Arithmetic and analytic properties of finite field hypergeometric functions

by

Catherine Lennon

B.A., Columbia University, June 2006

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2011

Author ....
Department of Mathematics
May 1, 2011

Certified by ....
Benjamin Brubaker
Cecil and Ida B. Green Career Development Chair
Assistant Professor of Mathematics
Thesis Supervisor

Accepted by ....
Bjorn Poonen
Chairman, Department Committee on Graduate Students

Arithmetic and analytic properties of finite field hypergeometric functions

by

Catherine Lennon

Submitted to the Department of Mathematics
on May 1, 2011, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

The intent of this thesis is to provide a detailed study of the arithmetic and analytic properties of Gaussian (finite field) hypergeometric series. We present expressions for the number of $\mathbb{F}_p$-points on certain families of varieties as special values of these functions. We also present "hypergeometric trace formulas" for the traces of Hecke operators on spaces of cusp forms of levels 3 and 9. These formulas lead to a simple expression for the Fourier coefficients of $\eta(3z)^8$, the unique normalized cusp form of weight 4 and level 9. We then use this to show that a certain threefold is "modular" in the sense that the number of its $\mathbb{F}_p$-points is expressible in terms of these coefficients. In this way, we use Gaussian hypergeometric series as a tool for connecting arithmetic and analytic objects.

We also discuss congruence relations between Gaussian and truncated classical hypergeometric series. In particular, we use hypergeometric transformation identities to express the p^{th} Fourier coefficient of the unique newform of level 16 and weight 4 as a special value of a Gaussian hypergeometric series, when $p \equiv 1 \pmod 4$. We then use this to prove a special case of Rodriguez-Villegas' supercongruence conjectures.

Thesis Supervisor: Benjamin Brubaker
Title: Cecil and Ida B. Green Career Development Chair
Assistant Professor of Mathematics

Acknowledgments

I would like to thank all of the people at MIT and elsewhere who have made my five years here enjoyable. I have made many great friends, and I know you will all be successful in whatever you decide to pursue.

I would also like to thank my adviser Ben Brubaker for his constant patience, and for all of his support and time. Special thanks are also due to Bjorn Poonen and Abhinav Kumar for all of the helpful comments on my thesis.

I appreciate all of the love from my family (including my mother and father and my sisters Debbie and Gabby) and their never ending faith in me.

Finally, I would like to thank my husband Aaron for all of his love, patience, and humor.

Contents

Chapter 1

Introduction

Gaussian hypergeometric series were first defined by Greene in [14] as finite field analogues of classical hypergeometric series. Greene then proved a number of transformation identities for Gaussian hypergeometric series that are analogous to those in the classical case. More recently, they have been shown to possess interesting arithmetic properties; in particular, special values of these functions can be used to express the number of $\mathbb{F}_p$-points on certain varieties. One can also express Hecke operator trace formulas, and consequently the Fourier coefficients of certain modular forms, in terms of hypergeometric series. We will explore these topics and others in this thesis.

Chapter 2 consists of background material that will be used throughout this thesis. We recall the definitions of various types of hypergeometric series and present some useful transformation identities. We also provide as reference some basic facts about elliptic curves, such as equations for their j-invariant and discriminant, and discuss the family of curves that will appear in the trace formulas later on. Finally, we present some motivation for deriving character sum expressions for point counting on varieties as a method for studying their analytic properties.

In Chapter 3, we demonstrate how Gaussian hypergeometric series can be used to express the number of points on a variety. This topic has been studied previously in [12, 23, 34] among others, and results in these papers have provided formulas for the traces of Frobenius for a number of families of elliptic curves, including the Legendre family. In Section 3.1, we build on the work of Fuselier to present a formula for the trace of Frobenius of an arbitrary elliptic curve E over $\mathbb{F}_q$, with the restrictions that $q \equiv 1 \pmod{12}$ and $j(E) \neq 0, 1728$. In particular, we show the following, where ${}_2F_1$ denotes the Gaussian hypergeometric series defined in Chapter 2.

Theorem 3.1.1. *Let q be a prime power such that $q \equiv 1 \pmod{12}$. In addition, let E be an elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$ and let $T \in \widehat{\mathbb{F}_q^\times}$ be a generator of* *the character group. The trace of the Frobenius map on E can be expressed as*

$$t_q(E) = -q \cdot T^{\frac{q-1}{12}}\left(\frac{1728}{\Delta(E)}\right) \cdot {}_2F_1\left(\left.\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \right| \frac{j(E)}{1728}\right)_q,$$

where $\Delta(E)$ is the discriminant of E.

Note in particular that the identity is expressed in terms of invariants of the curve E, so does not depend on the model of the curve.

In Theorem 3.2.2 we provide an expression for the trace of Frobenius on the family of curves equipped with a 3-torsion point discussed in Section 2.2.1. This formula, which requires $q \equiv 1 \pmod 3$ and $j(E) \neq 0, 1728$, is simpler than Theorem 3.1.1 and contains only characters of order 3. We will use this formula in Chapter 4 in the expressions for the traces of Hecke operators on spaces of cusp forms. This will lead to an expression of the Fourier coefficients of a certain modular form as special values of Gaussian hypergeometric series.

Chapter 4 is primarily devoted to computation of traces of Hecke operators via a refined version of the Eichler-Selberg trace formula due to Hijikata. Recent work (see for example [1, 3, 10, 12]) has shown that trace formulas for Hecke operators can often be naturally expressed in terms of Gaussian hypergeometric series. We further explore the connections between trace formulas and hypergeometric series and provide simple recursive formulas for Hecke operators on spaces of cusp forms of levels 3 and 9. In both of these results we will make use of Theorem 3.2.2 to provide "hypergeometric" trace formulas.

The following is an example of the theorems obtained in Chapter 4. Let $\mathrm{tr}_k(\Gamma_0(3), p)$ denote the trace of the p^{th} Hecke operator on the space of cusp forms of level 3 and weight k.

Theorem 4.2.4. *Let ρ be a multiplicative character of order 3 on $\mathbb{F}_{p^{k-2}}^{\times}$ and let ϵ be the trivial character on $\mathbb{F}_{p^{k-2}}^{\times}$. The trace formula for $p \neq 3$ and $k \geq 6$ even may be written as*

$$\mathrm{tr}_k(\Gamma_0(3), p) = p^{k-2}\sum_{t=2}^{p-1} {}_2F_1\left(\left.\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix}\right| t\right)_{p^{k-2}} + p \cdot \mathrm{tr}_{k-2}(\Gamma_0(3), p) + 2p - 2 - \beta_k(p),$$

where

$$\beta_k(p) := \begin{cases} 0 & p \equiv 1 \pmod 3 \textit{ and } k \equiv 0,1 \pmod 3 \\ -p^{k-2} \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \middle| 9 \cdot 8^{-1} \right)_{p^{k-2}} & p \equiv 1 \pmod 3 \textit{ and } k \equiv 2 \pmod 3 \\ 2(-p)^{k/2-1} & p \equiv 2 \pmod 3. \end{cases}$$

As an application, we use the results obtained to provide a simple expression for the Fourier coefficients of $\eta(3z)^8$, the unique normalized cusp form of weight 4 and level 9, in terms of Jacobi sums. Using purely elementary techniques, we are able then to construct a threefold whose number of points over $\mathbb{F}_p$ can be expressed in terms of the Fourier coefficients of a modular form.

In Chapter 5 we explore the relationship between Gaussian, classical, and truncated hypergeometric functions. In Proposition 5.1.2, we give a congruence mod p between Gaussian and truncated hypergeometric series evaluated at arbitrary points that follows from a classical character sum congruence relation. We then give an example illustrating that the result does not hold modulo higher powers of p in general. We go on to discuss when such "supercongruences" might hold, mentioning in particular the results of Mortenson in the case of hypergeometric functions evaluated at 1.

In Section 5.2.2, we discuss the supercongruence conjectures of Rodriguez-Villegas from [36] and what progress has been made towards proving them. These conjectures state that special values of certain truncated hypergeometric series are congruent modulo a prime power to the Fourier coefficients of modular forms. Using this as a guide, we conjecture that the Fourier coefficients of the modular forms in Rodriguez-Villegas' conjectures are equal to special values of specific Gaussian hypergeometric series. In particular, we use results of Ahlgren and Ono [2] and transformation formulas for hypergeometric series to give an expression for the p^{th} Fourier coefficients of a level 16 cusp form when $p \equiv 1 \pmod 4$. We combine this with a supercongruence result of McCarthy [28] to prove the level 16 conjecture of Rodriguez-Villegas when $p \equiv 1 \pmod 4$.

Finally, we provide two appendices intended to aid any readers who wish to further explore the problems discussed in this thesis. In Appendix A, we derive simple explicit formulas for the function $c(s, f, N)$ that appears in Hijikata's version of the trace formula in the special case where the level N is either prime or the square of a prime. Though straightforward, these require a bit of tedious computation and case analysis. We also show in Lemma A.2.2 how to use these expressions to eliminate the function

$c(s, f, \ell^2)$ from the trace formula whenever the level is the square of a prime. This is a generalization of Lemma 4.5.2 which applied only to the level 9 case. In this way, we make some progress towards a trace formula for Hecke operators on spaces of cusp form of level $N = \ell^2$ in the general case. Appendix B contains some of the Magma code that was used during the preparation of this thesis for computing finite field hypergeometric functions and truncated hypergeometric functions. Some of our results in this thesis have appeared previously in [25] and [26].

Chapter 2

Background

2.1 Hypergeometric functions

Throughout this thesis, we will be working with Gaussian (or finite field) hypergeometric functions, first defined by Greene [14] to act as finite field analogs of classical hypergeometric functions. As we will often want to compare these series to classical ones, we begin by recalling the definition of classical hypergeometric series and list a few transformations.

Define the Pochhammer symbol $(a)_k$ as the rising factorial

$$\begin{aligned}(a)_k =& a(a+1)...(a+k-1)\\ (a)_0 =& 1.\end{aligned}$$

Let $a_0, .., a_n, b_1, .., b_n$ be real or complex parameters such that no b_i is a nonpositive integer. The *classical hypergeometric series* ${}_{n+1}F_n$ is the formal power series

$${}_{n+1}F_n\left(\left.\begin{matrix} a_0 & a_1 & \dots & a_n \\ & b_1 & \dots & b_n \end{matrix}\right| x\right) := \sum_{k=0}^{\infty} \frac{(a_0)_k...(a_n)_k}{(b_1)_k...(b_n)_k k!} x^k. \tag{2.1.1}$$

These functions satisfy the inductive integral formula (see Theorem 3.1 in [4])

$$\begin{aligned} &{}_{n+1}F_n\left(\left.\begin{matrix} a_0 & a_1 & \dots & a_n \\ & b_1 & \dots & b_n \end{matrix}\right| x\right) \qquad (2.1.2)\\ &= \frac{\Gamma(b_n)}{\Gamma(a_n)\Gamma(b_n-a_n)} \int_0^1 {}_nF_{n-1}\left(\left.\begin{matrix} a_0 & a_1 & \dots & a_{n-1} \\ & b_1 & \dots & b_{n-1} \end{matrix}\right| tx\right) t^{a_n}(1-t)^{b_n-a_n} \frac{dt}{t(1-t)}. \end{aligned}$$

On the other hand, Gaussian hypergeometric series are finite character sums.

Specifically, let $q = p^e$ be a power of an odd prime and let $\mathbb{F}_q$ be the finite field of q elements. Extend each character $\chi \in \widehat{\mathbb{F}_q^\times}$ to all of $\mathbb{F}_q$ by setting $\chi(0) := 0$. For any two characters $A, B \in \widehat{\mathbb{F}_q^\times}$ one can define the normalized Jacobi sum by

$$\binom{A}{B} := \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x)\overline{B}(1-x) = \frac{B(-1)}{q} J(A, \overline{B}), \tag{2.1.3}$$

where $J(A, B)$ denotes the usual Jacobi sum.

For any positive integer n and characters $A_0, A_1, ..., A_n, B_1, B_2, ..., B_n \in \widehat{\mathbb{F}_q^\times}$, the *Gaussian hypergeometric series* ${}_{n+1}F_n$ *over* $\mathbb{F}_q$ is defined to be

$${}_{n+1}F_n\left(\begin{matrix} A_0 & A_1 & \dots & A_n \\ & B_1 & \dots & B_n \end{matrix} \middle| \, x\right)_q := \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} \binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x). \tag{2.1.4}$$

See also Katz [21] (in particular Section 8.2) for more information on how these sums naturally arise as the traces of Frobenius at closed points of certain ℓ-adic hypergeometric sheaves.

Remarkably, Gaussian hypergeometric series satisfy an inductive formula similar to (2.1.2). Specifically,

Theorem 2.1.5 ([14], Theorem 3.13).

$$\begin{aligned} &{}_{n+1}F_n\left(\begin{matrix} A_0 & A_1 & \dots A_n \\ & B_1 & \dots & B_n \end{matrix} \middle| \, x\right) \\ &= \frac{A_nB_n(-1)}{q} \sum_y {}_nF_{n-1}\left(\begin{matrix} A_0 & A_1 & \dots & A_{n-1} \\ & B_1 & \dots & B_{n-1} \end{matrix} \middle| \, xy\right) A_n(y)\overline{A_n}B_n(1-y). \end{aligned} \tag{2.1.6}$$

In fact, these functions satisfy many transformation laws similar to their classical counterparts. We present two such laws here that we will use in Sections 3.1 and 3.2.

Theorem 2.1.7 ([14], Theorem 4.4(i)). *For characters A, B, C of $\mathbb{F}_q^\times$ and $x \in \mathbb{F}_q$, $x \neq 0, 1$,*

$${}_2F_1\left(\begin{matrix} A & B \\ & C \end{matrix} \middle| \, x\right)_q = A(-1) \cdot {}_2F_1\left(\begin{matrix} A & B \\ & AB\overline{C} \end{matrix} \middle| \, 1-x\right)_q.$$

Theorem 2.1.8 ([14], Theorem 4.2(ii)). *For characters A, B, C of $\mathbb{F}_q^\times$ and $x \in \mathbb{F}_q^\times$,*

$${}_2F_1\left(\begin{matrix} A & B \\ & C \end{matrix} \middle| \, x\right)_q = ABC(-1)\overline{A}(x) \cdot {}_2F_1\left(\begin{matrix} A & A\overline{C} \\ & A\overline{B} \end{matrix} \middle| \, \frac{1}{x}\right)_q.$$

Compare these for example with the classical hypergeometric series identity in [13] (ignoring convergence issues)

$$
\begin{aligned}
{}_2F_1\left(\begin{matrix} a\ b \\ c \end{matrix}\middle| z\right) =& \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}{}_2F_1\left(\begin{matrix} a & b \\ & a+b-c+1 \end{matrix}\middle| 1-z\right) \\
&+ (1-z)^{c-a-b}\frac{\Gamma(c)\Gamma(a+b-c)}{\Gamma(a)\Gamma(b)}{}_2F_1\left(\begin{matrix} c-a & c-b \\ & c-a-b+1 \end{matrix}\middle| 1-z\right).
\end{aligned}
$$

2.1.1 Character sum identities

We will also need the Davenport-Hasse relation when expressing the trace of Frobenius on elliptic curves as a special value of a hypergeometric function. We state here the general theorem and then also the precise formulas for the specific cases that we will need.

Let tr : $\mathbb{F}_q \to \mathbb{F}_p$ be the trace map, i.e. $\operatorname{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{p^{e-1}}$, and let $\zeta_p = e^{\frac{2\pi i}{p}}$. Recall that if $\chi \in \widehat{\mathbb{F}_q^\times}$, then the Gauss sum $G(\chi)$ is defined to be

$$G(\chi) := \sum_{x\in\mathbb{F}_q} \chi(x)\zeta_p^{\operatorname{tr}(x)}.$$

Then the Davenport-Hasse relation can be stated as follows.

Theorem 2.1.9 (Davenport-Hasse Relation [24], Theorem 10.1). *Let m be a positive integer and let $q = p^e$ be a prime power such that $q \equiv 1 \pmod m$. For multiplicative characters $\chi, \psi \in \widehat{\mathbb{F}_q^\times}$ we have*

$$\prod_{\psi^m=1} G(\chi\psi) = -G(\chi^m)\chi(m^{-m}) \prod_{\psi^m=1} G(\psi).$$

The cases for $m = 3$, $m = 2$ may be restated as follows.

Corollary 2.1.10 (Davenport-Hasse for $q \equiv 1 \pmod 3$). *If q satisfies $q \equiv 1 \pmod 3$ and $\rho \in \widehat{\mathbb{F}_q^\times}$ is a character of order 3, then*

$$G(\chi)G(\chi\rho)G(\chi\rho^2) = qG(\chi^3)\overline{\chi}(27)$$

for any character $\chi \in \widehat{\mathbb{F}_q^\times}$.

Corollary 2.1.11 (Davenport-Hasse for $q \equiv 1 \pmod 2$). *If q satisfies $q \equiv 1 \pmod 2$*

and ϕ is the character of order 2 then

$$G(\chi)G(\chi\phi) = G(\chi^2)\overline{\chi}(4)G(\phi)$$

for any character $\chi \in \widehat{\mathbb{F}_q^\times}$.

2.2 Elliptic curves

An elliptic curve is a smooth, projective algebraic curve of genus 1, with a specified rational point. We will only discuss some of the facts related to elliptic curves which we will use throughout this thesis. For more information, one should consult Silverman [39]. Assume throughout that $p \neq 2, 3$.

In characteristic not equal to 2 or 3, any elliptic curve can be written in Weierstrass form as

$$E : y^2 = x^3 + ax + b.$$

The j-invariant of this curve is given by

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2},$$

and its discriminant is

$$\Delta(E) = -16(4a^3 + 27b^2) \neq 0.$$

For an elliptic curve defined over a finite field $\mathbb{F}_q$, the Frobenius endomorphism $\pi : E \to E$ is given by

$$\pi(x, y) = (x^q, y^q).$$

If we let $t_q(E)$ denote the trace of the Frobenius map, then it satisfies the relation

$$t_q(E) = q + 1 - |E(\mathbb{F}_q)|. \tag{2.2.1}$$

This will be used throughout this work. In addition, the trace can be written as a sum of algebraic integers

$$t_q(E) = \alpha + \overline{\alpha}, \tag{2.2.2}$$

where $\alpha\overline{\alpha} = q$. See Chapter V Section 2 in Silverman [39] for further details regarding equations (2.2.1) and (2.2.2).

2.2.1 Curves with a 3-torsion point

We now present a parametrization for all elliptic curves with nonzero j-invariant and equipped with a nontrivial 3-torsion point, up to isomorphism. In Section 3.2, we will express the traces of Frobenius on curves in this class as special values of a Gaussian hypergeometric function. Parameterizing curves with a 3-torsion point will become essential in Chapter 4, where we will see that Hijikata's trace formula can be stated in terms of counting isomorphism classes of elliptic curves with specified torsion.

By changing coordinates so that $(0,0)$ is a point of order 3, any elliptic curve E with a 3-torsion point can be written in the form

$$E : y^2 + a_1xy + a_3y = x^3, \tag{2.2.3}$$

with $a_3 \neq 0$ (see, for example, Chapter 4 Section 2 in [16]). The j-invariant of such a curve is

$$j(E) = \frac{a_1^3(a_1^3 - 24a_3)^3}{a_3^3(a_1^3 - 27a_3)}, \tag{2.2.4}$$

and its discriminant is

$$\Delta(E) = a_3^3(a_1^3 - 27a_3). \tag{2.2.5}$$

By considering the division polynomial Ψ_3, it was shown ([30], Corollary 5.2) that E has $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$ and $\Delta(E)$ is a cube in $\mathbb{F}_p$. We next show how to write any elliptic curve with $j \neq 0$ in terms of one parameter.

Assume that $j(E) \neq 0$, then (2.2.4) implies that $a_1 \neq 0$. Setting $u = a_3/a_1^2$, $t = a_1^3/a_3$, and making the change of variables $y \to u^3y$, $x \to u^2x$ gives the isomorphic curve

$$E_t : y^2 + txy + t^2y = x^3. \tag{2.2.6}$$

This curve has j-invariant $j(E_t) = t(t-24)^3/(t-27)$ and discriminant $\Delta_t := \Delta(E_t) = t^6(t^3 - 27t^2)$. This parameterizes all elliptic curves E with $j(E) \neq 0$ and equipped with a 3-torsion point.

Now, assume that $p \equiv 1 \pmod 3$. If $j(E) = 0$, then from equation (2.2.4) we know that $a_1 = 0$ or $a_1^3 = 24a_3$. If in addition $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ then Lemma 5.6 in [38] tells us that there is only one such isomorphism class over $\mathbb{F}_p$. In particular, E_{24} is an elliptic curve over $\mathbb{F}_p$ with $j(E_{24}) = 0$ and $\Delta_{24} = 24^6 \cdot 24^2 \cdot (-3) = -24^6 \cdot 2^6 \cdot 3^3$, a cube. This shows that any such E will be isomorphic to E_{24}. In particular, the curve given by $y^2 + y = x^3$ is isomorphic to E_{24}. Setting $u = 24^{-1}a_1$, and mapping $y \to u^3y$, $x \to u^2x$ shows that, when $a_1^3 = 24a_3$, $E \cong E_{24}$. The curves with $j(E) = 0$

and $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$ must have $a_1 = 0$ and are not of the form E_t for any t.

2.3 Motivation: Jacobi sums as Hecke characters

One motivation for expressing the number of points on a curve as a special value of a hypergeometric series comes from the work of Weil in [43, 42]. In [43], Weil shows how to express the number of $\mathbb{F}_q$-points on curves in the form

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \ldots + a_r x_r^{n_r} = b, \;\; a_i, b \in \mathbb{F}_q, \;\; n_i \in \mathbb{N}$$

in terms of Jacobi sums, and then explicitly computes the local zeta function of such curves. He then shows in [42] that Jacobi sums can be expressed in terms of Hecke characters. Combining these two results, he is able to prove a conjecture of Hasse, that the zeta function of curves of the form $Y^e = \gamma X^f + \delta$ defined over number fields are meromorphic and have functional equation. One hopes that similar techniques might be effective in using hypergeometric series expressions to obtain results about the zeta functions of other curves. For this reason, we discuss some of Weil's results now, though for simplicity only in the specific case of elliptic curves. For relevant background information, see Chapter 1 of Lang's *Cyclotomic Fields* [24] and Chapter 18 of Ireland and Rosen's *A Classical Introduction to Modern Number Theory* [19].

Let E be the smooth projective model of the curve

$$Y^2 = \gamma X^3 + \delta,$$

where γ, δ are nonzero elements of a field k of characteristic not equal to 2 or 3. Consider first the case where $k = \mathbb{F}_q$. If $q \equiv 1 \pmod 3$, let ϕ be the character of $\mathbb{F}_q^\times$ of order 2, and let ρ be a character of order 3. Then the number of projective points of E over $\mathbb{F}_q$ is given by

$$|E(\mathbb{F}_q)| = 1 + q + \rho(\gamma^{-1}\delta)\phi(\delta)J(\rho, \phi) + \rho^2(\gamma^{-1}\delta)\phi(\delta)J(\rho^2, \phi).$$

If on the other hand $q \equiv 2 \pmod 3$, then $|E(\mathbb{F}_q)| = 1 + q$.

Using a theorem of Hasse and Davenport relating values of Gauss sums in $\mathbb{F}_q$ to those over field extensions, Weil shows that the local zeta function of the curve E is a rational function. He then goes on to state the famous "Weil Conjectures," a list of properties satisfied by the zeta functions of varieties over finite fields. See Silverman [39], Chapter V, Section 2 for details.

On the other hand, let $m \in \mathbb{Z}$, and let ζ_m be a primitive m^{th} root of unity. We will be working in the field extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\zeta_m]$, and let $q = N\mathfrak{p}$. Define the character $\chi_\mathfrak{p}$ by setting each $\chi_\mathfrak{p}(x)$ for any $x \in \mathbb{Z}[\zeta_m]$ prime to $\mathfrak{p}$ to be the unique m^{th} root of unity satisfying

$$\chi_\mathfrak{p}(x) \equiv x^{\frac{q-1}{m}} \pmod{\mathfrak{p}}.$$

Let $a = (a_1, a_2) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ such that $a_1, a_2, a_1 + a_2 \not\equiv 0 \pmod{m}$. Define the function $J_a(\mathfrak{p})$ on prime ideals prime to m by

$$J_a(\mathfrak{p}) = -\sum_{x \pmod{p}} \chi_\mathfrak{p}(x)^{a_1} \chi_\mathfrak{p}(-1-x)^{a_2},$$

and extend multiplicatively to all ideals prime to m in $\mathbb{Z}[\zeta_m]$. Note that if we fix a prime $\mathfrak{p}$, then (up to a unit) this is just the Jacobi sum from before. The main result in [42] then is the following theorem.

Theorem 2.3.1 (Weil, [42]). *For each $a \neq (0,0)$, the function $J_a(\mathfrak{a})$ is a character on $\mathbb{Q}(\zeta_m)$ in the sense of Hecke, and m^2 is a defining ideal for it.*

Because $\mathbb{Q}(\zeta_m)$ is a CM field, a Hecke character on $\mathbb{Q}(\zeta_m)$ is straightforward to define. In particular, the main property to check is that there is some element $w(a) \in \mathbb{Z}[G]$, where G is the Galois group of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, such that $J_a((\alpha)) = \alpha^{w(a)}$ whenever $\alpha \in \mathbb{Z}[\zeta_m]$ satisfies $\alpha \equiv 1 \pmod{m^2}$. Weil proves this in two steps: he first uses the prime ideal decomposition of Gauss sums given by Stickelberger to show that

$$(J_a(\mathfrak{a})) = \mathfrak{a}^{w(a)}$$

for some element $w(a) \in \mathbb{Z}[G]$. In particular, this shows that $(J_a(\alpha)) = (\alpha^{w(a)})$ for elements as above. That is, it shows that the two quantities differ by a unit. To show equality, Weil uses Fourier analysis to show that this unit is 1.

Since L-functions corresponding to algebraic Hecke characters can be analytically continued and have a functional equation, Weil is able to combine Theorem 2.3.1 with the local zeta functions calculated in [43] to prove Hasse's conjecture. Because Gaussian hypergeometric series are defined as sums of products of Jacobi sums, it seems promising that similar techniques might provide straightforward methods of proving properties of zeta functions attached to other curves. However, we have not been able to generalize these results to other curves.

Chapter 3

Gaussian Hypergeometric Functions and Point Counting

The results of this chapter will follow mostly from basic Fourier analysis over finite fields. We will also use some of the transformation identities discussed in Chapter 2.

3.1 A coordinate-free expression for the trace of Frobenius

In all of the prior work on this topic (see for example [12, 23, 34]) the character parameters in hypergeometric series expressing the number of points on families of elliptic curves depended on the family. In addition, the values at which the hypergeometric series were evaluated were functions of the coefficients, and so depended on the model used. Here, we give a general formula expressing the number of $\mathbb{F}_q$-points of an elliptic curve in terms of more intrinsic properties of the curve. Consequently, this characterization is coordinate-free and can be used to describe the number of points on any elliptic curve $E(\mathbb{F}_q)$, with $j(E) \neq 0, 1728$ and $q = p^e \equiv 1 \pmod{12}$ without having to put the curve in a specific form. In particular, the formula holds over $\mathbb{F}_{p^2}$ for all $p > 3$ whenever $j \neq 0, 1728$.

Letting $t_q(E)$ denote the trace of the Frobenius endomorphism on E as discussed in Section 2.2.1, we have the following expression.

Theorem 3.1.1. *Let q be a prime power such that $q \equiv 1 \pmod{12}$. In addition, let E be an elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$ and let $T \in \widehat{\mathbb{F}_q^\times}$ be a generator of* *the character group. The trace of the Frobenius map on E can be expressed as*

$$t_q(E) = -q \cdot T^{\frac{q-1}{12}}\left(\frac{1728}{\Delta(E)}\right) \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}} \end{matrix} \,\middle|\, \frac{j(E)}{1728}\right)_q, \tag{3.1.2}$$

where $\Delta(E)$ is the discriminant of E.

Remark. It should be noted that the discriminant $\Delta(E)$ of the curve appears in the formula for the trace of Frobenius above. Although the discriminant itself depends on the Weierstrass model, isomorphic curves will differ by a twelfth power of an element of $\mathbb{F}_q$. Since the discriminant only appears as the argument of a character of order 12, the discriminants of isomorphic curves will output the same value, so the formula is indeed independent of Weierstrass model.

Remark. When $p \not\equiv 1 \pmod{12}$, information about $t_p(E)$ can still be gained from Theorem 3.1.1. Because $p^2 \equiv 1 \pmod{12}$ for all $p > 3$, Theorem 3.1.1 applies with $q = p^2$. Using the relationship

$$t_p(E)^2 = t_{p^2}(E) + 2p$$

one can then determine $t_p(E)$ up to a sign. Computations suggest that the sign is not determined simply by a character. It would be interesting to find a characterization of this sign and thus determine a hypergeometric expression for $t_p(E)$ for all primes.

Applying the transformation in Theorem 2.1.8 to the hypergeometric function in Theorem 3.1.1 above yields an expression for the trace of Frobenius that is remarkably similar to the classical hypergeometric series in Theorem 1.5 of [40]. This series is a solution of the differential equation satisfied by a period of the same elliptic curve. Theorem 3.1.1 also resembles Theorem 7 in [20], which gives a Gaussian hypergeometric expression for the Hasse invariant of elliptic curves in Weierstrass form. Since the theorem in [20] covers all possible congruence classes modulo 12, there is hope that Theorem 3.1.1 can also be extended to all congruence classes.

Before beginning the proof of this result, we demonstrate it with the following example.

Example 1. Consider the rational curve

$$E : y^2 = x^3 - 11x + 6,$$

which has j-invariant $35937/17$, discriminant $69632 = 2^{12} \cdot 17$, and conductor equal to 17. The space of cusp forms of weight 2 and level 17, $S_2(\Gamma_0(17))$, is one dimensional and spanned by the element

$$f = q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 - 3q^9 + 2q^{10} - 2q^{13} - 4q^{14} - q^{16} + \dots = \sum_{n=1}^{\infty} a_n(f)q^n.$$

The modularity result for elliptic curves [5] tells us in this case that $a_p(f) = t_p(E)$. When $p = 13$, we may apply Theorem 3.1.1 to find that

$$t_{13}(E) = -13 \cdot T\left(\frac{1728}{69632}\right) \cdot {}_2F_1\left(\begin{matrix} T & T \\ & T^8 \end{matrix} \middle| \frac{35937}{17 \cdot 1728}\right)_{13} = -2.$$

Comparing this with the coefficients of f, we see that indeed $a_{13}(f) = -2 = t_{13}(E)$.

When $p = 7$, however, we cannot apply Theorem 3.1.1 for $t_p(E)$, but instead must consider $t_{p^2}(E)$. We find that

$$t_{49}(E) = 2 = t_7(E)^2 - 2 \cdot 7 \implies t_7(E)^2 = 16,$$

which determines $t_7(E)$ up to sign. Comparing this with the Fourier coefficients of f again, we find that $a_7(f) = t_7(E) = 4$.

3.1.1 Elliptic curves in Weierstrass form

Theorem 3.1.1 will follow as a consequence of the next theorem after applying transformation laws for Gaussian hypergeometric series. Recall that in characteristic not 2 or 3 an elliptic curve can be written in Weierstrass form as

$$E : y^2 = x^3 + ax + b.$$

We prove the following theorem:

Theorem 3.1.3. *Let q be a prime power and assume that $q \equiv 1 \pmod{12}$. Let E be an elliptic curve over $\mathbb{F}_q$ in Weierstrass form with $j(E) \neq 0, 1728$. Then the trace of the Frobenius map on E can be expressed as*

$$t_q(E) = -q \cdot T^{\frac{q-1}{4}}\left(\frac{a^3}{27}\right) \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q.$$

This theorem extends Proposition III.2.4 of [11] to elliptic curves in the form given above and the method of proof follows similarly to that given in [12].

Proof. Let $|E(\mathbb{F}_q)|$ denote the number of projective points of E in $\mathbb{F}_q$. If we let

$$P(x,y) = x^3 + ax + b - y^2,$$

then $|E(\mathbb{F}_q)|$ satisfies the relation

$$|E(\mathbb{F}_q)| - 1 = \#\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x,y) = 0\}.$$

Define the additive character $\theta : \mathbb{F}_q \to \mathbb{C}^\times$ by

$$\theta(\alpha) = \zeta^{\mathrm{tr}(\alpha)} \tag{3.1.4}$$

where $\zeta = e^{2\pi i/p}$ and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map, i.e. $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{p^{e-1}}$. For any integer m, we may form the Gauss sum associated to the characters T^m and θ

$$G_m := G(T^m) = \sum_{x \in \mathbb{F}_q} T^m(x)\theta(x). \tag{3.1.5}$$

As in [12], we begin by repeatedly using the elementary identity from [19]

$$\sum_{z \in \mathbb{F}_q} \theta(z \cdot c) = \begin{cases} q \text{ if } c = 0 \\ 0 \text{ if } c \neq 0 \end{cases} \tag{3.1.6}$$

for any $c \in \mathbb{F}_q$ to express the number of points as

$$\begin{aligned} q \cdot (\#E(\mathbb{F}_q) - 1) =& \sum_{z \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \theta(zP(x,y)) \\ =& q^2 + \underbrace{\sum_{z \in \mathbb{F}_q^\times} \theta(zb)}_{A} + \underbrace{\sum_{y,z \in \mathbb{F}_q^\times} \theta(zb)\theta(-zy^2)}_{B} + \underbrace{\sum_{z,x \in \mathbb{F}_q^\times} \theta(zx^3)\theta(zax)\theta(zb)}_{C} \\ &+ \underbrace{\sum_{x,y,z \in \mathbb{F}_q^\times} \theta(zP(x,y))}_{D}. \end{aligned}$$

Here we have broken up the sum according to which of x, y, z are zero. We will evaluate each of these labeled terms using the following lemma from [12].

Lemma 3.1.7 ([12], Lemma 3.3). *For all $\alpha \in \mathbb{F}_q^\times$,*

$$\theta(\alpha) = \frac{1}{q-1} \sum_{m=0}^{q-2} G_{-m} T^m(\alpha),$$

where T is a fixed generator of the character group and G_{-m} is the Gauss sum defined in (3.1.5).

Since Lemma 3.1.7 holds only when the parameter α is nonzero, we require that $a \neq 0$ and $b \neq 0$ in the Weierstrass equation for E, or equivalently $j(E) \neq 0, 1728$. For A we have

$$A = \sum_{z \in \mathbb{F}_q^\times} \theta(zb) = -1$$

by equation (3.1.6). For B, we use Lemma 3.1.7 to write

$$B = \frac{1}{(q-1)^2} \sum_{i,j} G_{-i} G_{-j} T^i(b) T^j(-1) \sum_z T^{i+j}(z) \sum_y T^{2j}(y),$$

and the inner sums here are nonzero only when $2j \equiv 0 \pmod{q-1}$ and $j \equiv -i \pmod{q-1}$. Plugging in these values and using the fact that $G_{\frac{q-1}{2}} = \sqrt{q}$ when $q \equiv 1 \pmod 4$ (see Chapter 6 of [19]) gives

$$B = 1 + qT^{\frac{q-1}{2}}(b).$$

We simply expand C (because it will cancel soon) to get

$$C = \frac{1}{(q-1)^3} \sum_{i,j,k} G_{-i} G_{-j} G_{-k} T^j(a) T^k(b) \sum_z T^{i+j+k}(z) \sum_x T^{3i+j}(x).$$

Finally, we expand D

$$\begin{aligned} D =& \frac{1}{(q-1)^4} \sum_{i,j,k,l} G_{-i} G_{-j} G_{-k} G_{-l} T^j(a) T^k(b) T^l(-1) \\ & \cdot \sum_z T^{i+j+k+l}(z) \sum_x T^{3i+j}(x) \sum_y T^{2l}(y). \end{aligned}$$

Again, the only nonzero terms occur when $l = 0$ or $l = \frac{q-1}{2}$. The $l = 0$ term is

$$\frac{1}{(q-1)^3} \sum_{i,j,k} G_{-i} G_{-j} G_{-k} G_0 T^j(a) T^k(b) \sum_z T^{i+j+k}(z) \sum_x T^{3i+j}(x),$$

and since $G_0 = -1$ this term cancels with the C term in the expression for $q(|E(\mathbb{F}_q)|-1)$. Assuming now that $l = \frac{q-1}{2}$, both inner sums will be nonzero only when $j \equiv -3i \pmod{q-1}$ and $k \equiv \frac{q-1}{2} + 2i \pmod{q-1}$. We may write this term as

$$D_{\frac{q-1}{2}} := \frac{1}{q-1} \sum_i G_{-i} G_{3i} G_{-\frac{q-1}{2}-2i} G_{\frac{q-1}{2}} T^{-3i}(a) T^{\frac{q-1}{2}+2i}(b) T^{\frac{q-1}{2}}(-1) \tag{3.1.8}$$

and we may reduce this equation further by noting that $q \equiv 1 \pmod 4$ implies $G_{\frac{q-1}{2}} = \sqrt{q}$ and $T^{\frac{q-1}{2}}(-1) = 1$. Combining the above results yields the expression

$$q(|E(\mathbb{F}_q)| - 1) = q^2 + q \cdot T^{\frac{q-1}{2}}(b) + \frac{\sqrt{q}}{q-1} \sum_i G_{-i} G_{3i} G_{-\frac{q-1}{2}-2i} T^{-3i}(a) T^{\frac{q-1}{2}+2i}(b).$$

Now we expand G_{3i} and $G_{-\frac{q-1}{2}-2i} = G_{-2(\frac{q-1}{4}+i)}$ using the Davenport-Hasse relation, which we stated in Theorem 2.1.9. We may then write

$$\begin{aligned} G_{3i} &= \frac{G_i G_{i+\frac{q-1}{3}} G_{i+\frac{2(q-1)}{3}} T^i(27)}{q} \\ G_{-\frac{q-1}{2}-2i} &= \frac{G_{-i-\frac{q-1}{4}} G_{-i-\frac{3(q-1)}{4}}}{G_{\frac{q-1}{2}} T^{i+\frac{q-1}{4}}(4)}. \end{aligned}$$

Plugging this in to (3.1.8) gives

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(b)}{q(q-1)T^{\frac{q-1}{4}}(4)} \sum_i G_{-i} G_i G_{i+\frac{q-1}{3}} G_{i+\frac{2(q-1)}{3}} G_{-i-\frac{q-1}{4}} G_{-i-\frac{3(q-1)}{4}} T^i\left(\frac{27b^2}{4a^3}\right).$$

In order to write $t_q(E)$ as a finite field hypergeometric function, we use the fact that if T^{m-n} is not the trivial character, then

$$\binom{T^m}{T^n} = \frac{G_m G_{-n} T^n(-1)}{G_{m-n} q}. \tag{3.1.9}$$

This is another way of stating the classical identity $G(\chi_1)G(\chi_2) = J(\chi_1, \chi_2)G(\chi_1\chi_2)$ which holds whenever $\chi_1\chi_2$ is a primitive character.

Now use (3.1.9) to write

$$G_{i+\frac{q-1}{3}}G_{-i-\frac{q-1}{4}} = \binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}} G_{\frac{q-1}{12}}qT^{i+\frac{q-1}{4}}(-1) \tag{3.1.10}$$

$$G_{i+\frac{2(q-1)}{3}}G_{-i-\frac{3(q-1)}{4}} = \binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}} G_{-\frac{q-1}{12}}qT^{i+\frac{3(q-1)}{4}}(-1) \tag{3.1.11}$$

and plugging in (3.1.10) and (3.1.11) gives

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(b)q}{(q-1)T^{\frac{q-1}{4}}(4)}G_{\frac{q-1}{12}}G_{-\frac{q-1}{12}}\sum_i G_iG_{-i}\binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}}\binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}}T^i\left(\frac{27b^2}{4a^3}\right).$$

Since $G_{\frac{q-1}{12}}G_{-\frac{q-1}{12}} = qT^{\frac{q-1}{12}}(-1)$ we may write

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{12}}(-1)q^2}{(q-1)T^{\frac{q-1}{4}}(4)}\sum_i G_iG_{-i}\binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}}\binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}}T^i\left(\frac{27b^2}{4a^3}\right).$$

Next, we eliminate the G_iG_{-i} term. If $i \neq 0$ then $G_iG_{-i} = qT^i(-1)$, and if $i = 0$ then $G_iG_{-i} = 1 = qT^i(-1) - (q-1)$. Plugging in the appropriate identities for each i we may write (3.1.8) as

$$\begin{aligned}D_{\frac{q-1}{2}} =& \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{12}}(-1)q^3}{(q-1)T^{\frac{q-1}{4}}(4)}\sum_i \binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}}\binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}}T^i\left(-\frac{27b^2}{4a^3}\right)\\ &- \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{12}}(-1)q^2}{T^{\frac{q-1}{4}}(4)}\binom{T^{\frac{q-1}{3}}}{T^{\frac{q-1}{4}}}\binom{T^{\frac{2(q-1)}{3}}}{T^{\frac{3(q-1)}{4}}}.\end{aligned}$$

By (3.1.9) we have

$$\binom{T^{\frac{q-1}{3}}}{T^{\frac{q-1}{4}}}\binom{T^{\frac{2(q-1)}{3}}}{T^{\frac{3(q-1)}{4}}} = \frac{G_{\frac{q-1}{3}}G_{-\frac{q-1}{4}}G_{\frac{2(q-1)}{3}}G_{-\frac{3(q-1)}{4}}}{G_{\frac{q-1}{12}}G_{-\frac{q-1}{12}}q^2} = \frac{T^{\frac{q-1}{3}}(-1)T^{\frac{q-1}{4}}(-1)}{qT^{\frac{q-1}{12}}(-1)}$$

and so the second term reduces to $-(T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q)/(T^{\frac{q-1}{4}}(4))$. Equation (3.1.8) becomes

$$\begin{aligned}D_{\frac{q-1}{2}} =& \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{12}}(-1)q^3}{(q-1)T^{\frac{q-1}{4}}(4)}\sum_i \binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}}\binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}}T^i\left(-\frac{27b^2}{4a^3}\right)\\ &- \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q}{T^{\frac{q-1}{4}}(4)}.\end{aligned}$$

Make the substitution $i \to i - \frac{q-1}{4}$ to get

$$\begin{aligned} D_{\frac{q-1}{2}} =& T^{\frac{q-1}{12}}(-1)q^2 T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) \cdot \frac{q}{q-1}\sum_i \binom{T^{i+\frac{q-1}{12}}}{T^i}\binom{T^{i+\frac{5(q-1)}{12}}}{T^{i+\frac{q-1}{2}}} T^i\left(-\frac{27b^2}{4a^3}\right) \\ &- \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q}{T^{\frac{q-1}{4}}(4)} \\ =& T^{\frac{q-1}{12}}(-1)q^2 T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q \\ &- \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q}{T^{\frac{q-1}{4}}(4)}. \end{aligned}$$

Putting this all together then gives

$$\begin{aligned} q(|E(\mathbb{F}_q)|-1) =& q^2 + qT^{\frac{q-1}{2}}(b) - \frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q}{T^{\frac{q-1}{4}}(4)} \\ &+ T^{\frac{q-1}{12}}(-1)T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) q^2 \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q. \end{aligned}$$

Equivalently,

$$\begin{aligned} |E(\mathbb{F}_q)| =& q + 1 + T^{\frac{q-1}{2}}(b)\left(1 - \frac{T^{\frac{q-1}{4}}(-1)}{T^{\frac{q-1}{4}}(4)}\right) \\ &+ T^{\frac{q-1}{12}}(-1)T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) q \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q. \end{aligned}$$

Noting that $T^{\frac{q-1}{12}}(-1)T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) = T^{\frac{q-1}{4}}\left(\frac{a^3}{27}\right)$ and $T^{\frac{q-1}{4}}(-1) = T^{\frac{q-1}{2}}(2)$ (both depend only on the congruence of $q \pmod 8$) reduces the expression to

$$|E(\mathbb{F}_q)| = q + 1 + T^{\frac{q-1}{4}}\left(\frac{a^3}{27}\right) q \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q.$$

Since $t_q(E) = q + 1 - |E(\mathbb{F}_q)|$, we have proven that

$$t_q(E) = -q \cdot T^{\frac{q-1}{4}}\left(\frac{a^3}{27}\right) \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| -\frac{27b^2}{4a^3}\right)_q.$$

□

3.1.2 Proof of Theorem 3.1.1

We now prove Theorem 3.1.1 as a consequence of Theorem 3.1.3 and the transformation laws 2.1.7, 2.1.8 from Chapter 2.

Proof of Theorem 3.1.1. We begin by noting that we may apply Theorem 2.1.7 to the expression in Theorem 3.1.3 because the parameter $-27b^2/4a^3$ will equal 1 if and only if the discriminant of E is 0, which we exclude. Similarly, it will equal 0 if and only if $b = 0$, in which case $j = 1728$, and we exclude this case as well. So we begin by applying Theorem 2.1.7 to obtain the expression

$$t_q(E) = -q \cdot T^{\frac{q-1}{4}}\left(-\frac{a^3}{27}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{5(q-1)}{12}} \\ & T^{q-1}\end{matrix} \,\middle|\, \frac{4a^3+27b^2}{4a^3}\right)_q .$$

Applying Theorem 2.1.8 to this then gives

$$\begin{aligned} t_q(E) &= -\, q \cdot T^{\frac{q-1}{4}}\left(\frac{-a^3}{27}\right) T^{\frac{q-1}{12}}\left(\frac{4a^3}{4a^3+27b^2}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \,\middle|\, \frac{4a^3}{4a^3+27b^2}\right)_q \\ &= -\, q \cdot T^{\frac{q-1}{12}}\left(\frac{-4a^{12}}{3^9(4a^3+27b^2)}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \,\middle|\, \frac{4a^3}{4a^3+27b^2}\right)_q \\ &= -\, q \cdot T^{\frac{q-1}{12}}\left(\frac{a^{12}}{3^{12}} \cdot \frac{4^3 3^3}{-16(4a^3+27b^2)}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \,\middle|\, \frac{4a^3}{4a^3+27b^2}\right)_q \\ &= -\, q \cdot T^{\frac{q-1}{12}}\left(\frac{1728}{-16(4a^3+27b^2)}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \,\middle|\, \frac{4a^3}{4a^3+27b^2}\right)_q \\ &= -\, q \cdot T^{\frac{q-1}{12}}\left(\frac{1728}{\Delta(E)}\right) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}}\end{matrix} \,\middle|\, \frac{j(E)}{1728}\right)_q , \end{aligned}$$

where $\Delta(E) = -16(4a^3+27b^2)$ is the discriminant of E and $j(E) = (1728 \cdot 4a^3)/(4a^3+27b^2)$ is the j-invariant of E. □

3.2 Trace of Frobenius for elliptic curves with a 3-torsion point

Now let $q = p^e \equiv 1 \pmod 3$, $p > 3$ a prime. Let E_{a_1,a_3} be the curve

$$E_{a_1,a_3} : y^2 + a_1xy + a_3y = x^3, \qquad (3.2.1)$$

where $a_i \in \mathbb{F}_q^\times$, $\Delta(E_{a_1,a_3}) \neq 0$. Recall from Section 2.2.1 that this curve has a nontrivial 3-torsion point, and up to isomorphism all curves with a nontrivial 3-torsion point may be written in this form, except for certain curves with j-invariant 0. We have the following expression for the number of points on E_{a_1,a_3} in terms of Gaussian hypergeometric functions.

Theorem 3.2.2. *Let E_{a_1,a_3} be an elliptic curve over $\mathbb{F}_q$ in the form given in* (3.2.1). *Let $\rho \in \widehat{\mathbb{F}_q^\times}$ be a character of order* 3*, and let ϵ be the trivial character. Then the trace of the Frobenius map on E_{a_1,a_3} is given by*

$$t_q(E_{a_1,a_3}) = -q \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \,\middle|\, 27a_1^{-3}a_3 \right)_q .$$

Proof. If we let

$$P(x,y) = y^2 + a_1xy + a_3y - x^3$$

then

$$|E_{a_1,a_3}(\mathbb{F}_q)| - 1 = \#\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x,y) = 0\}.$$

Recall from (3.1.4) that the additive character $\theta : \mathbb{F}_q \to \mathbb{C}^\times$ is defined to be

$$\theta(\alpha) = \zeta^{\mathrm{tr}(\alpha)}. \tag{3.2.3}$$

Using equation (3.1.6), we write

$$\begin{aligned} q(|E_{a_1,a_3}(\mathbb{F}_q)| - 1) &= \sum_{z\in\mathbb{F}_q} \sum_{x,y\in\mathbb{F}_q} \theta(zP(x,y)) \\ &= q^2 + (q-1) + \underbrace{\sum_{z\in\mathbb{F}_q^\times} \sum_{x\in\mathbb{F}_q^\times} \theta(-zx^3)}_{B} + \underbrace{\sum_{z\in\mathbb{F}_q^\times} \sum_{y\in\mathbb{F}_q^\times} \theta(zy^2)\theta(za_3y)}_{C} \\ &\quad + \underbrace{\sum_{x,y,z\in\mathbb{F}_q^\times} \theta(zP(x,y))}_{D}. \end{aligned}$$

As before, we compute each individual sum using Lemma 3.1.7.

Computing B: Use Lemma 3.1.7 to replace $\theta(-zx^3)$, and then apply the orthogonality relation (3.1.6)

$$B = \sum_{z,x\in\mathbb{F}_q^\times} \frac{1}{q-1}\sum_m G_{-m}T^m(-x^3)T^m(z) = \frac{1}{q-1}\sum_m G_{-m}\sum_{x\in\mathbb{F}_q^\times} T^m(-x^3)\sum_{z\in\mathbb{F}_q^\times} T^m(z)$$
$$= \sum_{x\in\mathbb{F}_q^\times} G_0 = -(q-1).$$

Computing C:

$$C = \sum_{z,y\in\mathbb{F}_q^\times} \frac{1}{(q-1)^2}\sum_{k,m} G_{-k}G_{-m}T^{k+m}(z)T^{2k+m}(y)T^m(a_3)$$
$$= \frac{1}{(q-1)^2}\sum_{k,m} G_{-k}G_{-m}T^m(a_3)\sum_{z\in\mathbb{F}_q^\times} T^{k+m}(z)\sum_{y\in\mathbb{F}_q^\times} T^{2k+m}(y)$$

We see here that $k+m \equiv 0 \pmod{q-1} \implies m \equiv -k \pmod{q-1}$ and $2k+m \equiv 0 \pmod{q-1} \implies k \equiv m \equiv 0 \pmod{q-1}$. So this becomes $G_0^2 = 1$.

Computing D:

$$D = \sum_{x,y,z\in\mathbb{F}_q^\times} \frac{1}{(q-1)^4}\sum_{j,k,l,m} G_{-j}G_{-k}G_{-l}G_{-m}T^{j+k+l+m}(z)T^{2j+k+l}(y)T^{k+3m}(x)T^k(a_1)$$
$$\cdot T^l(a_3)T^m(-1)$$
$$= \frac{1}{(q-1)^4}\sum_{j,k,l,m} G_{-j}G_{-k}G_{-l}G_{-m}T^m(-1)T^k(a_1)T^l(a_3)\sum_{x\in\mathbb{F}_q^\times} T^{k+3m}(x)$$
$$\cdot \sum_{y\in\mathbb{F}_q^\times} T^{2j+k+l}(y)\sum_{z\in\mathbb{F}_q^\times} T^{j+k+l+m}(z)$$

Solving each of these equations $j+k+l+m \equiv 0 \pmod{q-1}$, $k+3m \equiv 0 \pmod{q-1}$, $2j+k+l \equiv 0 \pmod{q-1}$ gives $k \equiv -3m$ and $l \equiv m \equiv j$. Plugging this in we have

$$D = \frac{1}{q-1}\sum_m G_{-m}^3 G_{3m}T^{-3m}(a_1)T^m(-a_3).$$

Putting this all together then gives

$$q(|E_{a_1,a_3}(\mathbb{F}_q)| - 1) = q^2 + 1 + \frac{1}{q-1}\sum_m G_{-m}^3 G_{3m}T^{-3m}(a_1)T^m(-a_3),$$

and so

$$|E_{a_1,a_3}(\mathbb{F}_q)| = 1 + q + \frac{1}{q} + \frac{1}{q(q-1)} \sum_m G_{-m}^3 G_{3m} T^{-3m}(a_1) T^m(-a_3).$$

We have therefore shown that

$$t_q(E_{a_1,a_3}) = q + 1 - |E_{a_1,a_3}(\mathbb{F}_q)| = -\frac{1}{q} - \frac{1}{q(q-1)} \sum_m G_{-m}^3 G_{3m} T^{-3m}(a_1) T^m(-a_3).$$

First we use Corollary 2.1.10 to write $G_{3m} = G_m G_{m+\frac{q-1}{3}} G_{m+\frac{2(q-1)}{3}} T^m(27)/q$, giving

$$t_q(E_{a_1,a_3}) = -\frac{1}{q} - \frac{1}{q^2(q-1)} \sum_m G_{-m}^3 G_m G_{m+\frac{q-1}{3}} G_{m+\frac{2(q-1)}{3}} T^m(27) T^{-3m}(a_1) T^m(-a_3).$$

Next, make the substitution $G_m G_{-m} = qT^m(-1)$, which holds whenever $m \neq 0$. For $m = 0$, we write $G_m G_{-m} = T^m(-1) = qT^m(-1) - (q-1)T^m(-1)$:

$$t_q(E_{a_1,a_3}) = -\frac{1}{q} - \frac{1}{q(q-1)} \sum_m G_{-m}^2 G_{m+\frac{q-1}{3}} G_{m+\frac{2(q-1)}{3}} T^{-3m}(a_1) T^m(27a_3) + \frac{G_{\frac{q-1}{3}} G_{\frac{2(q-1)}{3}}}{q^2}.$$

For the last term above, note that $G_{\frac{q-1}{3}} G_{\frac{2(q-1)}{3}} = q$ and cancel with the first term, giving

$$t_q(E_{a_1,a_3}) = -\frac{1}{q(q-1)} \sum_m G_{-m}^2 G_{m+\frac{q-1}{3}} G_{m+\frac{2(q-1)}{3}} T^{-3m}(a_1) T^m(27a_3).$$

Now apply (3.1.9) to write $G_{m+\frac{q-1}{3}} G_{-m} = \binom{T^{m+\frac{q-1}{3}}}{T^m} G_{\frac{q-1}{3}} qT^m(-1)$ and $G_{m+\frac{2(q-1)}{3}} G_{-m} = \binom{T^{m+\frac{2(q-1)}{3}}}{T^m} G_{\frac{2(q-1)}{3}} qT^m(-1)$. Plugging this in yields

$$t_q(E_{a_1,a_3}) = -\frac{q\left(G_{\frac{q-1}{3}} G_{\frac{2(q-1)}{3}}\right)}{q-1} \sum_m \binom{T^{m+\frac{q-1}{3}}}{T^m} \binom{T^{m+\frac{2(q-1)}{3}}}{T^m} T^{-3m}(a_1) T^m(27a_3).$$

Again use the fact that $G_{\frac{q-1}{3}}G_{\frac{2(q-1)}{3}} = q$ to get

$$\begin{aligned} t_q(E_{a_1,a_3}) &= -\frac{q^2}{q-1}\sum_m \binom{T^{m+\frac{q-1}{3}}}{T^m}\binom{T^{m+\frac{2(q-1)}{3}}}{T^m} T^m(27a_1^{-3}a_3) \\ &= -q \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{3}} & T^{\frac{2(q-1)}{3}} \\ & \epsilon \end{matrix} \middle| 27a_1^{-3}a_3\right)_q . \quad \square \end{aligned}$$

Later in this thesis, we will look at the family of curves $E_t := E_{t,t^2}$. That is, we will consider the family of curves indexed by some parameter $t \in \mathbb{F}_q$ and in the form of (3.2.1) with $a_1 = t$ and $a_3 = t^2$. In this case, the above result reduces to

$$t_q(E_t) = -q \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \middle| \frac{27}{t}\right)_q .$$

We illustrate Theorem 3.2.2 with the following example.

Example 2. Consider the curve

$$E : y^2 - xy + y^2 = x^3,$$

which is in the form of (3.2.1) with $a_1 = -1$, $a_3 = 1$. This curve has conductor 14, and the space of cusp forms of weight 2 and level 14 again is one dimensional. It is spanned by the modular form

$$f = q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 - 2q^{12} - 4q^{13} - q^{14} + q^{16} + \ldots = \sum_{n=1}^{\infty} a_n(f)q^n.$$

When $p = 7$, for example, Theorem 3.2.2 tells us that

$$t_7(E) = -7 \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \middle| -27\right)_7 = 1,$$

which agrees with $a_7(f)$ above.

3.2.1 Curves with $j = 0$

In the previous section, we provided a formula for the trace of Frobenius for all elliptic curves E_{a_1,a_3} such that $a_1 \neq 0$. It is left to consider now the case of curves such that $a_1 = 0$, all of which will have j-invariant 0. Let $\alpha \in \mathbb{F}_p^{\times}$ be an element that is not a cube. There are three isomorphism classes over $\mathbb{F}_p$ containing curves of the form E_{0,a_3} and the curves $E_{0,\alpha}, E_{0,\alpha^2}, E_{0,\alpha^3}$ are representatives of these classes. In fact, the curve $E_{0,\alpha^3} \cong E_{0,1} \cong E_{24,24^2}$, so the results of the previous section provide a formula for expressing the trace of Frobenius of this curve in terms of hypergeometric functions. On the other hand, the curves $E_{0,\alpha}$, E_{0,α^2} cannot be written in the form E_{a_1,a_3} with $a_1 \neq 0$.

We will now provide formulas for the traces of Frobenius of curves of the form E_{0,α^i}, and then use these to prove a relation between traces that will be used in Chapter 4 in formulas for the traces of Hecke operators.

Lemma 3.2.4. *The trace of Frobenius of curves of the form E_{0,α^i} is given by*

$$t_q(E_{0,\alpha^i}) = -q\left(\binom{\rho}{\rho^2} T^{\frac{2(q-1)}{3}}(\alpha^i) + \binom{\rho^2}{\rho} T^{\frac{q-1}{3}}(\alpha^i)\right).$$

In particular, we have the formula

$$t_q(E_{0,1}) = -q\left(\binom{\rho}{\rho^2} + \binom{\rho^2}{\rho}\right).$$

Proof. As in the proof of Theorem 3.2.2, set $P(x,y) = y^2 + \alpha^i y - x^3$ and compute

$$\begin{aligned}
q(|E_{0,\alpha^i}(\mathbb{F}_q)| - 1) &= \sum_{z\in\mathbb{F}_q} \sum_{x,y\in\mathbb{F}_q} \theta(zP(x,y)) \\
&= q^2 + (q-1) - (q-1) + 1 + \sum_{x,y,z\in\mathbb{F}_q^\times} \theta(zP(x,y)) \\
&= q^2 + 1 + \frac{1}{(q-1)^3} \sum_{j,k,l} G_{-j}G_{-k}G_{-l}T^k(\alpha^i)T^l(-1) \\
&\quad \cdot \sum_{z\in\mathbb{F}_q^*} T^{j+k+l}(z) \sum_{x\in\mathbb{F}_q^\times} T^{3l}(x) \sum_{y\in\mathbb{F}_q^\times} T^{2j+k}(y).
\end{aligned}$$

The terms above will be nonzero when $3l \equiv 0 \pmod{q-1}$ and $j \equiv k \equiv l \pmod{q-1}$. Plugging this in above gives

$$q(|E_{0,\alpha^i}(\mathbb{F}_q)| - 1) = q^2 + 1 + \sum_{j=0,\frac{q-1}{3},\frac{2(q-1)}{3}} G_{-j}^3 T^j(\alpha^i).$$

And so

$$\begin{aligned} t_q(E_{0,\alpha^i}) &= -\frac{1}{q} - \frac{1}{q} \sum_{j=0,\frac{q-1}{3},\frac{2(q-1)}{3}} G_{-j}^3 T^j(\alpha^i) \\ &= -\frac{1}{q} G^3_{\frac{2(q-1)}{3}} T^{\frac{q-1}{3}}(\alpha^i) - \frac{1}{q} G^3_{\frac{q-1}{3}} T^{\frac{2(q-1)}{3}}(\alpha^i) \\ &= -q\left(\binom{\rho}{\rho^2} T^{\frac{2(q-1)}{3}}(\alpha^i) + \binom{\rho^2}{\rho} T^{\frac{q-1}{3}}(\alpha^i)\right), \end{aligned}$$

where the final equality follows from applying equation (3.1.9) and the relation $G_j G_{-j} = qT^j(-1)$. □

Finally, we prove the following lemma, which will allow us to represent the sums of the trace of Frobenius of elliptic curves with j-invariant 0 in terms of Gaussian hypergeometric functions.

Lemma 3.2.5. *When* $p \equiv 1 \pmod 3$ *and* α *is not a cube in* $\mathbb{F}_p^\times$*,*

$$\frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) = \begin{cases} 0 & k \equiv 0, 1 (\text{mod } 3) \\ -p^{k-2} \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \middle| \, 9 \cdot 8^{-1}\right)_{p^{k-2}} & k \equiv 2 \pmod 3. \end{cases}$$

Proof. Using Lemma 3.2.4 and summing over all three traces gives

$$t_q(E_{0,\alpha}) + t_q(E_{0,\alpha^2}) + t_q(E_{0,\alpha^3}) = -q\left(\binom{\rho}{\rho^2} + \binom{\rho^2}{\rho}\right)\left(1 + T^{\frac{q-1}{3}}(\alpha) + T^{\frac{2(q-1)}{3}}(\alpha)\right).$$

Now let $q = p^{k-2}$ and let $g \in \mathbb{F}_{p^{k-2}}^\times$ generate the group. Since $\alpha \in \mathbb{F}_p^\times$, we know that $\alpha^{p-1} = 1$, and so $\alpha = g^{a\frac{p^{k-2}-1}{p-1}} = g^{a(p^{k-3}+p^{k-4}+\ldots+1)}$ for some integer a. Since $p \equiv 1 \pmod 3$, it follows that $p^{k-3} + p^{k-4} + \ldots + 1 \equiv k - 2 \pmod 3$.

By the above argument, when $k \equiv 0, 1 \pmod 3$, α is not a cube in $\mathbb{F}_{p^{k-2}}^\times$ (recall that α was initially chosen as a noncube in $\mathbb{F}_p^\times$). Therefore

$$1 + T^{\frac{q-1}{3}}(\alpha) + T^{\frac{2(q-1)}{3}}(\alpha) = 0.$$

If however $k \equiv 2 \pmod 3$, then α is a cube in $\mathbb{F}_{p^{k-2}}$, and

$$t_q(E_{0,\alpha}) = t_q(E_{0,\alpha^2}) = t_q(E_{0,\alpha^3}).$$

It follows that

$$\frac{1}{3}\left(t_q(E_{0,\alpha}) + t_q(E_{0,\alpha^2}) + t_q(E_{0,\alpha^3})\right) = -q\left(\binom{\rho}{\rho^2} + \binom{\rho^2}{\rho}\right).$$

In particular, all curves with j invariant equal to 0 will have the same trace of Frobenius. We have already shown that E_{24} is a curve with j invariant equal to 0 with trace of Frobenius equal to

$$t_q(E_{24}) = -q \cdot {}_2F_1\left(\begin{matrix} \rho\ \rho^2 \\ \epsilon \end{matrix} \middle| 27 \cdot 24^{-1}\right)_q .$$

Using this equality then gives

$$\frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) = -p^{k-2}{}_2F_1\left(\begin{matrix} \rho\ \rho^2 \\ \epsilon \end{matrix} \middle| 9 \cdot 8^{-1}\right)_{p^{k-2}} . \quad \square$$

Chapter 4

Hypergeometric Trace Formulas

4.1 Background and prior work

Let N be a positive integer and let Ψ be a Dirichlet character mod N. Recall that the congruence subgroup $\Gamma_0(N)$ is defined to be

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

For each integer $k \geq 2$ we denote the corresponding space of cusp forms of weight k and character Ψ on $\Gamma_0(N)$ by $S_k(\Gamma_0(N), \Psi)$. Then any $f \in S_k(\Gamma_0(N), \Psi)$ satisfies the relation $f(\gamma \cdot \tau) = (c\tau + d)^k \Psi(d) f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. For each integer n such that $\gcd(n, N) = 1$, one can define a "Hecke operator" on this space, which is denoted by $T_k(n)$. Recall briefly the action of these operators: let $f \in S_k(\Gamma_0(N), \Psi)$ have Fourier expansion at infinity equal to $f(\tau) = \sum_{j=1}^{\infty} a(j) e^{2\pi i j \tau}$. For each n, the action of $T_k(n)$ on f is defined by

$$(T_k(n)f)(\tau) = \sum_{j=1}^{\infty} \left(\sum_{\substack{c>0 \\ c|(j,n)}} \Psi(c) c^{k-1} a(nj/c^2) \right) e^{2\pi i j \tau}.$$

In [15], Hijikata gives a formula for the traces of Hecke operators acting on $S_k(\Gamma_0(N), \Psi)$, as well as $S_k(\Gamma, \Psi)$, where $\Gamma \subset \Gamma_0(N)$ is a normal subgroup of "Fricke type". His formula holds very generally and consequently is quite complicated. Subsequent works such as [1, 3, 10, 12] have simplified the formula in specific cases by exploring the link between traces of Hecke operators and class numbers of imaginary quadratic orders, and have related such expressions to counting isomorphism classes of elliptic curves. We next present some of these results. Consider the following families of elliptic curves:

$$
\begin{aligned}
{}_2E_1(\lambda) &: y^2 = x(x-1)(x-\lambda), \lambda \neq 0, 1 \\
{}_3E_2(\lambda) &: y^2 = (x-1)(x^2+\lambda), \lambda \neq 0, -1
\end{aligned}
$$

and let ${}_2A_1(p,\lambda)$, ${}_3A_2(p,\lambda)$ denote the corresponding traces of Frobenius on these curves. Also, if $p \equiv 1 \pmod 4$, then let a, b be integers such that $p = a^2 + b^2$. For each integer $k \geq 2$ we denote the space of cusp forms of weight k and trivial character on $\Gamma_0(N)$ by $S_k(\Gamma_0(N))$, and write $\mathrm{tr}_k(\Gamma_0(N), n)$ for the trace of $T_k(n)$ on this space. See also equation (4.3.3) for a definition of $G_k(s,p)$. Then the following was shown:

Proposition 4.1.1 ([1], Theorems 1-2 and [3], Theorems 1-2). *If p is an odd prime and $k \geq 4$ is even, then*

1. $\mathrm{tr}_k(\Gamma_0(4), p) = -3 - \sum_{\lambda=2}^{p-1} G_k({}_2A_1(p,\lambda), p)$,
2. $\mathrm{tr}_k(\Gamma_0(8), p) = -4 - \sum_{\lambda=2}^{p-2} G_k({}_2A_1(p,\lambda^2), p)$.

Proposition 4.1.2 ([10], Theorem 2.3). *For a prime $p \geq 3$ and $k \geq 4$ even*

$$\mathrm{tr}_k(\Gamma_0(2), p) = -2 - \delta_k(p) - \sum_{\lambda=1}^{p-2} G_k({}_3A_2(p,\lambda), p)$$

where

$$\delta_k(p) = \begin{cases} \frac{1}{2}G_k(2a,p) + \frac{1}{2}G_k(2b,p) & \text{if } p \equiv 1 \pmod 4; \\ (-p)^{k/2-1} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

4.2 Statement of results

For any $t \in \mathbb{Z}$ such that $t \neq 0, 27$, define the rational elliptic curve E_t by the equation

$$E_t : y^2 + txy + t^2y = x^3,$$

and write the Hasse-Weil L-function of E_t as

$$L(s, E_t) = \sum_{n=1}^{\infty} a_n(E_t) n^{-s}.$$

If p is a prime for which E_t has good reduction, then $a_p(E_t) = t_p(E_t)$[1]. We will prove that $\mathrm{tr}_k(\Gamma_0(3), p)$ can be expressed as follows:

Theorem 4.2.1. *Let $p \neq 3$ be a prime. For any even $k \geq 4$, the trace of $T_k(p)$ on $S_k(\Gamma_0(3))$ can be written as*

$$\mathrm{tr}_k(\Gamma_0(3), p) = -\sum_{\substack{t=1 \\ t \not\equiv 27 \pmod p}}^{p-1} a_{p^{k-2}}(E_t) - \gamma_k(p) - 2,$$

where

$$\gamma_k(p) := \begin{cases} \frac{1}{3}(a_{p^{k-2}}(E_{0,\alpha}) + a_{p^{k-2}}(E_{0,\alpha^2}) + a_{p^{k-2}}(E_{0,\alpha^3})) & p \equiv 1 \pmod 3, \\ (-p)^{k/2-1} & p \equiv 2 \pmod 3. \end{cases} \tag{4.2.2}$$

In the expression for $\gamma_k(p)$, α is not a cube modulo p, and E_{0,α^i} are the elliptic curves discussed in Section 3.2.1.

Combining Theorems 3.2.2 and 4.2.1 and using the relation $t_{p^k}(E) = a_{p^k}(E) - p \cdot a_{p^{k-2}}(E)$ (see Section 4.4.3) then yields the corollary:

Corollary 4.2.3. *Let $p \neq 3$ be prime and let $k \geq 4$ be an even integer. One can alternately express the trace formula as*

$$\mathrm{tr}_k(\Gamma_0(3), p) = \sum_{i=0}^{k/2-2} p^{k-2-i} \sum_{t=2}^{p-1} {}_2F_1\left(\begin{matrix} \rho \; \rho^2 \\ \epsilon \end{matrix} \,\middle|\, t\right)_{p^{k-2-2i}} - p^{k/2-1}(p-2) - \gamma_k(p) - 2.$$

Remark. Because the weight k is even, each $q = p^{k-2-2i}$ automatically satisfies $q \equiv 1 \pmod 3$, and so Theorem 3.2.2 can be used in the expression for $\mathrm{tr}_k(\Gamma_0(3), p)$ for all $p \neq 3$.

Remark. The function $\gamma_k(p)$ can also be expressed in terms of Gaussian hypergeometric functions as

$$\gamma_k(p) = \begin{cases} -\sum_{i=0 \; 3|(k-2-2i)}^{k/2-2} p^{k-2-i} \cdot {}_2F_1\left(\begin{matrix} \rho \; \rho^2 \\ \epsilon \end{matrix} \,\middle|\, 9 \cdot 8^{-1}\right)_{p^{k-2-2i}} + p^{k/2-1} & p \equiv 1 \pmod 3 \\ (-p)^{k/2-1} & p \equiv 2 \pmod 3 \end{cases}$$

and so the trace formula in Corollary 4.2.3 can be expressed entirely in terms of such functions.

[1] Throughout this chapter, when we write $t_p(E_t)$, we are considering the trace of the Frobenius map on the reduction of the curve E_t modulo p.

One can also use these results to prove "inductive trace formulas" as in [12, 10]. Theorem 4.2.1 is particularly well suited for this kind of expression. A straightforward consequence of Theorem 4.2.1 is the following theorem.

Theorem 4.2.4. *The trace formula for $p \neq 3$ and $k \geq 6$ even may be written as*

$$\mathrm{tr}_k(\Gamma_0(3),p) = p^{k-2}\sum_{t=2}^{p-1} {}_2F_1\left(\begin{matrix}\rho \ \rho^2 \\ \epsilon\end{matrix}\middle| t\right)_{p^{k-2}} + p\cdot \mathrm{tr}_{k-2}(\Gamma_0(3),p) + 2p - 2 - \beta_k(p),$$

where

$$\beta_k(p) := \begin{cases} 0 & p \equiv 1 \pmod 3 \text{ and } k \equiv 0,1 \pmod 3 \\ -p^{k-2}\cdot {}_2F_1\left(\begin{matrix}\rho \ \rho^2 \\ \epsilon\end{matrix}\middle| 9\cdot 8^{-1}\right)_{p^{k-2}} & p \equiv 1 \pmod 3 \text{ and } k \equiv 2 \pmod 3 \\ 2(-p)^{k/2-1} & p \equiv 2 \pmod 3. \end{cases} \tag{4.2.5}$$

Many of the same methods used in the $\Gamma_0(3)$ case may be adapted to prove trace formulas for $\Gamma_0(9)$ as well. We discuss this in Section 4.5 and present a number of formulas for the trace in forms like those above. As an example, we have the following inductive formula.

Theorem 4.2.6. *Let $k \geq 4$ and let $p \equiv 1 \pmod 3$. Then the trace is given by*

$$\begin{aligned}\mathrm{tr}_k(\Gamma_0(9),p) = p^{k-2}\sum_{\substack{t=2\\ t^3\neq 1}}^{p-1} {}_2F_1\left(\begin{matrix}\rho \ \rho^2 \\ \epsilon\end{matrix}\middle| t^3\right)_{p^{k-2}} + p^{k-2}{}_2F_1\left(\begin{matrix}\rho \ \rho^2 \\ \epsilon\end{matrix}\middle| 9\cdot 8^{-1}\right)_{p^{k-2}} \\ -4 + 4p - \delta(k-2)p(p+1) + p\cdot \mathrm{tr}_{k-2}(\Gamma_0(9),p),\end{aligned}$$

where $\delta(k) = 1$ if $k = 2$ and 0 otherwise. When $p \equiv 2 \pmod 3$, we have $\mathrm{tr}_k(\Gamma_0(9),p) = \mathrm{tr}_k(\Gamma_0(3),p)$.

In fact, when $p \equiv 2 \pmod 3$, we will see that $\mathrm{tr}_k(\Gamma_0(3^m),p) = \mathrm{tr}_k(\Gamma_0(3),p)$ for every m.

Let $q = e^{2\pi i z}$ and recall that the Dedekind eta function is defined to be

$$\eta(z) = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n).$$

Then $\eta(3z)^8$ is the unique normalized Hecke eigenform in $S_4(\Gamma_0(9))$ and we write its

Fourier expansion as

$$\eta(3z)^8 = \sum b(n)q^n.$$

We will show using trace formula results such as Theorem 4.2.6 that the Fourier coefficients of $\eta(3z)^8$ are given by the following simple expression.

Corollary 4.2.7. *Let $p \equiv 1 \pmod 3$, and let $\rho \in \widehat{\mathbb{F}_p^\times}$ be a character of order 3. The p^{th} Fourier coefficient of $\eta(3z)^8$ is given by*

$$b(p) = -p^3\left(\binom{\rho^2}{\rho}^3 + \binom{\rho}{\rho^2}^3\right) = -p^3{}_2F_1\left(\begin{matrix}\rho & \rho^2 \\ & \epsilon\end{matrix}\,\middle|\, 9\cdot 8^{-1}\right)_{p^3}.$$

When $p \equiv 2 \pmod 3$, $b(p) = 0$.

In addition, let V be the threefold defined by the following equation:

$$x^3 = y_1y_2y_3(y_1+1)(y_2+1)(y_3+1) \tag{4.2.8}$$

and let $N(V,p)$ denote the number of projective $\mathbb{F}_p$-points on V. Then one can use the results above to show that V is "modular" in the sense that $N(V,p)$ relates to the Fourier coefficients of $\eta(3z)^8$ by the following expression:

$$b(p) = p^3 + 3p^2 + 1 - N(V,p).$$

We begin in Section 4.3 by stating Hijikata's version of the Eichler-Selberg trace formula for Hecke operators on $S_k(\Gamma_0(\ell))$ where ℓ is prime, and then work to simplify this formula into an expression in terms of the number of isomorphism classes of elliptic curves in different isogeny classes. This expression will hold whenever $p \equiv 1 \pmod{\ell}$ or $\left(\frac{p}{\ell}\right) = -1$. We then specialize this formula further to the case where $\ell = 3$ in Section 4.4 and prove Theorem 4.2.1. At the end of this section we will derive other expressions for the trace on this space, such as Corollary 4.2.3 and the inductive trace formula in Theorem 4.2.4. In Section 4.5 we show how methods similar to those in Section 4.4 can be used to prove results when $\ell = 9$, such as Theorems 4.5.3 and 4.2.6. We then use these trace formulas to prove Corollary 4.2.7, an explicit expression for the Fourier coefficients of a weight four modular form. Using this, we show in Section 4.6.2 that the number of points on the threefold given by equation (4.2.8) can be expressed in terms of the Fourier coefficients of the same modular form.

While simplifying the expression for $\mathrm{tr}_k(\Gamma_0(3),p)$, we use theorems of Schoof to rewrite sums of class numbers which comes up in the expression in terms of the number of isomorphism classes of elliptic curves. These theorems only hold when p, ℓ satisfy certain congruence properties. Although it is possible when $\ell = 3, 9$ to reduce the trace formula expression for all values of p, this seems to pose a real difficulty for proving trace formulas for general p, ℓ.

4.3 Trace formulas

4.3.1 Hijikata's trace formula

Let p, ℓ be distinct odd primes, and let $k \geq 2$ be even. We will specialize the trace formula given by Hijikata in [15] to the case where $T_k(p)$ acts on $S_k(\Gamma_0(\ell))$. Some preliminary notation is necessary to state the theorem.

For each s in the range $0 < s < 2\sqrt{p}$, let $t > 0$ and D be the unique integers satisfying

$$s^2 - 4p = t^2 D \tag{4.3.1}$$

and such that D is a fundamental discriminant of an imaginary quadratic field. Additionally, for any $d < 0$, $d \equiv 0, 1 \pmod 4$, write $h(d) := h(\mathcal{O})$ for the class number of the order $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ of discriminant d, and write $\omega(d) := \frac{1}{2}|\mathcal{O}^\times|$ for one half of the number of units in that order. Set $h^*(d) := h(d)/\omega(d)$.

Define the polynomial $\Phi(X) := X^2 - sX + p$ and let x, y be the complex roots of $\Phi(X)$. Define

$$G_k(s,p) := \frac{x^{k-1} - y^{k-1}}{x - y}. \tag{4.3.2}$$

One can verify that when k is even $G_k(s,p)$ can be alternately expressed as

$$G_k(s,p) = \sum_{j=0}^{k/2-1} (-1)^j \binom{k-2-j}{j} p^j s^{k-2j-2}. \tag{4.3.3}$$

Finally, for any integer f dividing t, define a function $c(s, f, \ell)$:

$$c(s,f,\ell) := \begin{cases} 1 + \left(\frac{D}{\ell}\right) & \text{if } \operatorname{ord}_\ell(f) = \operatorname{ord}_\ell(t), \\ 2 & \text{if } \operatorname{ord}_\ell(f) < \operatorname{ord}_\ell(t). \end{cases} \tag{4.3.4}$$

Then Hijikata's version of the trace formula yields the following:

Theorem 4.3.5 ([15], Theorem 2.2). *Let p, ℓ be distinct odd primes, and let $k \geq 2$*

be even. Then

$$\mathrm{tr}_k(\Gamma_0(\ell),p) = -\sum_{0<s<2\sqrt{p}} G_k(s,p) \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,\ell) - K(p,\ell) + \delta(k)(1+p) \tag{4.3.6}$$

where

$$K(p,\ell) := 2 + \frac{1}{2}(-p)^{k/2-1}\left(1+\left(\frac{-p}{\ell}\right)\right) H^*(-4p)$$
$$\delta(k) := \begin{cases} 1 \text{ } \textit{if } k=2, \\ 0 \text{ } \textit{otherwise.} \end{cases}$$

In the following we will often write $H^*(s^2-4p) := \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right)$ and $H(s^2-4p) := \sum_{f|t} h\left(\frac{s^2-4p}{f^2}\right)$ for simplicity.

4.3.2 Simplifying the formula

The aim of this section is to rewrite Hijikata's trace formula given in Theorem 4.3.5 in a more convenient form for our purposes by expressing $\mathrm{tr}_k(\Gamma_0(\ell),p)$ in terms of the number of isomorphism classes of elliptic curves with specified torsion. This formula will hold for all p satisfying $p \equiv 1 \pmod{\ell}$ or $\left(\frac{p}{\ell}\right) = -1$. In particular, we see that it will hold for all $p \neq 3$ when $\ell = 3$. In the following section we will specialize further to $\ell = 3$ to obtain an explicit trace formula.

We begin by eliminating the $c(s,f,\ell)$ term from (4.3.6). Specifically, we show the following:

Lemma 4.3.7.

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,\ell) = \begin{cases} \left(1+\left(\frac{D}{\ell}\right)\right) H^*(s^2-4p) & \textit{when } \ell \nmid t, \\ H^*(s^2-4p) + \ell H^*((s^2-4p)/\ell^2) & \textit{when } \ell | t. \end{cases}$$

Proof. Consider first the case where $\ell \nmid t$. Then $\mathrm{ord}_\ell(f) = \mathrm{ord}_\ell(t)$ is automatically satisfied, so $c(s,f,\ell) = \left(1+\left(\frac{D}{\ell}\right)\right)$, and the result follows.

When $\ell | t$, we use the following theorem from [8]:

Theorem 4.3.8 ([8], Corollary 7.28). *Let $\mathcal{O}$ be an order of discriminant d in an imaginary quadratic field, and let $\mathcal{O}' \subset \mathcal{O}$ be an order with $[\mathcal{O} : \mathcal{O}'] = \iota$. Then*

$$h^*(\mathcal{O}') = h^*(\mathcal{O}) \cdot \iota \prod_{\ell|\iota,\ \ell \text{ prime}} \left(1 - \left(\frac{d}{\ell}\right)\frac{1}{\ell}\right).$$

Substituting the explicit description of $c(s,f,\ell)$ given in (4.3.4) and manipulating the terms algebraically gives

$$\begin{aligned}\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,\ell) &= \left(1+\left(\frac{D}{\ell}\right)\right)\sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right) + 2\sum_{f|(t/\ell)} h^*\left(\frac{s^2-4p}{f^2}\right)\\ &= \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) + \ell \sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right) + \sum_{f|(t/\ell)} h^*\left(\frac{s^2-4p}{f^2}\right)\\ &\quad - \ell\left(1-\left(\frac{D}{\ell}\right)\frac{1}{\ell}\right)\sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right). \end{aligned} \tag{4.3.9}$$

Applying Theorem 4.3.8, we find that

$$\begin{aligned}&\ell\left(1-\left(\frac{D}{\ell}\right)\frac{1}{\ell}\right)\sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right) + \ell\sum_{f|(t/\ell)} h^*\left(\frac{s^2-4p}{f^2}\right)\\ &= \sum_{f|t} \ell\left(1-\left(\frac{(s^2-4p)/f^2}{\ell}\right)\frac{1}{\ell}\right) h^*\left(\frac{s^2-4p}{f^2}\right)\\ &= \sum_{f|t} h^*\left(\ell^2\frac{s^2-4p}{f^2}\right) \quad \text{by Theorem 4.3.8}\\ &= \sum_{f|(t/\ell)} h^*\left(\frac{s^2-4p}{f^2}\right),\end{aligned}$$

and so the final term in (4.3.9) can therefore be written as

$$-\ell\left(1-\left(\frac{D}{\ell}\right)\frac{1}{\ell}\right)\sum_{f|t,f\nmid t/\ell} h^*\left(\frac{s^2-4p}{f^2}\right) = (\ell-1)\sum_{f|t/\ell} h^*\left(\frac{s^2-4p}{f^2}\right),$$

and finally (4.3.9) becomes

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) + \ell\sum_{f|t/\ell} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right) = H^*(s^2-4p) - \ell H^*((s^2-4p)/(\ell^2)).$$

□

Using this, the trace formula may be written as

$$\operatorname{tr}_k(\Gamma_0(\ell),p) = -\sum_{0<s<2\sqrt{p}} G_k(s,p)H^*(s^2-4p)\left(1+\left(\frac{s^2-4p}{\ell}\right)\right) \tag{4.3.10}$$
$$-\ell\sum_{\substack{0<s<2\sqrt{p}\\ \ell|t}} G_k(s,p)H^*\left(\frac{s^2-4p}{\ell^2}\right) - K(p,\ell)+\delta(k)(p+1).$$

We now rewrite the above equation in terms of the function H instead of H^*, so that we may apply Schoof's results counting isomorphism classes of elliptic curves in the next section. Recall that $h^*(d) = h(d)/\omega(d)$, where $\omega(d) = \frac{1}{2}|\mathcal{O}(d)^\times|$. Therefore, whenever $d \neq -3, -4$, we have that $h^*(d) = h(d)$. If $s^2-4p = t^2D$ and $D \neq -3, -4$ this implies that $H(s^2-4p) = H^*(s^2-4p)$. If $s^2-4p = -3t^2$, then

$$H(-3t^2) = \sum_{f|t} h\left(\frac{-3t^2}{f^2}\right) = \sum_{f|t, f\neq t} h^*\left(\frac{-3t^2}{f^2}\right) + 3h^*(-3)$$
$$= \sum_{f|t} h^*\left(\frac{-3t^2}{f^2}\right) + 2\underbrace{h^*(-3)}_{=1/3} = H^*(-3t^2)+2/3$$

and similarly, $H(-4t^2) = H^*(-4t^2)+1/2$.

It is left to determine which s satisfy either $s^2-4p=-4t^2$ or $s^2-4p=-3t^2$. By considering the splitting of p in $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, we see that the former equality will occur for some $s < 2\sqrt{p}$ if and only if $p \equiv 1 \pmod 4$ and the latter if and only if $p \equiv 1 \pmod 3$. Additionally, by looking at the units in these rings, we see that when $p \equiv 1 \pmod 4$ (respectively $p \equiv 1 \pmod 3$), there are exactly 2 (resp. 3) values of $s > 0$ and $t > 0$ for which $s^2-4p=-4t^2$ (resp. $s^2-4p=-3t^2$).

When $p \equiv 1 \pmod 4$ let a, b be positive integers satisfying $p = a^2+b^2$, and similarly when $p \equiv 1 \pmod 3$, let c, d be positive integers satisfying $p = \frac{c^2+3d^2}{4}$. Then the set of all $(s,t) \in \mathbb{N}\times\mathbb{N}$ such that $s^2-4p=-4t^2$ is

$$S_4 = \{(2a,b),(2b,a)\} \tag{4.3.11}$$

and the set of all (s,t) such that $s^2-4p=-3t^2$ is

$$S_3 = \left\{(c,d),\left(\frac{c+3d}{2},\left|\frac{c-d}{2}\right|\right),\left(\left|\frac{c-3d}{2}\right|,\frac{c+d}{2}\right)\right\}. \tag{4.3.12}$$

By a simple congruence argument mod ℓ, we see that there can be at most one pair

$(s,t)\in S_4$ such that $\ell|t$, and similarly for S_3. Label the elements of these sets so that in the first case, if $\ell|t$, then $(s,t)=(2a,b)$ and in the second if $\ell|t$ then $(s,t)=(c,d)$.

Define the following corrective factors

$$\epsilon_4(p,\ell)=\begin{cases}\frac{1}{2}(G_k(2a,p)+G_k(2b,p))\left(1+\left(\frac{-4}{\ell}\right)\right) & \text{if } p\equiv 1 \pmod 4,\ \ell\nmid b,\\ \frac{1}{2}G_k(2b,p)\left(1+\left(\frac{-4}{\ell}\right)\right)+\frac{1}{2}(1+\ell)G_k(2a,p) & \text{if } p\equiv 1 \pmod 4,\ \ell|b,\\ 0 & \text{if } p\equiv 3 \pmod 4\end{cases} \tag{4.3.13}$$

and

$$\epsilon_3(p,\ell)=\begin{cases}\frac{2}{3}\left(G_k(c,p)+G_k(\frac{c+3d}{2},p)+G_k(\frac{c-3d}{2},p)\right)\left(1+\left(\frac{-3}{\ell}\right)\right) & p\equiv 1 \pmod 3,\ \ell\nmid d,\\ \frac{2}{3}(G_k(\frac{c+3d}{2},p)+G_k(\frac{c-3d}{2},p))\left(1+\left(\frac{-3}{\ell}\right)\right)+\frac{2}{3}(1+\ell)G_k(c,p) & p\equiv 1 \pmod 3,\ \ell|d,\\ 0 & p\equiv 2 \pmod 3.\end{cases} \tag{4.3.14}$$

Using this, the trace formula can be written as

$$\begin{aligned}\mathrm{tr}_k(\Gamma_0(\ell),p)=&-\sum_{0<s<2\sqrt{p}}G_k(s,p)\left(1+\left(\frac{s^2-4p}{\ell}\right)\right)H(s^2-4p)-\ell\sum_{\substack{0<s<2\sqrt{p}\\ \ell|t}}G_k(s,p)H\left(\frac{s^2-4p}{\ell^2}\right)\\ &-K(p,\ell)+\epsilon_4(p,\ell)+\epsilon_3(p,\ell)+\delta(k)(p+1).\end{aligned} \tag{4.3.15}$$

4.3.3 Trace in terms of elliptic curves

For an elliptic curve E defined over $\mathbb{F}_p$, let $E(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-rational points on E, and let $E(\mathbb{F}_p)[n]$ denote its n-torsion subgroup. Furthermore, let $\mathcal{I}_p$ denote the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ and write $[E]$ for the isomorphism class containing E. Define the sets

$$\begin{aligned}I(s)&:=\{\mathcal{C}\in\mathcal{I}_p:\forall E\in\mathcal{C},|E(\mathbb{F}_p)|=p+1-s\}\\ I_n(s)&:=\{\mathcal{C}\in I(s):\forall E\in\mathcal{C},\mathbb{Z}/n\mathbb{Z}\subset E(\mathbb{F}_p)[n]\}\\ I_{n\times n}(s)&:=\{\mathcal{C}\in I(s):\forall E\in\mathcal{C},E(\mathbb{F}_p)[n]\cong\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\}\end{aligned}$$

and from these define the quantities $N(s):=|I(s)|$, $N_n(s):=|I_n(s)|$, $N_{n\times n}(s):=|I_{n\times n}(s)|$.

We use the following two theorems of Schoof to rewrite (4.3.15) in terms of the above quantities. Although the theorems given in [38] hold for curves defined over fields $\mathbb{F}_{p^e}$, we specialize to the prime order case.

Theorem 4.3.16 ([38], Theorems 4.6, 4.9). *Let $s \in \mathbb{Z}$ satisfy $s^2 < 4p$. Then*

$$N(s) = H(s^2 - 4p).$$

Suppose in addition that $n \in \mathbb{Z}_{\geq 1}$ is odd. Then

$$N_{n\times n}(s) = \begin{cases} H\left(\frac{s^2-4p}{n^2}\right) & \text{if } p \equiv 1 \pmod{n} \text{ and } s \equiv p+1 \pmod{n^2}; \\ 0 & \text{otherwise.} \end{cases}$$

If E is an elliptic curve such that $|E(\mathbb{F}_p)| = p+1-s$ then $\mathbb{Z}/n\mathbb{Z} \subset E(\mathbb{F}_p)[n] \iff n \mid |E(\mathbb{F}_p)| \iff s \equiv p+1 \pmod{n}$. It follows from this that $N_n(s) = N(s)$ if $s \equiv p+1 \pmod{n}$ and $N_n(s) = 0$ otherwise.

We may apply Theorem 4.3.16 to replace $H(s^2-4p)$ by $N(s)$ for each s in (4.3.15). However, since s is not necessarily congruent to $p+1 \pmod{\ell^2}$, we cannot simply replace $H\left(\frac{s^2-4p}{\ell^2}\right)$ by $N_{\ell\times\ell}(s)$ in (4.3.15). Instead, we can use the following lemma when $p \equiv 1 \pmod{\ell}$.

Lemma 4.3.17. *Assume that $p \equiv 1 \pmod{\ell}$. Then $\ell^2 | s^2 - 4p \iff \ell^2 | p+1-s$ or $\ell^2 | p+1+s$.*

Proof. We see that $\ell | p-1 \iff \ell^2 | (p-1)^2 \iff p^2 - 2p + 1 \equiv 0 \pmod{\ell^2}$. Adding $4p$ to both sides then gives

$$\ell | p-1 \iff (p+1)^2 \equiv 4p \pmod{\ell^2}.$$

Assuming first that $\ell^2 | s^2 - 4p$, this implies that $(p+1)^2 \equiv s^2 \pmod{\ell^2} \implies (p+1-s)(p+1+s) \equiv 0 \pmod{\ell^2}$. There are now three possibilities. If $\ell^2 | p+1-s$ or $\ell^2 | p+1+s$ then we are done. Otherwise, it must be that $\ell | p+1-s$ and $\ell | p+1+s$. Then, since we assume throughout that $\ell \neq 2$, this implies that $s \equiv 0 \pmod{\ell}$. This is a contradiction, since then $0 \equiv s^2 \equiv 4p \pmod{\ell^2}$ and we assumed that $\ell \neq p$.

Conversely, if $\ell^2 | p+1-s$ or $\ell^2 | p+1+s$, then $(p+1)^2 \equiv s^2 \pmod{\ell^2} \implies 4p \equiv s^2 \pmod{\ell^2}$. □

This lemma shows that if ℓ^2 divides $s^2 - 4p$ (or equivalently, $\ell | t$) and $p \equiv 1 \pmod{\ell}$, then either s or $-s$ satisfies the hypotheses of Theorem 4.3.16. Therefore, either $H\left(\frac{s^2-4p}{\ell^2}\right) = N_{\ell\times\ell}(s)$ or $H\left(\frac{s^2-4p}{\ell^2}\right) = N_{\ell\times\ell}(-s)$. Since s and $-s$ cannot both be congruent $p+1 \pmod{\ell^2}$, it follows that $H\left(\frac{s^2-4p}{\ell^2}\right) = N_{\ell\times\ell}(s) + N_{\ell\times\ell}(-s)$ and so summing over all s in the range $0 < |s| < 2\sqrt{p}$ gives

$$\sum_{0<s<2\sqrt{p},\ell|t} G_k(s,p)H((s^2-4p)/\ell^2) = \sum_{0<|s|<2\sqrt{p}} G_k(s,p)N_{\ell\times\ell}(s).$$

Similarly, if $p \not\equiv 1 \pmod{\ell}$ but $\left(\frac{p}{\ell}\right) = -1$, then $\ell \nmid t$ for any t satisfying $s^2-4p = t^2D$. The second sum in (4.3.15) is empty and also $N_{\ell\times\ell}(s) = 0$ for all s and so we may replace $H\left(\frac{s^2-4p}{\ell^2}\right)$ by $N_{\ell\times\ell}(s)$ in this sum without affecting the value. This shows that when $p \equiv 1 \pmod{\ell}$ or $\left(\frac{p}{\ell}\right) = -1$ the trace formula can be written as

$$\begin{aligned} \mathrm{tr}_k(\Gamma_0(\ell),p) = &- \sum_{0<|s|<2\sqrt{p}} G_k(s,p)\left(\frac{1}{2}\left(1+\left(\frac{s^2-4p}{\ell}\right)\right)N(s) + \ell N_{\ell\times\ell}(s)\right) \\ &- K(p,\ell) + \epsilon_4(p,\ell) + \epsilon_3(p,\ell) + \delta(k)(p+1). \qquad (4.3.18)\end{aligned}$$

4.4 Level 3

We are now in a position to prove Theorem 4.2.1, a trace formula for $\ell = 3$ and arbitrary prime $p \neq 3$.

4.4.1 The case where $p \equiv 1 \pmod{3}$

We first prove the theorem in the case where $p \equiv 1 \pmod{3}$. We begin by considering the main term in (4.3.18). This term is

$$\sum_{0<|s|<2\sqrt{p}} G_k(s,p)\left(\frac{1}{2}\left(1+\left(\frac{s^2-4p}{3}\right)\right)N(s) + 3N_{3\times 3}(s)\right).$$

For each congruence class of $s \pmod{3}$, consider the term $\frac{1}{2}\left(1+\left(\frac{s^2-4p}{3}\right)\right)N(s)$. When $s \equiv 0 \pmod{3}$, we have $\left(\frac{s^2-4p}{3}\right) = -1$, so $\frac{1}{2}\left(1+\left(\frac{s^2-4p}{3}\right)\right)N(s) = 0$, and also $N_3(s) = 0$. When $s \equiv 1, 2 \pmod{3}$, $\left(1+\left(\frac{s^2-4p}{3}\right)\right) = 1$, and the terms in the sum corresponding to s and $-s$ are $\frac{1}{2}N(s) + \frac{1}{2}N(-s) = N(s)$. Since exactly one of $s, -s$ will be congruent to $p+1 \pmod{3}$, exactly one of $N_3(s)$ and $N_3(-s)$ will be nonzero and equal to $N(s)$. We may therefore write

$$\frac{1}{2}N(s) + \frac{1}{2}N(-s) = N(s) = N_3(s) + N_3(-s).$$

The main term is then

$$\sum_{0<|s|<2\sqrt{p}} G_k(s,p)(N_3(s)+3N_{3\times 3}(s)).$$

We next determine the values of $K(p,3), \epsilon_4(p,3)$ and $\epsilon_3(p,3)$. It is clear from the definition of $K(p,3)$ and the fact that $\left(\frac{-p}{3}\right)=\left(\frac{-1}{3}\right)=-1$ that

$$K(p,3)=2.$$

Now, if $p\equiv 1 \pmod 4$, then $p=a^2+b^2\equiv 1 \pmod 3$, and 3 must divide exactly one of a or b. By our previous convention we assume $3|b$. This gives

$$\epsilon_4(p,3)=\begin{cases} 2G_k(2a,p) & \text{if } p\equiv 1 \pmod 4, \\ 0 & \text{if } p\equiv 3 \pmod 4. \end{cases} \tag{4.4.1}$$

Again, writing $p=(c^2+3d^2)/4$, a congruence argument shows that $3|d$, and

$$\epsilon_3(p,3)=\frac{2}{3}\left(G_k(c,p)+G_k\left(\frac{c+3d}{2},p\right)+G_k\left(\frac{c-3d}{2},p\right)\right)+2G_k(c,p) \tag{4.4.2}$$

and the trace formula becomes

$$\begin{aligned} \mathrm{tr}_k(\Gamma_0(3),p) = &-\sum_{0<|s|<2\sqrt{p}} G_k(s,p)(N_3(s)+3N_{3\times 3}(s))-2+2G_k(c,p)+\epsilon_4(p,3) \\ &+\frac{2}{3}\left(G_k(c,p)+G_k\left(\frac{c+3d}{2},p\right)+G_k\left(\frac{c-3d}{2},p\right)\right)+\delta(k)(p+1). \end{aligned}$$

The problem then reduces to parameterizing elliptic curves with a nontrivial 3-torsion point and counting isomorphism classes. To do this, we use the parametrization of curves with a 3-torsion point discussed in Section 2.2.1. Recall that $\mathcal{I}_p$ is the set of isomorphism classes of curves over $\mathbb{F}_p$. Define the following sets

$$\begin{aligned}
L(s) &:= \{t \in \mathbb{F}_p : \Delta(E_t) \neq 0, |E_t| = p + 1 - s\} \\
I(s) &:= \{\mathcal{C} \in \mathcal{I}_p : \forall E \in \mathcal{C}, |E| = p + 1 - s\} \\
I_3(s) &:= \{[E] \in I(s) : \mathbb{Z}/3\mathbb{Z} \subset E(\mathbb{F}_p)[3]\} \\
J_3(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}, j(E) \neq 0, 1728\} \\
J_{3\times3}(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, j(E) \neq 0, 1728\} \\
J_3^0(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}, j(E) = 0\} \\
J_{3\times3}^0(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, j(E) = 0\} \\
J_3^{1728}(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}, j(E) = 1728\} \\
J_{3\times3}^{1728}(s) &:= \{[E] \in I(s) : E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, j(E) = 1728\}.
\end{aligned}$$

Then $I_3(s) = J_3(s) \cup J_{3\times3}(s) \cup J_3^0(s) \cup J_{3\times3}^0(s) \cup J_3^{1728}(s) \cup J_{3\times3}^{1728}(s)$ and by construction this is a union of disjoint sets. Note next that $1728 = 12^3$ is a cube and that this implies that a curve E with j-invariant 1728 has a discriminant that is a cube and therefore $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This shows that $J_3^{1728}(s) = \emptyset$ for all s.

The goal now is to express the value $|L(s)|$ in terms of the sets above. This is accomplished with the following proposition.

Proposition 4.4.3. *For every s, $L(s)$ satisfies the relationship*

$$|L(s)| = |J_3(s)| + 4|J_{3\times3}(s)| + |J_{3\times3}^0(s)| + 2|J_{3\times3}^{1728}(s)|.$$

To see this result, define the map

$$\phi_s : L(s) \to I_3(s) \text{ by } t \mapsto [E_t]. \tag{4.4.4}$$

By the previous discussion, $\phi_s(t) \notin J_3^0(s)$ for any t, and so ϕ_s maps $L(s)$ onto $J_3(s) \cup J_{3\times3}(s) \cup J_{3\times3}^0(s) \cup J_{3\times3}^{1728}(s)$, and the following lemma describes the structure of this map.

Lemma 4.4.5. *Let $[E] \in I_3(s)$. Then $[E]$ has exactly 1 preimage under ϕ_s when $[E] \in J_3(s) \cup J_{3\times3}^0(s)$, exactly 2 preimages when $[E] \in J_{3\times3}^{1728}(s)$ and exactly 4 preimages when $[E] \in J_{3\times3}(s)$.*

Proof. **Case 1:** Let $[E] \in J_{3\times3}^0(s)$. Then $[E] = [E_{24}]$. Since $0 = j(E_t) = \frac{t(t-24)^3}{t-27}$ the only possible preimages of $[E]$ are $t = 24, 0$. But $\Delta(E_0) = 0$, so t cannot be zero and there is exactly one preimage.

Case 2: Assume now that $p \equiv 1 \pmod 4$, because otherwise $J_{3\times3}^{1728}(s) = \emptyset$, by [38], Lemma 5.6. Let $[E] \in J_{3\times3}^{1728}(s)$. Again, $[E] \cong [E_t]$ for some t, and $1728 = \frac{t(t-24)^3}{t-27}$. Solving for t, we find that the only possible solutions are $t_1 = 18+6\sqrt{3}$, $t_2 = 18-6\sqrt{3}$. Since $\sqrt{3} \in \mathbb{F}_p$ when $p \equiv 1 \pmod 4$, both solutions are in $\mathbb{F}_p$. By [38] Lemma 5.6, there is only one isomorphism class of curve with $j(E) = 1728$ so $\phi_s(t_1) = \phi_s(t_2) = [E]$.

Case 3: We next consider the case where $[E] \in J_3(s) \cup J_{3\times3}(s)$, and $j(E) = j_0$. Define the polynomial

$$f(t) = t(t-24)^3 - j_0(t-27).$$

This has roots at all t such that $j(E_t) = j_0$. Since $E \cong E_{t_0}$ for some t_0, we know that there is at least one solution to $f(t)$ in $\mathbb{F}_p$. Recalling that ρ satisfies $\rho^2 + \rho + 1 = 0$ and defining w so that $w^3 = (t_0^3 - 27t_0^2)$, we may factor f over $\overline{\mathbb{F}}_p[x]$ as

$$\begin{aligned} f(t) = (t - t_0)\left(t - \frac{(w - t_0 + 36)(2w + t_0)}{3w}\right)\left(t - \frac{(\rho w - t_0 + 36)(2\rho w + t_0)}{3\rho w}\right) \\ \cdot \left(t - \frac{(\rho^2 w - t_0 + 36)(2\rho^2 w + t_0)}{3\rho^2 w}\right). \end{aligned}$$

Since $w \in \mathbb{F}_p$ if and only of Δ is a cube in $\mathbb{F}_p$ or equivalently E has full 3-torsion, we see that $[E]$ has exactly one preimage when $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$. If w is a cube, then there are four values of t that map to curves isomorphic over $\overline{\mathbb{F}}_p$ to E. These four curves are either isomorphic over $\mathbb{F}_p$ to E or a quadratic twist of E. The second case cannot occur because by construction each of the four curves have nontrivial 3-torsion, and so all have their trace of Frobenius congruent to 1 modulo 3 and a quadratic twist of E would have trace of Frobenius congruent to 2 modulo 3. Therefore, $[E]$ has four preimages only when $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

The proposition now follows easily from the above lemma. Returning then to the main term of the trace formula, we may write

$$\begin{aligned}
&\sum_{0<|s|<2\sqrt{p}} G_k(s,p)(N_3(s)+3N_{3\times 3}(s)) \\
&= \sum_{0<|s|<2\sqrt{p}} G_k(s,p)(\underbrace{|J_3(s)|+4|J_{3\times 3}(s)|+|J^0_{3\times 3}(s)|+2|J^{1728}_{3\times 3}(s)|}_{|L(s)|}+3|J^0_{3\times 3}(s)| \\
&\quad +2|J^{1728}_{3\times 3}(s)|+|J^0_3(s)|) \\
&= \sum_{0<|s|<2\sqrt{p}} G_k(s,p)|L(s)| + \sum_{0<|s|<2\sqrt{p}} G_k(s,p)(3|J^0_{3\times 3}(s)|+2|J^{1728}_{3\times 3}(s)|+|J^0_3(s)|) \\
&= \sum_{\substack{t=1 \\ t\not\equiv 27 \pmod p}}^{p-1} G_k(a_p(E_t),p) + \sum_{0<|s|<2\sqrt{p}} G_k(s,p)(3|J^0_{3\times 3}(s)|+2|J^{1728}_{3\times 3}(s)|+|J^0_3(s)|).
\end{aligned}$$

It remains to identify for which s are $J^0_{3\times 3}(s), J^{1728}_{3\times 3}(s), J^0_3(s)$ nonempty. From Schoof [37], [38], we know that when $p \equiv 1 \pmod 3$, there are six curves E with $j(E)=0$ and each has $\mathrm{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. For each such curve E, its trace of Frobenius s therefore satisfies $s^2-4p=-3t^2$ for some t. As discussed previously, the six traces s satisfying this equation are $s=\pm c, \pm\frac{c+3d}{2}, \pm\frac{c-3d}{2}$ and for each such s, exactly one of s or $-s$ will be congruent to $p+1 \pmod 3$, the proper congruence in order to have nontrivial 3-torsion. Of these three, a congruence argument shows that exactly one will further satisfy $s \equiv p+1 \pmod 9$, and by construction $|s|=c$. Similarly, If $p \equiv 1 \pmod 4$, the E such that $j(E)=1728$ have $\mathrm{End}(E) \cong \mathbb{Z}[i]$ and as before the trace of Frobenius of such an E will satisfy $s^2-4p=-4t^2$. We use the following lemma from [38].

Lemma 4.4.6 ([38], Lemma 5.6). *Let $\mathbb{F}_p$ be a finite field,*

1. *There is at most one elliptic curve E with $j=0$ and $|E(\mathbb{F}_p)[3]|=9$. There is exactly one if and only if $p \equiv 1 \pmod 3$ and this curve has the trace of its Frobenius endomorphism equal to c as above.*

2. *There is at most one elliptic curve E with $j=1728$ and $|E(\mathbb{F}_p)[3]|=9$. There is exactly one if and only if $p \equiv 1 \pmod{12}$ and this curve has the trace of its Frobenius endomorphism equal to $2a$.*

Then if $p \equiv 3 \pmod 4$, $J^{1728}_{3\times 3}(s)=\emptyset$ for all s, and if $p \equiv 1 \pmod 4$, $|J^{1728}_{3\times 3}(2a)|=1$ and $J^{1728}_{3\times 3}(s)=\emptyset$ for all other s. Recalling that $\epsilon_4(p,3)=2G_k(2a,p)$, this gives:

$$\sum_{0<|s|<2\sqrt{p}} G_k(s,p)(N_3(s)+3N_{3\times 3}(s)) = \sum_{\substack{t=1\\ t\not\equiv 27 \ (\mathrm{mod}\ p)}}^{p-1} G_k(a_p(E_t),p) + 3G_k(c,p)$$
$$+G_k\left(\frac{c+3d}{2},p\right) + G_k\left(\frac{c-3d}{2}\right) + \epsilon_4(p,3).$$

Finally, we relate this back to the trace.

$$\begin{aligned}
&\mathrm{tr}_k(\Gamma_0(3),p)\\
=&-\sum_{0<|s|<2\sqrt{p}} G_k(s,p)(N_3(s)+3N_{3\times 3}(s)) - 2 + \epsilon_4(p,3)\\
&+\frac{2}{3}\left(G_k(c,p)+G_k\left(\frac{c+3d}{2},p\right)+G_k\left(\frac{c-3d}{2},p\right)\right)+2G_k(c,p)+\delta(k)(p+1)\\
=&-\sum_{\substack{t=1\\ t\not\equiv 27 \ (\mathrm{mod}\ p)}}^{p-1} G_k(a_p(E_t),p) - 3G_k(c,p) - G_k\left(\frac{c+3d}{2},p\right) - G_k\left(\frac{c-3d}{2}\right) - \epsilon_4(p,3) - 2\\
&+\epsilon_4(p,3)+\frac{2}{3}\left(G_k(c,p)+G_k\left(\frac{c+3d}{2},p\right)+G_k\left(\frac{c-3d}{2},p\right)\right)+2G_k(c,p)+\delta(k)(p+1)\\
=&-2-\sum_{\substack{t=1\\ t\not\equiv 27 \ (\mathrm{mod}\ p)}}^{p-1} G_k(a_p(E_t),p) - \frac{1}{3}\left(G_k(c,p)+G_k\left(\frac{c+3d}{2},p\right)+G_k\left(\frac{c-3d}{2},p\right)\right)+\delta(k)(p+1).
\end{aligned}$$

This can be simplified with the following lemma.

Lemma 4.4.7. *Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime for which E has good reduction. Recall that*

$$L(E,s)=\sum_n a_n(E)n^{-s}$$

is the Hasse-Weil L-function of E. Then the p power coefficients of $L(E,s)$ can be written explicitly as a function of $a_p(E)$ by

$$a_{p^{k-2}}(E) = G_k(a_p(E),p) \text{ when } k\geq 2.$$

Proof. Recall that we can define $G_k(s,p)$ by

$$G_k(s,p) := \frac{x^{k-1}-y^{k-1}}{x-y}$$

where $x+y=s$ and $xy=p$.

We will show that the function $G_k(a_p(E),p)$ satisfies the same recurrence as the p power coefficients of $L(E,s)$. This recurrence for the coefficients $a_{p^e}(f)$ of the L-function where E has good reduction at p, is

$$a_{p^e}(E) = a_p(E)a_{p^{e-1}}(E) - p \cdot a_{p^{e-2}}(E)$$

and $a_{p^0}(E) := 1$.

Explicitly evaluating $G_2(a_p(E),p)$ shows

$$G_2(a_p(E),p) = 1 = a_{p^0}(E).$$

Now assume that the relation holds for all weights less than k. Then in particular

$$a_{p^{k-3}}(E) = G_{k-1}(a_p(E),p) \tag{4.4.8}$$
$$a_{p^{k-4}}(E) = G_{k-2}(a_p(E),p). \tag{4.4.9}$$

Computing $a_{p^{k-2}}(E)$ using the known recurrence relation and equations (4.4.8) and (4.4.9) we have

$$\begin{aligned} a_{p^{k-2}}(E) &= a_p(E)a_{p^{k-3}}(E) - p \cdot a_{p^{k-4}}(E) \\ &= a_p(E)G_{k-1}(a_p(E),p) - pG_{k-2}(a_p(E),p) \\ &= a_p(E)\left(\frac{x^{k-2}-y^{k-2}}{x-y}\right) - p\left(\frac{x^{k-3}-y^{k-3}}{x-y}\right). \end{aligned}$$

Since $a_p(E) = x+y$ and $xy = p$, we may replace these in the equation above

$$\begin{aligned} &= (x+y)\left(\frac{x^{k-2}-y^{k-2}}{x-y}\right) - (xy)\left(\frac{x^{k-3}-y^{k-3}}{x-y}\right) \\ &= \frac{x^{k-1}-y^{k-1}}{x-y} \\ &= G_k(a_p(E),p) \end{aligned}$$

which proves the lemma.

□

Let $\alpha \in \mathbb{Z}$ be chosen so that α is not a cube modulo p. That is, if we consider α as an element of $\mathbb{F}_p^\times$, it is not a cube. Then one can check that

$$\{|a_p(E_{0,\alpha})|, |a_p(E_{0,\alpha^2})|, |a_p(E_{0,\alpha^3})|\} = \left\{c, \frac{c+3d}{2}, \left|\frac{c-3d}{2}\right|\right\}$$

so that the final form of the trace formula is

$$\mathrm{tr}_k(\Gamma_0(3),p) = -\sum_{\substack{t=1 \\ t\not\equiv 27 \pmod p}}^{p-1} a_{p^{k-2}}(E_t) - \frac{1}{3}\left(a_{p^{k-2}}(E_{0,\alpha}) + a_{p^{k-2}}(E_{0,\alpha^2}) + a_{p^{k-2}}(E_{0,\alpha^3})\right)$$
$$+\delta(k)(p+1) - 2.$$

4.4.2 The case where $p \equiv 2 \pmod 3$

Next, we prove the version of the trace formula for $p \equiv 2 \pmod 3$. The argument follows similarly to the case where $p \equiv 1 \pmod 3$. Also, we assume that $p > 3$ since the $p = 2$ case is straightforward. We begin by noting that $\left(\frac{p}{3}\right) = -1$, so that the trace formula in this case is given by (4.3.18). Also, $\epsilon_3(p,3) = 0$ and $\epsilon_4(p,3) = 0$ so that the trace formula can be written as

$$\mathrm{tr}_k(\Gamma_0(3),p) = -\frac{1}{2}\cdot \sum_{0<|s|<2\sqrt{p}} G_k(s,p)\left(1+\left(\frac{D}{3}\right)\right)N(s) - K(p,3) + \delta(k)(1+p).$$

Recall that $N_3(s)$ is the number of isomorphism classes of elliptic curves with trace of Frobenius s and a point of order 3. Since $|E(\mathbb{F}_p)| = p+1-s$ we see that in our case, $N_3(s) = N(s)$ when $s \equiv 0 \pmod 3$ and $N_3(s) = 0$ otherwise. Still using the relation $s^2 - 4p = t^2 D$, we also find that

$$s \equiv 0 \pmod 3 \iff D \equiv 1 \pmod 3 \iff \left(1+\left(\frac{D}{3}\right)\right) = 2$$
$$s \equiv 1,2 \pmod 3 \iff D \equiv 2 \pmod 3 \iff \left(1+\left(\frac{D}{3}\right)\right) = 0$$

so we can write the trace formula as

$$\begin{aligned}\mathrm{tr}_k(\Gamma_0(3),p) &= -\sum_{0<|s|<2\sqrt{p}} G_k(s,p)N_3(s) - 2 - (-p)^{k/2-1}H(-4p) + \delta(k)(1+p) \\ &= -\sum_{0<|s|<2\sqrt{p}} G_k(s,p)N_3(s) - 2 - G_k(0,p)N(0) + \delta(k)(1+p) \\ &= -\sum_{0\leq|s|<2\sqrt{p}} G_k(s,p)N_3(s) - 2 + \delta(k)(1+p). \qquad (4.4.10)\end{aligned}$$

Again define $E_t : y^2 + txy + t^2y = x^3$, which has $(0,0)$ as a point of order 3 and the sets

$$L(s) := \{t \in \mathbb{F}_p : \Delta(E_t) \neq 0, |E_t(\mathbb{F}_p)| = p + 1 - s\}$$
$$I(s) := \{\mathcal{C} \in \mathcal{I}_p : \forall E \in C, |E(\mathbb{F}_p)| = p + 1 - s\}$$
$$I_3(s) := \{[E] \in I(s) : \mathbb{Z}/3\mathbb{Z} \subset E(\mathbb{F}_p)[3]\}$$

and consider the map

$$\phi_s : L(s) \to I_3(s) \text{ to } t \mapsto [E_t].$$

We will prove the following lemma.

Lemma 4.4.11. *Assuming that $s \equiv 0 \pmod 3$, the map $\phi_s : L(s) \to I_s(s)$ is injective, and when $s \neq 0$ it is a bijection.*

Proof. When $s \neq 0$, surjectivity is clear, since any elliptic curve with 3-torsion and nonzero j-invariant can be written in the form given above, and curves with j invariant equal to 0 will be supersingular. When $s = 0$, the isomorphism classes of curves E_t^0 with $j(E_t^0) = 0$ given by $E_t^0 : y^2 + ty = x^3$ are not in the image of ϕ_0. Any two curves $E_{t_0}^0$ and $E_{t_1}^0$ in this form will have the Weierstrass forms $E_{t_0}^0 : y^2 = x^3 - (108t_0)^2$ and $E_{t_1}^0 : y^2 = x^3 - (108t_1)^2$. These curves isomorphic over $\mathbb{F}_p$, since all elements of $\mathbb{F}_p$ are cubes. This shows that when $s = 0$, there is exactly one isomorphism class over $\mathbb{F}_p$ that is not in the image of ϕ_0.

For injectivity, consider first the case where the j-invariant is nonzero. Let $[E_{t_0}] \in I_3(s)$ be an isomorphism class of curve over $\mathbb{F}_p$ with j-invariant j_0, and consider its preimage in $L(s)$. As in the case for $p \equiv 1 \pmod 3$, define the polynomial

$$f(t) = t(t - 24)^3 - j_0(t - 27).$$

Any element of $L(s)$ mapping to $[E_{t_0}]$ will be a root of $f(t)$. Now, define $w \in \mathbb{F}_p$ to be the unique element of $\mathbb{F}_p$ satisfying

$$w^3 = (t_0^3 - 27t_0^2).$$

Then as before, $f(t)$ factors over $\overline{\mathbb{F}}_p$ as

$$\begin{aligned} f(t) =&(t-t_0)\left(t-\frac{(w-t_0+36)(2w+t_0)}{3w}\right)\left(t-\frac{(\rho w-t_0+36)(2\rho w+t_0)}{3\rho w}\right) \\ &\cdot\left(t-\frac{(\rho^2 w-t_0+36)(2\rho^2 w+t_0)}{3\rho^2 w}\right), \end{aligned}$$

where ρ is a third root of unity. Since $p \equiv 2 \pmod 3$, it follows that $\rho \notin \mathbb{F}_p$. Therefore, $f(t)$ factors over $\mathbb{F}_p$ into two linear terms and a quadratic term. Let $t_1 := (w-t_0+36)(2w+t_0)/3w$ be the second root of $f(t)$ in $\mathbb{F}_p$.

We have now shown that there are exactly two roots of $f(t)$ in $\mathbb{F}_p$, and so the corresponding curves E_{t_0} and E_{t_1} are isomorphic over $\overline{\mathbb{F}}_p$. We can easily see that they are not isomorphic over $\mathbb{F}_p$ since E_{t_0} will have a quadratic twist defined over $\mathbb{F}_p$ with the same j-invariant. Since the trace of Frobenius of this twist is $-s \equiv 0 \pmod 3$, it will also have a 3-torsion point, and so can be written as E_t for some t. Such a curve will be isomorphic to E_{t_0} over $\overline{\mathbb{F}}_p$ but not $\mathbb{F}_p$, so it must be isomorphic to E_{t_1} over $\mathbb{F}_p$. This shows that $[E_{t_0}]$ has exactly one preimage in $L(s)$.

Now, if $j(E_t) = 0$, and $[E_t]$ is in the image of ϕ_0, by a previous discussion in fact $t = 24$ and so the map is also injective.

□

This lemma shows that $|L(s)| = |I_3(s)| = N_3(s)$ when $s \neq 0$ and $|L(0)| = |I_3(0)| - 1 = N(0) - 1$. Using this in the trace formula gives

$$\begin{aligned} \mathrm{tr}_k(\Gamma_0(3), p) &= -\sum_{0\leq|s|<2\sqrt{p}} G_k(s,p)|L(s)| - G_k(0,p) - 2 + \delta(k)(1+p) \\ &= -\sum_{\substack{t=1 \\ t\not\equiv 27 \ (\mathrm{mod}\ p)}}^{p-1} G_k(a_p(E_t),p) - (-p)^{k/2-1} - 2 + \delta(k)(1+p) \\ &= -\sum_{\substack{t=1 \\ t\not\equiv 27 \ (\mathrm{mod}\ p)}}^{p-1} a_{p^{k-2}}(E_t) - (-p)^{k/2-1} - 2 + \delta(k)(1+p), \qquad (4.4.12) \end{aligned}$$

which proves Theorem 4.2.1 in all cases.

4.4.3 Proof of Corollary 4.2.3

Corollary 4.2.3 now follows quickly from Theorems 3.2.2 and 4.2.1.

Proof of Corollary 4.2.3. Begin with the formula

$$\mathrm{tr}_k(\Gamma_0(3),p) = -\sum_{\substack{t=1\\ t\not\equiv 27 \pmod p}}^{p-1} a_{p^{k-2}}(E_t) - \gamma_k(p) - 2$$

and use the relation

$$a_{p^{k-2}}(E_t) = t_{p^{k-2}}(E_t) + p \cdot a_{p^{k-4}}(E_t) \tag{4.4.13}$$

to replace each $a_{p^{k-2}}(E_t)$ to give

$$\mathrm{tr}_k(\Gamma_0(3),p) = -\sum_{\substack{t=1\\ t\not\equiv 27 \pmod p}}^{p-1} t_{p^{k-2}}(E_t) - p \cdot \sum_{\substack{t=1\\ t\not\equiv 27 \pmod p}}^{p-1} a_{p^{k-4}}(E_t) - \gamma_k(p) - 2.$$

One can see (4.4.13) by recalling that

$$a_p(E) = t_p(E) = \alpha + \overline{\alpha}$$

where $\alpha\overline{\alpha} = p$, and that for each k, $t_{p^k}(E) = \alpha^k + \overline{\alpha}^k$. Then

$$\begin{aligned}(\alpha-\overline{\alpha})t_{p^k}(E) &= (\alpha-\overline{\alpha})(\alpha^k+\overline{\alpha}^k) = \alpha^{k+1} - \overline{\alpha}^{k+1} - \alpha\overline{\alpha}(\alpha^{k-1} - \overline{\alpha}^{k-1})\\ &= \alpha^{k+1} - \overline{\alpha}^{k+1} - p(\alpha^{k-1} - \overline{\alpha}^{k-1})\end{aligned}$$

and so

$$\begin{aligned}t_{p^k}(E) &= \frac{\alpha^{k+1} - \overline{\alpha}^{k+1}}{\alpha-\overline{\alpha}} - p\frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha-\overline{\alpha}} = G_{k+2}(a_p(E),p) - p \cdot G_k(a_p(E),p)\\ &= a_{p^k}(E) - p \cdot a_{p^{k-2}}(E),\end{aligned}$$

where the final equality follows from Lemma 4.4.7.

Apply again (4.4.13) to each $a_{p^{k-4}}(E_t)$ and so on, until reaching $a_p^0(E_t) = 1$. The result is the following formula:

$$\mathrm{tr}_k(\Gamma_0(3),p) = -\sum_{i=0}^{k/2-2} p^i \sum_{\substack{t=1\\ t\not\equiv 27 \pmod p}}^{p-1} t_{p^{k-2-2i}}(E_t) - p^{k/2-1}(p-2) - \gamma_k(p) - 2.$$

Applying Theorem 3.2.2 to each $t_{p^{k-2-2i}}(E_t)$ then yields the corollary. □

4.4.4 Inductive trace

Now that we have proven Theorem 4.2.1, we can prove Theorem 4.2.4, a version of the trace formula which expresses $\mathrm{tr}_k(\Gamma_0(3), p)$ in terms of traces on spaces of smaller weight, as well as an additional inductive formula.

Proof of Theorem 4.2.4. We show the theorem when $p \equiv 1 \pmod 3$, but the $p \equiv 2 \pmod 3$ case follows similarly. We use the relation 4.4.13 in order to phrase Theorem 4.2.1 in terms of traces of Frobenius, and then Theorem 3.2.2 to express this in terms of Gaussian hypergeometric functions.

Replacing each $a_{p^{k-2}}(E_t)$ by $t_{p^{k-2}}(E_t) + p \cdot a_{p^{k-4}}(E_t)$ in the sum then gives that $\mathrm{tr}_k(\Gamma_0(3), p)$ is equal to

$$\begin{aligned}
&- \sum_{\substack{t \in \mathbb{F}_p \\ \Delta(E_t) \neq 0}} t_{p^{k-2}}(E_t) - p \sum_{\substack{t=1 \\ t \not\equiv 27 \pmod p}}^{p-1} a_{p^{k-4}}(E_t) - \frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) \\
&- \frac{1}{3}(p \cdot a_{p^{k-4}}(E_{0,\alpha}) + p \cdot a_{p^{k-4}}(E_{0,\alpha^2}) + p \cdot a_{p^{k-4}}(E_{0,\alpha^3})) - 2 \\
= &- \sum_{\substack{t \in \mathbb{F}_p \\ \Delta(E_t) \neq 0}} t_{p^{k-2}}(E_t) - \frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) \\
&+ p \cdot \mathrm{tr}_{k-2}(\Gamma_0(3), p) + 2p - 2 \\
= &\, p^{k-2} \sum_{t=2}^{p-1} {}_2F_1 \left(\left. \begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \right| t \right)_{p^{k-2}} + p \cdot \mathrm{tr}_{k-2}(\Gamma_0(3), p) \\
&- \frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) + 2p - 2 \text{ by Theorem 3.2.2.}
\end{aligned}$$

Finally, we showed in Lemma 3.2.5 that

$$\frac{1}{3}(t_{p^{k-2}}(E_{0,\alpha}) + t_{p^{k-2}}(E_{0,\alpha^2}) + t_{p^{k-2}}(E_{0,\alpha^3})) = \begin{cases} 0 & k \equiv 0, 1 \pmod 3 \\ -p^{k-2} \cdot {}_2F_1 \left(\left. \begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \right| 9 \cdot 8^{-1} \right)_{p^{k-2}} & k \equiv 2 \pmod 3 \end{cases}$$

which completes the proof when $p \equiv 1 \pmod 3$. □

4.5 Level 9

4.5.1 Proof of Theorems 4.5.3, 4.2.6

Now we sketch a proof of Theorem 4.2.6, a trace formula for Hecke operators on $S_k(\Gamma_0(9))$. Notation and methods are similar to the level 3 case, so we only outline the important differences. Its not hard to see (from the definition of $c(s,f,9)$ given below) that when $p \equiv 2 \pmod 3$, $\mathrm{tr}_k(\Gamma_0(9),p) = \mathrm{tr}_k(\Gamma_0(3),p)$. Therefore the level 3 formulas hold in this case. Because of this, we may assume throughout that $p \equiv 1 \pmod 3$. Applying Hijikata's trace formula results in the following expression:

$$\mathrm{tr}_k(\Gamma_0(9),p) = -\frac{1}{2}\sum_{0<|s|<2\sqrt{p}} G_k(s,p)\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,9) - 2 + \delta(k)(1+p).$$

The following lemma characterizes the function $c(s,f,9)$.

Proposition 4.5.1. *Let $s^2-4p = t^2D$ where D is a fundamental discriminant of an imaginary quadratic field and let $f|t$. Let*

$$\tau := \mathrm{ord}_3 t,$$

$$\rho := \mathrm{ord}_3 f.$$

Then the value of $c(s,f,9)$ is given by:
If $\tau = \rho$:

$$c(s,f,9) = \begin{cases} 2, \text{ if } D \equiv 1 \pmod 3; \\ 0, \text{ if } D \equiv 2 \pmod 3; \\ 0, \text{ if } D \equiv 0 \pmod 3. \end{cases}$$

If $\tau = \rho + 1$:

$$c(s,f,9) = \begin{cases} 5, \text{ if } D \equiv 1 \pmod 3; \\ 3, \text{ if } D \equiv 2 \pmod 3; \\ 4, \text{ if } D \equiv 0 \pmod 3. \end{cases}$$

If $\tau > \rho + 1$:

$$c(s,f,9) = 4.$$

Because $p \equiv 2 \pmod 3 \implies \tau = \rho$, we have $c(s,f,9) = 1 + \left(\frac{D}{3}\right)$ when $p \equiv 2 \pmod 3$. This agrees with the $\ell = 3$ case, and the same calculations as in Section 4.4.2 show that $\mathrm{tr}_k(\Gamma_0(3),p) = \mathrm{tr}_k(\Gamma_0(9),p)$. In fact, one can show, using the definition of $c(s,f,N)$ from [15] that $c(s,f,3^m) = 1 + \left(\frac{D}{3}\right)$ for each m, and so all of these traces are equal.

Now, as in Lemma 4.3.7, we remove the $c(s,f,9)$ term from the trace formula by applying Theorem 4.3.8. See Appendix A for a statement and proof of this lemma for a general prime ℓ.

Lemma 4.5.2. *Assume that* $p \equiv 1 \pmod 3$. *We can write*

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,9) = \begin{cases} 12H^*\left(\frac{s^2-4p}{9}\right) & \textit{if } 3|t; \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Consider first the case where $3 \nmid t$. Then $\mathrm{ord}_3 f = \mathrm{ord}_3 t = 0$. Also, $s^2 - 4p \equiv 0, 2 \pmod 3$, so if $3 \nmid t$ this implies that $t^2 D \equiv D \equiv 0, 2 \pmod 3$. In either case, $c(s,f,9) = 0$ for all $f|t$. This shows that the whole term is 0, agreeing with the lemma.

Now we assume that $3|t$. When $D \equiv 1 \pmod 3$, applying 4.3.8 in the second equality below yields the following:

$$2 \sum_{f|t, f\nmid(t/3)} h^*\left(\frac{s^2-4p}{f^2}\right) = 2 \sum_{f|(t/3), f\nmid(t/9)} h^*\left(\frac{s^2-4p}{(3f)^2}\right) = \sum_{f|(t/3), f\nmid(t/9)} h^*\left(\frac{s^2-4p}{f^2}\right).$$

This shows that

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,9) = \sum_{\substack{f|(t/3) \\ f\nmid(t/9)}} h^*\left(\frac{s^2-4p}{f^2}\right) \begin{Bmatrix} 6 \text{ if } D \equiv 1 \pmod 3 \\ 3 \text{ if } D \equiv 2 \pmod 3 \\ 4 \text{ if } D \equiv 0 \pmod 3 \end{Bmatrix} + 4 \sum_{f|(t/9)} h^*\left(\frac{s^2-4p}{f^2}\right).$$

Now apply Theorem 4.3.8 to both terms above. The first one becomes:

$$\begin{aligned} \sum_{\substack{f|(t/3) \\ f\nmid(t/9)}} h^*\left(\frac{s^2-4p}{f^2}\right) \begin{Bmatrix} 6 \\ 3 \\ 4 \end{Bmatrix} &= \sum_{\substack{f|(t/3) \\ f\nmid(t/9)}} h^*\left(\frac{s^2-4p}{(3f)^2}\right) \begin{Bmatrix} 6 \\ 3 \\ 4 \end{Bmatrix} \cdot \begin{Bmatrix} 2 \\ 4 \\ 3 \end{Bmatrix} \\ &= 12 \sum_{\substack{f|(t/3) \\ f\nmid(t/9)}} h^*\left(\frac{s^2-4p}{(3f)^2}\right). \end{aligned}$$

The second becomes

$$4 \sum_{f|(t/9)} h^*\left(\frac{s^2-4p}{f^2}\right) = 12 \sum_{f|(t/9)} h^*\left(\frac{s^2-4p}{(3f)^2}\right).$$

Replacing these two quantities into the expression above and combining the sums gives

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f,9) = 12 \sum_{f|(t/3)} h^*\left(\frac{s^2-4p}{(3f)^2}\right) = 12H^*\left(\frac{s^2-4p}{9}\right).$$

□

Now we have (using the definitions of ϵ_4, ϵ_3, a, c in equations (4.3.14) and (4.3.13) to rewrite the expressions in H^* in terms of H)

$$\begin{aligned}
\mathrm{tr}_k(\Gamma_0(9),p) &= -6 \sum_{\substack{0<|s|<2\sqrt{p},\\ 3|t}} G_k(s,p)H^*\left(\frac{s^2-4p}{9}\right) - 4 + \delta(k)(1+p) \\
&= -6 \sum_{\substack{0<|s|<2\sqrt{p},\\ 3|t}} G_k(s,p)H\left(\frac{s^2-4p}{9}\right) + 12\cdot\frac{1}{2}G_k(2a,p)\delta_4(p) + 12\cdot\frac{2}{3}G_k(c,p) \\
&\quad -4+\delta(k)(1+p) \\
&= -12 \sum_{0<|s|<2\sqrt{p}} G_k(s,p)N_{3\times 3}(s) + 6G_k(2a,p)\delta_4(p) + 8G_k(c,p) - 4 + \delta(k)(1+p)
\end{aligned}$$

where $\delta_4(p) = 1$ if $p \equiv 1 \pmod 4$ and 0 otherwise. Keeping notation as in Section 4.4, this is equal to:

$$\begin{aligned}
&-3 \sum_{0<|s|<2\sqrt{p}} G_k(s,p)\left(4|J_{3\times 3}(s)| + |J^0_{3\times 3}(s)| + 2|J^{1728}_{3\times 3}(s)| + 3|J^0_{3\times 3}(s)| + 2|J^{1728}_{3\times 3}(s)\right) \\
&+6G_k(2a,p) + 8G_k(c,p) - 4 + \delta(k)(1+p) \\
&= -3 \sum_{\substack{t=1,\ t\neq 27\\ t^3-27t^2 \text{ a cube}}}^{p-1} G_k(a_p(E_t),p) - G_k(c,p) - 4 + \delta(k)(1+p) \\
&= -3 \sum_{\substack{t=2\\ 1-t \text{ a cube}}}^{p-1} G_k(a_p(E_{27/t}),p) - G_k(c,p) - 4 + \delta(k)(1+p) \\
&= -3 \sum_{\substack{t=2\\ 1-t \text{ a cube}}}^{p-1} G_k\left(p\cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\,\middle|\, t\right)_p, p\right) - G_k(c,p) - 4 + \delta(k)(1+p).
\end{aligned}$$

Now apply the transformation law in Theorem 2.1.7, to write this as

$$\begin{aligned}
&= -3 \sum_{\substack{t=2\\ 1-t \text{ a cube}}}^{p-1} G_k\left(p\cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\,\middle|\, 1-t\right)_p, p\right) - G_k(c,p) - 4 + \delta(k)(1+p) \\
&= -3 \sum_{\substack{t=2\\ t \text{ a cube}}}^{p-1} G_k\left(p\cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\,\middle|\, t\right)_p, p\right) - G_k(c,p) - 4 + \delta(k)(1+p).
\end{aligned}$$

This gives the following expression for the trace formula.

Theorem 4.5.3. *Let $p \equiv 1 \pmod 3$ and $k \geq 4$. Then the trace of the p^{th} Hecke* *operator on $S_k(\Gamma_0(9))$ is given by the expression*

$$\mathrm{tr}_k(\Gamma_0(9),p) = -\sum_{\substack{t=2\\ t^3\not\equiv 1 \pmod p}}^{p-1} G_k\left(p\cdot {}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, t^3\right)_p, p\right) - G_k(c,p) - 4 + \delta(k)(1+p).$$

From here we may derive a number of expressions as in the level 3 case. For example, using Lemma 4.4.7, it follows that when $k \geq 4$,

$$\mathrm{tr}_k(\Gamma_0(9),p) = -\sum_{\substack{t=1\\ t^3\not\equiv 27}}^{p-1} a_{p^{k-2}}(E_{t^3}) - a_{p^{k-2}}(E_{24}) - 4.$$

Also, using (4.4.13) we can write when $k \geq 4$

$$\begin{aligned}\mathrm{tr}_k(\Gamma_0(9),p) = &\sum_{i=0}^{k/2-2}\sum_{\substack{t=2\\ t^3\not\equiv 1}}^{p-1} p^{k-2-i}{}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, t^3\right)_{p^{k-2-2i}}\\ &+\sum_{i=0}^{k/2-2} p^{k-2-i}{}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, 9\cdot 8^{-1}\right)_{p^{k-2-2i}} - 4 - p^{k/2-1}(p-1).\end{aligned}$$

Finally, arguing as in Section 4.4.4 we derive an inductive formula for all $k \geq 6$:

$$\begin{aligned}\mathrm{tr}_k(\Gamma_0(9),p) = &\, p^{k-2}\sum_{\substack{t=2\\ t^3\not\equiv 1}}^{p-1} {}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, t^3\right)_{p^{k-2}} + p^{k-2}{}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, 9\cdot 8^{-1}\right)_{p^{k-2}} - 4 + 4p\\ &+p\cdot \mathrm{tr}_{k-2}(\Gamma_0(9),p).\end{aligned}$$

4.6 Applications

4.6.1 Fourier coefficients of $\eta(3z)^8$

Let

$$\eta(3z)^8 = \sum b(n)q^n,\ q = e^{2\pi i z}$$

be the Fourier expansion of the unique Hecke eigenform in $S_4(\Gamma_0(9))$. We now prove Corollary 4.2.7, which states that the Fourier coefficients of $\eta(3z)^8$ when $p \equiv 1 \pmod 3$ are given by the expression

$$b(p) = -p^3\left(\binom{\rho^2}{\rho}^3 + \binom{\rho}{\rho^2}^3\right) = -p^3{}_2F_1\left(\begin{matrix}\rho\ \rho^2\\ \epsilon\end{matrix}\,\middle|\, 9\cdot 8^{-1}\right)_{p^3}.$$

Proof. We begin with the alternate trace formula expression from Theorem 4.5.3 and derive the corollary from this. Applying Theorem 4.5.3 with $k = 4$ and noting that the dimension for $S_4(\Gamma_0(9))$ is one, we can write

$$\begin{aligned}
b(p) = &-\sum_{t=1}^{p-1} G_4\left(p \cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right), p\right)(\rho^2(t)+\rho(t)+1) - G_4(c,p) - 4\\
&-3G_4\left(p \cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| 1\right), p\right)\\
=&-\sum_{t=1}^{p-1} p^2{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)^2 (\rho(t)+\rho^2(t)+1) - c^2 + p^2 - 3p - 1.
\end{aligned}$$

Now compute the term $\sum_{t=1}^{p-1} p^2{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)^2 \rho(t)$. Use Definition 3.5 and Theorem 3.6 of Greene [14], which in our case (switching A and B in the definition) states that

$${}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right) = \frac{1}{p}\sum_{y\in\mathbb{F}_p} \rho(y)\rho^2(1-y)\rho(1-ty).$$

Then

$$\begin{aligned}
\sum_{t=1}^{p-1} p^2{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)^2 \rho(t) =&\sum_{t=1}^{p-1} p \cdot {}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)\sum_{y}\rho(y)\rho^2(1-y)\rho(1-ty)\rho(t)\\
=&p^2\sum_{y=1}^{p-1}\rho^2(1-y)\left(\frac{1}{p}\sum_{t=1}^{p-1}{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)\rho(ty)\rho(1-ty)\right)\\
=&p^2\sum_{y=1}^{p-1}\rho^2(1-y)\left(\frac{1}{p}\sum_{t=1}^{p-1}{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| ty^{-1}\right)\rho(t)\rho(1-t)\right).
\end{aligned}$$

Now apply Theorem 3.13 of [14], stated in this thesis as equation (2.1.6). This gives that the above is equal to

$$\begin{aligned}
p^2\sum_{y=1}^{p-1}\rho^2(1-y){}_3F_2\left(\begin{matrix}\rho & \rho^2 & \rho\\ & \epsilon & \rho^2\end{matrix}\middle| y^{-1}\right) =&p^2\sum_{y=1}^{p-1}\rho^2(1-y^{-1}){}_3F_2\left(\begin{matrix}\rho & \rho^2 & \rho\\ & \epsilon & \rho^2\end{matrix}\middle| y\right)\\
=&p^2\sum_{y=1}^{p-1}\rho(y)\rho^2(1-y){}_3F_2\left(\begin{matrix}\rho & \rho^2 & \rho\\ & \epsilon & \rho^2\end{matrix}\middle| y^{-1}\right)\\
=&p^3{}_4F_3\left(\begin{matrix}\rho & \rho^2 & \rho & \rho\\ & \epsilon & \rho^2 & \epsilon\end{matrix}\middle| 1\right).
\end{aligned}$$

By the same method we can show that

$$\sum_{t=1}^{p-1} p^2{}_2F_1\left(\begin{matrix}\rho\ \rho^2 \\ \epsilon\end{matrix}\middle| t\right)^2 \rho^2(t) = p^3{}_4F_3\left(\begin{matrix}\rho\ \rho^2\ \rho^2\ \rho^2 \\ \epsilon\ \ \rho\ \ \epsilon\end{matrix}\middle| 1\right), \tag{4.6.1}$$

and

$$\sum_{t=1}^{p-1} p^2{}_2F_1\left(\begin{matrix}\rho\ \rho^2 \\ \epsilon\end{matrix}\middle| t\right)^2 = p^3{}_4F_3\left(\begin{matrix}\rho\ \rho^2\ \epsilon\ \epsilon \\ \epsilon\ \rho^2\ \rho\end{matrix}\middle| 1\right). \tag{4.6.2}$$

We reduce (4.6.2) further using identity 2.15 from [14]

$$\binom{A}{B}\binom{C}{A} = \binom{C}{B}\binom{C\overline{B}}{A\overline{B}} - \frac{p-1}{p^2}B(-1)\delta(A) = \frac{p-1}{p^2}AB(-1)\delta(B\overline{C}), \tag{4.6.3}$$

where $\delta(A) = 1$ if $A = \epsilon$ and 0 otherwise. When $\chi \neq \epsilon, \rho, \rho^2$, applying equation (4.6.3) and using Jacobi sum identities gives the equality

$$\binom{\rho\chi}{\chi}\binom{\chi}{\rho\chi}\binom{\rho^2\chi}{\chi}\binom{\chi}{\rho^2\chi} = \frac{1}{p^2}.$$

There are $p-4$ such terms. We must consider the exceptional three cases separately. We have shown so far that:

$$\begin{aligned}
p^3{}_4F_3\left(\begin{matrix}\rho\ \rho^2\ \epsilon\ \epsilon \\ \epsilon\ \rho^2\ \rho\end{matrix}\middle| 1\right) =& \frac{p^4}{p-1}\sum_{\chi}\binom{\rho\chi}{\chi}\binom{\chi}{\rho\chi}\binom{\rho^2\chi}{\chi}\binom{\chi}{\rho^2\chi} \\
=& \frac{p^4}{p-1}\binom{\rho}{\epsilon}\binom{\epsilon}{\rho}\binom{\rho^2}{\epsilon}\binom{\epsilon}{\rho^2} + \frac{p^4}{p-1}\binom{\rho^2}{\rho}\binom{\rho}{\rho^2}\binom{\epsilon}{\rho}\binom{\rho}{\epsilon} \\
&+ \frac{p^4}{p-1}\binom{\epsilon}{\rho^2}\binom{\rho^2}{\epsilon}\binom{\rho}{\rho^2}\binom{\rho^2}{\rho} + \frac{p^2(p-4)}{p-1} \\
=& \frac{p^2(p-4)}{p-1} + \frac{1}{p-1} + \frac{2p^2}{p-1}\binom{\rho^2}{\rho}\binom{\rho}{\rho^2} \\
=& \frac{p^3-4p^2+2p+1}{p-1} = p^2-3p-1.
\end{aligned} \tag{4.6.4}$$

Combining these results, we have

$$b(p) = -p^3{}_4F_3\left(\begin{matrix}\rho\ \rho^2\ \rho^2\ \rho^2 \\ \epsilon\ \ \epsilon\ \ \rho\end{matrix}\middle| 1\right) - p^3{}_4F_3\left(\begin{matrix}\rho^2\ \rho\ \rho\ \rho \\ \epsilon\ \epsilon\ \rho^2\end{matrix}\middle| 1\right) - c^2.$$

Reducing this further, we use Theorem 2.15 again to write

$$p^3{}_4F_3\left(\begin{matrix}\rho & \rho^2 & \rho^2 & \rho^2\\ & \epsilon & \epsilon & \rho\end{matrix}\middle|\, 1\right) = p^3\binom{\rho^2}{\rho}{}_3F_2\left(\begin{matrix}\rho^2 & \rho^2 & \rho^2\\ & \epsilon & \epsilon\end{matrix}\middle|\, 1\right) - p^2\binom{\rho}{\rho^2}\binom{\rho}{\rho^2}$$

and similarly

$$p^3{}_4F_3\left(\begin{matrix}\rho^2 & \rho & \rho & \rho\\ & \epsilon & \epsilon & \rho^2\end{matrix}\middle|\, 1\right) = p^3\binom{\rho}{\rho^2}{}_3F_2\left(\begin{matrix}\rho & \rho & \rho\\ & \epsilon & \epsilon\end{matrix}\middle|\, 1\right) - p^2\binom{\rho^2}{\rho}\binom{\rho^2}{\rho}.$$

Now, we can evaluate these hypergeometric series using Theorem 4.35 from [14]. Using this, we have

$${}_3F_2\left(\begin{matrix}\rho^2 & \rho^2 & \rho^2\\ & \epsilon & \epsilon\end{matrix}\middle|\, 1\right) = \binom{\rho^2}{\rho}\binom{\rho^2}{\rho} - \frac{1}{p}\binom{\rho}{\rho^2}$$

$${}_3F_2\left(\begin{matrix}\rho & \rho & \rho\\ & \epsilon & \epsilon\end{matrix}\middle|\, 1\right) = \binom{\rho}{\rho^2}\binom{\rho}{\rho^2} - \frac{1}{p}\binom{\rho^2}{\rho}.$$

So

$$\begin{aligned} b(p) =& -p^3\binom{\rho^2}{\rho}^3 + p^2\binom{\rho^2}{\rho}\binom{\rho}{\rho^2} + p^2\binom{\rho}{\rho^2}\binom{\rho}{\rho^2}\\ & -p^3\binom{\rho}{\rho^2}^3 + p^2\binom{\rho}{\rho^2}\binom{\rho^2}{\rho} + p^2\binom{\rho^2}{\rho}\binom{\rho^2}{\rho} - c^2\\ =& -p^3\left(\binom{\rho}{\rho^2}^3 + \binom{\rho^2}{\rho}^3\right) + p^2\left(\binom{\rho}{\rho^2} + \binom{\rho^2}{\rho}\right)^2 - c^2. \end{aligned}$$

Finally, recall that c is the trace of Frobenius of the curve $E : y^2 + y = x^3$ over $\mathbb{F}_p$, which we computed in Lemma 3.2.4 and is given by

$$c = -p\binom{\rho}{\rho^2} - p\binom{\rho^2}{\rho}. \tag{4.6.5}$$

Using this in the equation above, we have that

$$b(p) = -p^3\left(\binom{\rho}{\rho^2}^3 + \binom{\rho^2}{\rho}^3\right).$$

For the second equality in Corollary 4.2.7, let $\alpha = -p\binom{\rho^2}{\rho}$. Then by equation

(4.6.5), $t_p(E) = \alpha + \overline{\alpha}$ and $\alpha\overline{\alpha} = p$. It follows then that $t_{p^3}(E) = \alpha^3 + \overline{\alpha}^3 = b(p)$. Theorem 3.2.2 now implies that

$$b(p) = t_{p^3}(E) = -p^3 {}_2F_1 \left(\begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \middle| \, 9 \cdot 8^{-1} \right)_{p^3} .$$

□

4.6.2 A modular threefold

Now let V be the threefold defined by the equation

$$x^3 = y_1 y_2 y_3 (y_1 + 1)(y_2 + 1)(y_3 + 1),$$

and let $N(V, p)$ denote the number of projective $\mathbb{F}_p$-points on V. Then we will show that V is "modular" in the sense that the number of points on V can be expressed in terms of the Fourier coefficients of a modular form. In particular, the function $\eta(3z)^8 = \sum b(n) q^n$ discussed in Section 4.6.1 has Fourier coefficients given by the expression

$$b(p) = p^3 + 3p^2 + 1 - N(V, p). \tag{4.6.6}$$

We consider first the case where $p \equiv 1 \pmod 3$. Define the set W to be

$$W = \{(y_1, y_2, y_3, x) \in \mathbb{F}_p^4 : y_1 y_2 y_3 (1 + y_1)(1 + y_2)(1 + y_3) = x^3\}.$$

Then,

$$\begin{aligned} \#W &= \sum_{\substack{y_1, y_2, y_3 \\ \in \mathbb{F}_p}} (1 + \rho(y_1 y_2 y_3 (1 - y_1)(1 - y_2)(1 - y_3)) + \rho^2(y_1 y_2 y_3 (y_1 - 1)(y_2 - 1)(y_3 - 1))) \\ &= p^3 + \sum_{y_1} \rho(y_1)\rho(1 - y_1) \sum_{y_2} \rho(y_2)\rho(1 - y_2) \sum_{y_3} \rho(y_3)\rho(1 - y_3) \\ &\quad + \sum_{y_1} \rho^2(y_1)\rho^2(1 - y_1) \sum_{y_2} \rho^2(y_2)\rho^2(1 - y_2) \sum_{y_3} \rho(y_3)\rho(1 - y_3) \\ &= p^3 + p^3 \binom{\rho}{\rho^2}^3 + p^3 \binom{\rho^2}{\rho} \end{aligned} \tag{4.6.7}$$

Now we compute the value $N(V, p)$, the number of projective points on V, in terms of $\#W$. Begin by homogenizing the equation:

$$y_1 y_2 y_3 (y_1 + z)(y_2 + z)(y_3 + z) = x^3 z^3.$$

The points corresponding to $z = 0$ are on the curve

$$y_1^2 y_2^2 y_3^2 = 0.$$

First we count the points where $x \neq 0$, (so fix $x = 1$). At least one y_i must be zero and the other two can be anything. There are exactly $3(p-1)^2 + 3(p-1) + 1$ possible choices for y_1, y_2, y_3.

Now, we count the points corresponding to $x = 0$. We choose one of the y_i to be zero (three choices) and there are $(p-1)^2/(p-1)$ values for the other y_i's. There are another 3 points corresponding to when exactly two of the y_i are 0. So the number of projective points is

$$N(V,p) = \#W + 3(p-1)^2 + 3(p-1) + 1 + 3(p-1) + 3 = \#W + 1 + 3p^2.$$

Finally, combining the above with equation (4.6.7) it follows that, when $p \equiv 1 \pmod 3$,

$$b(p) = p^3 - \#W = p^3 + 3p^2 + 1 - N(V,p).$$

If however, $p \equiv 2 \pmod 3$, then every element of $\mathbb{F}_p$ is a cube, and so for any choice of y_1, y_2, y_3 there is a unique x satisfying equation (4.2.8). There are p^3 such choices for the $y_i's$, so $\#W = p^3$. Since $b(p) = 0$ for all $p \equiv 2 \pmod 3$, it follows that

$$b(p) = 0 = p^3 - \#W = p^3 + 3p^2 + 1 - N(V,p).$$

It would be interesting to learn more about this variety V, or to use Corollary 4.2.7 to describe the point counts on other more well understood varieties, such as those in [29].

Chapter 5

Relation to Classical Hypergeometric Functions

5.1 Preliminaries

We have seen in the previous chapters how Gaussian hypergeometric series naturally arise when counting the number of points on varieties and computing the Fourier coefficients of cusp forms. In this chapter, we will discuss explicit relationships between Gaussian hypergeometric series, classical hypergeometric series, and truncated hypergeometric series. We will present some known supercongruence results of Mortenson [32, 33] relating special values of these objects to each other, and discuss further conjectural relationships given by Rodriguez-Villegas [36]. Finally, we discuss some promising methods for potentially solving these conjectures.

Define the *hypergeometric series truncated at* m to be

$$ {}_{n+1}F_n\left(\begin{matrix} a_0 & a_1 & \dots & a_n \\ & b_1 & \dots & b_n \end{matrix}\,\middle|\, x\right)_{\mathrm{tr}(m)} := \sum_{k=0}^{m-1} \frac{(a_0)_k \dots (a_n)_k}{(b_1)_k \dots (b_n)_k k!} x^k. \qquad (5.1.1)$$

We begin by proving a congruence relation between Gaussian hypergeometric series and truncated hypergeometric series modulo a prime p. This proposition follows as an easy consequence of a classical result relating Jacobi sums to binomial coefficients modulo p. Despite this, we write out the details, since such a congruence provides an explicit link between Gaussian hypergeometric functions and truncated hypergeometric functions evaluated at arbitrary points. The relationship is given by the following:

Proposition 5.1.2. *Let* $\omega = \omega_{\mathfrak{P}}$ *be the generator of* $\widehat{\mathbb{F}_q^\times}$ *defined below. Let* m *and* d

be integers such that $1 \leq m < d$ *and* $d|q-1$. *Then for any* $x \in \mathbb{Z}$,

$$-q \cdot {}_2F_1\left(\begin{matrix}\omega^{\frac{m(q-1)}{d}} & \omega^{\frac{(d-m)(q-1)}{d}} \\ & \epsilon\end{matrix}\;\middle|\; x\right)_q \equiv {}_2F_1\left(\begin{matrix}\frac{m}{d} & \frac{d-m}{d} \\ & 1\end{matrix}\;\middle|\; x\right)_{\mathrm{tr}(q)} \pmod{p}.$$

This congruence is a result of the following two lemmas. To state the first one, we need a bit of notation.

Let p be a prime, and let $q = p^f$ be some power of p. Let ζ_p denote a primitive p^{th} root of unity, and similarly for ζ_{q-1}. Let $L = \mathbb{Q}(\zeta_{q-1}, \zeta_p)$, and let $\mathcal{O}_L$ denote its ring of integers. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime above p. Finally, define the character $\omega_{\mathfrak{P}}$ of $\mathcal{O}_L/\mathfrak{P} = \mathbb{F}_q$ so that $\omega_{\mathfrak{P}}(x + \mathfrak{P})$ is the power of ζ_{q-1} satisfying the congruence

$$\omega_{\mathfrak{P}}(x + \mathfrak{P}) \equiv x \pmod{\mathfrak{P}}.$$

Then the following congruence holds.

Proposition 5.1.3. *If a and b are integers such that* $1 \leq a, b \leq q-2$ *we have*

$$J(\omega^{-a}, \omega^{-b}) \equiv -\binom{a+b}{a} \equiv -\frac{(a+b)!}{a!b!} \pmod{\mathfrak{P}}.$$

See, for example, Proposition 3.6.4 in [7] for a proof of this result. We will also use the following straightforward lemma about the Pochhammer symbol.

Lemma 5.1.4. *Let* $d|q-1$, $0 < m < d$. *Then*

$$\left(\frac{d-m}{d}\right)_k \equiv \frac{\left(\frac{m(q-1)}{d} + k\right)!}{\left(\frac{m(q-1)}{d}\right)!} \pmod{q}.$$

Proof.

$$\begin{aligned}
\left(\frac{d-m}{d}\right)_k &= \left(\frac{d-m}{d}\right)\left(\frac{d-m}{d}+1\right)\cdot\ldots\cdot\left(\frac{d-m}{d}+k-1\right)\cdot\frac{(q-1)^k}{(q-1)^k}\\
&= \left(\frac{(d-m)(q-1)}{d}\right)\left(\frac{(d-m)(q-1)}{d}+(q-1)\right)\cdot\ldots\\
&\quad\cdot\left(\frac{(d-m)(q-1)}{d}+(q-1)(k-1)\right)\cdot\frac{1}{(q-1)^k}\cdot\frac{(-1)^k}{(-1)^k}\\
&= \left(\frac{(m-d)(q-1)}{d}\right)\left(\frac{(m-d)(q-1)}{d}-(q-1)\right)\cdot\ldots\\
&\quad\cdot\left(\frac{(m-d)(q-1)}{d}-(q-1)(k-1)\right)\cdot\frac{(-1)^k}{(q-1)^k}\\
&= \left(\frac{m(q-1)}{d}-(q-1)\right)\left(\frac{m(q-1)}{d}-2(q-1)\right)\cdot\ldots\cdot\left(\frac{m(q-1)}{d}-(q-1)k\right)\cdot\frac{(-1)^k}{(q-1)^k}\\
&\equiv \left(\frac{m(q-1)}{d}+1\right)\left(\frac{m(q-1)}{d}+2\right)\cdot\ldots\cdot\left(\frac{m(q-1)}{d}+k\right) \pmod q\\
&\equiv \frac{\left(\frac{m(q-1)}{d}+k\right)!}{\left(\frac{m(q-1)}{d}\right)!} \pmod q
\end{aligned}$$

□

In particular, it follows then from the above lemma that

$$\frac{\left(\frac{d-m}{d}\right)_k}{k!} \equiv \binom{\frac{m(q-1)}{d}+k}{k} \pmod p$$

and

$$\frac{\left(\frac{m}{d}\right)_k}{k!} \equiv \binom{\frac{(d-m)(q-1)}{d}+k}{k} \pmod p.$$

Proof of Proposition 5.1.2. By definition, we have

$$-q\cdot {}_2F_1\left(\begin{matrix}\omega^{\frac{m(q-1)}{d}} & \omega^{\frac{(d-m)(q-1)}{d}}\\ & \epsilon\end{matrix}\,\middle|\, x\right)_q = \frac{-q^2}{q-1}\sum_{\chi}\binom{\omega^{\frac{m(q-1)}{d}}\chi}{\chi}\binom{\omega^{\frac{(d-m)(q-1)}{d}}\chi}{\chi}\chi(x).$$

Now, use the relation $\binom{A}{B}=\binom{B\bar{A}}{B}B(-1)$ (equation. 2.7 in [14]) to write this as

$$\begin{aligned}
&= \frac{-q^2}{q-1}\sum_{\chi}\binom{\omega^{-\frac{m(q-1)}{d}}}{\chi}\binom{\omega^{-\frac{(d-m)(q-1)}{d}}}{\chi}\chi(x)\\
&\equiv \sum_{k=0}^{q-2} J(\omega^{-\frac{m(q-1)}{d}},\omega^{-k})J(\omega^{-\frac{(d-m)(q-1)}{d}},\omega^{-k})\omega^k(x) \pmod p.
\end{aligned}$$

We will prove the congruence by showing that the k^{th} term in the sum above is congruent to the k^{th} term in the expression for the truncated series. In particular, when $k = 0$, we have

$$J(\omega^{-\frac{m(q-1)}{d}}, \epsilon) J(\omega^{-\frac{(d-m)(q-1)}{d}}, \epsilon) \equiv 1 \pmod{p}$$

and

$$\frac{\left(\frac{m}{d}\right)_0 \left(\frac{d-m}{d}\right)_0}{0!0!} \equiv 1 \pmod{p}.$$

For the other values of k, we may apply Proposition 5.1.3, to give the congruence

$$-q \cdot {}_2F_1\left(\begin{matrix} \omega^{\frac{m(q-1)}{d}} & \omega^{\frac{(d-m)(q-1)}{d}} \\ & \epsilon \end{matrix} \middle| x \right)_q \equiv 1 + \sum_{k=1}^{q-2} \binom{\frac{m(q-1)}{d} + k}{\frac{m(q-1)}{d}} \binom{\frac{(d-m)(q-1)}{d} + k}{\frac{(d-m)(q-1)}{d}} x^k \pmod{\mathfrak{P}}$$

and then by Lemma 5.1.4 (using the fact that the $q - 1$ term in the truncated sum is $0 \pmod{p}$)

$$\equiv \sum_{k=0}^{q-2} \frac{\left(\frac{m}{d}\right)_k \left(\frac{d-m}{d}\right)_k}{k!k!} x^k \equiv {}_2F_1\left(\begin{matrix} \frac{m}{d} & \frac{d-m}{m} \\ & 1 \end{matrix} \middle| x \right)_{\text{tr}(q)} \qquad \pmod{\mathfrak{P}}.$$

Thus we have shown that

$$-q \cdot {}_2F_1\left(\begin{matrix} \omega^{\frac{m(q-1)}{d}} & \omega^{\frac{(d-m)(q-1)}{d}} \\ & \epsilon \end{matrix} \middle| x \right)_q \equiv {}_2F_1\left(\begin{matrix} \frac{m}{d} & \frac{d-m}{d} \\ & 1 \end{matrix} \middle| x \right)_{\text{tr}(q)} \qquad \pmod{\mathfrak{P}},$$

where, as we recall, $\mathfrak{P} \subset \mathcal{O}_L$ is a prime above p. When $x \in \mathbb{Z}$, the right hand side is necessarily rational. A priori, the left hand side lives in $\mathbb{Q}(\zeta_{q-1})$, but in fact is rational because the sum can be separated into conjugate pairs. Therefore, the congruence holds modulo $\mathfrak{P} \cap \mathbb{Q} = p\mathbb{Z}$. □

Although this congruence holds modulo p, it does not necessarily hold modulo larger powers of p, as the following example shows.

Example 3. Consider for instance the case where $m = 1$, $d = 3$, $p = 7$, and ρ is a character of order 3. Then if we evaluate at the point $x = 2$, we find that

$$-p \cdot {}_2F_1\left(\begin{matrix} \rho & \rho^2 \\ & \epsilon \end{matrix} \middle| 2 \right)_p = -1.$$

On the other hand,

$$ {}_2F_1\left(\begin{array}{cc|c} \frac{1}{3} & \frac{2}{3} & 2 \\ & 1 & \end{array}\right)_{\mathrm{tr}(p)} = \frac{352362349}{43046721}. $$

We have that $-1 \cdot 43046721 \equiv 352362349 \pmod{7}$ but $-1 \cdot 43046721 \not\equiv 352362349$ $\pmod{7^2}$.

5.2 Conjectures of Rodriguez-Villegas

As we saw in Example 3, congruences between special values of Gaussian and truncated hypergeometric series do not necessarily hold modulo powers of p greater than 1. However, Mortenson proved in [32, 33, 31] that under certain hypotheses, congruences modulo p^2 hold. This line of research was inspired by the conjectures of Rodriguez-Villegas in [36], which proposed supercongruence relationships between special values of certain truncated hypergeometric series and the number of $\mathbb{F}_p$-points of Calabi- Yau manifolds. We will discuss these conjectures briefly in Section 5.2.1, and present some of the related results of Mortenson.

A consequence of research toward proving these supercongruences has been proving actual equalities between the Fourier coefficients of certain modular forms and special values of Gaussian hypergeometric series. In fact, the supercongruence conjectures of Rodriguez-Villegas provide a guide for determining exact expressions for the Fourier coefficients of modular forms in terms of Gaussian hypergeometric series. In Section 5.2.2, we will list a series of conjectures for the coëfficients of modular forms of weight 4 based on translating the conjectures of Rodriguez-Villegas into the finite field setting. We will discuss how these might be used to prove the supercongruence conjectures of Rodriguez-Villegas.

5.2.1 Dimension $d < 3$

In [36], Rodriguez-Villegas conjectured 22 supercongruences between truncated hypergeometric series corresponding to fundamental periods of the Picard-Fuchs differential equation for Calabi-Yau manifolds of dimension $d \leq 3$ and expressions related to their $\mathbb{F}_p$-points. The supercongruences corresponding to $d = 1$ were proven by Mortenson in [32, 31]. For $d = 2$, one of the supercongruences was proven by Van Hamme [41] and the rest were proven (at least up to sign) by Mortenson [33]. For $d = 3$, one of the 14 supercongruences was proven by Kilbourne [22], and another by McCarthy[28]. The rest remain open, and will be discussed further in Section 5.2.2.

We begin by stating the results of Mortenson in [32, 33]. His results are of particular interest to us, because his proofs for the $d = 1, 2$ cases of Rodriguez-Villegas' conjectures follow as corollaries of more general supercongruences between truncated hypergeometric series and Gaussian hypergeometric series. They therefore illustrate a general principle that has been used to prove these as well as other supercongruence conjectures: use Gaussian hypergeometric series as an intermediate step, by describing the objects on both sides of the congruence in terms of them.

The following theorems were proven by Mortenson in [32]. His proofs use properties of the p-adic Γ-function, and so he considers characters mapping into $\mathbb{C}_p$.

Theorem 5.2.1 ([32], Theorem 1). *Let m and r be integers with $1 \leq m < r$. If $p \equiv 1 \pmod{r}$ is prime and ρ is a character of order r on $\mathbb{F}_p^{\times}$, then*

$$ {}_2F_1\left(\begin{matrix} \frac{m}{r} & \frac{r-m}{r} \\ & 1 \end{matrix} \middle| 1 \right)_{\mathrm{tr}(p)} \equiv -p \cdot {}_2F_1\left(\begin{matrix} \rho^m & \bar{\rho}^m \\ & \epsilon \end{matrix} \middle| 1 \right)_p \quad (\mathrm{mod}\ p^2). $$

Theorem 5.2.2 ([32], Theorem 2). *Let m and r be integers with $1 \leq m < r$. If $p \equiv -1 \pmod{r}$ is prime and ρ is a character of order r on $\mathbb{F}_{p^2}^{\times}$, then*

$$ {}_2F_1\left(\begin{matrix} \frac{m}{r} & \frac{r-m}{r} \\ & 1 \end{matrix} \middle| 1 \right)_{\mathrm{tr}(p)}^2 \equiv -p^2 \cdot {}_2F_1\left(\begin{matrix} \rho^m & \bar{\rho}^m \\ & \epsilon \end{matrix} \middle| 1 \right)_{p^2} \quad (\mathrm{mod}\ p^2). $$

The supercongruence conjectures of Rodriguez-Villegas for $d = 1$ then follow from Theorems 5.2.1, 5.2.2 and explicit evaluations of the Gaussian hypergeometric series above.

In [33], Mortenson proved a generalization of this for ${}_{n+1}F_n$ hypergeometric functions. A corollary of his work is the following theorem.

Theorem 5.2.3 ([33], Corollary 1). *If p is a prime, $p \equiv 1 \pmod{r_i}$, $1 \leq m_i \leq r_i$, and ρ_i is a character of order r_i on $\mathbb{F}_p$, then*

$$ {}_4F_3\left(\begin{matrix} \frac{m_1}{r_1} & 1-\frac{m_1}{r_1} & \frac{m_2}{r_2} & 1-\frac{m_2}{r_2} \\ & 1 & 1 & 1 \end{matrix} \middle| 1 \right)_{\mathrm{tr}(p)} \equiv -p^3 \cdot {}_4F_3\left(\begin{matrix} \rho_1^{m_1} & \bar{\rho}_1^{m_1} & \rho_2^{m_2} & \bar{\rho}_2^{m_2} \\ & \epsilon & \epsilon & \epsilon \end{matrix} \middle| 1 \right)_p $$
$$ -(-1)^{\frac{m_1}{r_1}(p-1)+\frac{m_2}{r_2}(p-1)} p \quad (\mathrm{mod}\ p^2). $$

We illustrate these results with a particular example.

Example 4. Let $p = 5$, $m = 1$, and $r = 3$. Also, let ρ be a character over $\mathbb{F}_{p^2}$ of order

3. Then

$$-p^2 \cdot {}_2F_1\left(\begin{matrix}\rho\ \rho^2 \\ \epsilon\end{matrix}\,\middle|\,1\right)_{p^2} = 1.$$

Computing the corresponding truncated series, we have

$${}_2F_1\left(\begin{matrix}\frac{1}{3}\ \frac{2}{3} \\ 1\end{matrix}\,\middle|\,1\right)_{\mathrm{tr}(p)} = \frac{88351}{59049} \equiv 24 \pmod{5^2},$$

and so

$${}_2F_1\left(\begin{matrix}\frac{1}{3}\ \frac{2}{3} \\ 1\end{matrix}\,\middle|\,1\right)^2_{\mathrm{tr}(p)} \equiv 1 \pmod{5^2},$$

as is consistent with Mortenson.

If we compute modulo 5^3 instead, we find that

$${}_2F_1\left(\begin{matrix}\frac{1}{3}\ \frac{2}{3} \\ 1\end{matrix}\,\middle|\,1\right)^2_{\mathrm{tr}(p)} \equiv 51 \pmod{5^3}.$$

So the congruence does not hold for higher powers of p.

5.2.2 Dimension $d = 3$

Now we discuss the conjectures of Rodriguez-Villegas corresponding to manifolds of dimension $d = 3$. The supercongruences are between truncated ${}_4F_3$ hypergeometric functions evaluated at 1 and the Fourier coefficients of modular forms of weight 4 and varying level, and are conjectured to hold modulo p^3. Of these conjectures, Kilbourne [22] proved the level 8 case and McCarthy [28] proved the level 25 case. We will prove in Section 5.2.3 the level 16 case, but only for primes $p \equiv 1 \pmod 4$.

The remarkable fact about these results is that one can prove actual equality between special values of Gaussian hypergeometric series (assuming the specified characters exist) and the Fourier coefficients of the corresponding modular form. For example, Ahlgren and Ono proved in [2] that the p^{th} Fourier coefficient of $\eta(2z)^4\eta(4z)^4 \in S_4(\Gamma_0(8))$ is equal to $-p^3 \cdot {}_4F_3\left(\begin{matrix}\phi\ \phi\ \phi\ \phi \\ \epsilon\ \epsilon\ \epsilon\end{matrix}\,\middle|\,1\right) - p$. The corresponding level 25 result follows as a corollary of McCarthy's.

It seems empirically that this phenomenon holds more generally- for each of the supercongruences of Rodriguez-Villegas we have noticed equalities between expressions in terms of the Gaussian hypergeometric functions analogous to Rodriguez-Villegas' truncated series and the Fourier coefficients of the same modular forms in his conjectures. Such equalities would be interesting in their own right, as they give exact formulas for the Fourier coefficients of modular forms. Additionally, they can be used as tools for proving additional supercongruences, as we will show in Section 5.2.3.

We summarize the known results (indicated with a † and ‡) together with our conjectures in the third column of Table 5.1. For convenience, we also list the functions from the conjectures of Rodriguez- Villegas in the second column of this table.

Level	Truncated ${}_4F_3$	Gaussian ${}_4F_3$	Magma newform
8†	${}_4F_3\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_1
9	${}_4F_3\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} & \frac{1}{3} & \frac{2}{3}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_4 & \psi_4^3 & \rho & \rho^2\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{12}}p$	f_1
16	${}_4F_3\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} & \frac{1}{2} & \frac{1}{2}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_4 & \psi_4^3 & \phi & \phi\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{4}}p$	f_1
25‡	${}_4F_3\left(\begin{matrix}\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{tr(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_5 & \psi_5^2 & \psi_5^3 & \psi_5^4\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_1
27	${}_4F_3\left(\begin{matrix}\frac{1}{3} & \frac{1}{3} & \frac{2}{3} & \frac{2}{3}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\rho & \rho & \rho^2 & \rho^2\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{3}}p$	f_2
32	${}_4F_3\left(\begin{matrix}\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{3}{4}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_4 & \psi_4 & \psi_4^3 & \psi_4^3\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_3
36	${}_4F_3\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2} & \frac{1}{2}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\phi & \phi & \rho & \rho^2\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{6}}p$	f_1
72	${}_4F_3\left(\begin{matrix}\frac{1}{6} & \frac{5}{6} & \frac{1}{2} & \frac{1}{2}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_6 & \psi_6^5 & \phi & \phi\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_2
108	${}_4F_3\left(\begin{matrix}\frac{1}{6} & \frac{2}{6} & \frac{4}{6} & \frac{5}{6}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_6 & \psi_6^5 & \rho & \rho^2\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{6}}p$	f_4
128	${}_4F_3\left(\begin{matrix}\frac{1}{8} & \frac{3}{8} & \frac{5}{8} & \frac{7}{8}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_8 & \psi_8^3 & \psi_8^5 & \psi_8^7\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_3
144	${}_4F_3\left(\begin{matrix}\frac{1}{6} & \frac{5}{6} & \frac{1}{4} & \frac{3}{4}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_6 & \psi_6^5 & \psi_4 & \psi_4^3\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-(-1)^{\frac{p-1}{12}}p$	f_5
200	${}_4F_3\left(\begin{matrix}\frac{1}{10} & \frac{3}{10} & \frac{7}{10} & \frac{9}{10}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_{10} & \psi_{10}^3 & \psi_{10}^7 & \psi_{10}^9\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_1
216	${}_4F_3\left(\begin{matrix}\frac{1}{6} & \frac{5}{6} & \frac{1}{6} & \frac{5}{6}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_6 & \psi_6^5 & \psi_6 & \psi_6^5\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_1
864	${}_4F_3\left(\begin{matrix}\frac{1}{12} & \frac{5}{12} & \frac{7}{12} & \frac{11}{12}\\ & 1 & 1 & 1\end{matrix}\middle\vert\, 1\right)_{\mathrm{tr}(p)}$	$-p^3{}_4F_3\left(\begin{matrix}\psi_{12} & \psi_{12}^5 & \psi_{12}^7 & \psi_{12}^{11}\\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle\vert\, 1\right)-p$	f_4

Table 5.1: Conjectures for cusp form coefficients: ϕ is a character of order 2, ρ is a character of order 3, and ψ_d is a character of order d.

[†] The supercongruence in the second column was proven in [22] and the equality of the third column was proven in [2].

[‡] The supercongruence of the second column and the equality in the third column were both proven in [28].

Conjecture 5.2.4. *For each level in Table 5.1 below, let p be a prime number such that the characters in the corresponding Gaussian hypergeometric series exist. Then the values of the Gaussian hypergeometric function given in the third column of Table 5.1 match the Fourier coefficients of the newform listed.*

5.2.3 Partial progress

We will now prove the level 16 case of Conjecture 5.2.4, and show how this implies the level 16 case of Rodriguez-Villegas' conjectures for $p \equiv 1 \pmod 4$. We discuss other partial progress towards proving the Gaussian hypergeometric series expressions given in Table 5.1 as well as the conjectures of Rodriguez-Villegas.

Level 16 Case

We will now prove the following.

Theorem 5.2.5. *Let $f \in S_4(\Gamma_0(16))$ be the unique newform of level 16 and weight 4, and write the Fourier expansion of f as*

$$f = \sum c_n q^n.$$

When $p \equiv 1 \pmod 4$, c_p can be written as

$$c_p = -p^3{}_4F_3\left(\begin{array}{cccc|c} \psi_4 & \psi_4^3 & \phi & \phi & \\ & \epsilon & \epsilon & \epsilon & 1 \end{array}\right) - \psi_4(-1)p.$$

By applying Corollary 4.9 in McCarthy [28], we have the conjectured supercongruence as a corollary, assuming still that $p \equiv 1 \pmod 4$.

Corollary 5.2.6. *With notation as above, and $p \equiv 1 \pmod 4$*

$$c_p \equiv {}_4F_3\left(\begin{array}{cccc|c} \frac{1}{4} & \frac{3}{4} & \frac{1}{2} & \frac{1}{2} & \\ & 1 & 1 & 1 & 1 \end{array}\right)_{\mathrm{tr}(p)} \pmod{p^3}.$$

Proof of Theorem 5.2.5. Note that f is a twist of the unique newform of level 8 and weight 4. Specifically, if we write $\eta(2z)^4\eta(4z)^4 \in S_4(\Gamma_0(8))$ as

$$\eta(2z)^4\eta(4z)^4 = \sum a_n q^n,$$

then $c_p = \phi_p(-1)a_p$ whenever $p \equiv 1 \pmod 2$, where ϕ_p is the character of order two in $\mathbb{F}_p^{\times}$.

Ahlgren and Ono have shown in [2] that

$$a_p = -p^3{}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi\\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) - p.$$

When $p \equiv 1 \pmod 4$, $\phi_p(-1) = 1$, and proving Theorem 5.2.5 therefore reduces to proving the hypergeometric transformation

$${}_4F_3\left(\begin{matrix}\phi & \phi & \psi & \psi^3\\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) + \frac{\psi(-1)}{p^2} = {}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi\\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) + \frac{1}{p^2}.$$

Begin by expanding ${}_4F_3\left(\begin{matrix}\phi & \phi & \psi & \psi^2\\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right)$ according to its definition.

$$\begin{aligned}
{}_4F_3\left(\begin{matrix}\phi & \phi & \psi & \psi^3\\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) &= {}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi\\ & \epsilon & \psi & \psi^3\end{matrix}\,\middle|\, 1\right) \text{ by Theorem 4.2 in [14]}\\
&= \frac{p}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi}{\psi\chi}\binom{\phi\chi}{\psi^3\chi}\binom{\phi\chi}{\chi}\\
&= \frac{p}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi}{\psi\chi}\binom{\phi\chi}{\psi^3\chi}\binom{\chi^2}{\chi}\bar{\chi}(4) + \frac{1}{p^2}\\
&= \frac{1}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi}{\psi\chi}\binom{\phi\chi}{\psi^3\chi}\sum_{t}\chi\left(\frac{-t^2}{4(1-t)}\right) + \frac{1}{p^2}\\
&= \frac{1}{p}\sum_{t}{}_3F_2\left(\begin{matrix}\phi & \phi & \phi\\ & \psi & \psi^3\end{matrix}\,\middle|\, \frac{-t^2}{4(1-t)}\right) + \frac{1}{p^2}\\
&= \frac{1}{p}\sum_{t}{}_3F_2\left(\begin{matrix}\phi & \phi & \phi\\ & \psi & \psi^3\end{matrix}\,\middle|\, \frac{-(1-t)^2}{4t}\right) + \frac{1}{p^2}\\
&= \frac{1}{p}\sum_{t}{}_3F_2\left(\begin{matrix}\phi & \psi & \psi^3\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, \frac{-4t}{(1-t)^2}\right)\phi(t) + \frac{1}{p^2}. &&(5.2.7)
\end{aligned}$$

The second equality here follows from the expression

$$\binom{\phi\chi}{\chi} = \binom{\chi^2}{\chi}\binom{\phi}{\epsilon}\binom{\chi}{\epsilon}^{-1}\bar{\chi}(4) = \begin{cases}\binom{\chi^2}{\chi}\bar{\chi}(4), & \chi \neq \epsilon\\ \binom{\chi^2}{\chi}\bar{\chi}(4) - \frac{p-1}{p}, & \chi = \epsilon\end{cases} \qquad (5.2.8)$$

which can be derived from applying Davenport-Hasse.

Using Theorem 3.13 in [14] (stated in Chapter 2, Theorem 2.1.6) we can write ${}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle| 1\right)$ inductively as

$$ {}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle| 1\right) = \frac{1}{p}\sum_t {}_3F_2\left(\begin{matrix}\phi & \phi & \phi \\ & \epsilon & \epsilon\end{matrix}\middle| t\right)\phi(t(1-t)). $$

Now, the quadratic transformation formula in Corollary 4.30 in [14] implies that

$$ \begin{aligned} {}_3F_2\left(\begin{matrix}\phi & \phi & \phi \\ & \epsilon & \epsilon\end{matrix}\middle| t\right) =& \delta(1-t)\left(\binom{\psi}{\phi}\binom{\psi}{\psi^3}+\binom{\psi^3}{\phi}\binom{\psi^3}{\psi}\right) \\ & + \frac{1}{p}\delta(1+t) + \binom{\psi}{\phi}\binom{\phi}{\psi^3}^{-1}\phi(2)\phi(1-t){}_3F_2\left(\begin{matrix}\psi & \psi^3 & \phi \\ & \epsilon & \epsilon\end{matrix}\middle| \frac{-4t}{(1-t)^2}\right), \end{aligned} $$

where we recall that $\delta(0) = 1$ and 0 otherwise. This shows that

$$ {}_4F_3\left(\begin{matrix}\phi & \phi & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix}\middle| 1\right) = \frac{1}{p}\sum_t {}_3F_2\left(\begin{matrix}\psi & \psi^3 & \phi \\ & \epsilon & \epsilon\end{matrix}\middle| \frac{-4t}{(1-t)^2}\right)\phi(t) + \frac{1}{p^2}\psi(-1), \qquad (5.2.9) $$

where we use the fact that $\psi(-1) = \phi(2)$ when $p \equiv 1 \pmod 4$. Comparing (5.2.9) and (5.2.7) we see that the identity is proven. □

Level 9

In Chapter 4, we gave numerous expressions for the traces of Hecke operators on spaces of cusp forms of level 9. When the weight $k = 4$, we even gave a simple Jacobi sum expression for the Fourier coefficients of the unique newform in $S_4(\Gamma_0(9))$. We would like to use these expressions as well as Gaussian hypergeometric transformation laws to prove the conjectured equality of Fourier coefficients given in Table 5.1. Once this equality has been established, we hope to use supercongruence results to prove Rodriguez-Villegas' conjecture in the level 9 case, at least for primes $p \equiv 1 \pmod{12}$.

The work below represents an attempt to rewrite the Gaussian hypergeometric series in the trace formula in Theorem 4.5.3 into one more similar to that in the conjectured expression. Recall again that $\eta(3z)^8 = \sum b(n)q^n \in S_4(\Gamma_0(9))$ is the unique newform in this space and that Theorem 4.5.3 implies that when $p \equiv 1$

(mod 3),

$$\begin{aligned} b(p) &= -\sum_{t=1}^{p-1} p^2 {}_2F_1\left(\begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \middle| t\right)^2 \left(1+\rho(t)+\rho^2(t)\right) - c^2 + p^2 - 3p - 1 \\ &= -\sum_{t=1}^{p-1} p^2 {}_2F_1\left(\begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \middle| t\right)^2 \left(\rho(t)+\rho^2(t)\right) - c^2, \end{aligned} \qquad (5.2.10)$$

where the second equality follows from (4.6.2) and (4.6.4). The following lemma will convert these functions into ${}_3F_2$ series.

Lemma 5.2.11. *Let $t \in \mathbb{F}_p$ satisfy $t \neq 0, 1/2, 1$. Then the following equality of Gaussian hypergeometric functions holds:*

$${}_2F_1\left(\begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \middle| t\right)^2 = {}_3F_2\left(\begin{matrix} \rho \ \rho^2 \ \phi \\ \epsilon \ \epsilon \end{matrix} \middle| 4t(1-t)\right) + \frac{1}{p}.$$

Proof. This will follow as a result of the identity in Theorem 1.7 in Evans and Greene [9] stated below.

Theorem 5.2.12 ([9], Theorem 1.7). *Let $C \neq \phi$, $A \notin \{\epsilon, C, C^2\}$, and $u^2 \notin \{0,1\}$. Then*

$$\begin{aligned} &{}_3F_2\left(\begin{matrix} A \ \bar{A}C^2 \ C\phi \\ C^2 \quad C \end{matrix} \middle| \frac{1}{1-u^2}\right) \\ &= -\frac{\phi(-1)C\phi(1-u^2)}{p} + \frac{\phi(-1)\overline{A}C^2(1-u)A(1+u)J(A,\overline{A}C^2)}{J(C\phi, C\phi)} {}_2F_1\left(\begin{matrix} \overline{C}\phi \ \ C\phi \\ C\overline{A}\phi \end{matrix} \middle| \frac{1-u}{2}\right)^2. \end{aligned}$$

We will apply the theorem above to the function

$${}_2F_1\left(\begin{matrix} \rho \ \rho^2 \\ \epsilon \end{matrix} \middle| t\right)^2.$$

Setting $(1-u)/2 = t$, we have that $u = 1-2t$ and $1/(1-u^2) = 1/(4t(1-t))$. Also, $u^2 \notin \{0,1\} \iff t \notin \{1/2, 0, 1\}$, but for all other t we may apply the theorem. Finally, set $A = \rho^2$ and $C = T^{\frac{p-1}{6}} =: \chi_6$.

Then

$$
\begin{aligned}
{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| t\right)^2 &= \left({}_3F_2\left(\begin{matrix}\rho^2 & \rho^2 & \rho^2\\ & \rho & \chi_6\end{matrix}\middle|\frac{1}{4t(1-t)}\right)+\frac{\phi(-1)\rho^2(4t(1-t))}{p}\right)\frac{\phi(-1)}{\rho^2(2t)\rho^2(2(1-t))}\\
&= \frac{\phi(-1)}{\rho^2(4t(1-t))}\cdot {}_3F_2\left(\begin{matrix}\rho^2 & \rho^2 & \rho^2\\ & \rho & \chi_6\end{matrix}\middle|\frac{1}{4t(1-t)}\right)+\frac{1}{p}.
\end{aligned}
$$

Applying the transformation in Theorem 4.2 of Greene [14] (see Chapter 2, Theorem 2.1.8 for a statement of the theorem), we have that this is equal to

$$
\begin{aligned}
&\frac{\phi(-1)\chi_6(-1)}{\rho^2(4t(1-t))}\rho^2(4t(1-t)){}_3F_2\left(\begin{matrix}\rho^2 & \rho & \phi\\ & \epsilon & \epsilon\end{matrix}\middle| 4t(1-t)\right)+\frac{1}{p}\\
&= {}_3F_2\left(\begin{matrix}\rho^2 & \rho & \phi\\ & \epsilon & \epsilon\end{matrix}\middle| 4t(1-t)\right)+\frac{1}{p}.
\end{aligned}
$$

□

By Theorem 4.9 in Greene, ${}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| 1\right) = -1/p$, and by equation 4.15 in Greene,

$$
{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| \frac{1}{2}\right) = \rho(2)\left(\binom{\rho^2}{\rho}+\binom{\rho^2\phi}{\rho}\right) = \rho(2)\binom{\rho^2}{\rho}+\rho^2(2)\binom{\rho}{\rho^2}.
$$

The second equality above follows from applying Greene equation 2.16 (an application of Davenport-Hasse) and a Jacobi sum identity ([19] p. 305) to give

$$
\binom{\phi\rho^2}{\rho} = \binom{\phi}{\rho^2}\rho(4) = \binom{\rho}{\rho^2}\rho(2). \tag{5.2.13}
$$

Therefore we find that

$$
\begin{aligned}
&p^2{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\middle| \frac{1}{2}\right)^2\\
&= p^2\left(\rho^2(2)\binom{\rho^2}{\rho}^2+\rho(2)\binom{\rho}{\rho^2}^2+2\binom{\rho^2}{\rho}\binom{\rho}{\rho^2}\right)\\
&= p^2\left(\rho^2(2)\binom{\rho^2}{\rho}^2+\rho(2)\binom{\rho}{\rho^2}^2\right)+2p.
\end{aligned}
$$

On the other hand, applying Theorem 4.38 of [14] yields the evaluation

$$\begin{aligned}
p^2{}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) &= \binom{\rho^2}{\phi}\binom{\rho^2}{\phi\rho^2} + \binom{\phi\rho^2}{\phi}\binom{\phi\rho^2}{\rho^2}\\
&= p^2\left(\binom{\rho\phi}{\rho}^2 + \binom{\rho^2\phi}{\rho^2}^2\right)\\
&= p^2\left(\binom{\rho}{\rho^2}^2\rho(2) + \binom{\rho^2}{\rho}\rho^2(2)\right)\\
&= p^2{}_2F_1\left(\begin{matrix}\rho & \rho^2\\ & \epsilon\end{matrix}\,\middle|\,\frac{1}{2}\right) - 2p.
\end{aligned}$$

This gives

$$\begin{aligned}
b(p) = &-\sum_{t=2}^{p-1}\left(p^2{}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, 4t(1-t)\right) + p\right)(\rho(t)+\rho^2(t))\\
&- p(\rho(2)+\rho^2(2)) - c^2 - 2\\
= &-\sum_{t=1}^{p-1} p^2{}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, 4t(1-t)\right)(\rho(t)+\rho^2(t))\\
&- c^2 - p(\rho(2)+\rho^2(2)) - 2 + 2p.
\end{aligned}$$

On the other hand, we can consider the expression in Table 5.1. We will use the following simple lemma to rewrite it in a manner similar to that above.

Lemma 5.2.14. *Let* $p \equiv 1 \pmod 4$ *and let* ψ *be a character in* $\widehat{\mathbb{F}_p^\times}$ *of order* 4. *Then*

$$\binom{\psi\chi}{\chi}\binom{\psi^3\chi}{\chi} = \binom{\phi\chi}{\chi}\binom{\phi\chi^2}{\chi}\bar{\chi}(4) + \frac{p-1}{p^2}\delta(\phi\chi),$$

where $\delta(\epsilon) = 1$ *and 0 otherwise.*

Proof. We begin by writing $\binom{\psi\chi}{\chi}\binom{\psi^3\chi}{\chi}$ in terms of Gauss sums and applying Davenport-

Hasse.

$$\begin{aligned}
\binom{\psi\chi}{\chi}\binom{\psi^3\chi}{\chi} =& \frac{1}{p^2}\frac{G(\psi\chi)G(\psi^3\chi)G(\bar{\chi})^2}{G(\psi)G(\psi^3)} \\
=& \frac{\psi^3(-1)}{p^3}G(\bar{\chi})^2G(\phi\chi^2)\bar{\chi}\psi^3(4)G(\phi) && \text{by Davenport-Hasse} \\
=& \frac{1}{p^2}\frac{G(\phi\chi^2)G(\bar{\chi})}{G(\phi\chi)}\frac{G(\phi\chi)G(\bar{\chi})}{G(\phi)}\bar{\chi}(4) && \text{using } G(\phi)^2 = p \\
=& \binom{\phi\chi}{\chi}\binom{\phi\chi^2}{\chi}\bar{\chi}(4) + \frac{p-1}{p^2}\delta(\phi\chi).
\end{aligned}$$

□

Using this we have

$$\begin{aligned}
p^3{}_4F_3\left(\begin{matrix}\rho & \rho^2 & \psi & \psi^3 \\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) =& \frac{p^4}{p-1}\sum_{\chi}\binom{\rho\chi}{\chi}\binom{\rho^2\chi}{\chi}\binom{\psi\chi}{\chi}\binom{\psi^3\chi}{\chi} \\
=& \frac{p^4}{p-1}\sum_{\chi}\binom{\rho\chi}{\chi}\binom{\rho^2\chi}{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi^2}{\chi}\bar{\chi}(4) \\
&+ \frac{p^4}{p-1}\binom{\rho\phi}{\phi}\binom{\rho^2\phi}{\phi}\frac{p-1}{p^2} \\
=& \frac{p^4}{p-1}\sum_{\chi}\binom{\rho\chi}{\chi}\binom{\rho^2\chi}{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi^2}{\chi}\bar{\chi}(4) + p.
\end{aligned}$$

Now, use the fact that

$$\binom{\phi\chi^2}{\chi}\bar{\chi}(4) = \binom{\phi\bar{\chi}}{\chi}\bar{\chi}(-4) = \frac{1}{p}\sum_{t}\phi(t)\bar{\chi}(4t(1-t)) \tag{5.2.15}$$

to write the hypergeometric function as

$$\begin{aligned}
p^3{}_4F_3\left(\begin{matrix}\rho & \rho^2 & \psi & \psi^3 \\ & \epsilon & \epsilon & \epsilon\end{matrix}\,\middle|\, 1\right) =& \frac{p^3}{p-1}\sum_{\chi}\binom{\rho\chi}{\chi}\binom{\rho^2\chi}{\chi}\binom{\phi\chi}{\chi}\sum_{t}\bar{\chi}(4t(1-t))\phi(t) + p \\
=& p^2\sum_{t}{}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi \\ & \epsilon & \epsilon\end{matrix}\,\middle|\, \frac{1}{4t(1-t)}\right)\phi(t) + p.
\end{aligned}$$

And so proving the level 9 conjecture would be equivalent to proving the identity

$$
\begin{aligned}
&-\sum_{t=1}^{p-1} p^2 {}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, 4t(1-t)\right)\left(\rho(t)+\rho^2(t)\right) - c^2 - p(\rho(2)+\rho^2(2)) - 2 + 2p \\
&= -\sum_{t=2}^{p-1} p^2 {}_3F_2\left(\begin{matrix}\rho & \rho^2 & \phi\\ & \epsilon & \epsilon\end{matrix}\,\middle|\, \frac{1}{4t(1-t)}\right)\phi(t) - (\psi(-1)+1)p.
\end{aligned}
$$

Appendix A

Further Trace Formula Calculations

In this appendix we use the definition of the function $c(s, f, N)$ from [15] to provide simple formulas for $c(s, f, \ell)$ and $c(s, f, \ell^2)$, where ℓ is prime. We use these formulas within the text for $\ell = 3$, but as we will see, it is possible to write similar expressions for any value of $\ell \neq 2$. All of the following calculations are straightforward but extremely tedious.

We begin by presenting the definition for $c(s, f, \ell^\nu)$ given in [15]. Let $\rho = \operatorname{ord}_\ell(f)$, and let $\Phi(X) = X^2 - sX + p$. Construct the following sets

$$\begin{aligned}\tilde{A} &:= \{x \in \mathbb{Z} : \Phi(x) \equiv 0 \pmod{\ell^{\nu+2\rho}}, 2x \equiv s \pmod{\ell^\rho}\}\\ \tilde{B} &:= \{x \in \tilde{A} : \Phi(x) \equiv 0 \pmod{\ell^{\nu+1+2\rho}}\}\end{aligned}$$

and define A and B to be systems of representative of elements mod $\ell^{\nu+\rho}$ of $\tilde{A}$, $\tilde{B}$, respectively. Then $c(s, f, \ell^\nu)$ is defined to be

$$c(s, f, \ell^\nu) := \begin{cases} |A| & \text{if } (s^2 - 4p)/f^2 \not\equiv 0 \pmod{\ell} \\ |A| + |B| & \text{if } (s^2 - 4p)/f^2 \equiv 0 \pmod{\ell}. \end{cases}$$

A.1 Computation of $c(s, f, \ell)$

Lemma A.1.1. *Write $s^2 - 4p = t^2 D$ with D a fundamental discriminant of a quadratic imaginary field. Then* $c(s, f, \ell) = \begin{cases} 1 + \left(\frac{D}{\ell}\right) & \textit{if } \operatorname{ord}_\ell(f) = \operatorname{ord}_\ell(t); \\ 2 & \textit{if } \operatorname{ord}_\ell(f) < \operatorname{ord}_\ell(t). \end{cases}$

Proof. Break this up into different cases.

Case 1: $\mathrm{ord}_\ell(f) = \mathrm{ord}_\ell(t)$

First assume that $\left(\frac{D}{\ell}\right) = 1$. We know that disc($\Phi$)=$s^2-4p$ and $\mathrm{ord}_\ell(s^2-4p) = 2\cdot\rho$, so $s^2 - 4p \equiv 0 \pmod{\ell^{2\rho}}$ but $s^2 - 4p \not\equiv 0 \pmod{\ell^{1+2\rho}}$. Since D is a square mod ℓ by assumption, we can write $D = (s^2-4p)/t^2 = y^2 + \ell k$ for some y, k. Then this implies that $s^2 - 4p = (ty)^2 + t^2\ell k \equiv (ty)^2 \pmod{\ell^{1+2\rho}}$ so the discriminant is a square mod $\ell^{1+2\rho}$. So we can factor Φ as

$$\Phi(X) = \left(X - \frac{s+\sqrt{s^2-4p}}{2}\right)\left(X - \frac{s-\sqrt{s^2-4p}}{2}\right) \pmod{\ell^{1+2\rho}}.$$

We also check that $2\cdot\frac{s\pm\sqrt{s^2-4p}}{2} \equiv s \pmod{\ell^\rho}$, so this shows that $x = \frac{s\pm\sqrt{s^2-4p}}{2}$ are two elements of A. If $x_0 \in A$ is another such element then $2x_0 \equiv s \pmod{\ell^\rho}$ so we can write $x_0 = \frac{s}{2} + x_1\ell^\rho$

$$\begin{aligned}\Phi(x_0) \equiv 0 \pmod{\ell^{1+2\rho}} &\iff \left(x_1\ell^\rho - \tfrac{\sqrt{s^2-4p}}{2}\right)\left(x_1\ell^\rho + \tfrac{\sqrt{s^2-4p}}{2}\right) \equiv 0 \pmod{\ell^{1+2\rho}}\\ &\iff \left(x_1 - \tfrac{\sqrt{s^2-4p}}{2\ell^\rho}\right)\left(x_1 + \tfrac{\sqrt{s^2-4p}}{2\ell^\rho}\right) \equiv 0 \pmod{\ell}\\ &\iff x_1 = \pm\tfrac{\sqrt{s^2-4p}}{2\ell^\rho} + x_2\ell\end{aligned}$$

for some x_2.

Then $x_0 = \frac{s}{2} \pm \left(\frac{\sqrt{s^2-4p}}{2\ell^\rho} + x_2\ell\right)\ell^\rho \implies x_0 \equiv \frac{s\pm\sqrt{s^2-4p}}{2} \pmod{\ell^{1+\rho}}$ so it is in the same equivalence class as one of the other values of x which shows that $|A| = 2$. Also, since $\mathrm{ord}_\ell(f) = \mathrm{ord}_\ell(t)$ and $D \not\equiv 0 \pmod{\ell}$ we see that $(s^2-4p)/f^2 \not\equiv 0 \pmod{\ell}$ so $c(s,f) = |A|$. So $c(s,f) = 2$. Since $1 + \left(\frac{D}{\ell}\right) = 2$ the formulas agree in this case.

Next assume that D is not a square mod ℓ. Then $s^2 - 4p$ is not a square mod $\ell^{1+2\rho}$ and so $\Phi(X)$ cannot have any solutions mod $\ell^{1+\rho}$. So $|A| = |B| = 0$ and $c(s,f) = 0$. Since $1 + \left(\frac{D}{\ell}\right) = 0$, the formulas agree.

Finally, if $D \equiv 0 \mod \ell$ then $\mathrm{ord}_\ell(s^2-4p) = 1 + 2\rho$ and $s^2 \equiv 4p \pmod{\ell^{1+2\rho}}$ and so

$$\Phi(X) = \left(X - \frac{s}{2}\right)^2 \pmod{\ell^{1+2\rho}}.$$

We require that $2x \equiv s \pmod{\ell^\rho}$ and so we get that $|A| = 1$.

Now, we compute $|B|$. The only possible element of B is $s/2$ but plugging this in shows that

$$\Phi(s/2) = -\frac{s^2}{4} + p$$

which is zero $\pmod{\ell^{2+2\rho}}$ if and only if

$$s^2 - 4p \equiv 0 \pmod{\ell^{2+2\rho}}.$$

This is not the case, since we already saw that $\mathrm{ord}_\ell(s^2 - 4p) = 2\rho + 1$.

Now since we assumed that $D \equiv 0 \pmod{\ell}$, we fall under case 2 for the known formula for $c(s, f)$ and using this we find that that $c(s, f) = 1$ in this case. Since $1 + \left(\frac{D}{\ell}\right) = 1$ now also, the formulas agree.

Case 2: $\mathrm{ord}_\ell(f) < \mathrm{ord}_\ell(t)$
Then automatically $(s^2 - 4p)/f^2 \equiv 0 \mod \ell$ so $c(s, f) = |A| + |B|$. Also, $\mathrm{ord}_\ell(f) < \mathrm{ord}_\ell(t) \implies \mathrm{ord}_\ell(s^2 - 4p) \geq 2 \cdot \mathrm{ord}_\ell(f) + 2$ so Φ still factors as

$$\Phi(X) = (x - s/2)^2 \mod \ell^{2+2\rho}$$

so $|A| = |B| = 1$, $c(s, f) = 2$, which again agrees. □

A.2 Computation of $c(s, f, \ell^2)$

The following lemma characterizes the function $c(s, f, \ell^2)$.

Lemma A.2.1. *Let $s^2 - 4p = t^2 D$ where D is a fundamental discriminant of an imaginary quadratic field and let $f|t$. Let*

$$\tau := \mathrm{ord}_\ell t,$$
$$\rho := \mathrm{ord}_\ell f.$$

Then the value of $c(s, f, \ell^2)$ is given by:
If $\tau = \rho$:

$$c(s, f, \ell^2) = \begin{cases} 2, \text{ if } \left(\frac{D}{\ell}\right) = 1; \\ 0, \text{ if } \left(\frac{D}{\ell}\right) = -1; \\ 0, \text{ if } \left(\frac{D}{\ell}\right) = 0. \end{cases}$$

If $\tau = \rho + 1$*:*

$$c(s,f,\ell^2) = \begin{cases} \ell+2, \text{ if } \left(\frac{D}{\ell}\right) = 1; \\ \ell, \quad\ \text{ if } \left(\frac{D}{\ell}\right) = -1; \\ \ell+1, \text{ if } \left(\frac{D}{\ell}\right) = 0. \end{cases}$$

If $\tau > \rho + 1$*:*

$$c(s,f,\ell^2) = \ell + 1.$$

Proof. Consider each of the above cases separately:

Case 1: $\tau = \rho$

Within each case we split further depending on the value of the Legendre symbol $\left(\frac{D}{\ell}\right)$.

(a) $\left(\frac{D}{\ell}\right) = 1$

Then in particular $\ell \nmid D$, and so $\mathrm{ord}_\ell(s^2 - 4p) = 2\rho$. Also, by considering the squares mod ℓ^2, we see that in fact $D \equiv a^2 \pmod{\ell^2}$. So $\frac{s^2-4p}{t^2} = D = a^2 + \ell^2 k$ for some k.

$$\implies s^2 - 4p = t^2 D = (ta)^2 + (\ell t)^2 k, \text{ where } \mathrm{ord}_\ell(\ell t)^2 = 2(\mathrm{ord}_\ell \ell + \mathrm{ord}_\ell t) = 2\rho + 2.$$

This shows that $s^2 - 4p$ is a square mod $\ell^{2+2\rho}$ so $\Phi(X)$ factors as

$$\Phi(X) = \left(X - \frac{s + \sqrt{s^2-4p}}{2}\right)\left(X - \frac{s - \sqrt{s^2-4p}}{2}\right) \pmod{\ell^{2+2\rho}}.$$

Also, $2 \cdot \frac{s \pm \sqrt{s^2-4p}}{2} = s \pm \sqrt{s^2-4p} \equiv s \pmod{\ell^\rho}$.

This shows that $\frac{s\pm\sqrt{s^2-4p}}{2}$ (taking the square root mod $\ell^{2+2\rho}$) are in $\tilde{A}$. Also, they are distinct coset representative in A because otherwise then $\frac{s+\sqrt{s^2-4p}}{2} \equiv \frac{s-\sqrt{s^2-4p}}{2} \pmod{\ell^{2+\rho}} \implies \sqrt{s^2-4p} \equiv 0 \pmod{\ell^{2+\rho}}$ which contradicts the fact that $\mathrm{ord}_\ell(s^2 - 4p) = 2\rho$.

Finally, we show that there are no other possible elements of A. If there were an additional element x_0, then by definition $2x_0 \equiv s \pmod{\ell^\rho}$, so we write $x_0 = \frac{s}{2} + x_1\ell^\rho$.

Then

$$\begin{aligned}
&\Phi(x_0) \equiv 0 \pmod{\ell^{2+2\rho}} \\
\iff &\left(\frac{s}{2} + x_1\ell^\rho - \frac{s+\sqrt{s^2-4p}}{2}\right)\left(\frac{s}{2} + x_1\ell^\rho - \frac{s-\sqrt{s^2-4p}}{2}\right) \equiv 0 \pmod{\ell^{2+2\rho}} \\
\iff &\left(x_1\ell^\rho - \frac{\sqrt{s^2-4p}}{2}\right)\left(x_1\ell^\rho + \frac{\sqrt{s^2-4p}}{2}\right) \equiv 0 \pmod{\ell^{2+2\rho}} \\
\iff &\left(x_1 - \frac{\sqrt{s^2-4p}}{2\cdot\ell^\rho}\right)\left(x_1 + \frac{\sqrt{s^2-4p}}{2\cdot\ell^\rho}\right) \equiv 0 \pmod{\ell^2}.
\end{aligned}$$

So $x_1 \equiv \pm\frac{\sqrt{s^2-4p}}{2\cdot\ell^\rho} \pmod{\ell^2}$, and $x_0 = \frac{s}{2} \pm \frac{\sqrt{s^2-4p}}{2} + \ell^{\rho+2}k$, so its one of the representatives already listed. This shows that $c(s, f, \ell^2) = 2$ as claimed.

(b) $\left(\frac{D}{\ell}\right) = -1$ or $\left(\frac{D}{\ell}\right) = 0$
In either case, D will not be a square mod ℓ^2 and so there will be no solutions.

Case 2: $\tau = \rho + 1$
We first compute the elements of A in all three cases. If $\tau = \rho + 1$, then $s^2 - 4p \equiv 0 \pmod{\ell^{2\rho+2}}$, and $\Phi(X)$ factors as $\Phi(X) = \left(X - \frac{s}{2}\right)^2 \pmod{\ell^{2\rho+2}}$. Therefore $\frac{s}{2}$ is one element of A.

Let x_0 be another element of A. Then as before, $x_0 = \frac{s}{2} + x_1\ell^\rho$, and

$$\Phi(x_0) \equiv 0 = (\ell^\rho x_1)^2 \pmod{\ell^{2\rho+2}} \implies \ell | x_1.$$

This shows that x_0 is of the form $x_0 = \frac{s}{2} + x_2\ell^{\rho+1}$. Checking we see that any residue mod ℓ will work as a value of x_2, and that these are the only unique such values. This gives ℓ solutions in total, so $|A| = \ell$. It is left to compute the elements of B, since in this case $c(s, f, \ell^2) = |A| + |B|$.

(a) $\left(\frac{D}{\ell}\right) = 1$
Since D is a square mod ℓ, we know that $s^2 - 4p \equiv a^2 \pmod{\ell^{2\rho+3}}$, so $\Phi(X)$ factors and has two distinct solutions.

These two are distinct from each other as before. Also, there are no other solutions, since any possible solution would be of the form (from above) $\frac{s}{2} + x_2\ell^{\rho+1}$, where x_2 was taken mod ℓ. Also, write $\frac{\sqrt{s^2-4p}}{2} = \ell^{\rho+1}k$. Then if this element was a root, we would have

$$0 \equiv \left(\frac{s}{2} + \ell^{\rho+1}x_2 - \frac{s+\sqrt{s^2-4p}}{2}\right)\left(\frac{s}{2} + \ell^{\rho+1}x_2 - \frac{s-\sqrt{s^2-4p}}{2}\right) \pmod{\ell^{2\rho+2}}$$

$$\implies 0 \equiv (x_2 - k)(x_2 + k) \pmod{\ell}$$

and this can only hold for two of the elements.

So $|B| = 2$ and $c(s, f, \ell^2) = \ell + 2$.

(b) $(\frac{D}{\ell}) = -1$
Then D is not a square, and Φ does not factor mod $\ell^{2\rho+3}$, so $|B| = 0$ and $c(s, f, \ell^2) = \ell$.

(c) $(\frac{D}{\ell}) = 0$
Then $s^2 - 4p \equiv 0 \pmod{\ell^{2\rho+3}}$, and $\Phi(X) = (x - \frac{s}{2})^2 \pmod{\ell^{2\rho+3}}$.

There is only one solution, because $0 \equiv (\frac{s}{2} + x_2\ell^{\rho+1} - \frac{s}{2})^2 \equiv x_2^2\ell^{2\rho+2} \pmod{\ell^{2\rho+3}}$ this implies that $\ell | x_2$ which holds for only one value. So $|B| = 1$ and $c(s, f, \ell^2) = \ell + 1$.

Case 3: $\tau > \rho + 1$
Arguing as in the previous section shows that $|A| = \ell$ and $|B| = 1$ in all cases so $c(s, f, \ell^2) = \ell + 1$.

□

With this characterization of $c(s, f, \ell^2)$, we may prove the following generalization of Lemma 4.5.2, which describes the case where $\ell = 3$.

Lemma A.2.2. *Let $\ell \neq 2$ be a prime number, let s, p, t be integers satisfying $s^2 - 4p = t^2D$, where D is the fundamental discriminant of an imaginary quadratic field. Then, when $\ell | s^2 - 4p$,*

$$\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s, f, \ell^2) = (\ell^2 + \ell)H^*\left(\frac{s^2-4p}{\ell^2}\right).$$

Proof. The proof follows as that for Lemma 4.5.2.

$$\begin{aligned}
&\sum_{\substack{f|(t/\ell)\\ f\nmid(t/\ell^2)}} h^*\left(\frac{s^2-4p}{f^2}\right)\left\{\begin{array}{l} \ell+2 \text{ if } \left(\frac{D}{\ell}\right)=1\\ \ell+1 \text{ if } \left(\frac{D}{\ell}\right)=0\\ \ell \quad\;\; \text{if } \left(\frac{D}{\ell}\right)=-1 \end{array}\right\}\\
&= \sum_{\substack{f|(t/\ell)\\ f\nmid(t/\ell^2)}} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right)\left\{\begin{array}{c} \ell+2\\ \ell+1\\ \ell \end{array}\right\}\cdot\left\{\begin{array}{c} \ell-1\\ \ell\\ \ell+1 \end{array}\right\}\\
&= (\ell^2+\ell)\sum_{\substack{f|(t/\ell)\\ f\nmid(t/\ell^2)}} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right) - \sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right)c(s,f,\ell).
\end{aligned}$$

Also, again applying 4.3.8

$$(\ell+1)\sum_{f|(t/\ell^2)} h^*\left(\frac{s^2-4p}{f^2}\right) = (\ell^2+\ell)\sum_{f|(t/\ell^2)} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right).$$

Combining this, we have

$$\begin{aligned}
\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right)c(s,f,\ell^2) &= \sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right)c(s,f,\ell^2) + (\ell^2+\ell)\sum_{\substack{f|(t/\ell)\\ f\nmid(t/\ell^2)}} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right)\\
&\quad - \sum_{\substack{f|t\\ f\nmid(t/\ell)}} h^*\left(\frac{s^2-4p}{f^2}\right)c(s,f,\ell) + (\ell^2+\ell)\sum_{f|(t/\ell^2)} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right)\\
&= (\ell^2+\ell)\sum_{f|(t/\ell)} h^*\left(\frac{s^2-4p}{(\ell f)^2}\right).
\end{aligned}$$

□

Appendix B

Magma code

The following Magma code was used to compute the Gaussian and truncated hypergeometric functions used throughout this thesis. To the best of my knowledge, Magma and Sage do not currently have built-in functions to compute finite field hypergeometric functions or truncated hypergeometric functions, and Magma does not have functions to compute Jacobi sums or Pochhammer symbols. I include this here in order to hopefully make future computations of these functions easier for others. The code to compute the p-adic gamma function is based on the results in Cohen [7].

```
Z:=Integers();
C:=ComplexField();

//Jacobi sum of A,B over F_p p prime
function jacobi(A,B,p)
  sum:=0;
  for x in [0..p-1] do
     sum:=sum+A(x)*B(1-x);
  end for;
  return sum;
end function;

//return character "binomial coefficient", B(-1)/p* J(A,\bar{b})
function bin(A,B,p)
  j:=jacobi(A,B^(-1),p);
  return (B(-1)/p)*j;
end function;

//returns GaussianHyper2F1(A,B;C|x)_p where A=T^((p-1)*pa)=1, etc
//note this requires p prime, for prime powers use gausshyperchar below
function gausshyper(pa,pb,pc,x,p)
  G:=FullDirichletGroup(p);
  T:=Generators(G)[1];
  A:=T^(Z!((p-1)*pa));
  B:=T^(Z!((p-1)*pb));
  C:=T^(Z!((p-1)*pc));
  sum:=0;
  for i in [1..p-1] do
      chi:=T^i;
      sum:=sum+bin(A*chi,chi,p)*bin(B*chi,C*chi,p)*chi(x);
  end for;
  return (p/(p-1))*sum;
end function;

//returns GaussianHyper3F2(A,B C;D, E|x)_p where A=T^((p-1)pa)=1, etc
```

```
function gausshyper32(pa,pb,pc,pd,pe,x,p)
  G:=FullDirichletGroup(p);
  T:=Generators(G)[1];
  A:=T^(Z!((p-1)*pa));
  B:=T^(Z!((p-1)*pb));
  C:=T^(Z!((p-1)*pc));
  D:=T^(Z!((p-1)*pd));
  E:=T^(Z!((p-1)*pe));
  sum:=0;
  for i in [1..p-1] do
     chi:=T^i;
     sum:=sum+bin(A*chi,chi,p)*bin(B*chi,D*chi,p)*bin(C*chi, E*chi,p)*chi(x);
  end for;
  return (p/(p-1))*sum;
end function;

// same as gausshyper (p prime) but implementing via the character definition
// called by gausshyperchar when p is prime
function gausshypercharprime(pa, pb, pc, x, p)
  G:=FullDirichletGroup(p);
  T:=Generators(G)[1];
  A:=T^(Z!((p-1)*pa));
  B:=T^(Z!((p-1)*pb));
  C:=T^(Z!((p-1)*pc));
  if x eq 0 then
      return 0;
  else
      sum:=0;
      for y in [1..p-1] do
          sum:=sum+ B(y)*(B^(-1)*C)(1-y)*(A^(-1))(1-x*y);
      end for;
      sum:=sum*(B*C)(-1)/p;
      return sum;
  end if;
end function;

//compute (p^exp)*2F1(A, B, C|x) over F_p^exp using character def
function gausshyperchar(pa,pb,pc,x,p,exp)
 if x eq 0 then
     return 0;
 else
     if exp eq 1 then
            return p*gausshypercharprime(pa,pb,pc,Z!x,p);
     else
            F:=FiniteField(p^exp);
            zetaA:=RootOfUnity(Denominator(pa))^(Numerator(pa));
            zetaB:=RootOfUnity(Denominator(pb))^(Numerator(pb));
            zetaC:=RootOfUnity(Denominator(pc))^(Numerator(pc));
            g:=F.1;
            sum:=0;
            for y in F do
                if y ne 0 and (1-y) ne 0 and (1-x*y) ne 0 then
                        t1:=Log(g,y);
                        t2:=Log(g,1-y);
                        t3:=Log(g,1-x*y);
                        sum:=sum+zetaB^t1*zetaB^(-t2)*zetaC^(t2)*zetaA^(-t3);
                end if;
            end for;
            t:=Log(g,F!-1);
            return ((zetaB^t*zetaC^t))*sum;
     end if;
   end if;
end function;

//return the order of p mod m, just exhaustively checking
//used to compute the Gauss sum below
function order(p,m)
   for i in [1..m] do
```

```
        if (p^i -1) mod m eq 0 then
            return i;
        end if;
   end for;
   return false;
end function;

//Gauss sum over F_q, q=p^f and character T^a
//use gaussfaster for large f to avoid constructing roots of unity
function gauss(a,p,f)
  q:=p^f;
  zetaq:=RootOfUnity(q-1);
  zetap:=RootOfUnity(p);
  F:=FiniteField(q);
  if f gt 1 then
        g:=F.1;
  else
    for t in [2..p-1] do
        if order(t,p) eq (p-1) then
           g:=F!t;
        end if;
    end for;
  end if;
  sum:=0;
  for y in F do
        if y ne 0 then
            log:=Log(g,y);
            sum:=sum+zetaq^(a*log)*zetap^(Z!Trace(y));
        end if;
  end for;
  return sum;
end function;

//compute the gauss sum G(w^a), where w is generator and sum is over q=p^f
//use if numbers are large, just computes e^(2pi i) etc
function gaussfaster(a,p,f)
    q:=p^f;
    pi:=Pi(C);
    zetaq:=Exp(2*pi*i/(q-1));
    zetap:=Exp(2*pi*i/p);
    F:=FiniteField(q);
    if f gt 1 then
        g:=F.1;
    else
        for t in [2..p-1] do
            if order(t,p) eq (p-1) then
                g:=F!t;
            end if;
        end for;
    end if;
    sum:=0;
    for y in F do
        if y ne 0 then
            log:=Log(g,y);
            sum:=sum+zetaq^(a*log)*zetap^(Z!Trace(y));
        end if;
    end for;
    return sum;
end function;

//return the Pochhammer symbol (a)_n
//used to computer the truncated series below
function poch(a,n)
    ps:=1;
    for i in [0..n-1] do
        ps:=ps*(a+i);
    end for;
    return ps;
```

```
end function;

//returns 2F1(a,b;c|z) truncated at trunc
function trunchyper(a,b,c,z,trunc)
    if c eq 0 then
        print "error div by 0";
        return 0;
    else
        sum:=0;
        for i in [0..trunc-1] do
            sum:=sum+((poch(a,i)*poch(b,i))/(Factorial(i)*poch(c,i)))*z^i;
        end for;
    end if;
    return sum;
end function;

function computeUK(p,k)
 sum:=0;
 for j in [0..Floor(k/p)] do
     sum:=sum+(1/(p^j*Factorial(j)*Factorial(k-p*j)));
 end for;
 return sum;
end  function;

function computeTK(p,k)
 m:=Maximum(0,k-p+1);
 sum:=0;
 for j in [m..k] do
     sum:=sum+computeUK(p,j);
 end for;
 return sum;
end function;

//estimate the p-adic gamma function
function estimateGammaPX(p,x,MAX)
sum:=0;
for k in [0..MAX] do
    xprod:=1;
    for i in [1..k] do
     xprod:=xprod*(x-i);
    end for;
    sum:=sum+(-1)^(k-1)*computeTK(p,k)*xprod;
end for;
return sum;
end  function;
```

Bibliography

[1] S. Ahlgren, *The points of a certain fivefold over finite fields and the twelfth power of the eta function*, Finite Fields Appl. **8** (2002), no. 1, 18-33.

[2] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. **518** (2000), 187-212.

[3] S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Monatsh. Math. **129** (2000), no. 3, 177-190.

[4] R. Askey, *Orthogonal polynomials and special functions*, SIAM, Philadelphia, PA, 1975.

[5] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises,* J. Amer. Math. Soc. **14** (2001), 843-939.

[6] C.H. Clemens, *A scrapbook of complex curve theory*, Graduate Studies in Mathematics, vol. 55, Plenum Press, New York, 1980.

[7] H. Cohen, *Number theory I: tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007.

[8] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley and Sons, New York, 1989.

[9] R.J. Evans and J. Greene, *Clausen's theorem and hypergeometric functions over finite fields*, Finite Fields Appl. **15** (2009), 97-109.

[10] S. Frechette, K. Ono, and M. Papanikolas, *Gaussian hypergeometric functions and traces of Hecke operators*, Int. Math. Res. Not. (2004), no. 60, 3233-3262.

[11] J. Fuselier, *Hypergeometric functions over finite fields and relations to modular forms and elliptic curves*, Ph.D. thesis, Texas A&M University, 2007.

[12] J. Fuselier, *Hypergeometric functions over $\mathbb{F}_p$ and relations to elliptic curves and modular forms*, Proc. Amer. Math. Soc. **138** (2010), 109-123.

[13] I.S. Gradshteyn and I.W. Ryzhik, *Tables of integrals, series and products,* Academic Press, New York, 1994.

[14] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77-101.

[15] H. Hijikata, A.K. Pizer, and T.R. Shemanske, *The basis problem for modular forms on $\Gamma_0(N)$*, Mem. Amer. Math. Soc. **82** (1989), no. 418, vi+159.

[16] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004.

[17] J. Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. **44** (1958), 312-314.

[18] Y. Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case*, Ann. of Math. **85** (1967), no. 2, 267-295.

[19] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[20] M. Ishibashi, H. Sato, and K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math. **48** (1994), 307-321.

[21] N. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies no. 124, Princeton University Press, New Jersey, 1990.

[22] T. Kilbourne, *An extension of the Apéry number supercongruence*, Acta Arith. **123** (2006), no. 4, 335-348.

[23] M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. **25** (1995), 43-52.

[24] S. Lang, *Cyclotomic fields I and II*, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990.

[25] C. Lennon, *Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **139** (2011), 1931-1938.

[26] C. Lennon, *Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold*, http://arxiv.org/abs/1003.1157. Accepted pending revision to the Journal of Number Theory.

[27] J.I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Trans. Amer. Math. Soc. **45** (1965), 245-264.

[28] D. McCarthy, *Supercongruence conjectures of Rodriguez-Villegas,* arXiv:0907.5089v1.

[29] C. Meyer, *Modular Calabi-Yau threefolds*, Fields Institute Monographs, **22**, American Mathematical Society, Providence, 2005.

[30] J. Miret, R. Moreno, A. Rio, and M. Valls, *Computing the ℓ-power torsion of an elliptic curve over a finite field*, Math. Comp. **78** (2009), 1767-1786.

[31] E. Mortenson, *A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function*, J. Number Theory **99** (2003), 139-147.

[32] E. Mortenson, *Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs*, Trans. Amer. Math. Soc. **355** (2003), 987-1007.

[33] E. Mortenson, *Supercongruences for truncated ${}_{n+1}F_n$ hypergeometric series with applications to certain weight three newforms*, Proc. Amer. Math. Soc. **133** (2004), 321-330.

[34] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), 1205-1223.

[35] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS, **102**, Amer. Math. Soc., Providence, RI, 2004.

[36] F. Rodriguez-Villegas, *Hypergeometric families of Calabi-Yau manifolds*, Calabi Yau varieties and mirror symmetry (Toronto, ON, 2001), Amer. Math. Soc., Providence, RI, 2003, 223-231.

[37] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Theorie des Nombres de Bordeaux **7** (1995), 219-254.

[38] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory, Ser. A **46** (1987), no. 2, 183-211.

[39] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[40] J. Stienstra and F. Beukers, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, Math. Ann. **271** (1985), 269-304.

[41] L. van Hamme, *Proof of a conjecture of Beukers on Apéry numbers*, Proceedings of the conference on p-adic analysis (Houthalen, 1987), Vrije Univ. Brussel, Brussels, 1986, 189-195.

[42] A. Weil, *Jacobi sums as 'Grössencharaktere'*, Trans. Amer. Math. Soc. **73** (1952), 487-495.

[43] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497-508.