Vladuţ bound. Let C_α be a $(X_\alpha, \mathcal{P}_\alpha, D_\alpha)_\Omega$ construction where $\mathcal{P}_\alpha$ is the set of $\mathbb{F}_q$ rational points of X_α . Then the parameters of the family of codes C_α lies on the line $R = 1 - \delta - 1/(\sqrt{(}q) - 1)$.*

Proof: The parameters of the codes C_α are given as $n_\alpha - a_\alpha + g_\alpha - 1$ and $a_\alpha - 2g_\alpha - 2$ as designed dimensions and designed minimum distances respectively. So, their designed relative distances are

$$\delta_\alpha = \frac{a_\alpha}{n_\alpha} - 2\frac{g_\alpha}{n_\alpha} - \frac{2}{n_\alpha} \tag{2.2}$$

and similarly, designed information rates are

$$R_\alpha = 1 - \frac{a_\alpha}{n_\alpha} + \frac{g_\alpha}{n_\alpha} - \frac{1}{n_\alpha}. \tag{2.3}$$

So, if we combine these two equations by replacing a_α's we get the equation

$$R_\alpha = 1 + \frac{1}{n_\alpha} - \frac{g_\alpha}{n_\alpha} - \delta_\alpha. \tag{2.4}$$

When g_α tends to infinity, the ratio $\frac{g_\alpha}{n_\alpha}$ will tend to the inverse of the Drinfeld-Vladuţ bound, $\frac{1}{\sqrt{q}-1}$ by the assumption. Therefore the parameters $(R_\alpha, \delta_\alpha)$ of the Goppa codes C_α will tend to the point (R, δ) satisfying $R = 1 - \delta - 1/(\sqrt{(}q) - 1)$.

QED

This important corollary of the Drinfeld- Vladuţ theorem shows that the codes on the family of curves having maximum number rational points have parameters better than the parameters of the codes lying on Gilbert-Varshamov bound. So, if there exists maximal curves then, there exists better codes than the codes on Gilbert Varshamov bound. Actually, there exist codes attaining Drinfeld-Vladuţ bound over the field of order q where q is a square.

Chapter 3

Elliptic Curves and Modular Curves

In this chapter, we have introduced fundamental properties of elliptic curves and modular curves. The scope of the subject is extremely wide but we have generally selected the facts we have used in our statements.

3.1 Elliptic Curves

Definition 1 An elliptic curve defined over a field k is a pair (E, O), where E is a nonsingular curve over k of genus 1 and $O \in E(k)$.

Given an elliptic curve E (we write just E, always remembering O) over algebraical closed field k, we can induce a group operation on E as follows: By Riemann-Roch theorem the map $\phi : E \to \mathrm{Pic}^0(E)$ (Picard group of E) given by $\phi(x) = (x) - (O)$ is a bijection. $\mathrm{Pic}^0(E)$ is a group, hence E is also a group with identity element O, and one can define the group operation as

$x_1 + x_2 = x_3$ if the divisor $(x_1) + (x_2) - (x_3) \sim (O)$ (that is, the divisors $(x_1) + (x_2) - (x_3)$ and (O) are in the same class) for $x_1, x_2, x_3 \in E$.

Again, by Riemann-Roch theorem dim$L(nO)$:=dim$\{f \in k(E) : div(f) + n(O) \geq 0\} = n$, $n \geq 1$. Hence $\exists x \in L(2O) \setminus L(O), y \in L(3O) \setminus L(2O)$. $1, x, y, xy, x^2, x^3, y^2 \in L(6O)$ and hence linearly dependent since dim$L(6O) = 6$. So

$y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3$ where $a_i, b_j \in k$. We can take coefficients of y^2 and x^3 to be 1 since $y^2, x^3 \in L(6O) \setminus L(5O)$. If char$k \neq 2, 3$ with appropriate linear change of variable we get cubic equation

$$y^2 = 4x^3 - g_2x - g_3; g_2, g_3 \in k$$

which is called Weierstrass form of elliptic curve. Also, any cubic equation in Weierstrass form in characteristic not 2 or 3 is an elliptic curve, taking ∞, which corresponds to the point $[x : y : z] = [0 : 1 : 0]$ satisfying the Weierstrass equation $y^2z = 4x^3 - g_2xz^2 - g_3z^3$ in the projective space, as identity element. Then, sum of three points satisfying the given cubic equation is zero if and only if they are collinear (By Bezout Theorem, a curve given by cubic equation intersects a line at three points).

3.1.1 j Invariant of Elliptic Curves

Let E: $y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve over a field k. Then, E is nonsingular, hence the polynomial $4x^3 - g_2x - g_3$ has distinct roots in k. That is, the discriminant,

$$\triangle := g_2^3 - 27g_3^2 \neq 0$$

Define $j(E) := 1728\frac{g_2^3}{\triangle}$. Let $E : y^2 = 4x^3 - g_2x - g_3$ and $E' : y^2 = 4x^3 - g_2'x - g_3'$ be two elliptic curves over a field k. Then E and E' are said to be isomorphic over k if $\exists$ a nonzero $c \in k$ such that $g_2' = c^4g_2$ and $g_3' = c^6g_3$ and such a $c \in k$ is said to be isomorphism. If k is algebraical closed then it is easy to check that $E \simeq E'$ (E is isomorphic to E') means exactly $j(E) = j(E')$.

Let $E : y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve over $\mathbb{C}$. Then the solutions $g_2 = c^4g_2$ and $g_3 = c^6g_3$ for $c \in \mathbb{C}$ (automorphisms of E) is $\{\pm 1\}$ for $g_2 \neq 0$ and $g_2 \neq 0$. If $g_2 = 0$ then the solution set for c is $\{\pm 1, \pm\omega, \pm\omega^2\}$ where ω is

the cubic root of unity, $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, and if $g_3 = 0$ then the solution set for c is $\{\pm 1, \pm i\}$. Hence, for E with $j(E) = 1728$, $\mathrm{Aut}(E) = \{\pm 1, \pm i\}$; for E with $j(E) = 0$, $\mathrm{Aut}(E) = \{\pm 1, \pm\omega, \pm\omega^2\}$. For any other elliptic curve E over $\mathbb{C}$ whose j-invariant different from 0 or 1728, $\mathrm{Aut}(E) = \{\pm 1\}$.

3.1.2 Isogenies

An isogeny between two elliptic curves is on one hand a morphism of varieties and on the other hand group homomorphism. Here is the formal definition:

Definition 2 Let E and E' be elliptic curves over a field k with identity elements O and O' respectively. Then, an isogeny between E and E' is a morphism

$$\phi : E \longrightarrow E'$$

satisfying $\phi(O) = O'$. Also, E and E' are said to be isogenous if there exists a non constant isogeny between them.

Since an isogeny is a morphism between curves, if it is not constant then it is a finite map (ie, onto map and inverse image of any point is a finite set). As usual, trivial isogeny, $[0](P) = O' \ \ \forall P \in E$, has degree

$$\deg[0] := 0$$

and any other isogeny $\phi \ : E \to E'$ different than [0] has degree

$$\deg\phi := [k(E) : \phi^* k(E')] = \sum_{\phi(P)=O'} e(P)$$

where

$$\phi^* : k(E') \longrightarrow k(E)$$
$$f \longrightarrow f \circ \phi$$

and $e(P)$ is ramification index of $P \in E$.

We say that ϕ is separable, inseparable or purely inseparable if the extension $k(E)$ over $\phi^*k(E')$ is separable, inseparable or purely inseparable extension respectively.

The most important property of isogenies is that they are group homomorphisms:

Theorem 3.1.1 *Let $\phi : E \to E'$ be an isogeny. Then,*

$$\phi(P+Q) = \phi(P) + \phi(Q), \quad \forall P, Q \in E$$

Proof: Trivially, $\phi = [0]$ is a group homomorphism. So, let's assume ϕ is a finite map. Let's define

$$\phi_* : \mathrm{Pic}^0(E) \longrightarrow \mathrm{Pic}^0(E')$$

$$\phi_*(\sum n_i(P_i)) = \sum n_i(\phi(P_i)).$$

Obviously, ϕ_* is a group homomorphism. But, $\mathrm{Pic}^0(E)$ is isomorphic to E and $\mathrm{Pic}^0(E')$ is isomorphic to E' as group isomorphism.

Let

$$\kappa : E \longrightarrow \mathrm{Pic}^0(E),$$

$$P \longrightarrow (P) - (O)$$

and

$$\kappa'^{-1} : \mathrm{Pic}^0(E') \longrightarrow E'$$

$$\sum n_i(P_i) \longrightarrow \sum n_i P_i$$

be isomorphisms. Then

$$\phi = \kappa'^{-1} \circ \phi_* \circ \kappa$$

and hence

$$\phi(P+Q) = \kappa'^{-1} \circ \phi_* \circ \kappa(P+Q) = \kappa'^{-1} \circ \phi_* \circ \kappa(P) + \kappa'^{-1} \circ \phi_* \circ \kappa(Q)$$

since κ'^{-1}, ϕ_* and κ are group homomorphisms.

QED

Let $\mathrm{Hom}(E, E') = \{\text{isogenies } \phi : E \to E'\}$. Then $\mathrm{Hom}(E, E')$ is a group under addition law. If $E = E'$ then, $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring with multiplication given by composition. Automorphisms of E, denoted by $\mathrm{Aut}(E)$, are invertible elements of End$E$. Recall that, for an elliptic curve E over $\mathbb{C}$ we have

$$\mathrm{Aut}(E) = \begin{cases} \{\pm 1, \pm i\} & \text{if } j(E) = 1728, \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } j(E) = 0, \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

For any $m \in \mathbb{Z}$, we can define multiplication by m:

$$[m] : E \longrightarrow E$$

$$[m](P) = P + \cdots + P \text{ (m terms), for } m > 0$$

and

$$[m](P) = [-m](-P) \text{ for } m < 0.$$

It is easy to check by induction that multiplication by $m \in \mathbb{Z}$ is an isogeny. For $m \neq 0$, $[m]$ is a non constant map. Here is the precise statement:

Proposition 3.1.1 [SIL 1, pp 72] *Let E and E' be elliptic curves over a field k, and $m \in \mathbb{Z}$, $m \neq 0$. Then*

a) $[m] : E \to E$ is a finite map.

b) Hom(E, E') is a torsion free $\mathbb{Z}$ - module.

c) End(E) is an integral domain of characteristic 0.

Given elliptic curves E and E' over a field k, the sets $\mathrm{Hom}(E, E')$ and $\mathrm{Hom}(E', E)$ are related by the following theorem:

Theorem 3.1.2 [SIL 1, pp 84] *Let $\phi : E \to E'$ be a non constant isogeny of degree m. Then, there exists a unique isogeny*

$$\widehat{\phi} : E \longrightarrow E'$$

satisfying $\widehat{\phi} \circ \phi = [m] \in End(E)$ and $\phi \circ \widehat{\phi} = [m] \in End(E')$

Definition 3 $\widehat{\phi}$ in the above theorem is called the dual isogeny of ϕ.

Proposition 3.1.2 [SIL 1, pp 87] *Let $\phi \in End(E, E')$ be a non constant isogeny. Then duality of isogenies has the following properties:*

i) $deg\widehat{\phi} = deg\phi$

ii) $\widehat{\widehat{\phi}} = \phi$

iii) Let $\varphi \in (E', E'')$ be another non constant isogeny. Then

$$\widehat{\varphi \circ \phi} = \widehat{\phi} \circ \widehat{\varphi}$$

iv $\widehat{[m]} = [m]$ and $deg[m] = m^2$ $\forall m \in \mathbb{Z}$

Let $\phi \in \mathrm{Hom}(E, E')$, $\phi \neq [0]$. Then $\ker\phi$ is a finite subgroup of E. It is finite since ϕ is a finite map and it is a subgroup since ϕ is a group homomorphism. For a given elliptic curve E, there is a one to one correspondence between finite subgroups of E and elliptic curves E', isogenous to E. That is:

Proposition 3.1.3 [SIL 1, pp 78] *Let E be an elliptic curve and Φ be a finite subgroup of E. Then there is a unique elliptic curve E' and a separable isogeny $\phi : E \to E'$ such that*

$$ker\phi = \Phi$$

3.1.3 Elliptic Curves Over Complex Field and Lattices:

Let $\mathbb{H} = \{z : \text{im}z > 0\}$. A lattice L in $\mathbb{C}$ is a subgroup of $\mathbb{C}$ under addition law which is free $\mathbb{Z}$ - Module of dimension 2 and generates $\mathbb{C}$ over reals. We write $L = [\omega_1, \omega_2]$ if ω_1, ω_2 is a basis of the lattice L. We always assume that $\frac{\omega_1}{\omega_2} \in \mathbb{H}$. Because, otherwise $\frac{\omega_2}{\omega_1} \in \mathbb{H}$ and we can write $L = [\omega_2, \omega_1]$.

Let $L = [\omega_1, \omega_2]$ be a lattice. Then the quotient space $\mathbb{C}/L$ is homeomorphic to a torus and elements of $\mathbb{C}/L$ are uniquely represented in the fundamental parallelogram

$$\sqcap := \{\alpha\omega_1 + \beta\omega_2 : 0 \leq \alpha, \beta < 1\}.$$

Define the Weierstrass function

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Then,

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

The Weierstrass function and its derivative $\wp$ and $\wp'$ are rational functions of $\mathbb{C}/L$. That is:

Proposition 3.1.4 [KO] *$\wp(z)$, $\wp'(z) \in k(\mathbb{C}/L)$ and the map $\psi : \sqcap \to E \cup \infty$ given by*

$$\psi(z) = [\wp(z) : \wp'(z) : 1] \text{ for } z \neq 0 \text{ and } \psi(0) = [0 : 1 : 0].$$

is analytic bijection, where $\sqcap$ is fundamental parallelogram of L and $E : y^2 = 4x^3 - g_2x - g_3$, $g_2 = 60 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^4}$, $g_3 = 140 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^6}$.

So, a lattice corresponds to an elliptic curve over $\mathbb{C}$. Converse is also true:

Proposition 3.1.5 [LA 2, pp 39] *Let $E : y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve. Then, $\exists$ a lattice L such that $g_2 = 60\sum_{\omega\in L-\{0\}} \frac{1}{\omega^4}$ and $g_3 = 140\sum_{\omega\in L-\{0\}} \frac{1}{\omega^6}$.*

Let L be a lattice and $g_2 = 60\sum_{\omega\in L-\{0\}} \frac{1}{\omega^4}$, $g_3 = 140\sum_{\omega\in L-\{0\}} \frac{1}{\omega^6}$. The torus represented by the quotient space $\mathbb{C}/L$ is a group and for $z_1, z_2, z_3 \in \sqcap$, fundamental domain of $\mathbb{C}/L$, we have $z_1 + z_2 + z_3 = 0$ if and only if $z_1 + z_2 + z_3 \in L$. Hopefully, this is also equivalent to saying that the points $(\wp(z_1), \wp'(z_1))$, $(\wp(z_2), \wp'(z_2))$ and $(\wp(z_3), \wp'(z_3))$ on the elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$ are collinear. For more detail and the proof, one can refer to, for instance, Koblitz's book on Elliptic curves and Modular forms [KO].

Now, we know that there is a one to one correspondence between elliptic curves over $\mathbb{C}$ and lattices. We define two lattices L, L' to be proportional if $L = \lambda L'$ for some $\lambda \in \mathbb{C}^*$. Then, the elliptic curves over $\mathbb{C}$ determined by proportional lattices are isomorphic. Precisely

Proposition 3.1.6 [CO, pp 207] *Let $E : y^2 = 4x^3 - g_2x - g_3$ and $E' : y^2 = 4x^3 - g_2'x - g_3'$ be two elliptic curves over $\mathbb{C}$ and L, L' be corresponding lattices. Then, $E \simeq E'$ if and only if $L = \lambda L', \lambda \in \mathbb{C}^*$.*

Then, for a lattice L we can define $j(L) := j(E)$ where $E \cup \infty \simeq \mathbb{C}/L$ (from now on, I will skip the point of E at ∞). Let $L = [\omega_1, \omega_2]$. Then $\frac{1}{\omega_2}L = [\frac{\omega_1}{\omega_2}, 1]$ is proportional to L. Let's denote $\tau = \frac{\omega_1}{\omega_2}$ and then $j(L) = j(\frac{1}{\omega_2}L) = j([\tau, 1])$. Besides considering j as a function of lattices, we may suppose also j as a function on upper half plane, defined as

$$j(\tau) := j([\tau, 1]).$$

Here is an important property of j function:

Proposition 3.1.7 [KO] $j : \mathbb{H} \to \mathbb{C}$, $j(\tau) = j([\tau, 1])$ *is an analytic function and it has a simple pole at ∞.*

And the following lemma is about zeros of derivative of j function:

Lemma 3.1.1 [CO, pp 221] *For $z \in \mathbb{H}$, $j'(z) \neq 0$ except the following cases*

a) $z = \frac{ai+b}{ci+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $j'(z) = 0$, but $j''(z) \neq 0$.

b) $z = \frac{a\omega+b}{c\omega+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $j'(z) = 0$ and $j''(z) = 0$ but $j'''(z) \neq 0$.

Let $j(z) = j(z')$ $z, z' \in \mathbb{H}$. Then $\exists \lambda \in \mathbb{C}^*$ satisfying $\lambda[z', 1] = [z, 1]$. Hence $\exists \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}; ad - bc = 1 \right\}$ such that.

$$\lambda z' = az + b \text{ and } \lambda = cz + d.$$

Because both $\{z, 1\}$ and $\{\lambda z, \lambda\}$ are the basis for the lattice $L = [z, 1]$. Then, we get $z' = \frac{az+b}{cz+d}$

Conversely, let $z' = \frac{az+b}{cz+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then, let $\lambda = cz + d$. So,

$$\lambda z' = az + b \text{ and } \lambda = cz + d.$$

Hence $\lambda[z', 1] = [z, 1]$ which implies that $j(z) = j(z')$. In conclusion, we get that $j(z) = j(z')$ means $z' = \frac{az+b}{cz+d}$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

An isogeny between two elliptic curves E, E' over $\mathbb{C}$ is an analytic isomorphism of corresponding toruses. Because, for $\phi \in \mathrm{Hom}(E, E')$ $\exists \lambda$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\lambda} & \mathbb{C}/L' \\ \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & E' \end{array}$$

where L and L' are the lattices corresponding to E and E' respectively and the vertical maps are isomorphisms. Converse is also true. Hence $\mathrm{Hom}(E, E')$ is set of analytic homomorphisms from $\mathbb{C}/L$ onto $\mathbb{C}/L'$. Indeed, those analytic homomorphisms can be represented as multiplication by complex numbers:

Theorem 3.1.3 *Let L, L' be two lattices in $\mathbb{C}$ and $\lambda : \mathbb{C}/L \to \mathbb{C}/L'$ be an analytic homomorphism. Then $\exists \alpha \in \mathbb{C}$ such that the following diagram commutative*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\alpha} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/L & \xrightarrow{\lambda} & \mathbb{C}/L' \end{array}$$

where the map α is multiplication by α and the vertical maps are canonical homomorphism.

Proof: λ is a homomorphism of fundamental parallelograms of L and L'. That is

$$\lambda(z_1 + z_2) \equiv \lambda(z_1) + \lambda(z_2) \ (\mathrm{mod} L'), z_1, z_2 \in \mathbb{C}.$$

For z_1, z_2 very close to 0, we have

$$\lambda(z_1 + z_2) = \lambda(z_1) + \lambda(z_2).$$

Since λ is analytic, it must be of the form $\lambda(z) = \alpha z$, for z very close to 0. For arbitrary $z \in \mathbb{C}$, we can write $\lambda(\frac{z}{n}) = \alpha\frac{z}{n}$ for enough large $n \in \mathbb{Z}$. Therefore, $\lambda(z) \equiv \alpha z \bmod L'$, $z \in \mathbb{C}$. Since $\lambda(L) \subset L'$ we get $\alpha L \subset L'$. Conversely, for any $\alpha \in \mathbb{C}$ satisfying $\alpha L \subset L'$, the map $\lambda(z) \equiv \alpha z \bmod L'$ is obviously an analytic homomorphism.

QED

For elliptic curves $E \simeq \mathbb{C}/L$ and $E' \simeq \mathbb{C}/L'$ we have $\mathrm{Hom}(E, E') = \{\alpha \in \mathbb{C} : \alpha L \subset L'\}$. Observe that for $\alpha \in \mathrm{Hom}(E, E')$, if $\alpha^{-1} \in \mathrm{Hom}(E', E)$, that is, $\alpha^{-1}L' \in L$ then α is an isomorphism and the lattices L, L' are proportional since $\alpha L = L'$.

3.1.3.1 Complex Multiplication

Let E be an elliptic curve over $\mathbb{C}$. We know that for any $m \in \mathbb{Z}$ the isogeny $[m]$, induced by multiplication by m, is in $\mathrm{End}(E)$. Hence, we always have $\mathbb{Z} \subseteq \mathrm{End}(E)$. For some elliptic curves we have $\mathrm{End}(E) = \mathbb{Z}$, on the other hand, for

some other elliptic curves we have proper inclusion, $\mathbb{Z} \subsetneq \mathrm{End}(E)$. For an elliptic curve E over $\mathbb{C}$ if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$ then E is said to have complex multiplication. Let $L = [\tau, 1]$ be a lattice in $\mathbb{C}$ and $E \simeq \mathbb{C}/L$. Assume E has CM (standing for complex multiplication). Then $\exists \alpha \in \mathrm{End}(E)$ where $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. $\alpha \in \mathrm{End}(E) \Rightarrow \alpha L \subset L$. So

$$\alpha\tau = a\tau + b \text{ and } \alpha = c\tau + d, \text{ where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

Then $\tau = \frac{b}{\alpha - a}$ and since $\tau \in H$, α is not real. Also, τ satisfies the equation $cx^2 + (d-a)x - b = 0$. Hence τ is algebraic number of order 2 and $\alpha = c\tau + d \in \mathbb{Q}(\tau)$. So, $\mathrm{End}(E)$ is a ring in the imaginary quadratic field $\mathbb{Q}(\tau)$.

In fact, for an elliptic curve E over $\mathbb{C}$, having CM, $\mathrm{End}(E)$ is nothing but an order in an imaginary quadratic field. So, first let me introduce some general facts about orders;

An order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d}), d \in \mathbb{Z}^+$, is a subring of K which is a free $\mathbb{Z}$ - module of rank 2. It follows that ring of integers $\mathcal{O}_K$ of K is an order. In fact, it is the maximal order in K (see [CO, pp 133]). Let d_K be the discriminant of K. It is well known fact in algebraic number theory that $\mathcal{O}_K = [1, \omega_K]$, where $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$. Any order $\mathcal{O}$ in K has a finite index in $\mathcal{O}_K$ since both $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$ - Modules of rank 2. Let $f := [\mathcal{O}_K : \mathcal{O}]$ for an order $\mathcal{O}$ in K. We have $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$ since $f\mathcal{O}_K \subset \mathcal{O}$. But $\mathbb{Z} + f\mathcal{O}_K$ also has index f in $\mathcal{O}_K$. Hence $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K]$. The index $f := [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of the order $\mathcal{O}$ and $D = f^2 d_K$ is called the discriminant of $\mathcal{O}$. Then, D determines $\mathcal{O}$ uniquely and any negative integer $D \equiv 0, 1 (\mathrm{mod}\ 4)$ is the discriminant of an order in an imaginary quadratic field.

For an ideal $\mathcal{I}$ in an order $\mathcal{O}$ in imaginary quadratic field K we have $\mathcal{O} \subset \{\alpha \in K : \alpha\mathcal{I} \subset \mathcal{I}\}$ A fractional ideal $\mathcal{J} = \beta\mathcal{I}$, $\beta \in K^*$, is said to be a proper fractional ideal if we have the equality $\mathcal{O} = \{\alpha \in K : \alpha\mathcal{J} \subset \mathcal{J}\}$. A fractional ideal $\mathcal{J}$ is invertible if there exists another fractional ideal $\mathcal{J}'$ satisfying $\mathcal{J}\mathcal{J}' = \mathcal{O}$. Then

Proposition 3.1.8 [CO, pp 135] *Let $\mathcal{O}$ be an order in an imaginary quadratic*

field K and let $\mathcal{J}$ be a fractional $\mathcal{O}$ - ideal. Then $\mathcal{J}$ is invertible if and only if $\mathcal{J}$ is proper.

So, set of proper ideals of an order $\mathcal{O}$ in K is a group under multiplication of ideals, denoted by $I(\mathcal{O})$. Then, the set of principal $\mathcal{O}$ ideals (ideals of the form $\alpha\mathcal{O}$, $\alpha \in K^*$) is a subgroup of $I(\mathcal{O})$, denoted by $P(\mathcal{O})$. Then the quotient group $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ is a finite group (see [CO]) and called the ideal class group of the order $\mathcal{O}$. The order of $C(\mathcal{O})$ is called the class number of $\mathcal{O}$ and denoted as $h(\mathcal{O})$. We sometimes write $h(D)$ instead of $h(\mathcal{O})$, where D is the discriminant of $\mathcal{O}$.

Let $\mathcal{J}$ be a proper fractional $\mathcal{O}$ ideal. Then we can regard $\mathcal{J}$ as a lattice in $\mathbb{C}$. That is, we can write $\mathcal{J}= [\alpha, \beta]$ where $\alpha, \beta \in \mathbb{C}$ and $\frac{\alpha}{\beta} \notin \mathbb{R}$ (see [CO, pp 151]). Conversely, let $L = [\tau, 1]$ be a lattice and there exists $\alpha \in \mathbb{C}\backslash\mathbb{Z}$ such that $\alpha L \subset L$. Then $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field and $\mathcal{O}= \{\beta \in K : \beta L \subset L\}$ is an order in K, $\alpha \in \mathcal{O}$. Remark that L is a proper fractional ideal of $\mathcal{O}$.

In conclusion, we get that any proper fractional ideal of an order $\mathcal{O}$ in an imaginary quadratic field K is a lattice whose ring of endomorphism is the order $\mathcal{O}$. Converse is also true. Two lattices L, L' with endomorphism rings $\mathcal{O}$, are proportional if and only if they are in the same class in $I(\mathcal{O})$. Therefore, number of lattices up to proportionality whose ring of endomorphisms are $\mathcal{O}$ is nothing but the class number of $\mathcal{O}$, $h(\mathcal{O})$.

The following theorem gives a nice formula for the class number, $h(\mathcal{O})$:

Theorem 3.1.4 [CO, pp 146] *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_k^* : \mathcal{O}^*]} \prod_{p/f} \left(1 - \left(\begin{array}{c} d_K \\ p \end{array}\right) \frac{1}{p}\right)$$

where p's are primes dividing f. Furthermore, $h(\mathcal{O}_K)$ divides $h(\mathcal{O})$.

The symbol $\left(\begin{array}{c} d_K \\ p \end{array}\right)$ in the above theorem is the Kronecker Symbol for $p = 2$ which is defined as

$$\left(\begin{array}{c} d_K \\ 2 \end{array} \right) = \begin{cases} 0 & \text{if } 2/d_K \\ 1 & \text{if } d_K \equiv 1 \bmod 8 \\ -1 & \text{if } d_K \equiv 5 \bmod 8 \end{cases}$$

and for odd prime p, $\left(\begin{array}{c} d_K \\ p \end{array} \right)$ is the Legendre Symbol defined as

$$\left(\begin{array}{c} d_K \\ p \end{array} \right) = \begin{cases} 0 & \text{if } p/d_K \\ -1 & \text{if } d_K \text{ isn't divisible by } p, d_K \text{ is quadratic nonresidue modulo } p \\ 1 & \text{if } d_K \text{ isn't divisible by } p, d_K \text{ is quadratic residue modulo } p \end{cases}$$

Let K be an imaginary quadratic field and p be a prime number. Then, p is either prime or square of a prime or product of two primes in K. More explicitly

Proposition 3.1.9 [BO-SHA, pp 236] *In a quadratic field with discriminant D the prime number p has the decomposition*

$p = \mathcal{P}^2$, where $\mathcal{P}$ is a prime in K, if and only if p divides D.

If p is odd and does not divide D then $p = \mathcal{P}\mathcal{P}'$, $\mathcal{P} \neq \mathcal{P}'$, for $\left(\frac{D}{p}\right) = 1$ and $p = \mathcal{P}$ for $\left(\frac{D}{p}\right) = -1$. If 2 does not divide D then $2 = \mathcal{P}\mathcal{P}'$, $\mathcal{P} \neq \mathcal{P}'$, for $D \equiv 1 \bmod 8$ and $2 = \mathcal{P}$ for $D \equiv 5 \bmod 8$.

3.1.4 Elliptic Curves in Positive Characteristic

An elliptic curve E over a field of characteristic $p > 3$ can be written in Weierstrass form

$$E: \quad y^2 = 4x^3 - g_2 x - g_3$$

In characteristic 0, the set of elements of an elliptic curve of order N is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. The situation is slightly different in positive characteristic:

Proposition 3.1.10 [LA 2, pp 171] *Let E be an elliptic curve defined over a field of positive characteristic p. Then, either E has no point of order p or the set of elements of E of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Definition 4 Let E be an elliptic curve defined over a field of positive characteristic p. If E has no point of order p then E is said to be supersingular elliptic curve. If the set of elements of E of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ then E is said to be ordinary elliptic curve.

The situation for endomorphism rings of elliptic curves over a field of positive characteristic is more complicated then the case in characteristic 0. Endomorphism ring of an elliptic curve E determines whether E is supersingular or ordinary:

Theorem 3.1.5 [SIL 1, pp 137] *Let E be an elliptic curve over a field K of characteristic p. Then*

i) $End(E) = End_{\overline{K}}(E) = \mathbb{Z}$ if $j(E)$ is transcendental over $\mathbb{F}_p$.

ii) Assume $j(E)$ is algebraic over $\mathbb{F}_p$. Then $End(E) = End_{\overline{K}}(E)$ is an order in an imaginary quadratic field if and only if E is ordinary and $End(E) = End_{\overline{K}}(E)$ is an order in a quaternion algebra if and only if E is supersingular.

3.1.4.1 Supersingular Elliptic Curves

Supersingular elliptic curves are important points of the modular curve $X_0(\ell)$ over $\mathbb{F}_{p^2}$, $(\ell, p) = 1$, as being rational points. Supersingular elliptic curves have great importance also in examining the singularities of plane model $Z_0(\ell)$ in positive characteristic. The singular points of $Z_0(\ell)$ in positive characteristic, corresponding to supersingular elliptic curves have the most complicated singularities of $Z_0(\ell)$ which we are going to examine in chapter 5.

We know that endomorphism ring of a supersingular elliptic curve is an order in a quaternion algebra. More explicitly, if E is a supersingular elliptic curve in

characteristic p then End(E) is a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified only at ∞ and at p. A quaternion algebra H_p is ramified at p if $H_p \otimes \mathbb{Q}_p$ is a division algebra and H_p is ramified at ∞ if $H_p \otimes \mathbb{R}$ is the Hamilton quaternions. H_p is not ramified at other primes $\ell \neq p$. That is, $H_p \otimes \mathbb{Q}_\ell$ is 2×2 matrix algebra in $\mathbb{Q}_\ell$ (see [EIC]).

Let $\mathcal{O}$ be a maximal order in the quaternion algebra H_p ramified only at p and at ∞. Let $\mathcal{I}$ be a left ideal of $\mathcal{O}$. If $\mathcal{I}^{-1}\mathcal{I} = \{a \in H_p : \mathcal{I}a \subset \mathcal{I}\}$ is equal to $\mathcal{O}$ then we say that $\mathcal{I}$ is two sided ideal. Two sided ideals of $\mathcal{O}$ form a group (see [PI]). Let $H_{\mathcal{O}}$ denote the ideal class group of two sided $\mathcal{O}$ ideals. That is, the group of all two sided $\mathcal{O}$ ideals modulo principal two sided $\mathcal{O}$ ideals. Then $H_{\mathcal{O}}$ is either trivial or cyclic group of order 2. More explicitly

Proposition 3.1.11 [EIC] *Let E be a supersingular curve in characteristic p. Then, End$(E) = \mathcal{O}$ is a maximal order in a quaternion algebra H_p over $\mathbb{Q}$ ramified only at ∞ and p. Let $H_{\mathcal{O}}$ be the two sided ideal class group. Then $H_{\mathcal{O}}$ is trivial $\iff$ $j(E) \in \mathbb{F}_p \iff \exists$ an element of norm p in $\mathcal{O}$. $H_{\mathcal{O}}$ is cyclic of order 2 $\iff$ $j(E) \notin \mathbb{F}_p$*

A significant property of a supersingular elliptic curve E over a field of characteristic p is that E is defined over $\mathbb{F}_{p^2}$:

Theorem 3.1.6 [SIL 1, pp 137] *Let E be a supersingular elliptic curve over a field of characteristic p. Then $j(E) \in \mathbb{F}_{p^2}$.*

Let E and $E^{(p)}$ be elliptic curves in characteristic $p > 3$ given as

$$E : y^2 = 4x^3 - g_2 x - g_3$$

$$E^{(p)} : y^2 = 4x^3 - g_2^{(p)} x - g_3^{(p)}.$$

Then the Frobenious isogeny Fr is defined as

$$Fr : E \longrightarrow E^{(p)}$$

$$(x, y) \longmapsto (x^p, y^p).$$

Fr has degree p and is inseparable isogeny (see [SIL 1, pp 30]). We have $\triangle(E^{(p)}) = \triangle(E)^p$ and hence $j(E^{(p)}) = j(E)^p$. Let $\phi : E \longrightarrow E^{(p)}$ be another isogeny of degree p. Assume E is supersingular. Then $E^{(p)}$ is also supersingular since it is isogenous to E. We have $\widehat{\phi}\phi = [p] \in \text{End}(E)$ where $\widehat{\phi}$ is the dual of ϕ. But E is supersingular and hence has no element of order p and the separable degree of $[p]$ is number of elements of E of order p together with identity element (see [SIL 1, pp 76]). So, $[p]$ is inseparable. Hence ϕ is also inseparable. ϕ has the same degree as Fr. Thus, ϕ differs from Fr by automorphisms of E and $E^{(p)}$. That is, $\phi = \varepsilon' Fr \varepsilon$ where ε is an automorphism of E and ε' is an automorphism of $E^{(p)}$. Let's summarize the paragraph:

Proposition 3.1.12 *Let E and E' be supersingular elliptic curves over a field of characteristic p. If the Frobenious isogeny $Fr \in Hom(E, E')$ then $j(E) = \overline{j(E')}$ where $\overline{j(E')}$ is conjugate of $j(E')$ in $\mathbb{F}_{p^2}$. In addition, assume $\sigma \in Hom(E, E')$ is an isogeny of degree p^r. Then $\sigma = Fr^r$ modulo automorphisms of E and E'.*

3.1.4.2 Reduction and Lifting

The basic idea of reduction is considering an elliptic curve, which is defined over a number field K, in the finite field $\mathcal{O}_K/\mathcal{P}$ where $\mathcal{O}_K$ is the ring of integers of K and $\mathcal{P}$ is a prime ideal in $\mathcal{O}_K$. More explicitly, let K be number field and E be an elliptic curve given by

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in K.$$

Let $\mathcal{O}_K$ be the ring of integers of K and let's take a prime ideal $\mathcal{P}$ such that g_2 and g_3 can be written as $\frac{\alpha}{\beta}$ where $\alpha, \beta \in \mathcal{O}_K$ and $\beta \notin \mathcal{P}$ so that we can define the cosets of g_2 and g_3, $[g_2]$ and $[g_3]$ in $\mathcal{O}_K/\mathcal{P}$. Also, assume that

$$\triangle = [g_2]^3 - 27[g_3]^2 \neq 0 \text{ in } \mathcal{O}_K/\mathcal{P}.$$

Then we say that E has good (smooth) reduction modulo $\mathcal{P}$ and the curve

$$\overline{E} : y^2 = 4x^3 - [g_2]x - [g_3]$$

in $\mathcal{O}_K/\mathcal{P}$ is reduction of E modulo $\mathcal{P}$. If characteristic of $\mathcal{O}_K/\mathcal{P}$ is p then we also say that $\overline{E}$ is reduction of E modulo p.

In general, let $\mathcal{O}$ be a local ring with no divisor of zero, K be a field containing $\mathcal{O}$ and $\mathcal{M}$ be the maximal ideal of $\mathcal{O}$. Let

$$\omega \longmapsto \overline{\omega}$$

denote a place which extends the canonical homomorphism $\mathcal{O} \longmapsto \mathcal{O}/\mathcal{M}$, to an algebraic extension L of K.

Let E be an elliptic curve given in Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in \mathcal{O}.$$

Assume that characteristic of $\mathcal{O}/\mathcal{M}$ is not 2 or 3 and $\triangle$ is a unit in $\mathcal{O}$ ($\triangle \notin \mathcal{M}$).

Then we have a good reduction $\overline{E}$ of E modulo $\mathcal{M}$. Let E' be also an elliptic curve with good reduction over $\mathcal{O}$. If $\lambda : E \longrightarrow E'$ is an isogeny then λ is defined over L and has a good reduction $\overline{\lambda} : \overline{E} \longrightarrow \overline{E'}$ and the map

$$\lambda \longmapsto \overline{\lambda}$$

is injective homomorphism. $\overline{\lambda}$ is also an isogeny of the same degree as λ (for proof and more explanation, see [LA 2]). Deuring has described the endomorphism ring of reduction of an elliptic curve:

Theorem 3.1.7 (Deuring) [LA 2, pp 182] *Let E be an elliptic curve over a number field. Assume End(E) is an order $\mathcal{O}$ in an imaginary quadratic field K. Let $\mathcal{B}$ be a place of algebraic closure of $\mathbb{Q}$ over a prime number p where E has a good reduction $\overline{E}$. The curve $\overline{E}$ is supersingular if and only if p is prime or ramified (square of a prime) in K. Suppose that p splits completely (p is product of two primes) in K. Let c be the conductor of $\mathcal{O}$ and write $c = p^r c_0$ where $(p, c_0) = 1$. Then*

i) End($\overline{E}$) $= \mathbb{Z} + c_0\mathcal{O}_K$ is an order in K with conductor c_0.

ii) If $(p, c) = 1$ then the reduction map $\lambda \longmapsto \overline{\lambda}$ is an isomorphism of End(E) onto End($\overline{E}$).

Also, Deuring has proved that for any elliptic curve E over a positive characteristic, we can find an elliptic curve over a number field whose reduction is isomorphic to E:

Theorem 3.1.8 (Deuring) [LA 2, pp 184] *Let E_0 be an elliptic curve in characteristic p with nontrivial isogeny $\alpha_0 \in End(E_0)$. Then there exists an elliptic curve E defined over a number field with an isogeny α of E and a good reduction $\overline{E}$ of E at a place $\mathcal{B}$ lying above p such that E_0 is isomorphic to $\overline{E}$ and α_0 corresponds to $\overline{\alpha}$ under isomorphism.*

From these Deuring's theorems, for a given prime p we have a bijection of j invariants

$$j(z) \longmapsto \overline{j(z)}$$

where $j(z)$ is the j invariant of the lattice $[z, 1]$ whose ring of endomorphism is an order $\mathcal{O}$ in an imaginary quadratic field K where p splits completely in K and conductor of $\mathcal{O}$ is not divisible by p. $\overline{j(z)}$ is j invariant of an ordinary elliptic curve over a field of characteristic p. More explicitly

Theorem 3.1.9 (Deuring's Lifting Theorem) [LA 2, pp 187] *Let E_0 be an ordinary elliptic curve in positive characteristic p with ring of endomorphism $End(E_0) = \mathcal{O}$. Then there exists a unique elliptic curve E in characteristic 0 with $End(E) = \mathcal{O}$ such that reduction of E modulo p is isomorphic to E_0.*

3.2 Modular Curves

A modular curve, analytically, is a quotient space of the action of some specific subgroups of $SL_2(\mathbb{Z})$ on upper half plane, $\mathbb{H}$. For $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, let's define the action as

$$\sigma(z) = \frac{az + b}{cz + d} \quad , \quad z \in \mathbb{H}.$$

Then σ is map from $\mathbb{H}$ to $\mathbb{H}$ since

$$\mathrm{im}(\frac{az+b}{cz+d}) = \frac{\mathrm{im}(z)}{|cz+d|^2} \ > 0 \text{ for } z \in \mathbb{H}.$$

Hence, $\frac{az+b}{cz+d} \in \mathbb{H}$. Observe that σ and $-\sigma$ induces the same action on $\mathbb{H}$ and hence let's take

$$\Gamma := SL_2(\mathbb{Z})/\pm 1$$

and introduce discrete topology on Γ. Γ is called the full modular group. As usual, $\mathbb{H}$ has complex topology generated by open disks. Let's define

$$\Gamma(N) = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

$\Gamma(N)$ is called the principal congruence subgroup of level N. Any subgroup G of Γ which contains $\Gamma(N)$ for some $N \in \mathbb{Z}^+$ is called congruence subgroup. For such a congruence subgroup G we have also discrete topology. Then, it is easy to check that, as a topological group, G is an action on $\mathbb{H}$ where, similarly, the action is defined as

$$(\sigma, z) = \sigma z = \frac{az+b}{cz+d} \ , \ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \text{ and } z \in \mathbb{H}.$$

For a point $z \in \mathbb{H}$, we call the set $Gz = \{gz : g \in G\}$ as the orbit of z under G. Then, the quotient space $\mathbb{H}/G$ is the set of all G - orbits of points on $\mathbb{H}$. Any two points z_1, z_2 which are in the same orbit with respect to G are called G equivalent and we denote this fact as $z_1 \sim_G z_2$. Now, let's introduce the quotient topology on $\mathbb{H}/G$. That is, if $\phi : \mathbb{H} \longrightarrow \mathbb{H}/G$ is the natural projection defined as $\phi(z) = Gz$, then a subset A of $\mathbb{H}/G$ is open if it's inverse image, $\phi^{-1}(A)$ is open in $\mathbb{H}$.

Theorem 3.2.1 [SH, ch I] *With the above construction, $\mathbb{H}/G$ is a Riemann Surface.*

As in the case of torus, we can represent elements of the quotient space $\mathbb{H}/G$ in a fundamental domain. A fundamental domain D for a congruence subgroup

G is a connected subset of $\mathbb{H}$ such that every orbit of G has an element in D and any two elements in interior of D are in different orbits.

For a congruence subgroup G, the set $G_z = \{g \in G : gz = z\}$ is called the isotropy group (stabilizer) of the point $z \in \mathbb{H}$. If, for $z \in \mathbb{H}$, the isotropy group, G_z, is nontrivial then the point z is called elliptic point and $|G_z|$ is called the order of z.

Let $\Gamma = SL_2(\mathbb{Z})/\pm 1$ and G be a congruence subgroup of Γ. Then $[\Gamma : G] = n < \infty$. Let $\alpha_i G$ be cosets of G in Γ, $\alpha_i \in \Gamma$, $i = 1, \cdots, n$. Then $\Gamma = \bigcup_{i=1}^{n} \alpha_i G$. If D_Γ is a fundamental domain for Γ then $D_G = \bigcup_{i=1}^{n} \alpha_i^{-1} D_\Gamma$ will be a fundamental domain for G. Indeed, if $z \in \mathbb{H}$ then $\exists z' \in D_\Gamma$ which is in the same orbit as z's. That is, $\exists \alpha \in \Gamma$ such that $\alpha z = z'$. For some i, $\alpha = \alpha_i \sigma \quad \sigma \in \Gamma$. Then $\alpha_i \sigma z = z' \Rightarrow \sigma z = \alpha_i^{-1} z' \in D_G$. That is, for any element $z \in \mathbb{H}$, its orbit contains an element in D_G. Now, let's assume two elements of D_G, say $\alpha_i^{-1} z$ and $\alpha_j^{-1} z'$ for some z and z' in D_G are in the same orbit. That is, $\exists \sigma \in G$ such that $\sigma \alpha_i^{-1} z = \alpha_j^{1} z'$. Then $\alpha_j \sigma \alpha_i^{-1} z = z'$. But z and z' are in the fundamental domain of Γ and hence they are not interior points of D_Γ. Therefore, the points $\alpha_i^{-1} z$ and $\alpha_j^{-1} z'$ are not interior points of D_G. We see that D_G is actually a fundamental domain for the subgroup G. We can choose α_i's in the coset decomposition so that D_G is connected.

The next theorem describes fundamental domain of the full modular group Γ and also states stabilizers of points:

Theorem 3.2.2 [LA 3, ch III §1]

i) The set $D_\Gamma = \{z \in \mathbb{H} : -\frac{1}{2} \leq Rez \leq \frac{1}{2}$ *and* $|z| \geq 1\}$ *serves as a fundamental domain for* Γ. *Furthermore the elements*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generates Γ.

ii) $\Gamma_z = \{I\}$ *for* $z \in \mathbb{H}$, $z \not\sim_\Gamma i, \omega$ *(recall that* ω *is third root of unity) and*

$$\Gamma_i =< S >= \{I, S\}, \quad \Gamma_\omega =< ST >= \{I, ST, (ST)^2\}$$

where I is the 2 by 2 identity matrix.

In the fundamental domain D_Γ, described in the above theorem, the vertical lines $\mathrm{Re}z = -\frac{1}{2}$ and $\mathrm{Re}z = \frac{1}{2}$ are identical since the point z with $\mathrm{Re}z = -\frac{1}{2}$ is in the same orbit as the point $Tz = z + 1$ whose real part is, $\mathrm{Re}(z+1) = \frac{1}{2}$. Also, on the arc $|z| = 1$ of D_Γ, the points z and $Sz = -\frac{1}{z}$ are in the same orbit. Therefore, the Riemann Surface $\mathbb{H}/\Gamma$ is obtained by gluing the vertical lines $\mathrm{Re}z = -\frac{1}{2}$ and $\mathrm{Re}z = \frac{1}{2}$ of the fundamental domain D_Γ such that the points in the same orbit coincide and also by gluing the left part of the arc of D_Γ (that is, the set $\{z \in D_\Gamma : |z| = 1, \mathrm{Re}z \leq 0\}$) with the right part of the arc of D_Γ (that is, the set $\{z \in D_\Gamma : |z| = 1, \mathrm{Re}z \geq 0\}$) such that the points in the same orbit coincide.

Unfortunately, the Riemann Surface $\mathbb{H}/\Gamma$ is not compact and hence, for any congruence subgroup G, the the Riemann Surface $\mathbb{H}/G$ is also not compact since a fundamental domain D_G for G is nothing but a union of images of a fundamental domain D_Γ of Γ under some finitely many elements of Γ. To compactify $\mathbb{H}/\Gamma$, we should add the point ∞. But, this Riemann Surface is defined by an action and hence we should enlarge this action on ∞. For this, let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \infty$ since Γ (and any subgroup of Γ) acts on $\mathbb{Q} \cup \infty$. For a congruence subgroup G of Γ the quotient space $\mathbb{Q} \cup \infty/G$ is finite. That is, there exists finitely many orbits of G for the space $\mathbb{Q} \cup \infty$. Any orbit which is represented by an element is said to be a cusp. For instance, Γ has just one cusp, ∞, since any rational number $r \in \mathbb{Q}$ is Γ equivalent to ∞. If $r = \frac{a}{c}$, $a, c \in \mathbb{Z}$ are relatively prime, then $\exists b, d \in \mathbb{Z}$ such that $ad - bc = 1$. Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\sigma(\infty) = r$, which explains that only cusp of Γ is ∞.

The topology of $\mathbb{H}^*$ is generated by the neighborhoods of the points $z \in \mathbb{H}^*$ where for $z \in \mathbb{H}$ neighborhoods of z is as usual, for $z = \infty$, neighborhoods of ∞ are the sets

$$N_C = \{z \in \mathbb{H} : \mathrm{im}z > C\} \bigcup \{\infty\} \text{ for } C \in \mathbb{R}^+.$$

Finally, for a point $r \in \mathbb{Q}$, neighborhoods of r are open disks in $\mathbb{H}$ which are tangent to the real axis at r. Then, the charts of the Riemann Surface $\mathbb{H}^*/\Gamma$ are

z near $z \not\sim_\Gamma i, \omega, \infty$

$\left(\frac{z-i}{iz-1}\right)^2$ near $z \sim_\Gamma i$

$\left(\frac{z-\omega}{\omega z-1}\right)^3$ near $z \sim_\Gamma \omega$

$q = e^{2\pi i z}$ near $z \sim_\Gamma \infty$

For more detailed information about the charts above, one can refer to Silverman's second book on arithmetic of elliptic curves, [SIL 2].

$\mathbb{H}^*/\Gamma$ is compact. Because, any open covering of the fundamental domain D_Γ^* contains a neighborhood $N_C = \{z : -\frac{1}{2} \leq \mathrm{Re}z \leq \frac{1}{2},\ \mathrm{im}z > C\}$ of ∞ and $D_\Gamma - N_C$ is compact. Then, for any congruence subgroup G of Γ the Riemann Surface $\mathbb{H}^*/G$ is compact.

Now, we are ready to introduce main definition of this chapter:

Definition 5 Let G be a congruence subgroup of Γ. The Riemann Surfaces $\mathbb{H}^*/G$ and $\mathbb{H}/G$ are called modular curves.

3.2.1 Genus of Modular Curve

We know that the function $j : \mathbb{H} \to \mathbb{C}$ is analytic on $\mathbb{H}$ and has a simple pole at ∞. In addition $j(z) = j(z')$ if and only if z and z' are in the same orbit with respect to full modular group Γ. Hence, the j function is an analytic bijection between $\mathbb{H}^*/\Gamma$ and $\mathbb{P}^1(\mathbb{C})$. That is, the modular curve $\mathbb{H}^*/\Gamma$ is nothing but a projective line. Hence its genus is $g(\mathbb{H}^*/\Gamma) = 0$. In general we have:

Theorem 3.2.3 *Let G be a congruence subgroup of Γ and let*

$$[\Gamma : G] = n$$

$\nu_2 =$ *number of G - inequivalent elliptic points of order 2*

$\nu_3 =$ *number of* G *- inequivalent elliptic points of order 3*

$\nu_\infty =$ *number of* G *- inequivalent cusps*

Then, the genus of $\mathbb{H}^*/G$ *is given by*

$$g = 1 + \frac{n}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Proof: Consider the natural projection

$$\pi : \mathbb{H}^*/G \longmapsto \mathbb{H}^*/\Gamma$$

taking the point z in the fundamental domain of G to z' in the fundamental domain of Γ where z' is in the same orbit as z with respect to Γ. Then the point z has ramification index $e_z = [\Gamma_z : G_z]$. For z, not an elliptic point of Γ, i.e. $\Gamma_z = \mathrm{id}$, we have $[\Gamma : G] = n$ points in the fundamental domain of G which are Γ equivalent to z, and all their ramification indices are 1. Hence, the degree of π is nothing but the index $[\Gamma : G] = n$. Now, let $\nu_2' \quad (\nu_3')$ be the number of points in $\mathbb{H}^*/G$ which are Γ equivalent to $i \quad (\omega)$, but are not elliptic points with respect to G. Then, $n = \nu_2 + 2\nu_2' = \nu_3 + 3\nu_3'$, since, for a nonelliptic point z of $\mathbb{H}^*/G$ which is Γ equivalent to i, it is ramification index is $e_z = [\Gamma_z : G_z] = 2$ and for a nonelliptic point z of $\mathbb{H}^*/G$ which is Γ equivalent to ω, it is ramification index is $e_z = [\Gamma_z : G_z] = 3$. For the cusps $r \in \mathbb{Q} \bigcup \infty$ we have $\sum e_r = n$. Hence $\sum(e_r - 1) = \sum e_r - \nu_\infty = n - \nu_\infty$. The ramified points are exactly those nonelliptic points which are Γ equivalent to i or ω and some of the cusps. By Hurwitz genus formula, we have

$$2g(\mathbb{H}^*/G) - 2 = n(2g(\mathbb{H}^*/\Gamma) - 2) + \sum_{z \in \mathbb{H}^*/G} (e_z - 1)$$

The genus of $\mathbb{H}^*/\Gamma$ is zero. Hence

$$\begin{aligned} 2g(\mathbb{H}^*/G) - 2 &= -2n + \sum_{z \in \mathbb{H}^*/G} (e_z - 1) \\ &= -2n + 2\nu_3' + \nu_2' + n - \nu_\infty \\ &= -2n + 2\frac{n - \nu_3}{3} + \frac{n - \nu_2}{2} + n - \nu_\infty \end{aligned}$$

Then we get the result

$$g = g(\mathbb{H}^*/G) = 1 + \frac{n}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

QED

In this thesis, we are interested in the genera of modular curves $\mathbb{H}^*/\Gamma_0(\ell)$ where $\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod \ell \right\}$ for prime ℓ's. Let's denote the modular curves as

$$X_0(\ell) = \mathbb{H}/\Gamma_0(\ell) \text{ and } Y_0(\ell) = \mathbb{H}^*/\Gamma_0(\ell).$$

First let's calculate the genus of the curve $Y_0(\ell)$:

Theorem 3.2.4 *The genus $g = g(Y_0(\ell))$ of the modular curve for prime ℓ is*

$$g = \frac{\ell+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{\ell}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{\ell}\right)\right)$$

where

$$\left(\frac{-1}{\ell}\right) = \begin{cases} 0 & \text{if } \ell = 2, \\ 1 & \text{if } \ell \equiv 1 \bmod 4, \\ -1 & \text{if } \ell \equiv 3 \bmod 4 \end{cases}$$

and

$$\left(\frac{-3}{\ell}\right) = \begin{cases} 0 & \text{if } \ell = 3, \\ 1 & \text{if } \ell \equiv 1 \bmod 3, \\ -1 & \text{if } \ell \equiv 2 \bmod 3 \end{cases}$$

Proof: Let $C(\ell) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = \ell, a > 0, 0 \le b < d, \ \gcd(a,b,d) = 1 \right\}$ and let $\sigma_0 = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \in C(\ell)$. Then for $\sigma \in C(\ell)$ the set $\sigma_0^{-1}\Gamma\sigma \cap \Gamma$ is a right coset of $\Gamma_0(\ell)$. To see this, first let's show $\sigma_0^{-1}\Gamma\sigma_0 \cap \Gamma = \Gamma_0(\ell)$. For the element $\sigma_0^{-1}\gamma\sigma_0 \in \sigma_0^{-1}\Gamma\sigma_0 \cap \Gamma$ where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ we have $\sigma_0^{-1}\gamma\sigma_0 = \begin{pmatrix} a & b/\ell \\ c\ell & d \end{pmatrix} \in$

$\Gamma_0(\ell)$. Conversely, for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$ let $\gamma = \begin{pmatrix} a & b\ell \\ c/\ell & d \end{pmatrix} \in \Gamma$ since $c \equiv 0 \bmod \ell$. Then $\sigma_0^{-1}\gamma\sigma_0 = \alpha$. Therefore $\sigma_0^{-1}\Gamma\sigma_0 \cap \Gamma = \Gamma_0(\ell)$.

Now, for $\sigma \in C(\ell)$, let's see $\sigma_0^{-1}\Gamma\sigma \cap \Gamma$ is a right coset of $\Gamma_0(\ell)$. Let $\alpha_1 = \sigma_0^{-1}\gamma_1\sigma$ and $\alpha_2 = \sigma_0^{-1}\gamma_2\sigma$ be two elements of $\sigma_0^{-1}\Gamma\sigma \cap \Gamma$. Then $\alpha_1\alpha_2^{-1} = \sigma_0^{-1}\gamma_1\sigma\sigma^{-1}\gamma_2^{-1}\sigma_0 = \sigma_0^{-1}\gamma_1\gamma_2^{-1}\sigma_0 \in \sigma_0^{-1}\Gamma\sigma_0 \cap \Gamma$ and hence $\alpha_1\alpha_2^{-1} \in \Gamma_0(\ell)$. That is, all elements of $\sigma_0^{-1}\Gamma\sigma \cap \Gamma$ are in the same coset. For an element $\sigma_0^{-1}\gamma\sigma \in \sigma_0^{-1}\Gamma\sigma \cap \Gamma$ we have $\sigma_0^{-1}\Gamma\sigma \cap \Gamma \subseteq \Gamma_0(\ell)\sigma_0^{-1}\gamma\sigma$. Let $\alpha\sigma_0^{-1}\gamma\sigma \in \Gamma_0(\ell)\sigma_0^{-1}\gamma\sigma$, since $\sigma_0^{-1}\Gamma\sigma_0 \cap \Gamma = \Gamma_0(\ell)$ we can write α as $\alpha = \sigma_0^{-1}\gamma'\sigma_0$. Then $\alpha\sigma_0^{-1}\gamma\sigma = \sigma_0^{-1}\gamma'\sigma_0\sigma_0^{-1}\gamma\sigma = \sigma_0^{-1}\gamma'\gamma\sigma \in \sigma_0^{-1}\Gamma\sigma \cap \Gamma$. Hence, $\sigma_0^{-1}\Gamma\sigma \cap \Gamma = \Gamma_0(\ell)\sigma_0^{-1}\gamma\sigma$. For different elements $\sigma_1, \sigma_2 \in C(\ell)$, the cosets $\sigma_0^{-1}\Gamma\sigma_1 \cap \Gamma$ and $\sigma_0^{-1}\Gamma\sigma_2 \cap \Gamma$ are also different since $\sigma_1\sigma_2^{-1} \notin \Gamma$ for different σ_1 and $\sigma_2 \in C(\ell)$. Now, for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma - \Gamma_0(\ell)$ let's choose $\sigma = \begin{pmatrix} 1 & x \\ 0 & \ell \end{pmatrix} \in C(\ell)$ so that $d - cx \equiv 0 \bmod \ell$. Recall that $c \not\equiv 0 \bmod \ell$. Then for $\gamma' = \begin{pmatrix} a\ell & -ax + b \\ c & \frac{-cx+d}{\ell} \end{pmatrix} \in \Gamma$ we have $\sigma_0^{-1}\gamma'\sigma = \gamma$.

So, we have proved that elements of $C(\ell)$ are in one to one correspondence with the cosets of $\Gamma_0(\ell)$. Hence $[\Gamma : \Gamma_0(\ell)] = |C(\ell)|$. But, elements of $C(\ell)$ are σ_0 and $\begin{pmatrix} 1 & j \\ 0 & \ell \end{pmatrix}$ where $j = 0, ..., \ell - 1$. Hence $|C(\ell)| = \ell + 1$. That is, $[\Gamma : \Gamma_0(\ell)] = \ell + 1$.

Now, let's prove that the only cusps of $\Gamma_0(\ell)$ are 0 and ∞. Well, $S\infty = 0$ and $S \notin \Gamma_0(\ell)$. So $0 \not\sim_{\Gamma_0(\ell)} \infty$. Now, let's prove that any other rational number is $\Gamma_0(\ell)$ equivalent to 0 or ∞. Let $r = \frac{a}{c}, (a, c) = 1$. Assume $r \not\sim_{\Gamma_0(\ell)} \infty$, then $c \not\equiv 0 \bmod \ell$. Hence $(a\ell, c) = 1$. There exists $b, d \in \mathbb{Z}$ such that $cd - a\ell b = 1$. Let $\gamma = \begin{pmatrix} d & a \\ \ell b & c \end{pmatrix} \in \Gamma_0(\ell)$. Then $\gamma(0) = r$. Hence, $r \sim_{\Gamma_0(\ell)} 0$. Therefore there are just two cusps of $\Gamma_0(\ell)$, 0 and ∞.

Elliptic points of $\Gamma_0(\ell)$ of order 2 are Γ equivalent to i. Let $z = \gamma i$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. z is elliptic point if and only if $\gamma S\gamma^{-1} \in \Gamma_0(\ell)$. Because $\gamma S\gamma^{-1} \in \Gamma_z$. We have $\gamma S\gamma^{-1} = \begin{pmatrix} bd+ac & -b^2-a^2 \\ d^2+c^2 & -bd-ca \end{pmatrix}$. Hence, z is elliptic point if and only if $c^2 + d^2 \equiv 0 \bmod \ell$. Number of elliptic points of order 2 is number of solutions for c (or d) in $c^2 + d^2 \equiv 0 \bmod \ell$ and it is nothing but $1 + \left(\frac{-1}{\ell}\right)$.

Similarly, elliptic points of $\Gamma_0(\ell)$ of order 3 are Γ equivalent to ω. Let $z = \gamma\omega$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Then z is an elliptic point if and only if $\gamma ST\gamma^{-1} \in \Gamma_0(\ell)$ and $\gamma ST\gamma^{-1} \in \Gamma_0(\ell)$ means $c^2 - cd + d^2 \equiv 0 \bmod \ell$. Number of solutions for c (or d) in $c^2 - cd + d^2 \equiv 0 \bmod \ell$ is $1 + \left(\frac{-3}{\ell}\right)$.

So we have index $n = \ell + 1$, $\nu_\infty = 2$, $\nu_2 = 1 + \left(\frac{-1}{\ell}\right)$ and $\nu_3 = 1 + \left(\frac{-3}{\ell}\right)$. Hence, genus of the curve $Y_0(\ell)$ is

$$\begin{aligned} g &= 1 + \frac{\ell+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{\ell}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{\ell}\right)\right) - 1 \\ &= \frac{\ell+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{\ell}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{\ell}\right)\right) \end{aligned}$$

QED

We know that the elliptic curves $E_1 \simeq \mathbb{C}/\mathbb{Z}\tau_1 + \mathbb{Z}$ and $E_2 \simeq \mathbb{C}/\mathbb{Z}\tau_2 + \mathbb{Z}$ over $\mathbb{C}$ are isomorphic if and only if τ_1 is Γ equivalent to τ_2. That is, the points of the modular curve $\mathbb{H}/\Gamma$ are in one to one correspondence with the elliptic curves up to isomorphism. Hence, $\mathbb{H}/\Gamma$ is moduli space for the moduli problem of determining isomorphism classes of elliptic curves over $\mathbb{C}$. Similarly, for $\gamma \in \Gamma_0(\ell)$ and $\tau \in \mathbb{H}/\Gamma_0(\ell)$, the cyclic subgroup $\{\frac{1}{\ell}, \frac{2}{\ell}, \cdots, \frac{\ell-1}{\ell}\}$ of the elliptic curve $\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}$ remains invariant under the action of γ. Hence, $\mathbb{H}/\Gamma_0(\ell)$ is a moduli space for the problem of determining equivalence classes of pairs (E, C) where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order ℓ. Then, the points $(E, C) \in X_0(\ell)$ and $(E', C') \in X_0(\ell)$ are the same point if and only if there exists an isomorphism $\mu : E \longmapsto E'$ such that $\mu(C) = C'$. We know that there is a one to one correspondence between subgroups Φ of an elliptic curve E and

isogenies $\phi : E \longmapsto E'$ given by the association $\Phi = \ker\phi$. Therefore, we can view the points of the modular curve $X_0(\ell)$ as equivalence classes of triples (E, E', ϕ) where $\phi : E \longmapsto E'$ is a cyclic isogeny (isogeny, whose kernel is cyclic) of order ℓ.

3.2.2 Modular Equation

Definition 6 An analytic function $f : \mathbb{H} \longmapsto \mathbb{C}$ on the upper half plane, is said to be holomorphic modular function with respect to the full modular group Γ if

i) f is Γ invariant. i.e., $f(\gamma z) = f(z) \quad \forall \gamma \in \Gamma$

ii) f is meromorphic at ∞. That is, in a neighborhood of ∞, f has the q expansion

$$f(z) = \sum_{k \geq m} a_k q^k, \qquad q = e^{2\pi i z}, \;\; m \in \mathbb{Z}.$$

Then, we have the following lemma:

Lemma 3.2.1 [CO, pp 226] *A holomorphic modular function with respect to* Γ *is a polynomial in* $j(\tau)$.

Now, let the right cosets of $\Gamma_0(\ell)$ be $\Gamma_0(\ell)\gamma_i$; $i = 1, ..., \ell + 1$. Then considering the function

$$\Phi_\ell(X, j(\tau)) = \prod_{i=1}^{\ell+1} (X - j(\ell\gamma_i\tau))$$

it is clear that Φ_ℓ is a polynomial in X. Let's see that it is also a polynomial in $j(\tau)$. The coefficients of X in $\Phi_\ell(X, j(\tau))$ are symmetric polynomials in $j(\ell\gamma_i\tau)$. Hence, they are holomorphic. Also, because of symmetry, for $\gamma \in \Gamma$ in a coefficient of X, $j(\ell\gamma_i\gamma\tau)$'s are a permutation of the $j(\ell\gamma_i\tau)$'s. Hence coefficients are Γ invariant. On the other hand, we know that the right cosets of $\Gamma_0(\ell)$ are $\sigma_0^{-1}\Gamma\sigma \bigcap \Gamma$ where recall that $\sigma_0 = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ and $\sigma \in C(\ell)$. Hence, any γ_i can be written as $\sigma_0^{-1}\gamma\sigma = \gamma_i$ for some $\sigma \in C(\ell)$ and $\gamma \in \Gamma$. So, $\sigma_0\gamma_i = \gamma\sigma$. Then $j(\ell\gamma_i\tau) =$

$j(\sigma_0\gamma_i\tau) = j(\gamma\sigma z) = j(\sigma z)$ for some $\sigma \in C(\ell)$. On the other hand, the j function has a simple pole at ∞ and hence, has the q expansion

$$j(\tau) = \frac{c}{q} + \sum_{n=1}^{\infty} c_n q^n$$

where c and c_n's are constants, $q = e^{2\pi i z}$. Then

$$\begin{aligned} j(\sigma\tau) &= \frac{c}{e^{2\pi i \frac{a\tau+b}{d}}} + \sum_{n=1}^{\infty} c_n e^{2\pi i \frac{a\tau+b}{d}} \text{ for } \sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \\ &= \frac{c \cdot e^{\frac{-2\pi i ab}{\ell}}}{\left(e^{\frac{2\pi i z}{\ell}}\right)^{a^2}} + \sum_{n=1}^{\infty} c_n e^{\frac{2\pi i abn}{\ell}} \left(e^{\frac{2\pi i z}{\ell}}\right)^{a^2 n} \end{aligned}$$

and hence q expansion of $j(m\gamma_i\tau)$ has only finitely many negative exponents and the coefficients of X in Φ_ℓ are meromorphic at ∞ since those coefficients are polynomials in the $j(m\gamma_i\tau)$'s. Therefore, the coefficients of $\Phi_\ell(X, j(\tau))$ are holomorphic modular functions and thus by the previous lemma, they are polynomials in $j(\tau)$. So, we have seen that $\Phi_\ell(X, j(\tau))$ is also a polynomial in $j(\tau)$. This means that there exists a polynomial $\Phi_\ell(X, Y) \in \mathbb{C}[X, Y]$ satisfying

$$\Phi_\ell(X, j(\tau)) = \prod_{i=1}^{\ell+1} (X - j(\ell\gamma_i\tau)).$$

The equation $\Phi_\ell(X, Y) = 0$ is called the modular equation. By the way, since $j(\ell\gamma_i\tau)$ can be written as $j(\sigma\tau)$ for a unique $\sigma \in C(\ell)$, we can also write

$$\Phi_\ell(X, j(\tau)) = \prod_{\sigma \in C(\ell)} (X - j(\sigma\tau)).$$

Observe that for $\sigma_0 \in C(\ell)$, $\Phi_\ell(j(\sigma_0\tau), j(\tau)) = \Phi_\ell(j(\ell\tau), j(\tau)) = 0$. Note that the degree of Φ_ℓ in X is $\ell + 1$ and its total degree is 2ℓ.

The polynomial $\Phi_\ell(X, Y) \in \mathbb{C}[X, Y]$ satisfying the modular equation has gigantic coefficients and hence to compute Φ_ℓ is somehow very complicated, particularly for big ℓ and for the numbers ℓ which have a lot of divisors. Hermann computed Φ_ℓ for $\ell = 5$ and $\ell = 7$ (see [HER]). E. Kaltofen and N. Yui have computed Φ_ℓ for $\ell = 11$ (see [KA-YU]). Nowadays, powerful computer systems are in use and can manipulate very complex algorithms which enable to compute Φ_ℓ for non prime and big ℓ's.

The following proposition describes the solutions of the modular equation:

Proposition 3.2.1 [CO, pp 235] *For $u, v \in \mathbb{C}$, $\Phi_\ell(u, v) = 0$ if and only if there is a lattice L and a cyclic sublattice $L' \subset L$ of index ℓ such that $j(L') = u$ and $j(L) = v$.*

Chapter 4

Code Construction on Modular Curves

In this chapter, we give a brief introduction to two approaches on code construction over modular curves. The first one is called geometric approach. It is due to Klyachko (cf. [KLY]) and the other one is called group theoretic approach. This approach is due to Vladuţ and Tsfasman (cf. [TS-VLA]). The geometric approach studies local invariants of the plane model $Z_0(N)$ of the modular curve $Y_0(N)$ given by the modular equation Φ_N. The approach is based on describing the hyperplane of regular differentials of $Z_0(N)$ vanishing at a given $\mathbb{F}_{p^2}$ rational point. Unfortunately the plane model $Z_0(N)$ is highly singular curve. So, the elements of the hyperplane must vanish at singular points also.

The group theoretical approach considers the codes on modular curves $Y(N)$ as group modules and tries to describe them not as vector spaces but as group modules or in special cases, as group ideals. The group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ acts on curves $Y(N)$ fixing the set of cusp points and inverse image of j invariant of a supersingular elliptic curve E in $\mathbb{P}^1$ under the natural projection

$$\psi_N : Y(N) \longrightarrow \mathbb{P}^1.$$

So, the group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ acts on the Goppa codes constructed on $Y(N)$. The action is permuting the coordinates of code words of the code. So, the codes can

be considered as group codes.

4.1 Codes on Modular Curves

In this section. we give a proof that the number of rational points on modular curves attains the Drinfeld-Vladuţ bound. The results are from [TS-VLA-ZI]. It follows that the Goppa codes constructed on modular curves have asymptotically the best known parameters.

Deligne and Rapoport have proved that the modular curves $Y_0(N)$ and $Y(N)$ have good (smooth) reduction over any prime ideal not dividing N (see [DE-RA]). In particular, the modular curve $Y_0(N)$ is defined over $\mathbb{Q}$. So, for any prime p not dividing N, there exists a good reduction of $Y_0(N)$ modulo p. We consider the modular curves in positive characteristics as moduli spaces of elliptic curves with some special structures. The modular curve $Y_0(N)$ is the moduli space of elliptic curves E with cyclic subgroup of order N. Similarly, the modular curve $Y(N)$ is moduli space of the pairs (E, α_N), E is an elliptic curve and α_N is a structure of level N with determinant $det\alpha_N = 1$. That is, α_N is an isomorphism

$$\alpha_N : E_N \longrightarrow (\mathbb{Z}/N\mathbb{Z})^2$$

such that the inverse image of $e^{2\pi i/N}$ by Weil pairing in the Nth torsion group E_N, is mapped to 1. The following theorem makes use of the result by Deligne and Rapoport and shows that the modular curves have maximum possible number of rational points:

Theorem 4.1.1 *Let $Y(N)$ be family of modular curves over $\mathbb{F}_{p^2}$ with genus $g = g(Y(N))$. Then*

$$\lim_{N\to\infty} \frac{|Y(N)(\mathbb{F}_{p^2})|}{g(Y(N))} = p - 1.$$

Proof: Recall that the modular curve $Y(N)$ is moduli space of the pairs (E, α_N), E is an elliptic curve and α_N is a structure of level N with determinant

$det\alpha_N = 1$. Assume that E is a supersingular elliptic curve. We will show that the point (E, α_N) is an $\mathbb{F}_{p^2}$ rational point of $Y(N)$. It is enough to prove that the point is fixed by the Frobenious endomorphism Fr^2 of degree p^2 since it generates the Galois group, $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_{p^2})$. But, E is supersingular. So, Fr^2 is equivalent to multiplication by p up to automorphisms of E. If $AutE = \pm 1$ then $Fr^2 = \pm p$ and Fr^2 preserves α_N). If $|AutE| \neq 2$ then consider the representative (E, α'_N) where α'_N is obtained by the action of a nontrivial automorphism of E. For this representative (E, α'_N), we have again $Fr^2 = \pm p$. So, in all cases (E, α_N) remains fixed by the action of Frobenious map Fr^2. Hence (E, α_N) is $\mathbb{F}_{p^2}$ rational point of $Y(N)$.

Let

$$\psi_N : Y(N) \longrightarrow \mathbb{P}^1$$

be the projection map where $\mathbb{P}^1 = Y(1)$. The map ψ_N has degree $\mu_N = [\Gamma(N) : \Gamma(1)] = \frac{N^3}{2} \prod_{\ell|N}(1 - \ell^{-2})$ where product is taken over primes. The group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ of order μ_N acts on the inverse image of the point $j(E) \in \mathbb{P}^1$ in a way that the order of the isotropy group of $j(E)$ equals to $|AutE|/2$. Because isomorphic elliptic curves give the same point of $Y(N)$. Hence, the inverse image of $j(E)$ contains $\frac{2\mu_N}{|AutE|}$ points. Then, summing up the number of points (E, α_N) where E is supersingular, we get

$$\sum_E \frac{2\mu_N}{|AutE|} = \frac{\mu_N(p-1)}{12}. \tag{4.1}$$

where the summation is taken over isomorphism classes of supersingular elliptic curves. Recall that the above equality comes from the mass formula for automorphisms of supersingular elliptic curves. So, the number of $\mathbb{F}_{p^2}$ rational points of $Y(N)$ is bounded below by the quantity, $\frac{\mu_N(p-1)}{12}$.

The modular curve over complex field has no elliptic points. On the other hand, number of its cusp points is μ_N/N. So, the genus of the curve $Y(N)$ will be

$$g(Y(N)) = 1 - \frac{\mu_N}{12} - \frac{\mu_N}{2N} = 1 + \frac{(N-6)\mu_N}{12N}. \tag{4.2}$$

The number of $\mathbb{F}_{p^2}$ rational points of $Y(N)$ divided by genus is bounded belove

by

$$\frac{\mu_N N(p-1)}{12N+\mu_N(n-6)}.$$

Sending N to infinity, the limit (if exists) of

$$\frac{|Y(N)(\mathbb{F}_{p^2})|}{g(Y(N))}$$

is bounded below by $p-1$. But, this is the Drinfeld-Vladuţ bound and so the limit is also bounded above by the same bound. Hence, the limit really exits and equals to $p-1$.

QED

We have proved that the family of modular curves $Y(N)$ attains the Drinfeld-Vladuţ bound. So, the codes constructed over $Y(N)$ have the best known asymptotic parameters. One can prove similarly that the number of rational points of another family of modular curves, $Y_0(N)$, defined over $\mathbb{F}_p$ also attains the Drinfeld -Vladuţ bound. The argument in the proof of the previous theorem still works in this case. But, we can get the result for $Y_0(N)$ by a simple corollary:

Corollary 4.1.1 *Let $Y_0(N)$ be the modular curve defined over $\mathbb{F}_p$ with genus $g = g(Y_0(N))$. Then*

$$\lim_{N\to\infty} \frac{|Y_0(N)(\mathbb{F}_{p^2})|}{g(Y_0(N))} = p-1.$$

Proof: We have the projection

$$Y(N) \longrightarrow Y_0(N) \longrightarrow \mathbb{P}^1 \tag{4.3}$$

coming from $\Gamma(N) \subset \Gamma_0(N) \subset \Gamma(1)$. Let us denote the first projection as λ_N and the second as Θ_N. Then Θ_N has degree $\deg \Theta_N = [\Gamma_0(N) : \Gamma(1)] = N\prod_{\ell|N}(1+\ell^{-1})$ where product is taken over primes dividing N. The projection

$$Y(N) \longrightarrow \mathbb{P}^1$$

has degree $[\Gamma(N) : \Gamma(1)] = \frac{N^3}{2}\prod_{\ell|N}(1-\ell^{-2})$. So, the degree of the projection

$$\lambda_N : Y(N) \longrightarrow Y_0(N)$$

is $\deg \lambda_N = \frac{N^2}{2} \prod_{\ell|N}(1-\ell)$. So, we have

$$|Y_0(N)(\mathbb{F}_{p^2})| \geq \frac{|Y(N)(\mathbb{F}_{p^2})|}{\deg \lambda_N}. \tag{4.4}$$

As a conclusion, we have the lower bound

$$\frac{|Y_0(N)(\mathbb{F}_{p^2})|}{g(Y_0(N))} \geq \frac{|Y(N)(\mathbb{F}_{p^2})|}{g(Y(N))}. \tag{4.5}$$

But, we have already proved that the number $\frac{|Y(N)(\mathbb{F}_{p^2})|}{g(Y(N))}$ tends to the Drinfeld - Vladuţ bound, $p-1$, when N tends to infinity. So, the family of curves $Y_0(N)$ also attains the Drinfeld - Vladuţ bound.

QED

4.2 Geometric Approach

In this approach, we are interested in classical modular curves $Y_0(\ell)$ which is a moduli space of triples (E, E', ϕ) where $\phi : E \longmapsto E'$ is a cyclic isogeny of order ℓ between the elliptic curves E and E'. We assume that ℓ is a prime different than characteristic, p. The family of curves $Y_0(\ell)$ attains the Drinfeld-Vladuţ bound over $\mathbb{F}_{p^2}$ where $(\ell, p) = 1$. Deligne and Rapoport have proved that $Y_0(\ell)$ is defined over $\mathbb{Z}$ and has good (smooth) reduction modulo prime p for $(\ell, p) = 1$ (see [DE-RA]). So, in positive characteristic p where $(\ell, p) = 1$, the modular curve is still a moduli space of triples (E, E', ϕ). Recall that there are two types of elliptic curves in positive characteristic. The first type is an elliptic curve whose endomorphism ring is abelian. Let us call it *ordinary elliptic curve*. The second type of elliptic curves is that whose endomorphism ring is nonabelian. Let us call it *supersingular elliptic curve*. If E is a supersingular elliptic curve then its j invariant, $j(E)$, is in $\mathbb{F}_{p^2}$ and the point represented by the triple (E, E', ϕ) is a rational point of $Y_0(\ell)$ over $\mathbb{F}_{p^2}$ and number of supersingular elliptic curves is enough big so that the curves $Y_0(\ell)$ over $\mathbb{F}_{p^2}$ for $(\ell, p) = 1$, reach the Drinfeld-Vladuţ bound. For more explanation and proofs, one can refer to the book of Tsfasman and Vladuţ on algebraic geometric codes [TS-VLA] .

The modular curve $Y_0(\ell)$ has great significance in coding theory. They have maximum number of rational points asymptotically. So, the Goppa codes constructed on modular curves will have best asymptotic parameters on the segment where the algebraic geometric bound is lying above the Gilbert Varshamov bound. But, the difficulty arises in describing $Y_0(\ell)$ in an algebraic equation. Because of this, constructing Goppa codes on modular curves is one of the research problems in coding theory.

Our main problem is to find a way of constructing Goppa codes on modular curves $Y_0(\ell)$. We embed $Y_0(\ell)$ into $\mathbb{P}(\Omega)$ where $\Omega = \Omega[Y_0(\ell)]$ is the space of regular differentials of $Y_0(\ell)$. It is really an embedding of $Y_0(\ell)$ for $\ell \geq 71$ since it is not hyperelliptic for the case $\ell \geq 71$ (see [OGG]). Then Goppa codes are configurations of rational points on $\mathbb{P}(\Omega)$. We can divide the problem into two problems. One is finding a basis for the space $\Omega[Y_0(\ell)]$ and the other one is describing the hyperplanes of $\Omega[Y_0(\ell)]$ whose elements vanish at rational points. Consider

$$Y_0(\ell) \longrightarrow \mathbb{P}(\Omega^*)$$

$$x \mapsto \Omega_x = \{w \in \Omega : w(x) = 0\}.$$

Any configuration of the points Ω_x in $\mathbb{P}(\Omega^*)$ which does not lie in a hyperplane in $\mathbb{P}(\Omega^*)$, where Ω^* is the dual space of Ω, gives a Goppa code on the modular space $Y_0(\ell)$ for a set of $\mathbb{F}_q$ rational points x. So, we should find a description of regular differentials that vanish at a given rational point $x \in Y_0(\ell)(\mathbb{F}_q)$.

4.3 Group Theoretical Approach

The group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ acts on the modular curve $Y(N)$. Also, the action preserves inverse images of the natural projection

$$Y(N) \longrightarrow \mathbb{P}^1.$$

In particular, it preserves the inverse image of a supersingular point. The image of a cusp point under the action is also a cusp point. So, naturally the Goppa codes on modular curves $Y(N)$ are group codes.

4.3.1 Group Codes

Group codes are the generalization of cyclic codes. Let G be a finite group. Consider the group algebra over the field $\mathbb{F}_q$

$$\mathbb{F}_q[G] = \{f : G \longrightarrow \mathbb{F}_q\}$$

where the addition is inherited from $\mathbb{F}_q$ and the multiplication is defined as convolution:

$$(f_1 \cdot f_2)(g) = \sum_{h \in G} f_1(h) \cdot f_2(h^{-1} \cdot g).$$

The action of G on $\mathbb{F}_q[G]$ is defined as

$$(fg)(h) = f(gh).$$

For a subgroup $H \subset G$, the invariant space is defined as

$$\mathbb{F}_q[G/H] = \{f : G \longrightarrow \mathbb{F}_q, f(gh) = f(g) \ \ \forall g \in G \ \ \forall h \in H\}.$$

Both $\mathbb{F}_q[G]$ and $\mathbb{F}_q[G/H]$ are vector spaces over $\mathbb{F}_q$ of dimension order of G and index of H respectively. The group G itself forms a basis for the space $\mathbb{F}_q[G]$ whose elements are considered as functions sending themselves to the identity and vanishing on the other group elements. Similarly, we can form a basis $\{f_1, ..., f_k\}$ for the space $\mathbb{F}_q[G/H]$ where each function f_i is nonzero constant function on ith coset of H and vanishing on the other cosets. Then, any subspace C of $\mathbb{F}_q[G/H]$ is a linear code. In general, any G submodules of the G module $M = \mathbb{F}_q[G/H_1] \oplus \cdots \oplus \mathbb{F}_q[G/H_m]$ are linear codes for arbitrary subgroups $H_1, ..., H_m$ of G.

In contrast, let C be a linear code in $\mathbb{F}_q^n$. Let $G \subset S_n \cap AutC$ be a subgroup of automorphism group of C acting by permutation of coordinates. Let $B = \{e_1, ..., e_n\}$ be a basis for $\mathbb{F}_q^n$. The group G acts on B. Write B as disjoint union of G orbits, $B = O_1 \cup ... \cup O_m$ where each O_i is an orbit of a subset of B. Let H_i be stabilizer of any point in O_i. Then, O_i is G isomorphic to G/H_i. We can identify $\mathbb{F}_q^n$ as a G module:

$$\mathbb{F}_q^n \simeq \mathbb{F}_q[G/H_1] \oplus \cdots \oplus \mathbb{F}_q[G/H_m] \tag{4.6}$$

and the code C will be a G submodule in this G module.

So, we have seen that it is possible to consider the linear codes as group modules, in particular as group ideals. Also, group modules are linear codes. We can carry this notion on Goppa codes on curves. Let X be a smooth projective curve over $\mathbb{F}_q$. Let C be a $(X, P, D)_\Omega$ construction on X. Let $G \subset Aut_{\mathbb{F}_q}(X)$ be a subgroup of $\mathbb{F}_q$ automorphisms of X such that both the set P and the divisor D are left invariant under the action of G. In this case, $g^*(w) \in \Omega(D_0 - D) \forall \omega \in \Omega(D_0 - D), \forall g \in G$, where D_0 is the divisor defined by P. So, g^* will permute the coordinates of any code word of C. So, $G \subset S_n \cap AutC$. In conclusion, we have C is a group code lying in the G module $\mathbb{F}_q[G/H_1] \oplus \cdots \oplus \mathbb{F}_q[G/H_m]$ where H_i's are stabilizers of points in P. If we summarize this discussion, we have

Proposition 4.3.1 [TS-VLA, pp 283] *Let $G \subset Aut_{\mathbb{F}_q}(X)$, let P be a G invariant subset of $\mathbb{F}_q$ rational points of X and D be a G invariant $\mathbb{F}_q$ divisor on X. Supp$D \cap P = \emptyset$. Then the Goppa code $C = (X, P, D)_\Omega$ is a group code: $C \subset \mathbb{F}_q[G/H_1] \oplus \cdots \oplus \mathbb{F}_q[G/H_m]$ where H_i's are stabilizers of $O_i \in P$, $\{Q_1, ...Q_m\}$ being a set of orbit representatives of the action of G on P.*

We can consider the Goppa codes on $Y(N)$, defined over a field of characteristic p not dividing N, as group codes. Let D be a $PSL(2, \mathbb{Z}/N\mathbb{Z})$ invariant $\mathbb{F}_{p^2}$ rational divisor of the modular curve $Y(N)$ and $\mathcal{P}$ be a set of $\mathbb{F}_{p^2}$ rational points which is also invariant under the action of $PSL(2, \mathbb{Z}/N\mathbb{Z})$. Then the Goppa code $C = (Y(N), \mathcal{P}, D)_\Omega$ has a natural action of the group $PSL(2, \mathbb{Z}/N\mathbb{Z})$.

An example of group codes is proposed by taking D as the divisor of cusp points and $\mathcal{P}$ the set of supersingular points in [TS-VLA]. Recall that the group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ acts on the modular curve $Y(N)$ preserving the inverse images of the projection

$$\psi_N : Y(N) \longrightarrow \mathbb{P}^1. \tag{4.7}$$

So, we can consider the Goppa codes on $Y(N)$ as group codes. $\mathcal{P}$ be the set of inverse images of supersingular elliptic curves under the projection map ψ. Let S_∞ be the set of cusp points of $Y(N)$. Then, the action of $PSL(2, \mathbb{Z}/N\mathbb{Z})$

permutes the elements of S_∞. Recall that $|S_\infty| = \mu_N/N$ where $\mu_N = [\Gamma(N) : \Gamma(1)] = \frac{N^3}{2}\prod_{\ell|N}(1-\ell^{-2})$.As usual, the product is taken over primes. The only cusp point of $\mathbb{P}^1$, ∞, is an $\mathbb{F}_{p^2}$ rational point. So, the divisor $D = \sum_{Q\in S_\infty} n\cdot Q$ is defined over $\mathbb{F}_{p^2}$. Consider the code $C = (Y(N), \mathcal{P}, D)_\Omega$ over $\mathbb{F}_{p^2}$. Then we have,

Proposition 4.3.2 [TS-VLA, pp 433] *The code $C = (Y(N), \mathcal{P}, D)_\Omega$ over $\mathbb{F}_{p^2}$ has a natural action of the group $PSL(2, \mathbb{Z}/N\mathbb{Z})$. The number of the orbits of this action equals the number of $s(p)$ of supersingular values of j invariant in characteristic p. Also, the code C can be realized as a $PSL(2, \mathbb{Z}/N\mathbb{Z})$ submodule in the algebra $\mathbb{F}_{p^2}[PSL(2, \mathbb{Z}/N\mathbb{Z})]^{s(p)}$.*

We will restrict ourselves to the prime values ℓ different from p such that p does not divide $\ell^2 - 1$. In this case, the algebra $\mathbb{F}_{p^2}[PSL(2, \mathbb{Z}/\ell\mathbb{Z})]^{s(p)}$ is semisimple since the order of the group $PSL(2, \mathbb{Z}/\ell\mathbb{Z})$ is not divisible by p. Then, the problem of code construction is reduced to the description of the code as $PSL(2, \mathbb{Z}/\ell\mathbb{Z})$ submodule of $\mathbb{F}_{p^2}[PSL(2, \mathbb{Z}/\ell\mathbb{Z})]^{s(p)}$.

The main problem is investigating the structure of a group code $C = (Y(\ell), \mathcal{P}, D)_\Omega$ as $PS_2(\mathbb{F}_\ell)$ module. We propose a way of computing the characters of representations of a group code by using localization formula. This approach, including an application, is explained in detail in chapter 6.

Chapter 5

Geometric Approach

We have seen that the family of classical modular curves over a finite field $\mathbb{F}_q$ where q is a square, attains the Drinfeld-Vladuţ bound. So, the Goppa codes on modular curves have parameters lying on the algebraic geometric bound, $R = 1-\delta-(\sqrt{}(q)-1^{-1})$. So, it is known that the modular codes have good parameters. The problem is to find a feasible way to construct codes on modular curves. In this chapter we have explained the geometric approach on modular code construction in detail. There are still several open questions in the approach. Also, we have stated our developments in this approach (see [KLY-KA]).

5.1 General View

In this section we give a general overview of the geometric approach of code construction and state both the improvements and the unsolved problems.

We would like to have a canonical embedding of the curve $Y_0(\ell)$ in $\mathbb{P}(\Omega)$. So, the first problem is finding a basis for the space $\mathbb{P}(\Omega)$. That is:

Describe the space of regular differentials $\Omega = \Omega[Y_0(\ell)]$.

One can use the analytic interpretation of modular curves over $\mathbb{C}$. There is a

one to one correspondence between cusp forms of weight 2 and regular differential. Recall that a cusp form is a modular form that vanishes at each cusp (one can see the books by Shimura [SH] or by Lang [LA 1] for detailed information). So, the problem of finding a basis for the regular differential forms of the modular curve $Y_0(\ell)$ is equivalent to finding a basis for the cusp forms for the modular curves over the complex plane, $\mathbb{C}$.

We introduce two approaches on finding a basis for regular differentials. The first one is analytic and based on forming a basis for the space of cusp forms of weight 2 on $Y_0(\ell)$ in characteristic 0 (see [HE]). The second one uses the plane model $Z_0(\ell)$ of the modular curve $Y_0(\ell)$. The singular plane curve $Z_0(\ell)$ is given by the modular equation Φ_ℓ defined as

$$\Phi_\ell(X, j(\tau)) = \prod_{\gamma_i}(X - j(\ell\gamma_i\tau))$$

where $\Gamma_0(\ell)\gamma_i$'s are the right cosets of $\Gamma_0(\ell)$ in the full modular group Γ. So, the regular differentials are of the form

$$\omega = P\frac{xdy - ydx}{\Phi_z} = P\frac{xdz - zdx}{\Phi_y} = P\frac{zdy - ydz}{\Phi_x} \tag{5.1}$$

where $P = P(x, y, z)$ is a homogeneous polynomial of degree $2\ell - 3$, satisfying some extra conditions on singular points and Φ is homogeneous the modular polynomial Φ_ℓ. We should be careful that the plane model $Z_0(\ell)$ is a singular curve. So, the polynomial should satisfy some extra conditions on singular points so that the differential form $\omega = P\frac{xdy-ydx}{\Phi_z}$ has no pole. Naturally, the first step is describing those singularities. Then, we should impose local condition on the polynomial P at singular points. For instance, if a singular point is only an intersection of two smooth branches with the order of contact, say m, then P must have a zero of order at least $m - 1$ on any branch at the corresponding singular point. Then the differential form $\omega = P\frac{xdy-ydx}{\Phi_z}$ will be regular at that singular point. We should have similar conditions on the polynomial P at any singular point if the singularity is intersection of smooth branches. It seems it is difficult to determine the local conditions that P must satisfy at a cuspidal singularity.

Any configuration $\mathcal{P}$ of $\mathbb{F}_{p^2}$ rational points of $Y_0(\ell)$ is a Goppa code. That

code has a generator matrix whose columns are coordinates of the points of $\mathcal{P}$ in the space $\mathbb{P}(\Omega^*)$, dual of the projective space of regular differentials. A generator matrix for a code C is a matrix whose rows form a basis for C. So, first of all we should find out a basis for the space of regular differentials on $Y_0(\ell)$. Then, the image of a point $x \in Y_0(\ell)$ in $\mathbb{P}(\Omega^*)$ is the hyperplane in Ω consisting of $\omega \in \Omega$ such that $\omega(x) = 0$. So, we should describe the hyperspace of regular differentials vanishing at a given rational point.

The first step on code construction is describing the space of regular differentials. We introduce two approaches. The first one is an old and classical problem, based on describing the space of cusp forms. See [HE] for general information. The second one is by Klyachko ([KLY]).

5.1.1 First Approach

Recall that there is a nice analytic interpretation of modular curves over $\mathbb{C}$. A modular curve is a quotient space of the action of some specific subgroups of $SL_2(\mathbb{Z})$ on upper half plane, $\mathbb{H}$. For $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, the action was defined as

$$\sigma(z) = \frac{az+b}{cz+d} \quad , \quad z \in \mathbb{H}.$$

Then σ is map from $\mathbb{H}$ to $\mathbb{H}$ since

$$\mathrm{im}(\frac{az+b}{cz+d}) = \frac{\mathrm{im}(z)}{|cz+d|^2} > 0 \text{ for } z \in \mathbb{H}.$$

As usual, $\mathbb{H}$ has complex topology generated by open disks.

Any subgroup G of Γ which contains the principal congruence subgroup of level ℓ,

$$\Gamma(\ell) = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \ell \right\}.$$

for some $\ell \in \mathbb{Z}^+$ is called congruence subgroup. For such a congruence subgroup G we have also discrete topology. Then, as a topological group, G is an action

on $\mathbb{H}$ which is defined as

$$(\sigma, z) = \sigma z = \frac{az+b}{cz+d} \ , \ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \text{ and } z \in \mathbb{H}.$$

For a point $z \in \mathbb{H}$, recall that the set $Gz = \{gz : g \in G\}$ as the orbit of z under G. Then, the quotient space $\mathbb{H}/G$ is the set of all G - orbits of points on $\mathbb{H}$. Any two points z_1, z_2 which are in the same orbit with respect to G are called G equivalent and we denote this fact as $z_1 \sim_G z_2$. Now, let's introduce the quotient topology on $\mathbb{H}/G$.

To compactify $\mathbb{H}/\Gamma$, we should add the point ∞. For this, let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \infty$ since Γ (and any subgroup of Γ) acts on $\mathbb{Q} \cup \infty$. For a congruence subgroup G of Γ the quotient space $\mathbb{Q} \cup \infty/G$ is finite. That is, there exists finitely many orbits of G for the space $\mathbb{Q} \cup \infty$.

Recall that the modular curve $Y_0(\ell)$ is the quotient space $\mathbb{H}^*/\Gamma_0(\ell)$ where $\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod \ell \right\}$.

Constructing a basis for the space of regular differential forms on $Y_0(\ell)$ in characteristic 0 is one of the famous problems of the field of modular forms and elliptic functions. The space of cusp forms of weight 2 is isomorphic to the space of regular differential forms on a modular curve. Hecke has claimed that a certain explicit set of Θ series coming from quaternion algebras form a basis for the space of cusp forms of weight 2 on $Y_0(\ell)$ where ℓ is a prime (see [HE], p 884). Unfortunately, Hecke's conjecture did not hold in general. However, Hecke's idea led Pizer and he conjectured that a slightly modified version of the set of theta series proposed by Hecke can be a basis set for cusp forms (see [PI]). Then, taking reduction of cusp forms modulo a prime p, we get differential forms of $Y_0(\ell)$ in characteristic p.

5.1.2 Second Approach

Constructing a basis of differentials via cusp forms is one approach. Another approach makes use of a singular plane model of $Y_0(\ell)$. The curve $Y_0(\ell)$ has

singular plane model $Z_0(\ell)$ coming from projection

$$\pi : Y_0(\ell) \to \mathbb{P}^2 \tag{5.2}$$

given in affine coordinates by $\rho \mapsto (j(E), j(E'))$ where $\rho : E \to E'$ is a cyclic isogeny of degree ℓ between elliptic curves E and E' . One can define the curve $Z_0(\ell)$ explicitly by classical modular equation

$$Z_0(\ell) : \Phi_\ell(X, Y) = 0 \tag{5.3}$$

We make use the plane model $Z_0(\ell)$ to construct a basis for the space Ω of $Y_0(\ell)$. For this, first let us introduce how the regular differentials are formed for plane curves:

5.1.2.1 Differentials of a Plane Curve

Let $X \subset \mathbb{P}^2$ be a curve given by $F(x, y, z) = 0$ of degree d. If X is smooth then the regular differentials are of the form

$$\omega = P\frac{xdy - ydx}{F_z} = P\frac{xdz - zdx}{F_y} = P\frac{zdy - ydz}{F_x} \tag{5.4}$$

where $P = P(x, y, z)$ is a homogeneous polynomial of degree $d - 3$. We follow this approach to construct regular differentials. However, the projective plane model $Z_0(\ell)$ is a singular curve. But the differentials on a singular plane curve are still of the form given in equation 5.4. We should impose some additional local conditions on the polynomial P at singular points. Let us now assume that X is singular. If X has a normal self intersection of m smooth branches at a point $x \in X$ then P should have vanishing derivatives on each branch up to order $m-2$ at the point x to supply that the differential ω in 5.4 is regular at x. We should impose some other local conditions on the polynomial P at a general singular point.

So, constructing the regular differentials on $Z_0(\ell)$ as in the form 5.4, we should first describe the singularities of $Z_0(\ell)$. After then, next problem is to determine the local conditions on the polynomials P given in 5.4 at singular points. So, first let us examine the singularities of $Z_0(\ell)$.

5.2 Singularities of Modular Curve

One of the model of affine part $X_0(\ell)$ of $Y_0(\ell)$ is plane model, $Z_0(\ell)$, given by the projection map

$$\pi : X_0(\ell) \longrightarrow \mathbb{A}^2$$

$$(E, E', \phi) \longmapsto (j(E), j(E')).$$

Well, the points $(j(E), j(E'))$ of $Z_0(\ell)$, where there is a cyclic isogeny $\phi : E \longmapsto E'$ of degree ℓ, are exactly roots of the modular equation $\Phi_\ell(X, Y) = 0$, where $\Phi_\ell(X, Y) \in \mathbb{C}[X, Y]$ is a minimal polynomial such that $\Phi_\ell(j(z), j(\ell z)) = 0$. One can find singularities of $Z_0(\ell)$ via the modular equation $\Phi_\ell(X, Y) = 0$. But calculating Φ_ℓ is somehow very difficult problem even for small ℓ's (see [CO]).

The aim of this section is to describe the singularities of $\overline{Z_0(\ell)}$ for prime ℓ in both characteristic 0 and positive characteristic. We have shown that both in positive characteristic $p > 3$ for $(p, \ell) = 1$ and in characteristic 0, the map

$$\pi : X_0(\ell) \longmapsto \mathbb{A}^2$$

$$(E, E', \phi) \longmapsto (j(E), j(E')) \tag{5.5}$$

is immersion. That is, the differential, $d\pi$, is injective. So, π is local embedding of nonsingular branches. Hence, all singularities of $Z_0(\ell)$ are self intersections. We have also proved that two points of $\overline{Z_0(\ell)}$ at ∞ in projective space are cusps for odd prime ℓ which are analytically equivalent to the cusp of 0, given by the equation $x^\ell = y^{\ell-1}$ (see Proposition 5.2.2). These two cusps are permuted by Atkin-Lehner involution. The multiplicity of singularity of each cusp is $\frac{(\ell-1)(\ell-2)}{2}$. This result is valid in any characteristic $p \neq 2, 3$.

In the first part of the section we have found singularities of plane model $\overline{Z_0(\ell)}$ of $Y_0(\ell)$ for prime ℓ. What is new in this part is the description of the singularities of the plane projective curve $\overline{Z_0(\ell)}$. First, we have investigated that all singularities of $Z_0(\ell)$ are double points. Such self intersection comes from existence of two cyclic isogenies $\sigma, \rho : E \longmapsto E'$ of degree ℓ, which are not equivalent modulo automorphisms of E and E'. That is, $\sigma \neq \epsilon' \rho \epsilon$ where $\epsilon \in \mathrm{Aut}(E)$ and $\epsilon' \in \mathrm{Aut}(E')$. Then, the triples (E, E', σ) and (E, E', ρ) represent

two different points on $X_0(\ell)$ whereas their projections, $(j(E), j(E'))$ is a single point on $Z_0(\ell)$ which is a singularity. It turns out that there exists at most two such nonequivalent isogenies of degree ℓ and hence all self intersections are double (see theorem 5.2.4).

We have described self intersections explicitly. In two different parameterization in a neighborhood of a point of $Z_0(\ell)$ we get two different tangent vectors. That is, singularities of $Z_0(\ell)$ in characteristic 0 are not just double self intersections but they are exactly simple nodes (normal self intersections) (see proposition 5.2.3).

The following theorem describes the singularities of $Z_0(\ell)$ in characteristic 0. That theorem is combination of theorem 5.2.4 and proposition 5.2.3.

Theorem 5.2.1 *There exists a one to one correspondence between self intersections of the curve $Z_0(\ell)$ over $\mathbb{C}$ and the elliptic curves E having complex multiplication $\alpha : E \longmapsto E$ such that*

i) $N(\alpha) = \alpha\overline{\alpha} = \ell^2$ and

ii) $\frac{\alpha}{\ell}$ is not root of unity.

Moreover, all self intersections are simple nodes.

Using the theorem above, we can relate number of singularities of $Z_0(\ell)$ with Hurwitz class number

$$H(-D) = \sum \frac{2}{|\mathrm{Aut}Q|}$$

where summation is over equivalence classes of binary integer quadratic forms $Q = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, of discriminant $-D = b^2 - 4ac$. The quadratic form $x^2 + y^2$ is counted with weight $\frac{1}{2}$ and the quadratic form $x^2 + xy + y^2$ is counted with weight $\frac{1}{3}$. All other quadratic forms in other equivalent classes are counted with weight 1. Then, number of nodes is given as:

Theorem 5.2.2 *Number of simple nodes of $Z_0(\ell)$ is*

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2 - 4\ell^2).$$

As explained above the projective closure, $\overline{Z_0(\ell)}$, has additional two singular points at ∞, which are cusps analytically equivalent to $x^\ell = y^{\ell-1}$ (see proposition 5.2.2). The multiplicity of this cusp is $\frac{(\ell-1)(\ell-2)}{2}$. As a corollary, we get an independent proof of Hurwitz class number formula by comparing two genus formulas for $Y_0(\ell)$. One of them is calculated by Hurwitz genus formula, given in 1.6 independent from the projective plane model , $\overline{Z_0(\ell)}$, and the other one is calculated from the projective plane model, $\overline{Z_0(\ell)}$, by Plücker genus formula including singularities of $\overline{Z_0(\ell)}$. That independent proof of Hurwitz class number formula confirms all the statements in characteristic 0:

Corollary 5.2.1

$$\sum_{t=-2\ell}^{2\ell} H(\ell^2 - 4t^2) = 2\ell^2 + \ell$$

where $H(0) = \frac{-1}{12}$.

In the latter part, we have described the singularities of the projective plane model, $\overline{Z_0(\ell)}$ in positive characteristic $p > 3$.

First of all, since the canonical projection $\pi : X_0(\ell) \longmapsto \mathbb{A}^2$ is immersion in any characteristic $p \neq 2, 3$; we get

Proposition 5.2.1 *The singularities of $Z_0(\ell)$ in positive characteristic $p > 3$ are just multiple self intersections.*

In positive characteristic also, the singularities of $Z_0(\ell)$ are the points $(j(E), j(E'))$ where there exists at least two cyclic isogenies $\sigma, \rho : E \longmapsto E'$ of degree ℓ and those two isogenies σ, ρ are not equivalent modulo automorphisms of E and E'.

The results can be viewed in two parts:

i) The singularities corresponding to ordinary elliptic curves in positive characteristic. An ordinary elliptic curve defined over a finite field is an elliptic curve whose endomorphism ring is an order in an imaginary quadratic field.

ii) The singularities corresponding to supersingular elliptic curves. Recall that a supersingular elliptic curve is an elliptic curve in positive characteristic p, which has no element of order p. In difference with ordinary elliptic curves, endomorphism ring of a supersingular curve is an order in quaternion algebra. In addition, there are finitely many supersingular elliptic curves in positive characteristic p and all of them are defined over $\mathbb{F}_{p^2}$.

Structure of singularities of the affine curve $Z_0(\ell)$ essentially depends on these two types of elliptic curves.

It turns out that , the multiplicity of a self intersection is a power of characteristic p for ordinary case whereas it is more complicated for supersingular case. The following statement describes the multiplicities:

Theorem 5.2.3 *Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\rho, \sigma \in Hom(E, E')$, of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in End(E)$ where $\widehat{\rho}$ is the dual isogeny of ρ. If p^r is the p part of the conductor of $\mathbb{Z}[\alpha]$ then the multiplicity of intersection of these two branches is*

i) p^r if p splits in $\mathbb{Q}(\alpha)$,

i) $2 + 2p + \cdots + 2p^{r-1} + p^r$ if p is prime in $\mathbb{Q}(\alpha)$, and

ii) $2 + 2p + \cdots + 2p^{r-1} + 2p^r$ if p is ramified in $\mathbb{Q}(\alpha)$.

5.2.1 Singularities in Characteristic 0

Let $Z_0(\ell)$ be the curve given by the modular equation $\Phi_\ell(X, Y) = 0$. For a lattice $L = [z, 1]$, all its sublattices $L' \subset L$ of index ℓ has j invariant $j(\ell\gamma z)$ where $\Gamma_0(\ell)\gamma$ is a coset of $\Gamma_0(\ell)$ for $\gamma \in \Gamma$. We have $\Phi_\ell(j(L), j(L')) = 0$. For the fixed

$L = [z, 1]$, solutions of $\Phi_\ell(j(L), j(L')) = 0$ are $(j(\gamma_i z), j(\ell\gamma_i z)) = (j(z), j(\ell\gamma_i z))$ where $\Gamma_0(\ell)\gamma_i, \quad i = 1, \cdots, \ell + 1$, are all cosets of $\Gamma_0(\ell)$. Hence, the point $(j(z), j(\ell z))$ is generic point of the curve $Z_0(\ell)$. So, the curve $Z_0(\ell)$ has the local parameterization $z \longmapsto (j(z), j(\ell z))$. Let

$$\pi : X_0(\ell) \longrightarrow Z_0(\ell)$$

be a projection map taking the point (E, E', ϕ), where ϕ is a cyclic isogeny of degree ℓ between elliptic curves E and E', to $(j(E), j(E')) = (j(z), j(\ell z))$. Now, we are going to investigate singularities of projective closure $\overline{Z_0(\ell)}$ of $Z_0(\ell)$. First, $Z_0(\ell)$ can have only self intersections as singularity. For $z \in \mathbb{H}$ such that one of the elliptic curves $\mathbb{C}/[z, 1]$ or $\mathbb{C}/[\ell z, 1]$ has only trivial automorphisms then the tangent vector $(j'(z), \ell j'(\ell z))$ is not zero. Hence, locally there exists a tangent vector. If both of the curves E and E' have nontrivial isomorphisms then either both of the elliptic curves are $E = E' = \mathbb{C}/\mathbb{Z}i + \mathbb{Z}$ or $E = E' = \mathbb{C}/\mathbb{Z}\omega + \mathbb{Z}$. Because the curves $\mathbb{C}/\mathbb{Z}i + \mathbb{Z}$ and $\mathbb{C}/\mathbb{Z}\omega + \mathbb{Z}$ are not isogenous.

For the case $E = E' = \mathbb{C}/\mathbb{Z}i + \mathbb{Z}$ or $E = E' = \mathbb{C}/\mathbb{Z}\omega + \mathbb{Z}$, the point $(j(E), j(E')) \in Z_0(\ell)$ has also tangent vector. Let $(j(E), j(E')) = (j(z), j(\ell z)) \in Z_0(\ell)$ where $\mathrm{Aut}(E) = \mathrm{Aut}(E') = \{\pm 1, \pm i\}$. Then, at the point $(j(E), j(E'))$ our local parameter is $t = \left(\frac{z-i}{iz-1}\right)^2$. Hence tangent vector is

$$\begin{aligned} \frac{d}{dt}(j(z), j(\ell z)) &= (\frac{d}{dt}j(z), \frac{d}{dt}j(\ell z)) \\ &= \left(\frac{\frac{dj(z)}{dz}}{\frac{dt}{dz}}, \frac{\frac{dj(\ell z)}{dz}}{\frac{dt}{dz}}\right) \end{aligned}$$

Both numerators and denumerators vanish as z tends to i. Hence, taking limit we get

$$\frac{d}{dt}(j(z), j(\ell z)) = \left(\frac{\frac{d^2 j(z)}{dz^2}}{\frac{d^2 t}{dz^2}}, \frac{\frac{d^2 j(\ell z)}{dz^2}}{\frac{d^2 t}{dz^2}}\right)$$

which is nonzero since $j''(i) \neq 0$. Similarly, let $(j(E), j(E')) = (j(z), j(\ell z)) \in Z_0(\ell)$ where $\mathrm{Aut}(E) = \mathrm{Aut}(E') = \{\pm 1, \pm\omega, \pm\omega^2\}$. In this case our local parameter is $t = \left(\frac{z-\omega}{\omega z-1}\right)^3$ and tangent vector is

$$\frac{d}{dt}(j(z), j(\ell z)) = (\frac{d}{dt}j(z), \frac{d}{dt}j(\ell z)) = \left(\frac{\frac{dj(z)}{dz}}{\frac{dt}{dz}}, \frac{\frac{dj(\ell z)}{dz}}{\frac{dt}{dz}}\right)$$

again both numerators and denumerators vanish at $z = \omega$ and hence taking limit as z tends to ω we get

$$\frac{d}{dt}(j(z), j(\ell z)) = \left(\frac{\frac{d^2 j(z)}{dz^2}}{\frac{d^2 t}{dz^2}}, \frac{\frac{d^2 j(\ell z)}{dz^2}}{\frac{d^2 t}{dz^2}} \right).$$

Again both numerators and denumerators vanish at $z = \omega$. So, taking limit again as $z \longrightarrow \omega$ we get

$$\frac{d}{dt}(j(z), j(\ell z)) = \left(\frac{\frac{d^3 j(z)}{dz^3}}{\frac{d^3 t}{dz^3}}, \frac{\frac{d^3 j(\ell z)}{dz^3}}{\frac{d^3 t}{dz^3}} \right)$$

which is nonzero at $z = \omega$ since $j'''(\omega) \neq 0$.

Therefore, we have seen that the curve $Z_0(\ell)$ can have just self intersections as singularities. Well, actually there exists self intersections. Recall that $Y_0(\ell)$ has two points at ∞ represented by the cusps ∞ and 0. So, the plane model $\overline{Z_0(\ell)}$ of $Y_0(\ell)$ has two points at ∞. For odd prime ℓ, those points are cusps as singularity. Precisely:

Proposition 5.2.2 *$\overline{Z_0(\ell)}$ has two cusps as singularity at ∞ for odd prime ℓ. Each of the singularity has multiplicity $\frac{(\ell-1)(\ell-2)}{2}$.*

Proof: At the point ∞ of $Y_0(\ell)$ we have the parameterization $z \longmapsto q = e^{2\pi i z}$. So, $\overline{Z_0(\ell)}$ has parameterization

$$(j(q) : j(q^\ell) : 1) \text{ at } \infty.$$

We have $j(q) = \frac{c}{q} + \sum_{n \geq 0} c_n q^n$ where c and c_n's are constants. Hence

$$(j(q) : j(q^\ell) : 1) = (q^{\ell-1} + \sum_{n \geq 0} \frac{c_n}{c} q^{n+\ell} : 1 + \sum_{n \geq 0} \frac{c_n}{c} q^{n(\ell+1)} : q^\ell).$$

Let $x = q^{\ell-1}$ and $z = q^\ell$. Then the point $(j(q) : j(q^\ell) : 1)$ of $\overline{Z_0(\ell)}$ is analytically isomorphic to $(x : 1 : z)$. Let X be the curve given by $f(x, z) = x^\ell - z^{\ell-1} = 0$. We have the inclusion $k[t^\ell, t^{\ell-1}] \subset k[t]$ and the multiplicity of the singularity of the curve X at $(0, 0)$ is, by definition, the dimension of $k[t]/k[t^\ell, t^{\ell-1}]$. But, that dimension is nothing but the number of monomials of $k[t]$ which are not in $k[t^\ell, t^{\ell-1}]$. Those monomials are exactly t^n where $n = b\ell - a(\ell - 1)$, $\ell - 1 >$

$b \geq a \geq 0$. We have $\frac{(\ell-1)(\ell-2)}{2}$ choice of such a and b. Hence, multiplicity of the singularity at $(j(q) : j(q^\ell) : 1)$ is $\frac{(\ell-1)(\ell-2)}{2}$.

The other point of $Y_0(\ell)$ at ∞ is represented by the cusp 0. Let $w = \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}$. Then $w\Gamma_0(\ell)w^{-1} = \Gamma_0(\ell)$. By Atkin - Lehner involution

$$w : z \longmapsto -\frac{1}{\ell z}$$

0 is transformed to ∞. Therefore, projection of 0 to $\overline{Z_0(\ell)}$ also has singularity of multiplicity $\frac{(\ell-1)(\ell-2)}{2}$. Remark that, for $\ell = 2$ we have no singularity on the points of $\overline{Z_0(\ell)}$ at ∞.

QED

Now, let's describe the self intersections of $Z_0(\ell)$ in affine space:

Theorem 5.2.4 *There exists a one to one correspondence between self intersections of the curve $Z_0(\ell)$ over $\mathbb{C}$ and the elliptic curves E having complex multiplication such that $\exists \alpha \in$ End(E) satisfying*

i) $N(\alpha) = \alpha\overline{\alpha} = \ell^2$ and

ii) $\frac{\alpha}{\ell}$ is not root of unity.

Moreover, all self intersections are double.

Proof: Assume we have two different points (E, E', σ) and (E, E', ρ) in $X_0(\ell)$. Difference comes from the isogenies $\sigma, \rho \in$ Hom(E, E'). Then, there is a self intersection on the point $(j(E), j(E')) \in Z_0(\ell)$. Since those two triples (E, E', σ) and (E, E', ρ) represent two different points on $X_0(\ell)$, σ is not equivalent to ρ modulo automorphisms of E and E'. That is, $\sigma \neq \varepsilon'\rho\varepsilon$ for any $\varepsilon \in$ Aut(E) and $\varepsilon' \in$ Aut(E'). Because, otherwise we would have $\varepsilon(ker\rho) = ker\sigma$ for some $\varepsilon \in$ Aut(E) which means the triples represent the same point on the curve $X_0(\ell)$.

The isogeny $\widehat{\rho}\sigma \in$ End(E), where $\widehat{\rho}$ is the dual isogeny of ρ, has degree ℓ^2 and

$\widehat{\rho}\sigma$ is not multiplication by ℓ since otherwise $\rho = \sigma$. Hence E has CM. Similarly $\widehat{\sigma}\rho \in \text{End}(E')$ and $\widehat{\sigma}\rho \neq [\ell]$. Hence, E' has also CM.

Now, let $\alpha = \widehat{\rho}\sigma \in \text{End}(E)$. Then $N(\alpha) = \deg(\widehat{\rho}\sigma) = \deg\widehat{\rho}\,\deg\sigma = \ell^2$ and $\alpha = \widehat{\rho}\sigma \neq \widehat{\rho}\varepsilon'\rho\varepsilon = \varepsilon'\varepsilon\ell$ and hence $\frac{\alpha}{\ell}$ is not root of unity.

Conversely, for an elliptic curve $E = \mathbb{C}/[z, 1]$ assume $\exists\alpha \in \text{End}(E)$ satisfying

i) $N(\alpha) = \alpha\overline{\alpha} = \ell^2$ and

ii) $\frac{\alpha}{\ell}$ is not root of unity.

Let $ker\alpha = C$ and $C' \subset C$ be a cyclic subgroup of C of order ℓ. Then, there exists an elliptic curve E' and an isogeny $\sigma \in \text{Hom}(E, E')$ such that $ker\sigma = C'$. Then let's define $\rho' \in \text{Hom}(E', E)$, $\rho'(z') = \alpha(z)$ where $\sigma(z) = z'$. Then ρ' is cyclic of order ℓ and $\widehat{\rho'} \in \text{Hom}(E, E')$ is, cyclic isogeny of degree ℓ, not equivalent to σ modulo isomorphisms of E and E'. Assume, on the contrary that, $\sigma = \varepsilon'\widehat{\rho'}\varepsilon$. Then $\alpha = \rho'\varepsilon'\widehat{\rho'}\varepsilon = \varepsilon'\varepsilon\ell$ and hence $\frac{\alpha}{\ell}$ would be root of unity, contradiction. Therefore σ and $\widehat{\rho'}$ are not equivalent. That is, the point $(j(E), j(E'))$ is singular.

Now, let's assume $\exists\sigma, \rho \in \text{Hom}(E', E)$, $\sigma \neq \varepsilon\rho\varepsilon$ for any $\varepsilon \in \text{End}(E)$ and $\varepsilon' \in \text{End}(E')$ and $\alpha = \widehat{\rho}\sigma$. Let $E = \mathbb{C}/[z, 1]$, $E' = \mathbb{C}/[\ell z, 1]$. There are three possibilities for the decomposition of the ideal (ℓ) in the ring of integers $\mathcal{O}_K$ of the imaginary quadratic field $\mathbb{Q}(z)$:

i) (ℓ) is a prime ideal: In that case $(\alpha)(\overline{\alpha}) = (\ell)^2$. So, $(\alpha) = (\ell)$ which means $\frac{\alpha}{\ell}$ is a root of unity.

ii) $(\ell) = \mathcal{P}^2$, where $\mathcal{P}$ is a prime ideal. Then, $(\alpha)(\overline{\alpha}) = \mathcal{P}^4$ which implies that $(\alpha) = \mathcal{P}^2$ and hence, again, $\frac{\alpha}{\ell}$ is a root of unity.

iii) $(\ell) = \mathcal{P}\mathcal{P}'$ where $\mathcal{P}$ and $\mathcal{P}'$ are prime ideals. Then $(\alpha)(\overline{\alpha}) = \mathcal{P}^2\mathcal{P}'^2$. If $(\alpha) = \mathcal{P}\mathcal{P}'$ then again $(\alpha) = (\ell)$ which means $\frac{\alpha}{\ell}$ is a root of unity. So, for elliptic curves $E = \mathbb{C}/[z, 1]$ such that $\exists\alpha \in \text{End}(E)$ with $N(\alpha) = \ell^2$ and $\frac{\alpha}{\ell}$ is not a root of unity, we must have $(\ell) = \mathcal{P}\mathcal{P}'$ in the ring of integers $\mathcal{O}_K$ of $\mathbb{Q}(z)$ and $(\alpha) = \mathcal{P}^2$. Then $(\overline{\alpha}) = \mathcal{P}'^2$ and $\overline{\alpha}$ correspondence to the isogeny $\widehat{\sigma}\rho$ whereas $\alpha = \widehat{\rho}\sigma$. Hence,

all self intersections are double.

QED

Well, self intersections of the curve $Z_0(\ell)$ are indeed simple nodes (normal self intersections). Let's prove this fact in the following proposition:

Proposition 5.2.3 *All self intersections of the curve $Z_0(\ell)$ are simple nodes.*

Before proving the proposition, let's introduce a lemma:

Lemma 5.2.1 *Let $(j(E), j(E')) \in Z_0(\ell)$. Assume $(j(E), j(E'))$ is a self intersection. Then $Aut(E) = Aut(E')$.*

Proof of lemma: Assume $(j(E), j(E')) \in Z_0(\ell)$ is a self intersection. Then $\exists \rho, \sigma \in \mathrm{Hom}(E, E')$, cyclic isogenies of degree ℓ and σ is not equivalent to ρ modulo automorphisms of E and E'. Then, $\alpha = \widehat{\rho}\sigma \in \mathrm{End}(E)$ and $\alpha\overline{\alpha} = \ell^2$. If $\mathrm{Aut}(E) = \{\pm 1, \pm i\}$, then $\ell \equiv 1 \bmod 4$ and $\exists \lambda \in \mathbb{Z}[i]$, $\lambda\overline{\lambda} = \ell$, $\lambda \neq \overline{\lambda}$. So, $\alpha = \lambda^2$, $\sigma = \lambda$, $\rho = \overline{\lambda}$ and $\frac{\bar{\lambda}}{\lambda} \notin \mathbb{Z}[i]$. Similarly, if $\mathrm{Aut}(E) = \{\pm 1, \pm\omega, \pm\omega^2\}$ then $\exists \lambda \in \mathbb{Z}[\omega]$ such that $\alpha = \lambda^2$ and $\sigma = \lambda$, $\rho = \overline{\lambda}$. Hence, in both cases $\mathrm{Aut}(E) = \mathrm{Aut}(E')$, which is enough to prove the lemma. Because, if $\mathrm{Aut}(E) = \{\pm 1\}$ and $\{\pm 1\} \subsetneq \mathrm{Aut}(E')$ we can manipulate the same process as above for E' and get $\{\pm 1\} \subsetneq \mathrm{Aut}(E)$ which is contradiction.

QED

Proof of proposition: Assume $(j(E), j(E'))$ is self intersection. Then $\exists \alpha \in \mathrm{End}(E)$ such that $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity. Let σ and ρ be two nonequivalent cyclic isogenies of degree ℓ in $\mathrm{Hom}(E, E')$. We have three steps:

Step I: Assume $\mathrm{Aut}(E) = \{\pm 1\}$. Then by the lemma $\mathrm{Aut}(E') = \{\pm 1\}$. Let $E = \mathbb{C}/L$. Then $ker\sigma = \frac{L'}{L}$, $ker\rho = \frac{L''}{L}$ and $\frac{\alpha}{\ell}L' = L''$. Let

$$L = [\omega_1, \omega_2], \quad L' = [\frac{\omega_1}{\ell}, \omega_2] \text{ and } L'' = [\omega_1, \frac{\omega_2}{\ell}].$$

Then, $\frac{\alpha}{\ell}\frac{\omega_1}{\ell} = a\omega_1 + b\frac{\omega_2}{\ell}$ and $\frac{\alpha}{\ell}\omega_2 = c\omega_1 + d\frac{\omega_2}{\ell}$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. We have $\frac{\omega_1}{\omega_2} = z$, local parameter. Then $(j(z), j(\ell z))$ is a self intersection. On the other hand $\frac{z}{\ell} = \frac{a\ell z+b}{c\ell z+d} \Longrightarrow (j(z), j(\frac{a\ell z+b}{c\ell z+d}))$ is another parameterization of the self intersection. Since $\mathrm{Aut}(E) = \mathrm{Aut}(E') = \{\pm 1\}$, $j'(z)$ and $j'(\frac{z}{\ell})$ are nonzero. Then, tangent vectors for those two parameterizations are

$$(j'(z), \frac{1}{\ell}j'(\frac{z}{\ell})) \text{ and } (j'(z), \frac{\ell}{(c\ell z+d)^2}j'(\frac{a\ell z+b}{c\ell z+d})).$$

If, assume on the contrary, those two tangent vectors are equal then we would get

$$\frac{1}{\ell} = \frac{\ell}{(c\ell z+d)^2}.$$

But, $c\ell z + d = \alpha$. Hence, $\alpha^2 = \ell^2$. Contradiction since $\frac{\alpha}{\ell}$ is not a root of unity. Hence, we have different tangent vectors and so the self intersection is a simple node.

Step II: Assume $\mathrm{Aut}(E) = \{\pm 1, \pm i\}$. Same construction as in Step I for $L, L', L'' \Longrightarrow \alpha = c\ell z + d, \frac{\omega_1}{\omega_2} = z$. But, in this case, our local parameter is $t = \left(\frac{z-i}{iz-1}\right)^2$. Hence tangent vectors are

$$\begin{aligned} \frac{d}{dt}(j(z), j(z/\ell)) &= (\frac{d}{dt}j(z), \frac{d}{dt}j(z/\ell)) \\ &= \left(\frac{\frac{dj(z)}{dz}}{\frac{dt}{dz}}, \frac{\frac{dj(z/\ell)}{dz}}{\frac{dt}{dz}}\right) \end{aligned}$$

Both numerators and denumerators vanish as z tends to i. Hence, taking limit we get

$$\frac{d}{dt}(j(z), j(z/\ell)) = \left(\frac{\frac{d^2j(z)}{dz^2}}{\frac{d^2t}{dz^2}}, \frac{\frac{d^2j(z/\ell)}{dz^2}}{\frac{d^2t}{dz^2}}\right)$$

which is nonzero since $j''(i) \neq 0$ and $\frac{d^2t}{dz^2} \neq 0$ at $z = i$. Let $\frac{\frac{d^2j(z)}{dz^2}}{\frac{d^2t}{dz^2}} = A \neq 0$. Then $\frac{\frac{d^2j(z/\ell)}{dz^2}}{\frac{d^2t}{dz^2}} = \frac{1}{\ell^2}A$ and

$$\lim_{z \longrightarrow i} \frac{\frac{dj(\frac{a\ell z+b}{c\ell z+d})}{dz}}{\frac{dt}{dz}} = \frac{\frac{d^2j(\frac{a\ell z+b}{c\ell z+d})}{dz^2}}{\frac{d^2t}{dz^2}}$$

$$= \frac{\frac{d}{dz}\left(\frac{\ell}{(c\ell z+d)^2} j'\left(\frac{a\ell z+b}{c\ell z+d}\right)\right)}{\frac{d^2t}{dz^2}}$$
$$= \frac{\ell^2}{(c\ell z+d)^4} A$$

If these two tangent vectors were equal then we get

$$\frac{1}{\ell^2} A = \frac{\ell^2}{(c\ell z+d)^4} A = \frac{\ell^2}{\alpha^4} A \Longrightarrow \alpha^4 = \ell^4.$$

Contradiction. Hence, tangent vectors are different. So, again we have a simple node.

Step III: In this last step, let's assume $\mathrm{Aut}(E) = \{\pm 1, \pm\omega \pm \omega^2\}$. Then, this time our parameter is $t = \left(\frac{z-\omega}{\omega z-1}\right)^3$ and tangent vectors are

$$\left(\frac{dj(z)}{dt}, \frac{dj(z/\ell)}{dt}\right) = \left(\frac{\frac{d^3j(z)}{dz^3}}{\frac{d^3t}{dz^3}}, \frac{\frac{d^3j(z/\ell)}{dz^3}}{\frac{d^3t}{dz^3}}\right)$$

since $j'(z) = j''(z) = 0$ but $j'''(z) \neq 0$ for $z \sim_\Gamma \omega$ and $\frac{dt}{dz} = \frac{d^2t}{dz^2} = 0$ but $\frac{d^3t}{dz^3} \neq 0$ at $z = \omega$. The other tangent vector is

$$\left(\frac{dj(z)}{dt}, \frac{dj(\frac{a\ell z+d}{c\ell z+d})}{dt}\right) = \left(\frac{\frac{d^3j(z)}{dz^3}}{\frac{d^3t}{dz^3}}, \frac{\frac{d^3j(\frac{a\ell z+b}{c\ell z+d})}{dz^3}}{\frac{d^3t}{dz^3}}\right).$$

Let, again, $\frac{dj(z)}{dt}$ at $z = \omega$ be A. Then,

$$\frac{dj(z/\ell)}{dt} = \frac{\frac{d^3j(z/\ell)}{dz^3}}{\frac{d^3t}{dz^3}} = \frac{1}{\ell^3} A \text{ and}$$

$$\frac{dj(\frac{a\ell z+d}{c\ell z+d})}{dt} = \frac{\frac{d^3j(\frac{a\ell z+b}{c\ell z+d})}{dz^3}}{\frac{d^3t}{dz^3}} = \frac{\ell^3}{(c\ell z+d)^6} A.$$

Hence, again, if the tangent vectors were equal then $\frac{1}{\ell^3} A = \frac{\ell^3}{(c\ell z+d)^6} A \Longrightarrow \alpha^6 = \ell^6$. Contradiction. So, tangent vectors are different. Therefore, in all cases, we have seen that self intersections of $Z_0(\ell)$ are simple nodes.

QED

We have described the nodes of the curve $Z_0(\ell)$. Now, let's count them. Before, let me introduce Hurwitz class number. Hurwitz class number is defined as

$$H(-D) = \sum \frac{2}{|\mathrm{Aut}Q|}$$

where summation is over equivalence classes of binary integer quadratic forms $Q = ax^2 + bxy + cy^2,\ \ a, b, c \in \mathbb{Z}$, of discriminant $-D = b^2 - 4ac$. The quadratic form $x^2 + y^2$ is counted with weight $\frac{1}{2}$ and the quadratic form $x^2 + xy + y^2$ is counted with weight $\frac{1}{3}$. All other quadratic forms in other equivalent classes are counted with weight 1. Another interpretation of Hurwitz class number is that if $\mathcal{O}$ is an order with discriminant $-D$ in an imaginary quadratic field K then

$$H(-D) = H(\mathcal{O}) = \sum_{\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_K} \frac{2}{|\mathcal{O}'^*|} h(\mathcal{O}')$$

Where $\mathcal{O}_K$ is the ring of integers of K (see [CO]). Now, we are ready to state the theorem:

Theorem 5.2.5 *Number of nodes of $Z_0(\ell)$ is*

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2 - 4\ell^2).$$

Proof: There is a one to one correspondence between nodes of $Z_0(\ell)$ and elliptic curves E such that $\exists \alpha \in \ \mathrm{End}(E); \alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity. Let K be an imaginary quadratic field with discriminant $-d_K$, $d_K \in \mathbb{Z}^+$. Then, let $\alpha = \frac{a+b\sqrt{-d_k}}{2} \in \mathcal{O}_K$. $\alpha\overline{\alpha} = \ell^2 \Longrightarrow b^2 d_K = 4\ell^2 - a^2$. Hence, α is in the order $\mathcal{O} \in \mathcal{O}_K$ with the conductor b and also in any order $\mathcal{O}'$, $\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_K$. Number of elliptic curves, up to isomorphism, whose endomorphism rings are $\mathcal{O}$ is $h(\mathcal{O}) = h(-b^2 d_K)$. By the way, for $a = \ell$ we have $\alpha = \frac{\pm\ell + \ell\sqrt{-3}}{2}$ and $\frac{\alpha}{\ell} = \pm\frac{1}{2} + \frac{\sqrt{-3}}{2}$, which is a root of unity and if $a = 0$ then $d_K = 4$ and $\alpha = \pm\ell i$. Hence, again $\frac{\alpha}{\ell} = \pm i$, which is also a root of unity.

If $(j(z), j(\ell z)) \in Z_0(\ell)$ is a node and $\mathrm{Aut}\mathbb{C}/[z, 1] = \{\pm 1, \pm i\}$ then, $\Gamma_z = \{\mathrm{id}\ , S\}$ and hence, $(j(Sz), j(\ell Sz)) \in Z_0(\ell)$ is also a node. Similarly, for a node $(j(z), j(\ell z)) \in Z_0(\ell)$, if $\mathrm{Aut}\mathbb{C}/[z, 1] = \{\pm 1, \pm\omega, \pm\omega^2\}$

then, $\Gamma_z = \{\mathrm{id}\ , ST, (ST)^2\}$. Hence $(j(STz), j(\ell STz)) \in Z_0(\ell)$ and $(j((ST)^2z), j(\ell(ST)^2z)) \in Z_0(\ell)$ are also nodes of $Z_0(\ell)$. Therefore number of nodes of $Z_0(\ell)$ is

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2).$$

QED

As a corollary of the theorem we get an independent proof of the Hurwitz class number formula:

Corollary 5.2.2

$$\sum_{t=-2\ell}^{2\ell} H(\ell^2-4t^2) = 2\ell^2+\ell.$$

Proof: The projective closure $\overline{Z_0(\ell)}$ has two singular points at ∞, which are permuted by Atkin-Lehner involution. They are analytically isomorphic to $x^\ell = z^{\ell-1}$ with multiplicity of singularity $\frac{(\ell-1)(\ell-2)}{2}$.

Genus of $Y_0(\ell)$ is

$$g = \frac{(d-1)(d-2)}{2} - \quad \text{number of singularities}$$

where d is the degree of the modular equation. Then

$$\begin{aligned} g &= \frac{(2\ell-1)(2\ell-2)}{2} - 2\frac{(\ell-1)(\ell-2)}{2} - \sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2) \\ &= (\ell^2-1) - \sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2). \end{aligned}$$

On the other hand

$$\begin{aligned} g &= \frac{\ell+1}{12} - \frac{1}{4}\left(1+\left(\frac{-1}{\ell}\right)\right) - \frac{1}{3}\left(1+\left(\frac{-3}{\ell}\right)\right) \\ &= \frac{\ell-6}{12} - \frac{1}{4}\left(\frac{-1}{\ell}\right) - \frac{1}{3}\left(\frac{-3}{\ell}\right). \end{aligned}$$

We have for $d_K = 3$, $h(-d_K) = 1$ since there is only one elliptic curve E with $\mathrm{Aut}E = \{\pm 1, \pm\omega, \pm\omega^2\}$. Then, for the order $\mathcal{O} \subset \mathbb{Q}(\omega)$ with conductor ℓ, we

have $h(-3\ell^2) = \frac{1\cdot\ell}{3}\left(1 - \left(\frac{-3}{\ell}\right)\frac{1}{\ell}\right)$. Then, $H(-3\ell^2) = \frac{1\cdot\ell}{3}\left(1 - \left(\frac{-3}{\ell}\right)\frac{1}{\ell}\right) + \frac{1}{3}$. Because, the only orders including $\mathcal{O}$ are $\mathcal{O}$ itself and $\mathcal{O}_K$.

With a similar argument $h(-4\ell^2) = 1$ since there is only one elliptic curve E with $\mathrm{Aut}E = \{\pm 1, \pm i\}$. Let $\mathcal{O}$ be an order in $\mathbb{Q}(i)$ with conductor ℓ. Then, $h(-4\ell^2) = \frac{1\cdot\ell}{2}\left(1 - \left(\frac{-4}{\ell}\right)\frac{1}{\ell}\right) = \frac{\ell}{2}\left(1 - \left(\frac{-1}{\ell}\right)\frac{1}{\ell}\right)$ and hence $H(-4\ell^2) = \frac{\ell}{2}\left(1 - \left(\frac{-1}{\ell}\right)\frac{1}{\ell}\right) + \frac{1}{2}$ since the orders including $\mathcal{O}$ are $\mathcal{O}$ itself and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i$. By definition, $H(0) := -\frac{1}{12}$. Then

$$(\ell^2 - 1) - \sum_{0<t<2\ell, t\neq\ell} H(t^2 - 4\ell^2) = \frac{\ell - 6}{12} - \frac{1}{4}\left(\frac{-1}{\ell}\right) - \frac{1}{3}\left(\frac{-3}{\ell}\right) \Longrightarrow$$

$$\sum_{0<t<2l, t\neq\ell} H(t^2 - 4\ell^2) = \ell^2 - 1 + \frac{6 - \ell}{12} + \frac{1}{4}\left(\frac{-1}{\ell}\right) + \frac{1}{3}\left(\frac{-3}{\ell}\right) \Longrightarrow$$

$$\begin{aligned} 2\sum_{0<t\leq 2\ell,} H(t^2 - 4\ell^2) + H(4\ell^2) &= 2\ell^2 - 2 + \frac{6 - \ell}{6} + \frac{1}{2}\left(\frac{-1}{\ell}\right) + \frac{2}{3}\left(\frac{-3}{\ell}\right) \\ &+ \frac{2}{3}\ell\left(1 - \left(\frac{-3}{\ell}\right)\frac{1}{\ell}\right) + \frac{\ell}{2}\left(1 - \left(\frac{-1}{\ell}\right)\frac{1}{\ell}\right) + 1 \\ &= 2\ell^2 - \ell. \end{aligned}$$

QED

5.2.2 Singularities in Characteristic $p > 3$

In this section, we describe singularities of $Z_0(\ell)$ in characteristic $p > 3$ where ℓ is also prime not equal to p. In this section we always assume that ℓ is prime.

Recall that two cusps of $\overline{Z_0(\ell)}$ in positive characteristic are equivalent to $x^\ell = y^{\ell-1}$. Since $x^\ell = y^{\ell-1}$ has good reduction modulo any prime p, we have again two cusps of $\overline{Z_0(\ell)}$ for prime ℓ in positive characteristic with multiplicities $\frac{(\ell-1)(\ell-2)}{2}$ (see proposition 5.2.2).

A very powerful result of Deligne and Rapoport enables us to characterize the points of the modular curve $X_0(\ell)$ in positive characteristic:

Theorem 5.2.6 (Deligne and Rapoport) [DE-RA] *$X_0(\ell)$ is defined over $\mathbb{Z}[\frac{1}{\ell}]$ and has good (smooth) reduction modulo prime $p > 3$ where $(\ell, p) = 1$ and $X_0(\ell)$ mod p parameterize isogenies $\psi : E \longrightarrow E'$ with cyclic kernel $ker\psi = \mathbb{Z}/\ell\mathbb{Z}$.*

Hence, also in positive characteristic $p > 3$, $X_0(\ell)$ for $(\ell, p) = 1$, is a moduli space for the problem of determining equivalence classes of triples (E, E', ψ) where $\psi : E \longrightarrow E'$ is a cyclic isogeny of order ℓ. Hence, in this case, we have again the projection:

$$\pi : X_0(\ell) \longrightarrow Z_0(\ell)$$

$$(E, E', \psi) \longmapsto (j(E), j(E')).$$

In positive characteristic $p \neq 2, 3$, π is also immersion as in the case characteristic 0. Let's prove this statement in the following lemma:

Proposition 5.2.4 *The singularities of $Z_0(\ell)$ in a field k of characteristic not equal to 2 or 3 are just self intersections.*

Proof: Let k be a field of characteristic not equal to 2 or 3. Consider the projection

$$X_0(\ell) \longrightarrow Z_0(\ell) \longrightarrow \mathbb{A}^1(k)$$

$$(E, E', \phi) \longmapsto (j(E), j(E')) \longmapsto j(E)$$

where $\mathbb{A}^1(k)$ is the affine space. Recall that under the projection map

$$\mathbb{H}/\Gamma_0(\ell) \longrightarrow \mathbb{H}/\Gamma$$

if the point z in $\mathbb{H}/\Gamma_0(\ell)$ is ramified then the isotropy group $\Gamma_z = \{g \in \Gamma : gz = z\}$ is not trivial and $j(z) = 0$ or $j(z) = 12^3$. For that ramified point z, the ramification index is either 2 or 3 (see proof of the theorem 3.2.3). Let me remind that j invariant is bijection between the curves given as

$$\mathbb{H}/\Gamma \longrightarrow \mathbb{C}$$

$$z \longmapsto j(z).$$

So, let $X_0(\ell)$ be the modular curve over a field k of characteristic not equal to 2 or 3. If the projection given as

$$X_0(\ell) \longrightarrow \mathbb{A}^1(k)$$

$$(E, E', \phi) \longmapsto j(E)$$

is ramified at the point (E, E', ϕ) then $j(E) = 0$ or $j(E') = 12^3$. The characteristic of k is not 2 or 3. So, 0 and 12^3 are not equal in k. Hence, ramification index of (E, E', ϕ) is either 2 or 3. The curves $X_0(\ell)$ and $\mathbb{A}^1(k)$ are smooth curves. If (E, E', ϕ) is not ramified with respect to the projection

$$X_0(\ell) \longrightarrow \mathbb{A}^1(k)$$

$$(E, E', \phi) \longmapsto j(E)$$

then (E, E', ϕ) is not ramified with respect to the projection

$$X_0(\ell) \longrightarrow Z_0(\ell)$$

$$(E, E', \phi) \longmapsto (j(E), j(E')).$$

Hence, $Z_0(\ell)$ has locally smooth parameterization at $(j(E), j(E'))$. Now, let us assume that the point (E, E', ϕ) is ramified with ramification index 2 (or 3) with respect to the projection

$$X_0(\ell) \longrightarrow \mathbb{A}^1(k)$$

$$(E, E', \phi) \longmapsto j(E).$$

Then either (E, E', ϕ) is not ramified with respect to the projection

$$X_0(\ell) \longrightarrow Z_0(\ell)$$

$$(E, E', \phi) \longmapsto (j(E), j(E'))$$

or $(j(E), j(E'))$ is not ramified with respect to the projection

$$Z_0(\ell) \longrightarrow \mathbb{A}^1(k)$$

$$(j(E), j(E')) \longmapsto j(E)$$

since 2 (or 3) is a prime number. Therefore, for any point $(j(E), j(E')) \in Z_0(\ell)$ we have locally isomorphism either between curves $Z_0(\ell)$ and $X_0(\ell)$ or between

the curves $Z_0(\ell)$ and $\mathbb{A}^1(k)$ at the point $(j(E), j(E'))$. Since the curves $X_0(\ell)$ and $\mathbb{A}^1(k)$ are smooth curves, the only possibility for singularities of $Z_0(\ell)$ is self intersections.

QED

Those self intersections of $Z_0(\ell)$ corresponds to the points $(j(E), j(E')) \in Z_0(\ell)$ where there exists at least two cyclic isogenies of degree ℓ, $\sigma \in \text{Hom}(E, E')$ and $\rho \in \text{Hom}(E, E')$ such that σ is not equivalent to ρ modulo automorphisms of E and E'. Let $\widehat{\rho}$ be dual isogeny of ρ. Then, $\alpha = \widehat{\rho}\sigma \in \text{End}(E)$. $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity.

When studying such $\alpha \in \text{End}(E)$ with $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity, we treat the singularities of $Z_0(\ell)$ in two cases: Singular points $(j(E), j(E'))$ where $\text{End}(E)$ (same as saying $\text{End}(E')$ since E and E' are isogenous) is an order in an imaginary quadratic field. Let us call those singularities as singularities at ordinary points. The other singular points $(j(E), j(E'))$ are those where $\text{End}(E)$ (same as saying $\text{End}(E')$) is an order in a quaternion algebra. Let's call them as singularities at supersingular points.

5.2.2.1 The Singularities at Ordinary Points

Let $(j(E), j(E')) \in Z_0(\ell)$ be a singular point corresponding to pair of isogenies $\sigma \in \text{Hom}(E, E')$ where E is ordinary elliptic curve. That is, $\text{End}(E)$ is an order in imaginary quadratic field. Then the self intersection is double since there is just one $\alpha = \widehat{\rho}\sigma \in \text{End}(E)$ with $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity, up to conjugacy.

We know from proposition 5.2.4 that all singularities of $Z_0(\ell)$ are self intersections. The following proposition describes those self intersections which are simple nodes of $Z_0(\ell)$ in positive characteristic and gives the number of those nodes:

Proposition 5.2.5 *Let $Z_0(\ell)$ be the plane model of $X_0(\ell)$ in characteristic $p > 3$,*

$(p,\ell) = 1$. Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\sigma,\ \rho \in\ Hom(E, E')$ of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in\ End(E)$ where $\widehat{\rho}$ is the dual of ρ. Assume p splits in $\mathbb{Q}(\alpha)$ and the conductor of $\mathbb{Z}[\alpha]$ is coprime to p. Then the singularity at $(j(E), j(E'))$ is a simple node. The number of such nodes is

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ \left(\frac{t^2-4\ell^2}{p}\right) = 1}} H(t^2 - 4\ell^2).$$

Proof: Assume $(j(E), j(E')) \in Z_0(\ell)$ is a singular point of $Z_0(\ell)$ corresponding to the pair of nonequivalent cyclic isogenies $\sigma,\ \rho \in\ \mathrm{Hom}(E, E')$ of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in\ \mathrm{End}(E)$. The self intersection is double. In characteristic 0, the singularities are nodes. Since we have a good reduction, reduction of tangent vectors are tangent vectors of reduction. Hence, the self intersection is a simple node if $\alpha^2 \not\equiv \ell^2 \bmod p$. That is, $\alpha \not\equiv \overline{\alpha} \bmod p$. Let $\alpha = \frac{a+b\sqrt{-D}}{2}$ where $-D$ is the discriminant of the field $\mathbb{Q}(\alpha)$. Then, $\alpha\overline{\alpha} = \ell^2 = \frac{a^2+b^2D}{4} \Longrightarrow b^2D = 4\ell^2 - a^2$. $\alpha \not\equiv \overline{\alpha} \bmod p \Longleftrightarrow b \not\equiv 0 \bmod p$. Anyway, b is the conductor of $\mathbb{Z}[\alpha]$ and coprime to p. Hence $(j(E), j(E'))$ is a simple node.

Now, we should count the elliptic curves E in characteristic p, whose order $\mathcal{O}$ includes α with $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity. For $\alpha = \frac{a+b\sqrt{-D}}{2}$, the order $\mathcal{O}$ has conductor b which is coprime to p. Also p must split in k. Hence, the discriminant $-D$ of k is also coprime to p. So, the discriminant $-b^2D$ of $\mathcal{O}$ is coprime to p and p splits in k. That is $\left(\frac{-b^2D}{p}\right) = \left(\frac{t^2-4\ell^2}{p}\right) = 1$. Therefore, number of nodes is

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ \left(\frac{t^2-4\ell^2}{p}\right) = 1}} H(t^2 - 4\ell^2).$$

QED

In general, self intersection points $Z_0(\ell)$ are not simple nodes. We are going to calculate multiplicity of intersection of a singularity both in ordinary case and in supersingular case by perturbation method.

We need the following lemma in calculating number of contacts of a self intersection:

Lemma 5.2.2 *Let k be an imaginary quadratic field of discriminant $-D$ and p be a prime. Then the Hurwitz class number satisfies the following relation:*

$$H(-p^{2r}D) = \begin{cases} p^r H(-D) & \text{If } p \text{ splits in } k, \\ (2 + 2p + \cdots + 2p^{r-1} + p^r)H(-D) & \text{If } p \text{ is prime in } k, \\ (1 + p + \cdots + p^r)H(-D) & \text{If } p \text{ is ramified in } k. \end{cases}$$

Proof: Let us introduce the weighted class number h^* given as $h^*(-D) = \frac{h(-D)}{|\mathcal{O}^*|}$ where $\mathcal{O}$ is the order with discriminant $-D$. Then, for positive integer $r > 0$ we have

$$h^*(-p^{2r}D) = h^*(-D)p^r \left(1 - \left(\frac{-D}{p}\right)\frac{1}{p}\right)$$

by the theorem 3.1.4. we have by definition

$$H(-D) = \sum_{f^2|D} h^*(\frac{-D}{f^2}).$$

Then

$$\begin{aligned} H(-p^{2r}D) &= \sum_{0\le\alpha\le r} h^*(-p^{2\alpha}D) = h^*(-D) + \sum_{0<\alpha\le r} h^*(-D)p^\alpha \left(1 - \left(\frac{-D}{p}\right)\frac{1}{p}\right) \\ &= H(-D)\left[1 + \sum_{0<\alpha\le r} p^\alpha \left(1 - \left(\frac{-D}{p}\right)\frac{1}{p}\right)\right] \\ &= \begin{cases} p^r H(-D) & \text{If } p \text{ splits in } k, \\ (2 + 2p + \cdots + 2p^{r-1} + p^r)H(-D) & \text{If } p \text{ is prime in } k, \\ (1 + p + \cdots + p^r)H(-D) & \text{If } p \text{ is ramified in } k. \end{cases} \end{aligned}$$

QED

For given curves X and Y over a field k, the multiplicity of intersection of the curves X and Y at a point P_0 is equal to the number of simple intersection points close to P_0 of perturbed curves $\widetilde{X}$ and $\widetilde{Y}$.

More explicitly, let $\widetilde{X(\epsilon)}$ and $\widetilde{Y(\epsilon)}$ be the family of curves over the ring $k[\epsilon]$ depending on small parameter ϵ. Then, multiplicity of intersection of the curves X and Y at a point P_0 is equal to number of intersections with multiplicities of $\widetilde{X(\epsilon)}$ and $\widetilde{Y(\epsilon)}$ at points which project to the point P_0 for $\epsilon = 0$.

Assume that the curves X and Y are over a field of positive characteristic p and $\widetilde{X}$, $\widetilde{Y}$ are liftings into characteristic 0. Let $\widetilde{X}$ and $\widetilde{Y}$ be defined over $\mathbb{Z}$ and their coordinate rings have no element of finite order. Then, multiplicity of intersection of the curves X, Y at a point P_0 is equal to multiplicity of intersection of the liftings $\widetilde{X}$ and $\widetilde{Y}$ at the points which project into P_0.

By Deligne Rapoport theorem the modular curve $Z_0(\ell)$ is defined over $\mathbb{Z}[\frac{1}{\ell}]$. For $(\ell, p) = 1$ we can view the curve $Z_0(\ell)$ as defined over $\mathbb{Z}$ while taking reduction modulo p. Therefore, multiplicity of intersection of pair of branches of $Z_0(\ell)$ in positive characteristic p corresponding to pair of nonequivalent cyclic isogenies $\sigma, \rho : E \longmapsto E'$ of degree ℓ is nothing but number of liftings of the pair (σ, ρ) in characteristic 0. So, to calculate the multiplicity we should count number of liftings. The following theorem describes multiplicity of singularities corresponding to ordinary elliptic curves:

Theorem 5.2.7 *Let $Z_0(\ell)$ be the plane model of $X_0(\ell)$ in characteristic $p > 3$, $(p, \ell) = 1$. Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\sigma,\ \rho \in\ Hom(E, E')$ of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in\ End(E)$ where $\widehat{\rho}$ is the dual of ρ. Assume p splits in $\mathbb{Q}(\alpha)$. Then the singularity at $(j(E), j(E'))$ has multiplicity p^r where p^r is p part of the conductor of $\mathbb{Z}[\alpha]$. That is, if $f = p^r c_0$ where $c_0 \not\equiv 0$ mod p then multiplicity is p^r.*

Proof: Assume $(j(E), j(E')) \in Z_0(\ell)$ is a singular point of $Z_0(\ell)$ corresponding to pair of nonequivalent cyclic isogenies $\sigma,\ \rho \in\ \mathrm{Hom}(E, E')$ of degree ℓ. Let $\alpha = \widehat{\rho}\sigma \in\ \mathrm{End}(E)$. Then $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity. Let the conductor of $\mathbb{Z}[\alpha]$ be $f = p^r c_0$, $c_0 \not\equiv 0 \bmod p$ and the discriminant of $\mathbb{Q}(\alpha)$ be $-D$. By Deuring's lifting theorem there is a unique elliptic curve E_0 in characteristic 0

whose endomorphism ring $\mathrm{End}E_0 = \mathcal{O}_0$ with conductor c_0 such that reduction of E_0 modulo p is isomorphic to E.

Consider the points $(j(A), j(A')) \in Z_0(\ell)$ over characteristic 0 such that $\mathbb{Z}[\alpha] \subset \mathrm{End}(A) \subset \mathcal{O}_0$. Then $\alpha \in \mathrm{End}(A)$ and number of such elliptic curves is $H(-f^2D)$ (see proof of theorem 5.2.5). On the other hand, the number of points $(j(A_0), j(A_0')) \in Z_0(\ell)$ with $\alpha \in \mathrm{End}(A_0)$ in characteristic p is $H(-c_0^2D)$. Hence, there exists $\frac{H(-f^2D)}{H(-c_0^2D)}$ liftings of two branches corresponding to α at the point $(j(E), j(E'))$. Since p splits in k we have $\frac{H(-f^2D)}{H(-c_0^2D)} = p^r$ (see lemma 5.2.2). Therefore multiplicity of singularity of the point $(j(E), j(E'))$ is p^r.

QED

Corollary 5.2.3 *The number of self intersections of multiplicity p^r corresponding to ordinary elliptic curves is*

$$\sum_{\substack{0<t<2\ell, t\neq\ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}_p\right)=1}} H\left(\frac{t^2-4\ell^2}{p^{2r}}\right) = \frac{1}{p^r} \sum_{\substack{0<t<2\ell, t\neq\ell \\ t^2-4\ell^2=-p^{2r}D, \left(\frac{-D}{p}\right)=1}} H(t^2-4\ell^2).$$

Proof: Let k be an imaginary quadratic field with discriminant $-D$ and p split in k. Let $\mathcal{O}$ be an order in k with conductor p^rc_0, $c_0 \not\equiv 0 \bmod p$. Let $\alpha \in k$ such that $\alpha\overline{\alpha} = \ell^2$ and $\frac{\alpha}{\ell}$ is not root of unity. For $\alpha = \frac{a+b\sqrt{-D}}{2}$, $\alpha\overline{\alpha} = \ell^2 \Longrightarrow 4\ell^2 = a^2 + b^2D$. So, $b^2D = 4\ell^2 - a^2$. If the order $\mathcal{O}$ has discriminant $-b^2D$ then $b = p^rc_0$. Hence $c_0^2D = \frac{4\ell^2-a^2}{p^{2r}}$. So, now we should count the elliptic curves in an order of discriminant $-c_0^2D$. Anyway, we have counted those kind of elliptic curves in proposition 5.2.5 and their number is

$$\sum_{\substack{0<t<2\ell, t\neq\ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}_p\right)=1}} H\left(\frac{t^2-4\ell^2}{p^{2r}}\right).$$

From the identity $H(-p^{2r}D) = p^rH(-D)$ we have the equality

$$\sum_{\substack{0<t<2\ell, t\neq\ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}_p\right)=1}} H\left(\frac{t^2-4\ell^2}{p^{2r}}\right) = \frac{1}{p^r} \sum_{\substack{0<t<2\ell, t\neq\ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}_p\right)=1}} H(t^2-4\ell^2).$$

QED

Endomorphism ring of an ordinary elliptic curve has discriminant which is p-adic square. So, to find number of all self intersections corresponding to ordinary elliptic curves let me introduce the following

Lemma 5.2.3 [KI, pp 51] *For $a \in \mathbb{Z}_p^*, a = x^2$ for $x \in \mathbb{Q}_p^*$ if and only if $a \equiv 1$ mod 8 when $p = 2$, and $a \equiv y^2$ mod p for $y \in \mathbb{Z}$ with $(y, p) = 1$ when $p \neq 2$.*

Then, number of self intersections of ordinary points is given as:

Corollary 5.2.4 *Sum of the multiplicities of all self intersections corresponding to ordinary elliptic curves is*

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ t^2 - 4\ell^2 = p-adic\ square}} H(t^2 - 4\ell^2).$$

Proof: We know that number of self intersections of multiplicity p^r corresponding to ordinary elliptic curves is

$$\frac{1}{p^r} \sum_{\substack{0 < t < 2\ell, t \neq \ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}{p}\right) = 1}} H(t^2 - 4\ell^2).$$

So, if we count those singularities with multiplicity, we get

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}{p}\right) = 1}} H(t^2 - 4\ell^2).$$

The prime number p splits in an imaginary quadratic field k with discriminant $t^2 - 4\ell^2$ if and only if $t^2 - 4\ell^2$ is a square in the p-adic field $\mathbb{Q}_p$ (see the lemma 5.2.3). So, if we count all the singularities with multiplicity corresponding to ordinary elliptic curves, we get

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ t^2 - 4\ell^2 = p-\text{adic square}}} H(t^2 - 4\ell^2).$$

QED

Corollary 5.2.5 *Sum of the multiplicities of all self intersections corresponding to supersingular elliptic curves is*

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ t^2 - 4\ell^2 \neq p-adic\ square}} H(t^2 - 4\ell^2).$$

Proof: The genus of the curve $Y_0(\ell)$ is not changed in positive characteristics also since $Y_0(\ell)$ has good reduction. So, in characteristic 0, the genus was

$$\begin{aligned} g &= \frac{(2\ell-1)(2\ell-2)}{2} - 2\frac{(\ell-1)(\ell-2)}{2} - \sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2) \\ &= (\ell^2-1) - \sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2). \end{aligned}$$

In positive characteristic, the singularities of cusps of $\overline{Z_0(\ell)}$ are same as in characteristic 0. Hence, to get the same genus as in positive characteristic, we should have number of all singularities, counted with multiplicities, of $Z_0(\ell)$ in positive characteristic must be

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2-4\ell^2).$$

But, number of singularities of $Z_0(\ell)$ with multiplicities corresponding to ordinary elliptic curves is

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ t^2 - 4\ell^2 = p-\text{adic square}}} H(t^2 - 4\ell^2).$$

Hence, number of singularities of $Z_0(\ell)$ with multiplicities corresponding to supersingular elliptic curves is

$$\sum_{\substack{0 < t < 2\ell, t \neq \ell \\ t^2 - 4\ell^2 \neq p-\text{adic square}}} H(t^2 - 4\ell^2).$$

QED

5.2.2.2 The Singularities at Supersingular Points

The singularities of $Z_0(\ell)$ corresponding to supersingular elliptic curves in positive characteristic are the most complicated ones. Those singularities may not be just double self intersections. Also, counting number of liftings of two branches is more difficult than in the case of ordinary elliptic curves.

Proposition 5.2.6 *Let E be an elliptic curve whose endomorphism ring $\mathcal{O}$ is an order in imaginary quadratic field k. Assume a given prime number p is ramified in k and E has complex multiplication $\alpha \in \mathcal{O}$. Then the reduction $\overline{E}$ of E modulo p has j invariant $j(\overline{E}) \in \mathbb{F}_p$.*

Proof: Let E be an elliptic curve whose endomorphism ring $\mathcal{O}$ is an order in an imaginary quadratic field k. Let k have discriminant $-D$ and E has complex multiplication $\alpha \in \mathcal{O}$. Then

$$\alpha = \frac{a + b\sqrt{-D}}{2} \implies N(2\alpha - a) = (2\alpha - a)\overline{(2\alpha - a)} = b^2 D.$$

Let us define $\nu_P : \mathbb{Z} \longrightarrow \mathbb{Z}$ as $\nu_P(n) = r$ where $n = p^r c_0$, $c_0 \not\equiv 0 \bmod p$. p is ramified in k. So, $\nu_p(D) \equiv 1 \bmod 2$. Hence

$$\nu_p(N(2\alpha - a)) = 2\nu_p(b) + \nu_p(D) \equiv 1 \bmod 2.$$

Let $\nu_p(N(2\alpha - a)) = 2m + 1$, $m \in \mathbb{Z}$. Let's denote $\overline{E}$ as reduction of E modulo p and let $\mathrm{End}(\overline{E})$ be a maximal order $\mathcal{O}_{\overline{E}}$ in the quaternion algebra ramified only at ∞ and at p. Then, two sided ideal class group $H_{\mathcal{O}_{\overline{E}}}$ is either trivial or cyclic group of order 2. The reduction of the isogeny $2\alpha - a$ in $\mathcal{O}_{\overline{E}}$ has order also $N(2\alpha - a) = (2\alpha - a)\overline{(2\alpha - a)}$ with $\nu_p(N(2\alpha - a)) \equiv 1 \bmod 2$. p has norm p^2 in $\mathcal{O}_{\overline{E}}$. So, the element $\beta = \frac{2\alpha - a}{p^m}$ has norm p. That is, $N(\beta) = p$. Hence, by proposition 3.1.11, $j(\overline{E}) \in \mathbb{F}_p$.

QED

In ordinary case, we have used Deuring's lifting theorem to count the number of liftings. Unfortunately, there is no statement about canonical liftings of supersingular elliptic curves. But, we follow a similar procedure as Deuring's lifting

theorem while counting the liftings of a supersingular curve via orders. However, with this mechanism we may not get all the liftings and there may be some extra liftings.

We are going to use following statement, known as Gauss genus theory, to count some special liftings:

Lemma 5.2.4 [BO-SHA, pp 247] *Let k be an imaginary quadratic field with discriminant $-D$. Let H_2 be elements of order 2 of the ideal class group of ring of integers of k. Then $H_2 = \{\mathcal{P} \mid (-D) : \mathcal{O}$ is prime ideal and $\sqcap \mathcal{P} \simeq 1\}$ and $|H_2| = 2^{t-1}$ where t is the number of distinct prime numbers which divide D. Furthermore, class number of the ring of integers of k is odd if and only if D is divisible by only one prime.*

A special type of liftings of a supersingular elliptic curve over a finite field $\mathbb{F}_p$, where $p \equiv -1 \bmod 4$, is described in the following proposition:

Proposition 5.2.7 *Let E_0 be a supersingular curve with $j(E_0) \in \mathbb{F}_p$ and $p \equiv -1$ mod 4. Let $E = \mathbb{C}/L$ be a complex elliptic curve where L is a fractional ideal in $\mathbb{Z}[\sqrt{-p}]$. Assume reduction of E modulo p is isomorphic to E_0. Then the reduction of the curve $E' = \mathbb{C}/L^{-1}$ modulo p is also isomorphic to E_0.*

Proof: Let E_0 be a supersingular curve with $j(E_0) \in \mathbb{F}_p$. Assume $p \equiv -1 \bmod 4$. Then the class number $h(-p)$ is odd by the lemma 5.2.4. Let $E = \mathbb{C}/L$ be a complex elliptic curve where L is a fractional ideal in $\mathbb{Z}[\sqrt{-p}]$.

Complex conjugation acts on j invariant as follows:

$$\overline{j(L)} = j(L^{-1}).$$

On the other hand, complex conjugation acts on prime ideals $\mathcal{P}$, where $\mathcal{P}$ divides the ideal (p), generated by p, of the class field $K \supset \mathbb{Q}(\sqrt{-p})$. We have $[K : \mathbb{Q}(\sqrt{-p})] = h(-p)$ which is odd. So, there are odd number of primes $\mathcal{P}$ dividing (p). Hence, $\exists \mathcal{P}$ such that $\mathcal{P} = \overline{\mathcal{P}}$. Then $j(L) \bmod \mathcal{P} = \overline{j(L)} \bmod \overline{\mathcal{P}}$ since

$j(L) \in \mathbb{F}_p$ and $\mathcal{P} = \overline{\mathcal{P}}$. But $\overline{j(L)} = j(L^{-1})$. Hence, the curves $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L^{-1}$ have same reduction modulo p.

QED

In general, the multiplicity of two branches of a singular point of $Z_0(\ell)$ corresponding to supersingular elliptic curve in positive characteristic is explained in the following:

Theorem 5.2.8 *Let $(j(E), j(E')) \in Z_0(\ell)$ be an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\rho, \sigma \in Hom(E, E')$, of degree ℓ. Assume E is supersingular. Let $\alpha = \widehat{\rho}\sigma \in End(E)$. If p^r is the p part of the conductor of $\mathbb{Z}[\alpha]$ then the multiplicity of intersection of these two branches is*

i) $2 + 2p + \cdots + 2p^{r-1} + p^r$ *if p is prime in $\mathbb{Q}(\alpha)$, and*

ii) $2 + 2p + \cdots + 2p^{r-1} + 2p^r$ *if p is ramified in $\mathbb{Q}(\alpha)$.*

Proof: Assume E is a supersingular curve and $(j(E), j(E')) \in Z_0(\ell)$ is an intersection of two branches corresponding to the pair of nonequivalent cyclic isogenies $\rho, \sigma \in \mathrm{Hom}(E, E')$, of degree ℓ. Let $\alpha = \widehat{\rho}\sigma$. Assume $\mathbb{Z}[\alpha]$ has the conductor $f = p^r c_0$, $c_0 \not\equiv 0 \bmod p$ in the imaginary quadratic field $\mathbb{Q}(\alpha)$ with discriminant $-D$. p is either prime or ramified in k since E is supersingular.

Let L and L' be two lattices in $\mathbb{Z}[\alpha]$ such that $\mathcal{O}_0 L = \mathcal{O}_0 L'$ where $\mathcal{O}_0$ is the order in $\mathbb{Q}(\alpha)$ with conductor c_0. Then, $\mathcal{O}_0 L$ and $\mathcal{O}_0 L'$ are lattices in $\mathcal{O}_0$ and $L \subset \mathcal{O}_0 L$, $L' \subset \mathcal{O}_0 L'$. We have $[\mathcal{O}_0 : \mathcal{O}] = p^r$. Hence $[\mathcal{O}_0 L : \mathcal{O}L] = [\mathcal{O}_0 L' : \mathcal{O}L'] = p^r$. So, the natural projection maps

$$\varphi : \mathbb{C}/L \longrightarrow \mathbb{C}/\mathcal{O}_0 L \text{ and } \psi : \mathbb{C}/L' \longrightarrow \mathbb{C}/\mathcal{O}_0 L'$$

have degree p^r. $\mathbb{C}/\mathcal{O}_0 L$ and $\mathbb{C}/\mathcal{O}_0 L'$ are isomorphic. Reduction of $\mathbb{C}/L$ ($\mathbb{C}/L'$) and $\mathbb{C}/\mathcal{O}_0 L$ ($\mathbb{C}/\mathcal{O}_0 L'$) modulo p are supersingular. Hence, reductions of φ and ψ is Fr^r (see proposition 3.1.12). Let $\overline{\mathbb{C}/L}, \overline{\mathbb{C}/L'}, \overline{\mathbb{C}/\mathcal{O}_0 L}$ and $\overline{\mathbb{C}/\mathcal{O}_0 L'}$ denote the

reductions of $\mathbb{C}/L, \mathbb{C}/L', \mathbb{C}/\mathcal{O}_0L$ and $\mathbb{C}/\mathcal{O}_0L'$ respectively. Then we have

$$Fr^r : \overline{\mathbb{C}/L} \longrightarrow \overline{\mathbb{C}/\mathcal{O}_0L} \text{ and } Fr^r : \overline{\mathbb{C}/L'} \longrightarrow \overline{\mathbb{C}/\mathcal{O}_0L'}.$$

$\overline{\mathbb{C}/\mathcal{O}_0L}$ and $\overline{\mathbb{C}/\mathcal{O}_0L'}$ are isomorphic. Hence, $\overline{\mathbb{C}/L}$ and $\overline{\mathbb{C}/L'}$ are also isomorphic. That is, $\mathbb{C}/L$ and $\mathbb{C}/L'$ have same reduction. We have $H(-c_0^2D)$ number of lattices in $\mathcal{O}_0$ whereas $H(-p^{2r}c_0^2D)$ number of lattices in orders $\mathcal{O}'$ where $\mathbb{Z}[\alpha] \subset \mathcal{O}' \subset \mathcal{O}_0$. Hence, by the above argument we get $\frac{H(-p^{2r}c_0^2D)}{H(-c_0^2D)}$ number of liftings of the curve E. Recall that

$$\frac{H(-p^2c_0^2D)}{H(-c_0^2D)} = \begin{cases} 2 + 2p + \cdots + 2p^{r-1} + p^r & \text{If } p \text{ is prime in } k, \\ 1 + p + \cdots + p^r & \text{If } p \text{ is ramified in } k. \end{cases}$$

In supersingular case there may be some extra liftings. Let p be ramified in $\mathbb{Q}(\alpha)$ and $(p) = \mathcal{P}^2$ where (p) is the principal ideal generated by p and $\mathcal{P}$ is prime ideal. Let $\mathcal{O}_0L = M$. Then we have $[M : M\mathcal{P}] = p$ and hence the natural projection map

$$\vartheta : \mathbb{C}/M\mathcal{P} \longrightarrow \mathbb{C}/M$$

has degree p. So, reduction of ϑ is Fr by the proposition 3.1.12. Let $A_{M\mathcal{P}}$ and A_M denote the reduction of elliptic curves $\mathbb{C}/M\mathcal{P}$ and $\mathbb{C}/M$ modulo p respectively. Then $j(A_{M\mathcal{P}}) = \overline{j(A_M)}$ since $A_{M\mathcal{P}}$ and A_M are supersingular elliptic curves and $Fr \in \text{Hom}(A_{M\mathcal{P}}, A_M)$. But $j(A_M) \in \mathbb{F}_p$ by proposition 5.2.6. Hence, $j(A_{M\mathcal{P}}) = j(A_M)$. That is, $\mathbb{C}/M\mathcal{P}$ and $\mathbb{C}/M$ have the same reduction modulo p. For the lattice $M\mathcal{P}$ we have $1+p+\cdots+p^r$ liftings also. If $\mathcal{P}$ is not principal then $\mathbb{C}/M\mathcal{P}$ and $\mathbb{C}/M$ are different curves. So we get $2(1+p+\cdots+p^r)$ liftings. If $\mathcal{P}$ is principal then let H_2 be set of elements of order 2 of ideal class group of ring of integers of $\mathbb{Q}(\alpha)$. $\mathcal{P} \mid (-D)$ where $(-D)$ is the ideal of ring of integers of $\mathbb{Q}(\alpha)$ generated by $-D$. Then H_2 is trivial by lemma 5.2.4. Hence, $\mathbb{Q}(\alpha)$ has discriminant $-p$ by again the lemma 5.2.4. So, $p \equiv -1 \bmod 4$. Then by the proposition 5.2.7 again we have two liftings . Hence, when p is ramified in k we have 2 extra liftings. In conclusion we have at least $2 + 2p + \cdots + 2p^{r-1} + p^r$ lifting when p is prime in k and $2(1 + p + \cdots + p^r)$ lifting when p is ramified.

Well, number of liftings are exactly $2+2p+\cdots+2p^{r-1}+p^r$ when p is prime in k and $2(1+p+\cdots+p^r)$ when p is ramified. Because, number of all singularities with multiplicities corresponding to supersingular elliptic curve is, by the corollary 5.2.5

$$\sum_{\substack{t^2-4\ell^2 \neq p-\text{adic square} \\ 0<t<2\ell, t\neq \ell}} H(t^2-4\ell^2) = \sum_{\substack{t^2-4\ell^2=-p^{2r}D, \left(\frac{-D}{p}\right)=1 \\ 0<t<2\ell, t\neq \ell}} H(t^2-4\ell^2) + \sum_{\substack{t^2-4\ell^2=-p^{2r}D, p \mid D \\ 0<t<2\ell, t\neq \ell}} H(t^2-4\ell^2) \tag{5.6}$$

On the other hand, we have seen that there is a one to one correspondence with self intersections represented by (E,α) and lattices in $\mathcal{O}_0$ when p is prime and there is a one to two correspondence with self intersections represented by (E,α) and lattices in $\mathcal{O}_0$ when p is ramified. So, number of self intersections represented by (E,α), when p prime is,

$$\sum_{\substack{0<t<2\ell, t\neq \ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}\right)=-1}} H\left(\frac{t^2-4\ell^2}{p^{2r}}\right) = \frac{1}{2+2p+\cdots+2p^{r-1}+p^r} \sum_{\substack{t^2-4\ell^2=-p^{2r}D, \left(\frac{-D}{p}\right)=1 \\ 0<t<2\ell, t\neq \ell}} H(t^2-4\ell^2),$$

and number of self intersections represented by (E,α), when p is ramified, is

$$\frac{1}{2}\sum_{\substack{0<t<2\ell, t\neq \ell \\ \left(\frac{t^2-4\ell^2}{p^{2r}}\right)=0}} H\left(\frac{t^2-4\ell^2}{p^{2r}}\right) = \frac{1}{2+2p+\cdots+2p^{r-1}+2p^r} \sum_{\substack{t^2-4\ell^2=-p^{2r}D, \left(\frac{-D}{p}\right)=1 \\ 0<t<2\ell, t\neq \ell}} H(t^2-4\ell^2)$$

The multiplicity is at least $2 + 2p + \cdots + 2p^{r-1} + p^r$ when p is prime in k and $2(1 + p + \cdots + p^r)$ when p is ramified. But, we get 5.6 exactly when the multiplicities are $2 + 2p + \cdots + 2p^{r-1} + p^r$ if p is prime in k and $2(1 + p + \cdots + p^r)$ if p is ramified.

QED

5.3 Geometric Codes on Modular Curves

Assume we can solve the problem of finding a basis for the space of differential forms Ω on $X_0(\ell)$. Let $\{\omega_1, ..., \omega_g\}$ be a basis for Ω. Then we have the canonical embedding

$$Y_0(\ell) \hookrightarrow \mathbb{P}(\Omega)$$

$$x \mapsto (\omega_1(x) : ... : \omega_g(x)) \in \mathbb{P}(\Omega)$$

For convenience, consider the dual space Ω^*. Then, any configuration $\mathcal{P}$ of $\mathbb{F}_{p^2}$ rational points of $Y_0(\ell)$ is a Goppa code. That code has a generator matrix whose columns are coordinates of the points of $\mathcal{P}$ in the space $\mathbb{P}(\Omega^*)$. A generator matrix for a code C is a matrix whose rows form a basis for C. So, first of all we should find out a basis for the space of regular differentials on $Y_0(\ell)$. Then, the image of a point $x \in Y_0(\ell)$ in $\mathbb{P}(\Omega^*)$ is the hyperplane in Ω consisting of $\omega \in \Omega$ such that $\omega(x) = 0$. For a given set $\{x_1, ..., x_n\}$ of rational points of $Y_0(\ell)$, let their images in $\mathbb{P}(\Omega^*)$ be hyperplanes $\sigma(x_1), ..., \sigma(x_n)$. Then the matrix $[\sigma(x_1) : ... : \sigma(x_n)]$ is a generator matrix for the corresponding Goppa code. So, the last and main problem is constructing the generator matrix for Goppa codes on $Y_0(\ell)$. More explicitly we can state this problem as follows:

Consider

$$Y_0(\ell)(\mathbb{F}_{p^2}) \longrightarrow \mathbb{P}(\Omega^*)$$

$$x \mapsto \Omega_x$$

where $\Omega_x = \{w \in \Omega : w(x) = 0\}$. Describe the space Ω_x

Asymptotically, we know that almost all $\mathbb{F}_{p^2}$ rational points of $Y_0(\ell)$ are supersingular elliptic curves. So, we can take the point x mentioned in the problem as a supersingular point.

The problem above is really much more difficult than the previous problems. The extra condition on differentials in the last problem is very hard to analyze. We don't have to know something about modular equations for the problem of determining the differential forms of $Y_0(\ell)$. But, probably we need the modular equations in order to describe the spaces Ω_x. We impose some local conditions on differential forms ω of $Y_0(\ell)$ for most of the problems. Indeed, if we consider a differential ω as in the form given in 5.4 then the local conditions on the differential ω are exactly the local conditions on the polynomial P. The last problem, which may be seen as the main problem, states that the polynomial P must vanish at supersingular points. So, we must know local parametrizations of $Z_0(\ell)$ at both singular points and at supersingular points in order to describe the the space of regular differential forms of $Y_0(\ell)$ and also to describe hyperspaces of differential forms vanishing at supersingular points . So, these problems lead us to try to find local parametrization of $Z_0(\ell)$ for each branch through both singular points and supersingular points of $Z_0(\ell)$.

Chapter 6

Representations of Modular Codes

Let X be a smooth projective algebraic curve over a finite field $\mathbb{F}_q$ and G be an arbitrary subgroup of the automorphism group of X. Assume D is a G invariant $\mathbb{F}_q$ rational divisor. Then the vector spaces $H^0(X, \mathcal{L}_D) = L(D)$ and $H^1(X, \mathcal{L}_D) = \Omega(D)$ are G modules where $\mathcal{L}_D$ is the line bundle associated to the divisor D. The Goppa code on X associated to D is the realization of the space $H^0(X, \mathcal{L}_D)$ in a coordinate system of a vector space over $\mathbb{F}_q$ defined by $\mathbb{F}_q$ rational points of X. This construction corresponds to $L(D)$ construction of functions. Similarly, the space $H^1(X, \mathcal{L}_D)$ corresponds to $\Omega(D)$ construction of differential forms (we refer to first chapter for both Ω and L constructions). The Goppa codes corresponding to $H^0(X, \mathcal{L}_D) = L(D)$ and $H^1(X, \mathcal{L}_D) = \Omega(D)$ are G modules as group codes over $\mathbb{F}_q$. The notion of group codes is given in section 4.3. The main problem in this approach is investigating the structure of a group code on X as G module.

Problem: Evaluate the action of G on the Goppa code $C = L(D)$ over $\mathbb{F}_q$.

This problem is introduced in [TS-VLA] for the case of modular curves. Let the characteristic of the field $\mathbb{F}_q$ be p. We assume that p is coprime to the order of the group G. In this case, we can consider the representations of codes

in characteristic 0. Because, the reduction modulo p of an irreducible G representation over a number field remains irreducible if p is coprime to the order of the group G. In this chapter, we propose a way of computing the characters of representations of a group code by using the localization formula when X is the modular curve $Y(\ell)$. The localization formula has several forms associated to several applications. We refer to [HEJ] for extended applications. However, the most convenient form for our use can be found in [TH].

Recall from chapter 4 that we can consider the Goppa codes on $Y(\ell)$, defined over a field of characteristic $p \neq \ell$, as group codes. Let D be a $PSL_2(\mathbb{F}_\ell)$ invariant $\mathbb{F}_{p^2}$ rational divisor of the modular curve $Y(\ell)$ and $\mathcal{P}$ be a set of $\mathbb{F}_{p^2}$ rational points which is also invariant under the action of $PSL_2(\mathbb{F}_\ell)$. Then the Goppa code $C = L(D)$ has a natural action of the group $PSL_2(\mathbb{F}_\ell)$. In this chapter we also assume that $\ell > 3$ is a prime.

For a $PSL_2(\mathbb{F}_\ell)$ invariant divisor D, the space $H^0(Y(\ell), \mathcal{L}_D)$ corresponds to $L(D)$ construction of functions. Similarly, the space $H^1(Y(\ell), \mathcal{L}_D)$ corresponds to $\Omega(D)$ construction of differential forms. We make use of the localization formula which describes the characters of the action of $PSL_2(\mathbb{F}_\ell)$ on the difference of $H^0(Y(\ell), \mathcal{L}_D)$ and $H^1(Y(\ell), \mathcal{L}_D)$ in terms of action of the group $PSL_2(\mathbb{F}_\ell)$ in fibers Ω_x and $\mathcal{L}_D(x)$ over fixed points of group elements (This is known as the localization principle). The formula reduces the problem of computing the characters to a local problem each fixed point. Moreover, we give an example by considering the canonical divisor and we have described the characters of the corresponding modular code. It turns out that the multiplicities of irreducible components of code C depends on the class number $h(-\ell)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

The last two sections can be considered as appendices of the chapter which give fundamental facts and definitions about representations of finite groups and in particular representations of $SL_2(\mathbb{F}_\ell)$.

6.1 Description of Group Codes by Trace Formula

Let X be a smooth projective algebraic variety and $g : X \to X$ be an automorphism of X having isolated fixed points, X^g. Let E be a g bundle on X with action $g : E \to E$ compatible with the action $g : X \to X$. Let $\mathcal{E}$ be the sheaf of local sections of E. Then we have the localization formula given as (cf. [TH])

Theorem 6.1.1

$$tr(g : H^*(X, \mathcal{E})) := \sum_{d=0}^{dimX} (-1)^d tr(g : H^d(X, \mathcal{E})) = \sum_{x \in X^g} \frac{tr(g : E_x)}{det(1 - g^{-1} : T_x)} \quad (6.1)$$

where T_x is the tangent space at x and E_x is the fiber of vector bundle over x.

Let X be a smooth projective curve over $\mathbb{F}_q$. Let G be a subgroup of the automorphism group of X. Let D be a G invariant $\mathbb{F}_q$ rational divisor of X. The associated Goppa code on X for the divisor D is the realization of the space $H^0(X, \mathcal{L}_D)$ in a coordinate system defined by rational points where $\mathcal{L}_D$ is the line bundle associated with the divisor D. This construction corresponds to $L(D)$ construction of functions. Similarly, the space $H^1(X, \mathcal{L}_D)$ corresponds to $\Omega(D)$ construction of differential forms (cf. chapter 2). Both constructions $H^0(X, \mathcal{L}_D)$ and $H^1(X, \mathcal{L}_D)$ are group codes as G modules (cf. chapter 4).

The action of any element g of G on $\mathcal{L}_D$ is compatible with its action on X since D is G invariant. Let us assume that g has isolated fixed points and X^g is the set of these fixed points. The quantity $tr(g : L_x)$ is the trace of g on the linear space L_x, the fiber of the linear bundle over x, and $tr(g : T_x^*)$ is the trace of g on the dual of the tangent space T_x. The action of g on both spaces L_x and T_x^* is multiplication by some root of unity since these spaces are of dimension 1. The action of g on L_x is multiplication by a complex number, say ζ_x and the action of g on the dual space T_x^* is also multiplication by a complex number say η_x. In this case, the localization formula can be given as

Theorem 6.1.2

$$\begin{aligned} tr(g : H^0(X, \mathcal{L}_D)) - tr(g : H^1(Y(\ell), \mathcal{L}_D)) &= \sum_{x \in X^g} \frac{tr(g : L_x)}{1 - tr(g : T_x^*)} \\ &= \sum_{x \in X^g} \frac{\zeta_x}{1 - \eta_x}. \end{aligned} \tag{6.2}$$

The formula reduces the problem of computing the characters to a local problem each fixed point. If D is a non-special divisor of degree bigger then the degree of a canonical divisor then $H^1(X, \mathcal{L}_D)$ is trivial. This restriction simplifies the problem further. In this case, we have the formula

$$tr(g : H^0(X, \mathcal{L}_D)) = \sum_{x \in X^g} \frac{tr(g : L_x)}{1 - tr(g : T_x^*)}. \tag{6.3}$$

Let $D = \sum_x m_x \cdot x$ be g invariant. Then $\zeta_x = \eta_x^{m_x}$. The localization formula for this form is:

Theorem 6.1.3 *For $D = \sum_x m_x \cdot x$, the localization formula is given as*

$$tr(g : H^*(X, \mathcal{L}_D)) = \sum_{x \in X^g} \frac{\eta_x^{m_x}}{1 - \eta_x}.$$

Similarly, we can write down the localization formula for $\Omega = \Omega(D)$ construction of differential forms for the divisor $D = \sum_x m_x \cdot x$. The action of g on the fiber Ω_x is multiplication by $\eta_x^{m_x+1}$ if the action of g on the fiber L_x is multiplication by $\eta_x^{m_x+}$ since $\Omega(D) = \Omega \otimes L(D)$. So,

Theorem 6.1.4 *For $D = \sum_x m_x \cdot x$, the localization formula for differentials is given as*

$$tr(g : H^*(X, \Omega_D)) = \sum_{x \in X^g} \frac{\eta_x^{m_x+1}}{1 - \eta_x}.$$

If we take the multiplicities of points of D as equal, we have simpler formula:

Theorem 6.1.5 *Let $D = \sum_x m \cdot x$. Then $\zeta_x = \eta_x^m$. As a conclusion, the localization formula is of the form*

$$tr(g : H^*(X, \mathcal{L}_D)) = \sum_{x \in X^g} \frac{\eta_x^m}{1 - \eta_x}.$$

6.1.1 Application to Modular Curves

As we have pointed out, the group $PSL_2(\mathbb{F}_\ell)$ acts on the modular curve $Y(\ell)$. Let D be a $PSL_2(\mathbb{F}_\ell)$ invariant $\mathbb{F}_{p^2}$ rational divisor and $\mathcal{P}$ be a $PSL_2(\mathbb{F}_\ell)$ invariant set of $\mathbb{F}_{p^2}$ rational points. Then, $PSL_2(\mathbb{F}_\ell)$ acts also the corresponding Goppa code constructed by D and $\mathcal{P}$ on $Y(\ell)$. In this section, we propose a way of finding the characters of this action and we have computed the characters of representation of the code $C = L(K)$ corresponding to a canonical divisor K over the modular curve $Y(\ell)$, which is isomorphic to the space of regular differentials. Then, $H^1(Y(\ell), \mathcal{L}_K) \simeq \mathbb{C}$ and $H^0(Y(\ell), \mathcal{L}_K) \simeq \Omega$, the space of holomorphic differentials on $Y(\ell)$. By Riemann Roch theorem, we have

$$\dim H^0(Y(\ell), \mathcal{L}_K) = g(Y(\ell))$$

where $g(Y(\ell)) = 1 + \frac{(\ell-6)(\ell^2-1)}{24}$ is the genus for prime ℓ.

The localization formula for this case is given as

$$tr(g : H^0(Y(\ell), \mathcal{L}_K)) = 1 + \sum_{x \in Y(\ell)^g} \frac{tr(g : T_x^*)}{1 - tr(g : T_x^*)}. \tag{6.4}$$

where 1 in the formula corresponds to the trace of g on $\mathbb{C}$ and T_x^* is the dual of the tangent space at x.

It is clear that the only possible fixed points for any $g \in PSL_2(\mathbb{F}_\ell)$ are ramified points of the natural projection

$$Y(\ell) \longrightarrow Y(1) \simeq \mathbb{P}^1.$$

Recall that the set of points of ramification index 2 is the inverse image of i, the set of points of ramification index 3 is the inverse image of ω, third root of unity, and the set of points of ramification index ℓ is the set of cusp points. All the remaining points are not ramified. So, the only group elements of $PSL_2(\mathbb{F}_\ell)$ which may have fixed points are those having a conjugate lying in one of the subgroups $< s >$, $< h >$ or $< e_1^+ >$ where $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the generator of stabilizer of i, $h = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ is the generator of stabilizer of ω and $e_1^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is the

generator of the stabilizer of ∞. Remark that all the elements of the group $< s >$ are conjugate. Similarly, all the elements of the group $< h >$ are conjugate. But the elements of $< e_1^+ >$ are conjugate to either $e_1^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $e_\varepsilon^+ = \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}$ where ε denotes a quadratic nonresidue in $\mathbb{F}_\ell$. Then, there are only four conjugacy classes on which the trace is nontrivial. These classes are defined by $s, h, e_1^+, e_\varepsilon^+$. So, we should calculate the traces of these four elements on Ω. We give the traces in a statement and prove it one by one:

Theorem 6.1.6

$$tr(s:\Omega) = 1 - \frac{1}{4}(\ell - \left(\frac{-1}{\ell}\right)),$$

$$tr(h:\Omega) = 1 - \frac{1}{3}(\ell - \left(\frac{-3}{\ell}\right)),$$

$$tr(e_1^+:\Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \ mod\ 4, \\ \frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \ mod\ 4 \end{cases} \tag{6.5}$$

and

$$tr(e_\varepsilon^+:\Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \ mod\ 4, \\ -\frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \ mod\ 4 \end{cases} \tag{6.6}$$

where $\ell > 3$ is a prime, $h(-\ell)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-\ell})$ and $\left(\frac{*}{\ell}\right)$ is the Legendre symbol.

All the other group elements which are not conjugate any of h, s, e_1^+ and e_ϵ^+ have trace equal to 1.

We prove the theorem as a sequence of following lemmas.

Lemma 6.1.1 $tr(s:\Omega) = 1 - \frac{1}{4}(\ell - \left(\frac{-1}{\ell}\right))$

Proof: The centralizer

$$Z(< s >) = \{g : gs = sg\} = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x^2 + y^2 = 1\}$$

in $SL_2(\mathbb{F}_\ell)$. At the same time, the normalizer of $< s >$, $N(< s >) = \{g : gSg^{-1} \in < s >\}$ is equal to $Z(< s >)$. The number of fixed points of s in $SL_2(\mathbb{F}_\ell)$ is the order of the normalizer. But normalizer is equal the centralizer and hence its order is the number of the solutions of $x^2 + y^2 = 1$ in $\mathbb{F}_\ell$ which is $\ell - \left(\frac{-1}{\ell}\right)$ where $\left(\frac{-1}{\ell}\right)$ is the Legendre symbol. Also, s has order 2 and hence trace of s on one dimensional space T_x^* is second root of unity, -1. But we should take care that the centralizer of s in $PSL_2(\mathbb{F}_\ell)$ is $Z(< s >)/ \pm 1$. Hence

$$tr(s : \Omega) = 1 - \frac{1}{4}(\ell - \left(\frac{-1}{\ell}\right)).$$

QED

Lemma 6.1.2 $tr(h : \Omega) = 1 - \frac{1}{3}(\ell - \left(\frac{-3}{\ell}\right))$

Proof: The number of fixed points is the order of normalizer

$$N(< h >) = \{g : g < h > g^{-1} =< h >\}$$

in $SL_2(\mathbb{F}_\ell)$. We have the centralizer

$$Z(< s >) = \{g : gs = sg\} = \{\begin{pmatrix} x & -y \\ y & x+y \end{pmatrix} : x^2 + xy + y^2 = 1\}$$

and hence $|Z(< s >)| = \ell - \left(\frac{-3}{\ell}\right)$. Then

$$tr(h : \Omega) = 1 + [z(h) :< h >](\frac{\omega}{1-\omega} + \frac{\omega^{-1}}{1-\omega^{-1}})$$

where ω is the third root of unity. An easy calculation shows that $\frac{\omega}{1-\omega} + \frac{\omega^{-1}}{1-\omega^{-1}} = -1$. So

$$tr(h : \Omega) = 1 - \frac{1}{3}(\ell - \left(\frac{-3}{\ell}\right))$$

QED

For computing traces of $e_1^+ : \Omega$ and $e_\epsilon^+ : \Omega$ we need the following lemma:

Lemma 6.1.3 [SHI, Lemma 3]

$$\sum_a \binom{a}{\ell} \frac{1}{1-\xi^a} = \begin{cases} 0, & \text{if } \ell \equiv 1 \bmod 4, \\ \sqrt{-\ell}h(-\ell), & \text{if } \ell \equiv 3 \bmod 4 \end{cases} \tag{6.7}$$

where $h(-\ell)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

Lemma 6.1.4

$$tr(e_1^+ : \Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \bmod 4, \\ \frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \bmod 4 \end{cases} \tag{6.8}$$

and

$$tr(e_\varepsilon^+ : \Omega) = \begin{cases} 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 1 \bmod 4, \\ -\frac{\sqrt{-\ell}h(-\ell)}{2} + 1 - \frac{(\ell-1)}{4}, & \text{if } \ell \equiv 3 \bmod 4 \end{cases} \tag{6.9}$$

where $h(-\ell)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

Proof: Centralizer of both e_1^+ and e_ε^+ is

$$\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_\ell\}$$

in $SL_2(\mathbb{F}_\ell)$, and the normalizer of e_1^+ is

$$N(e_1^+) = \{g : ge_1^+g^{-1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, x \text{ quadratic residue}\}.$$

Hence, $[N(e_1^+) : Z(e_1^+)]$ is the number of quadratic residues, $\frac{\ell-1}{2}$.

So,

$$tr(e_1^+ : \Omega) = 1 + \sum_{a \ q.residue} \frac{\xi^a}{1-\xi^a}$$

where ξ is an ℓth root of unity. Similarly

$$tr(e_\varepsilon^+ : \Omega) = 1 + \sum_{n \ q.nonresidue} \frac{\xi^n}{1-\xi^n}.$$

Then, we have

$$tr(e_1^+ : \Omega) - tr(e_\varepsilon^+ : \Omega) = \sum_a \binom{a}{\ell} \frac{\xi^a}{1-\xi^a} \tag{6.10}$$

$$= \sum_a \binom{a}{\ell} \frac{1}{1-\xi^a}. \tag{6.11}$$

The quantity

$$\sum_a \binom{a}{\ell} \frac{1}{1-\xi^a}$$

is equal to

$$\begin{cases} 0, & \text{if } \ell \equiv 1 \bmod 4, \\ \sqrt{-\ell}h(-\ell), & \text{if } \ell \equiv 3 \bmod 4 \end{cases} \tag{6.12}$$

by previous lemma where $h(-\ell)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

On the other hand,

$$tr(e_1^+ : \Omega) + tr(e_\varepsilon^+ : \Omega) = 2 + \sum_a \frac{\xi^a}{1-\xi^a} \tag{6.13}$$

$$= 2 + tr(\frac{\xi}{1-\xi}) \tag{6.14}$$

$$= 2 - (\ell - 1) + tr(\frac{1}{1-\xi}). \tag{6.15}$$

For calculating $tr(\frac{1}{1-\xi})$, consider

$$\prod_{1<a<\ell} (x - \xi^a) = x^{\ell-1} + x^{\ell-2} + \cdots + 1.$$

Taking logarithmic derivatives of both sides:

$$\sum_{1<a<\ell} \frac{1}{x-\xi^a} = \frac{1 + 2x + \cdots + (\ell-1)x^{\ell-2}}{1 + \cdots + x^{\ell-1}}.$$

Letting $x = 1$ we get

$$tr(\frac{1}{1-\xi}) = \sum_{1<a<\ell} \frac{1}{1-\xi^a} = \frac{\ell-1}{2}.$$

Inserting the last quantity to the equation 6.15, we get the summation of the traces:

$$tr(e_1^+ : \Omega) + tr(e_\varepsilon^+ : \Omega) = 2 - \frac{\ell-1}{2}. \tag{6.16}$$

We have already computed the difference of the traces. By combining these two linear equations, we get the formulas 6.9 and 6.8.

QED

The multiplicities of the irreducible representations in the decomposition of the representation on Ω is given in the following theorem. The irreducible representations of $SL_2(\ell)$ are given in section 6.3.2. We follow the notations of this section.

Theorem 6.1.7 *Let $\chi = \chi_\rho$ be the character of a nontrivial irreducible representation ρ of $SL_2(\ell)$ which is trivial at -1. The multiplicity m_χ of ρ in Ω is given as*

$$m_\chi = \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) + \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] \qquad (6.17)$$

when $\ell \equiv 1 \ mod\ 4$ and

$$\begin{aligned} m_\chi &= \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) \\ &+ \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] + \frac{1}{2\ell}h(-\ell)\sqrt{(}-\ell)[\bar{\chi}(e_1^+) - \bar{\chi}(e_\epsilon^+)] \end{aligned} \qquad (6.18)$$

when $\ell \equiv 3 \ mod\ 4$. Here $\bar{\chi}$ is the complex conjugation of χ and $h(-\ell)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$.

The multiplicity is 0 for trivial representation.

Proof: Let m_χ be the multiplicity of an irreducible character of $SL_2(\ell)$ in Ω. Then we have the formula

$$m_\chi = \frac{1}{|SL_2(\ell)|}\sum_{g\in SL_2(\ell)} \bar{\chi}(g) tr(g:\Omega)$$

where $\bar{\chi}$ is the complex conjugation of χ. For simplicity we can write to formula as

$$m_\chi = \frac{1}{|SL_2(\ell)|}\sum_{g\in SL_2(\ell)} \bar{\chi}(g) + \frac{1}{|SL_2(\ell)|}\sum_{g\in SL_2(\ell)} \bar{\chi}(g)(tr(g:\Omega) - 1).$$

The quantity $\sum_{g\in SL_2(\ell)} \bar{\chi}(g)$ is zero except χ is identity representation and it is 1 otherwise. We follow the notations in 6.3.3. Let c_g be the number elements in the

conjugacy class of g. The dimension of Ω is the genus $g(Y(\ell)) = 1 + \frac{(\ell-6)(\ell^2-1)}{24}$. Then, the multiplicity of a nontrivial χ is given as

$$\begin{aligned} m_\chi &= \frac{1}{\ell(\ell^2-1)}[c_s\bar{\chi}(s)(tr(s:\Omega)-1) + c_h\bar{\chi}(h)(tr(h:\Omega)-1) \\ &+ c_{e_1^+}\bar{\chi}(e_1^+)(tr(e_1^+:\Omega)-1) + c_{e_1^-}\bar{\chi}(e_1^-)(tr(e_1^-:\Omega)-1) \\ &+ c_{e_\epsilon^+}\bar{\chi}(e_\epsilon^+)(tr(e_\epsilon^+:\Omega)-1) + c_{e_\epsilon^-}\bar{\chi}(e_\epsilon^-)(tr(e_\epsilon^-:\Omega)-1) \\ &+ 2(g(Y(\ell))-1)\chi(1)]. \end{aligned} \tag{6.19}$$

where the quantity $(g(Y(\ell)) - 1)\dim\chi$ is entered in the summation twice since we add it both for identity and for minus identity. We have the equality for the traces

$$tr(e_\epsilon^+ : \Omega) = tr(e_\epsilon^- : \Omega)$$

and

$$tr(e_1^+ : \Omega) = tr(e_1^- : \Omega)$$

since e_ϵ^+ (respectively e_1^+) is equivalent to e_ϵ^- (respectively e_1^-) modulo ± 1. Then the multiplicity is equal to

$$\begin{aligned} m_\chi &= \frac{1}{\ell(\ell^2-1)}[c_s\bar{\chi}(s)(tr(s:\Omega)-1) + c_h\bar{\chi}(h)(tr(h:\Omega)-1) \\ &+ (c_{e_1^+}\bar{\chi}(e_1^+) + c_{e_1^-}\bar{\chi}(e_1^-))(tr(e_1^+:\Omega)-1) \\ &+ (c_{e_\epsilon^+}\bar{\chi}(e_\epsilon^+) + c_{e_\epsilon^+}\bar{\chi}(e_\epsilon^+))(tr(e_\epsilon^+:\Omega)-1) \\ &+ \frac{(\ell-6)(\ell^2-1)}{12}\dim\chi]. \end{aligned} \tag{6.20}$$

The numbers of elements in concugacy classes are given in section 6.3.3. They are:

$$c_{e_\epsilon^+} = c_{e_\epsilon^-} = c_{e_1^+} = c_{e_1^-} = \frac{\ell^2-1}{2}$$

and $c_s = \ell(\ell+1)$ when $\ell \equiv 1 \bmod 4$, $c_s = \ell(\ell-1)$ when $\ell \equiv 3 \bmod 4$. Similarly, $c_h = \ell(\ell+1)$ when $\ell \equiv 1 \bmod 3$, $c_h = \ell(\ell-1)$ when $\ell \equiv 2 \bmod 3$.

The characters of irreducible representations are given in the characters tables in section 6.3.3. In the table observe that

$$\bar{\chi}(e_\epsilon^+) = \bar{\chi}(e_\epsilon^-)$$

for any irreducible character χ which is trivial on -1. Similarly,

$$\bar{\chi}(e_1^+) = \bar{\chi}(e_1^-).$$

So, substitution of the quantities in equation 6.19 we get

$$m_\chi = \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) + \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] \quad (6.21)$$

when $\ell \equiv 1 \bmod 4$ and

$$\begin{aligned} m_\chi &= \frac{\ell-6}{12\ell}\chi(1) - \frac{1}{4}\bar{\chi}(s) - \frac{1}{3}\bar{\chi}(h) \\ &+ \frac{1-\ell}{4\ell}[\bar{\chi}(e_1^+) + \bar{\chi}(e_\epsilon^+)] + \frac{1}{2\ell}h(-\ell)\sqrt{(}-\ell)[\bar{\chi}(e_1^+) - \bar{\chi}(e_\epsilon^+)] \end{aligned} \quad (6.22)$$

when $\ell \equiv 3 \bmod 4$.

For the identity representation, the multiplicity is

$$\begin{aligned} m_{id} &= 1 + \frac{1}{\ell(\ell^2-1)}[-\frac{\ell(\ell^2-1)}{3} - \frac{\ell(\ell^2-1)}{4} \\ &- \frac{(\ell-1)(\ell^2-1)}{2} + \frac{(\ell-6)(\ell^2-1)}{12}] \end{aligned}$$

which is equal to 0.

QED

6.2 Appendix A: Introduction to Representation Theory

As an appendix to this chapter, we introduce the remaining two section. This section covers the fundamental definitions and facts about representations of finite groups and the next section is about representations and characters of the group $SL_2(\mathbb{F}_\ell)$.

In this part, let us recall some fundamental definitions and facts of representation theory. We will not give the proofs of the statements. For the proofs, one

can refer to most of the intensive algebra books, for instance the algebra book [LA 4], by Lang.

Let V be a finite dimensional vector space over a finite field $\mathbb{F}_q$ and G be a finite group. In this text, we will always assume that the order of the group G is not divisible by the character of the field $\mathbb{F}_q$. A linear representation, or simply a representation of G on V is a group homomorphism ρ of G into $Aut_{\mathbb{F}_q}(V)$. We sometimes write V_ρ instead of V to indicate the representation ρ. The dimension of ρ is defined to be the dimension of the space $V = V_\rho$ also. We call a representation of G of dimension 1 as a character of G. Two representations ρ and ρ' with representation spaces V and V' are said to be isomorphic representations if there exists a vector space isomorphism θ

$$\theta : V \longrightarrow V',$$

such that $\theta\rho(g) = \rho'(g)\theta$ for all $g \in G$.

Let ρ be a representation of G and H be a subgroup of G. Suppose that μ is a character of H. If there exists a nonzero vector $v \in V_\rho$ such that $\rho(h)v = \mu(h)v$ for all $h \in H$ then μ is said to be an eigenvalue of H with respect to ρ and v is said to be an eigenvector of H that belongs to μ.

Let V be a G space with representation ρ and $V' \subset V$ be a subspace of V. If $\rho(g)V' = V'\ \forall g \in G$ then V' is called a G subspace of V. In this way, we obtain a new representation on V'. Let us denote it as ρ'. By Maschke's semisimplicity theorem, there is another G subspace V'' such that $V = V' \oplus V''$. Let ρ'' be the corresponding representation over V''. Then ρ is said to be the direct sum of ρ' and ρ'' and it is written as $\rho = \rho' \oplus \rho''$. The direct sum of n representations of G, all isomorphic to ρ, is denoted by $n\rho$. A representation ρ on V is said to be irreducible if it does not have a nontrivial subrepresentation of smaller dimension. By Maschke's theorem, every representation ρ of G can be decomposed as a direct sum of multiples of distinct irreducible representations

$$\rho = \bigoplus_{i=1}^{k} n_i\rho_i \tag{6.23}$$

in a unique way (cf. [LA 4] pp 666).

There are only finitely many irreducible representations $\rho_1, ..., \rho_h$ of G. Their number h is equal to the number of conjugacy classes of G. Their dimension satisfies the formula

$$\sum_{i=1}^{h} (\dim \rho_i)^2 = |G|. \tag{6.24}$$

Let G' be the commutator subgroup of G. Then the number of characters of G is equal to the index of G' in G, $[G : G']$.

Let ρ be a representation of G over the space V_ρ. Remark that V_ρ is a module over the group ring $\mathbb{F}_q[G]$. If ρ' is another representation over another space $V_{\rho'}$, then we define a form

$$(\rho, \rho')_G = \dim Hom_{\mathbb{F}_q[G]}(V_\rho, V_{\rho'}). \tag{6.25}$$

The form (ρ, ρ') is symmetric and bilinear with respect to direct sum. If both ρ and ρ' are irreducible then by a lemma of Schur, $(\rho, \rho') = 1$ if and only if $\rho = \rho'$ and $(\rho, \rho') = 0$ if and only if $\rho \neq \rho'$ (cf [LA 4], pp 643).

6.2.1 Induced Representation

Let G be a finite group. Let H be a subgroup of G and τ be a representation of H over a $\mathbb{F}_q$ space W. Define a vector space V to be the set of all functions $f : G \to W$ such that $f(hg) = \tau(h)f(g)$ for all $h \in H$ and for all $g \in G$, and define an action of G on V as

$$(sf)(g) = f(gs) \text{ for } s, g \in G \text{ and } f \in V.$$

The $\mathbb{F}_q[G]$ module V is called the induced module of W from H to G and is denoted by $Ind_H^G \tau$. W can be embedded into V by mapping each $w \in W$ to the function $f_w \in V$ defined by $f_w(g) = \tau(g)w$ if $g \in H$ and $f_w(g) = 0$ if $g \in G \setminus H$. The dimension of V is, $\dim V = [G : H] \dim W$.

Induced representations have the following properties:

Transitivity: If J is a subgroup of H and $\tau : J \to AutU$ is a representation of J, then we have

$$Ind_J^G U = Ind_H^G(Ind_J^H U).$$

Frobenious reciprocity theorem: Let E be an $\mathbb{F}_q[G]$ module and denote $Res_H^G E$ as the $\mathbb{F}_q[H]$ module obtained from E by considering only the action of H. Then we have the following canonical isomorphism:

$$Hom_{\mathbb{F}_q[G]}(Ind_H^G W, E) \cong Hom_{\mathbb{F}_q[H]}(W, Res_H^G E). \tag{6.26}$$

As a corollary we have

$$\dim Hom_{\mathbb{F}_q[G]}(Ind_H^G W, E) = \dim Hom_{\mathbb{F}_q[H]}(W, Res_H^G E). \tag{6.27}$$

If τ and σ are representations of H and G that correspond to W and E respectively then we can rewrite the last equality as

$$(Ind_H^G \tau, \sigma)_G = (\tau, Res_H^G \sigma)_H. \tag{6.28}$$

6.2.2 Characters of Representations

Let us remark that a one dimensional representation is also called a character. We will enlarge the definition of character for higher dimensional representations as follows. Given any representation ρ of a group G, *its character* is defined as

$$\chi(g) = tr\rho(g), \quad g \in G$$

where tr denotes the trace of matrix $\rho(g)$. For example, any representation of dimension 1 is its own character. Some basic properties of characters can be listed as

Proposition 6.2.1 [LA 4] *The character of a representation is independent of choice of basis. Equivalent representations have the same character. The converse is also true for complex representations. Moreover, each character is a class function on G. That is, it is constant on conjugacy classes:*

$$\chi(hgh^{-1}) = \chi(g), \quad g, h \in G.$$

The degree of χ is $\chi(1)$ and for any element g in G of order n, $\chi(g)$ is a sum of nth roots of unity.

If ρ_1 and ρ_2 are representations with characters χ_1 and χ_2 respectively then the characters of $\rho_1 \oplus \rho_2$ and $\rho_1 \otimes \rho_2$ are $\chi_1 + \chi_2$ and $\chi_1\chi_2$ respectively.

6.3 Appendix B: Representations of $SL_2(\mathbb{F}_\ell)$

In this section we present the irreducible complex representations and their characters of the group $SL_2(\mathbb{F}_\ell)$. The results of this section are covered in [NA-ŠT]. Essentially the group $PSL_2(\mathbb{F}_\ell)$ is acting on the modular curve $Y(\ell)$. But the representations of $PSL_2(\mathbb{F}_\ell)$ are also representations of $SL_2(\mathbb{F}_\ell)$. Indeed they are those of $SL_2(\mathbb{F}_\ell)$ which are trivial at -1.

6.3.1 Conjugacy Classes

There are $\ell + 4$ conjugacy classes in $SL_2(\mathbb{F}_\ell)$. Let us classify these classes as follows:

Let e be the identity matrix. Then, the conjugacy classes $\{e\}$ and $\{-e\}$.

The conjugacy classes denoted by A_λ and defined by the element $g_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ where $\lambda^2 \neq 1$.

The conjugacy classes defined by the elements

$$e_1^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad e_1^- = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \quad e_\varepsilon^+ = \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}, \quad e_\varepsilon^- = \begin{pmatrix} -1 & \varepsilon \\ 0 & -1 \end{pmatrix}$$

where $\varepsilon \in \mathbb{F}_\ell$ is a quadratic nonresidue.

And the conjugacy classes denoted by C_σ and defined by the element $g_\sigma = \begin{pmatrix} \sigma & \nu \\ \varepsilon\nu & \sigma \end{pmatrix}$ where $\sigma^2 - \varepsilon\nu^2 = 1$.

As a summary we have

Proposition 6.3.1 [NA-ŠT] *There are $\ell+4$ conjugacy classes of $SL_2(\mathbb{F}_\ell)$. $(\ell-1)/2$ of them are defined by C_σ and $(\ell-3)/2$ of them are defined by A_λ. Each conjugacy class C_σ contains $\ell(\ell-1)$ elements. Each conjugacy class A_λ contains $\ell(\ell+1)$ elements. The remaining classes are $\{\pm e\}$ and the classes defined by $e_1^{\pm}$, $e_\varepsilon^{\pm}$, each of them containing $\frac{\ell^2-1}{2}$ elements.*

6.3.2 Irreducible Representations

Let π be a character of $\mathbb{F}_\ell^\times$. Let H_π be the space of all complex valued functions $f(x,y)$ defined for nonzero vector $(x,y) \in \mathbb{F}_\ell \times \mathbb{F}_\ell$ and satisfying the condition

$$f(\lambda x, \lambda y) = \pi(\lambda) f(x,y). \tag{6.29}$$

Define a representation T_π on H_π by the formula

$$(T_\pi(g)f)(x,y) = f(ax+cy, bx+dy),\ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{6.30}$$

It is clear that T_π is a representation of $SL_2(\mathbb{F}_\ell)$ of dimension $\ell+1$. Moreover

Proposition 6.3.2 [NA-ŠT] *T_π is an irreducible representation of $SL_2(\mathbb{F}_\ell)$ for $\pi^2 \neq 1$ and two representations T_{π_1}, T_{π_2} are equivalent if and only if $\pi_1 = \pi_2$ or $\pi_1 = \pi_2^{-1}$.*

The space of constant functions, $f(x,y) = c$, lies in H_1 and the identity representation operates on this space. The complementary space of functions $f \in H_1$ such that $\sum f(x,y) = 0$ is also invariant under T_1. So, there exists a subrepresentation $\tilde{T}_1$ of T_1 which operates on this space of dimension ℓ. The representation $\tilde{T}_1$ is irreducible (cf. [NA-ŠT]).

Let $\pi_0 \neq 1$ be a character of $\mathbb{F}_\ell^\times$ assuming only the values 1 and -1. Then, consider the representation T_{π_0}. It has two irreducible components of equal dimensions, $\frac{\ell+1}{2}$, which are denoted by $T_{\pi_0}^+$ and $T_{\pi_0}^-$.

Let $U = \{t \in \mathbb{F}_{\ell^2} : N(t) = t\bar{t} = 1\}$ and ρ be a character of $\mathbb{F}_{\ell^2}$ such that $\rho(t) \neq 1$ on U. Consider the vector space H of all functions f on $\mathbb{F}_\ell^\times$ and define the representation S_ρ of $SL(2, \mathbb{F}_\ell)$ on H by

$$(S_\rho(g)f)(u) = \sum_{\nu \in \mathbb{F}_\ell^\times} K_\rho(u, \nu; g) f(\nu) \tag{6.31}$$

where $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and

$$K_\rho(u, \nu; g) = \begin{cases} \frac{-1}{\ell} \chi(\frac{du + a\nu}{b}) \sum_{t\bar{t} = u^{-1}\nu} \chi(-\frac{ut + \nu t^{-1}}{b}) \rho(t), & \text{if } b \neq 0, \\ \rho(d)\chi(dcu)\delta(d^2u - \nu), & \text{if } b = 0. \end{cases} \tag{6.32}$$

Here, δ is the Kronecker symbol and χ is a fixed nontrivial additive character of $\mathbb{F}_\ell$. Then S_ρ is a representation of dimension $\ell - 1$ (cf. [NA-ŠT]).

Let π be a restriction of ρ to U. Let S_π denote the representation S_ρ. Then

Proposition 6.3.3 [NA-ŠT] *The representations S_{π_1} and S_{π_2} are equivalent if and only if $\pi_1 = \pi_2$ or $\pi_1 = \pi_2^{-1}$. If $\pi^2 \neq 1$ then S_π is irreducible.*

Let $\pi_1^2 = 1$ and $\pi_1 \neq 1$. Then S_{π_1} has two irreducible components of equal dimensions, denoted by $S_{\pi_1}^+$ and $S_{\pi_1}^-$. $S_{\pi_1}^+$ is acting on the space H^+ consisting of functions vanishing on $\mathbb{F}_{\ell^2}^\times \setminus \mathbb{F}_\ell^\times$ whereas $S_{\pi_1}^-$ is acting on the space H^- consisting of functions vanishing on $\mathbb{F}_\ell^\times$ (cf. [NA-ŠT]).

If we collect all the information of this section, we have

Theorem 6.3.1 [NA-ŠT] *The set of $\ell+4$ irreducible representations of $SL(2, \mathbb{F}_\ell)$ are T_π ($\pi^2 \neq 1$), $\tilde{T}_1$, $T_{\pi_0}^+$, $T_{\pi_0}^-$, S_π ($\pi^2 \neq 1$), $S_{\pi_1}^+$, $S_{\pi_1}^-$.*

6.3.3 Character Table

We give the table of values of characters of irreducible representations of $SL(2, \mathbb{F}_\ell)$. For convenience in typing, we present two tables.

	e	$-e$	e_1^+	e_ε^+
T_π	$\ell+1$	$(\ell+1)\pi(-1)$	1	1
$\tilde{T}_1$	ℓ	ℓ	0	0
$T_{\pi_0}^+$	$\frac{\ell+1}{2}$	$\frac{(\ell+1)}{2}\pi_0(-1)$	$\frac{\Gamma(\pi_0)+1}{2}$	$\frac{-\Gamma(\pi_0)+1}{2}$
$T_{\pi_0}^-$	$\frac{\ell+1}{2}$	$\frac{(\ell+1)}{2}\pi_0(-1)$	$\frac{-\Gamma(\pi_0)+1}{2}$	$\frac{\Gamma(\pi_0)+1}{2}$
S_π	$\ell-1$	$(\ell-1)\pi(-1)$	-1	-1
$S_{\pi_1}^+$	$\frac{\ell-1}{2}$	$(\frac{\ell-1}{2})\pi_1(-1)$	$\frac{\Gamma(\pi_0)-1}{2}$	$-\frac{\Gamma(\pi_0)+1}{2}$
$S_{\pi_1}^-$	$\frac{\ell-1}{2}$	$(\frac{\ell-1}{2})\pi_1(-1)$	$-\frac{\Gamma(\pi_0)+1}{2}$	$\frac{\Gamma(\pi_0)-1}{2}$

The table above gives the values of the characters on the conjugacy classes represented by $e, -e, e_1^+$ and e_ε^+ whereas the table below gives the values of the characters on the conjugacy classes represented by $e_1^-, e_\varepsilon^-, g_\lambda$ and g_σ.

	e_1^-	e_ε^-	g_λ	g_σ
T_π	$\pi(-1)$	$\pi(-1)$	$\pi(\lambda)+\pi(\lambda^{-1})$	0
$\tilde{T}_1$	0	0	1	-1
$T_{\pi_0}^+$	$\frac{\Gamma(\pi_0)+1}{2}\pi_0(-1)$	$\frac{-\Gamma(\pi_0)+1}{2}\pi_0(-1)$	$\pi_0(\lambda)$	0
$T_{\pi_0}^-$	$\frac{-\Gamma(\pi_0)+1}{2}\pi_0(-1)$	$\frac{\Gamma(\pi_0)+1}{2}\pi_0(-1)$	$\pi_0(\lambda)$	0
S_π	$-\pi(-1)$	$-\pi(-1)$	0	$-\pi(t_0)-\pi(t_0^{-1})$
$S_{\pi_1}^+$	$\pi_1(-1)\frac{\Gamma(\pi_0)-1}{2}$	$-\pi_1(-1)\frac{\Gamma(\pi_0)+1}{2}$	0	$-\pi_1(t_0)$
$S_{\pi_1}^-$	$-\pi_1(-1)\frac{\Gamma(\pi_0)+1}{2}$	$\pi_1(-1)\frac{\Gamma(\pi_0)-1}{2}$	0	$-\pi_1(t_0)$

Here t_0 is the element of $\mathbb{F}_{\ell^2}$ with $N(t_0)=1$, $tr(t_0)=2\sigma$ and $\Gamma(\pi_0)=\sqrt{\left(\frac{-1}{\ell}\right)\ell}$.

Chapter 7

Conclusion

It has been pointed out that the Goppa codes on modular curves can have the best known asymptotic parameters so far. The modular curves $Y_0(N)$ and $Y(N)$ over $\mathbb{F}_{p^2}$ reach the Drinfeld-Vladuţ bound for $(N,p) = 1$. So the Goppa codes on modular curves have asypmtotic parameters lying on the line $R = 1 - \delta - 1/(\sqrt{}(q) - 1)$ which is above the Gilbert Varshamov bound in some interval. However, it is difficult to construct codes on modular curves efficiently. We have introduced two approaches on code construction on modular curves and stated the problems step by step. Moreover, we have given solutions of some problems in roadmap of code construction. But, there are still several unsolved problems in both approaches.

One of the approaches uses mostly geometric and algebraic tools. This approach studies local invariants of the plane model $\overline{Z_0(\ell)}$ of the modular curve $Y_0(\ell)$ given by the modular equation Φ_ℓ. We assume that ℓ is a prime different than the characteristic, p. The approach is based on describing the hyperplane of regular differentials of $\overline{Z_0(\ell)}$ vanishing at a given $\mathbb{F}_{p^2}$ rational point. Unfortunately the plane model $\overline{Z_0(\ell)}$ is highly singular curve. So, the elements of the hyperplane must vanish at singular points also.

As constructing a basis for the regular differentials of $\overline{Z_0(\ell)}$, we need to investigate its singularities. We have described the singularities of $\overline{Z_0(\ell)}$ for prime ℓ in

both characteristic 0 and positive characteristic (see [KLY-KA]). We have shown that both in positive characteristic $p > 3$ for $(p, \ell) = 1$ and in characteristic 0, the map

$$\pi : X_0(\ell) \longmapsto \mathbb{A}^2$$
$$(E, E', \phi) \longmapsto (j(E), j(E')) \tag{7.1}$$

is immersion. That is, the differential, $d\pi$, is injective. So, π is local embedding of nonsingular branches. This concludes that all singularities of $Z_0(\ell)$ are self intersections. These self intersections are all simple nodes in characteristic 0 whereas the order of contact of any two smooth branches passing though a singular point may be arbitrarily large in characteristic $p > 3$ where $p \neq \ell$. Moreover the self intersections in characteristic zero ar double (see theorem 5.2.1). Their number can be given by the Hurwitz class function:

$$\sum_{0<t<2\ell, t\neq\ell} H(t^2 - 4\ell^2).$$

The self intersections in positive characteristic may not be double. Indeed, structure of singularities of the affine curve $Z_0(\ell)$ essentially depends on two types of elliptic curves: The singularities corresponding to ordinary elliptic curves and the singularities corresponding to supersingular elliptic curves. The singularities corresponding to ordinary elliptic curves are all double points even though they are not necessarily simple nodes as in the case of characteristic 0. The singularities corresponding to supersingular elliptic curves are the most complicated ones and it may happen that there are more then two smooth branches passing though such kind of a singular point. We have computed the order of contact of any two smooth branches passing though a singular point both for ordinary case and for supersingular case (see theorem 5.2.3).

We have also proved that two points of $\overline{Z_0(\ell)}$ at ∞ in projective space are cusps for odd prime ℓ which are analytically equivalent to the cusp of 0, given by the equation $x^\ell = y^{\ell-1}$ (see proposition 5.2.2). These two cusps are permuted by Atkin-Lehner involution. The multiplicity of singularity of each cusp is $\frac{(\ell-1)(\ell-2)}{2}$. This result is valid in any characteristic $p \neq 2, 3$.

Any configuration $\mathcal{P}$ of $\mathbb{F}_{p^2}$ rational points of $Y_0(\ell)$ is a Goppa code. That code has a generator matrix whose columns are coordinates of the points of $\mathcal{P}$

in the space $\mathbb{P}(\Omega^*)$, dual of the projective space of regular differentials. So, first of all we should find out a basis for the space of regular differentials on $Y_0(\ell)$. Then, the image of a point $x \in Y_0(\ell)$ in $\mathbb{P}(\Omega^*)$ is the hyperplane in Ω consisting of $\omega \in \Omega$ such that $\omega(x) = 0$. So, we should describe the hyperspace of regular differentials vanishing at a given rational point.

We need the singularity structure of $\overline{Z_0(\ell)}$ for describing its regular differentials. Let $X \subset \mathbb{P}^2$ be a smooth curve given by $F(x, y, z) = 0$ of degree d. The regular differentials of X are of the form

$$\omega = P\frac{xdy - ydx}{F_z} = P\frac{xdz - zdx}{F_y} = P\frac{zdy - ydz}{F_x} \tag{7.2}$$

where $P = P(x, y, z)$ is a homogeneous polynomial of degree $d - 3$. We follow this approach to construct regular differentials. However, the projective plane model $\overline{Z_0(\ell)}$ is a singular curve. But the differentials on a singular plane curve are still of the form given in equation 7.2. We should impose some additional local conditions on the polynomial P at singular points. As a corollary, the problem of finding a basis for the regular differentials of the modular curves $Y_0(\ell)$ is still open.

For a given set $\{x_1, ..., x_n\}$ of rational points of $Y_0(\ell)$, let their images in $\mathbb{P}(\Omega^*)$ be hyperplanes $\sigma(x_1), ..., \sigma(x_n)$. Then the matrix $[\sigma(x_1) : ... : \sigma(x_n)]$ is a generator matrix for the corresponding Goppa code. So, the last and main problem is constructing the generator matrix for Goppa codes on $Y_0(\ell)$. More explicitly we can state this problem as follows:

Consider

$$Y_0(\ell)(\mathbb{F}_{p^2}) \longrightarrow \mathbb{P}(\Omega^*)$$

$$x \mapsto \Omega_x$$

where $\Omega_x = \{w \in \Omega : w(x) = 0\}$. The space Ω_x is unknown.

Asymptotically, we know that almost all $\mathbb{F}_{p^2}$ rational points of $Y_0(\ell)$ are supersingular elliptic curves. So, we can take the point x mentioned in the problem as a supersingular point.

The problem above is really much more difficult than the previous problems. The extra condition on differentials in the last problem is very hard to analyze. We don't have to know something about modular equations for the problem of determining the differential forms of $Y_0(\ell)$. But, probably we need the modular equations in order to describe the spaces Ω_x. We impose some local conditions on differential forms ω of $Y_0(\ell)$ for most of the problems. Indeed, if we consider a differential ω as in the form given in 7.2 then the local conditions on the differential ω are exactly the local conditions on the polynomial P. The last problem, which may be seen as the main problem in code construction, states that the polynomial P must vanish at supersingular points. So, we must know local parametrizations of $Z_0(\ell)$ at both singular points and at supersingular points in order to describe the the space of regular differential forms of $Y_0(\ell)$ and also to describe hyperspaces of differential forms vanishing at supersingular points . So, these problems lead us to try to find local parametrization of $Z_0(\ell)$ for each branch through both singular points and supersingular points of $Z_0(\ell)$.

The second approach is based on describing the Goppa codes on $Y(\ell)$ as $PSL_2(\mathbb{F}_\ell)$ module. The group $PSL_2(\mathbb{F}_\ell)$ acts on the Goppa codes constructed on $Y(\ell)$. The action is permuting the coordinates of vectors of the code. So, the codes can be considered as group codes. The main problem is describing the codes as group modules.

Let D be a $PSL_2(\mathbb{F}_\ell)$ invariant $\mathbb{F}_{p^2}$ rational divisor of the modular curve $Y(\ell)$ and $\mathcal{P}$ be a set of $\mathbb{F}_{p^2}$ rational points which is also invariant under the action of $PSL_2(\mathbb{F}_\ell)$. Then the Goppa code $C = (Y(\ell), \mathcal{P}, D)_\Omega$ has a natural action of the group $PSL_2(\mathbb{F}_\ell)$. The main problem is investigating the structure of a group code $C = (Y(\ell), \mathcal{P}, D)_\Omega$ as $PSL_2(\mathbb{F}_\ell)$ module. In this thesis, we propose a way of computing the characters of representations of a group code by using the localization formula and we applied this formula for calculating the traces of representations of the space of regular differentials. Remark that this space corresponds to a group code also. We further make a discussion on how to calculate the characters of the code space associated to arbitrary $PSL_2(\mathbb{F}_\ell)$ invariant divisor.

As a corollary, we have introduced two essentially different approaches and listed the problems in both approaches. Moreover, we have stated the progress particularly in one of the approaches. However, most of the problems remains still unsolved and they are pretty challenging.

Bibliography

[AAL] M.J. Aaltonen, Notes on the asymptotic behaviour of the information rate of block codes, *IEEE Trans.Info.Theory,* IT-30, 1984, pp 84-85.

[BO-SHA] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Acedemic Press, Inc., Orlando, 1966.

[CA] J.W.S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, 1991.

[CO] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, John Wiley, 1989.

[DE-RA] P. Deligne and M. Rapoport, Schemas des Modules de Courbes Elliptiques, *Lect. Notes Math.,* 349 (1973), 163-315.

[EIC] M. Eichler, The basis problem for modular forms and the traces of the Hecke operators, *Lecture Notes in Mathematics, no:320*, Springer-Verlag, 1973, pp 75-151.

[FUL] William Fulton, *Algebraic Curves*, Addison-Wesley Publishing Co., Inc.

[GA-STI] A. Garcia and H. Stichtenoth, A Tower of Artin-Schreier Extensions of Function Fields Attaining Drinfeld-Vladuţ Bound, *Invent. Math.,*121, 1995, pp 211-222.

[GO 1] V.G. Goppa, Codes on Algebraic Curves, *Soviet Math. Dokl.,* 24, 1981, pp. 170-172.

[GO 2] ——, Codes and Information, *Russ. Math. Surveys,* 39, no.1, 1984, pp. 87-141.

[GR-ZA] B.H.Gross and D. Zagier, On Singular Moduli, *J. Reine Angew. Math.* , 121, 1995, pp 191-220.

[HA] Robin Hartshorne, *Algebraic Geometry*, Graduate Text in Mathematics, No 133, Springer-Verlag, 1992.

[HE] E. Hecke, Analytische Arithmetic der positiven quadratischen Formen, *Math. Werke,* 789-918.

[HEJ] Hejhal, D.A., The Selberg trace formula for PSL(2, R). Vol. 2. Lecture Notes in Mathematics, 1001. Springer-Verlag, Berlin, 1983.

[HER] O. Hermann, Uber die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$, *J. Reine Angew. Math.,* 274/275, 1974, pp 187-195.

[HIR] F. Hirzebruch, Kurven auf Hilbertshen Modulflächen und Klassenzalrelationen, in "Gesammelte Abhandlungen," pp. 361-393, Springer Verlag, Berlin/New York, 1987.

[KA-YU] E. Kaltofen and N. Yui, On the modular equation of order 11, In the Third MAC-SYSMA User's Conference, Proceedings, *General Electric,* 1984, pp 472-485.

[KA-MA] Nicholas M. Katz and Barry Mazurs, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.

[KI] Yoshiyuki Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge University Press, 1993.

[KLY] Alexander Klyachko, Unpuplished Notes.

[KLY-KA] Alexander Klyachko and Orhun Kara, Singularities of the Modular Curve, *Finite Fields and Their Applications,* 7, 2001, pp. 415-420.

[KO] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, Newyork, 1984.

[LA 1] Serge Lang, *Introduction to Modular Forms*, Springer-Verlag, Berlin, 1976.

[LA 2] ——, *Elliptic Functions*, Addison Wesley, 1973.

[LA 3] ——, *Introduction to Algebraic and Abelian Functions*, Addison Wesley, 1972.

[LA 4] —, *Algebra* Addison Wesley, 1995.

[LAN] Peter S. Landweber, Supersingular Elliptic Curves and Congruences for Legendre Polynomials, *Lecture Notes on Math., no 1326*, Springer-Verlag, pp 69-93.

[MA-VLA] Y.I. Manin, S.G.Vladuţ, Linear Codes and Modular Curves, *J. Soviet. Math.,* 30 (1995) pp 2611-2643.

[NA-ŠT] M.A. Naimark, A.I. Štern, *Theory of Group Representations*, Springer-Verlag, Newyork, 1982.

[OGG] A. Ogg, Hyperelliptic Modular Curves, *Bull. Soc. Math. France,* 102, 1974, pp 449-462.

[PI-SHA] I. Piatetski-Shapiro, *Complex Representations of GL(2,K) for Finite Fields K*, American Mathematical Society, Providence Rhode Island, 1983.

[PI] Arnold Pizer, A Note on Conjecture of Hecke, *Pasific Journal of Mathematics*, vol.79 No 2, 1978, pp 541-547.

[SHA] C.E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.,* 27, 1948, pp. 379-423.

[SHI] Kuang-yen Shih, On the construction of Galois extensions of function fields and number fields, *Math. Ann.,* 207, 1974, pp 99-120.

[SH] Goro Shimura, *Introduction to The Arithmetic Theory of Automorphic Functions*, Iwamani Shoten and Princeton University Press, 1971.

[SIL 1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Newyork, 1986.

[SIL 2] ——, *Advanced Topics in The Arithmetic of Elliptic Curves*, Springer-Verlag, Newyork, 1994.

[STE] Serguei A. Stepanov, *Codes on Algebraic Curves*, Kluwer Academic/Plenum Publishers, New York, 1999.

[TH] Thomason, R. W., Une formula de Lefschetz en K théorie équivariante algébrique, *Duke Math. J.,* 68 (1992) no:3, pp 447-462.

[TS-VLA] M.A. Tsfasman and S.G. Vladuţ, *Algebraic Geometric Codes*, Kluwer Academic Publishers, 1991.

[TS-VLA-ZI] M.A. Tsfasman, S.G. Vladuţ, T.Zink, Modular Curves, Shimura Curves and Goppa Codes, better than the Varshamow-Gilbert bound, *Math. Nachr.,* 109, 1982, pp 21-28.

[VLA-DR] S.G. Vladuţ, V.G. Drinfeld, Number of points of Algebraic Curves, *Func. Anal.,* 17,no:1, 1984, pp 35-42.