HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS AND RELATIONS TO MODULAR FORMS AND ELLIPTIC CURVES

A Dissertation

by

JENNY G. FUSELIER

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

August 2007

Major Subject: Mathematics

HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS AND RELATIONS TO MODULAR FORMS AND ELLIPTIC CURVES

A Dissertation

by

JENNY G. FUSELIER

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Matthew Papanikolas
Committee Members,	Andreas Klappenecker
	Peter Stiller
	Paula Tretkoff
Head of Department,	Albert Boggess

August 2007

Major Subject: Mathematics

ABSTRACT

Hypergeometric Functions Over Finite Fields and Relations to Modular Forms and Elliptic Curves. (August 2007)

Jenny G. Fuselier, B.S., Texas A&M University

Chair of Advisory Committee: Dr. Matthew Papanikolas

The theory of hypergeometric functions over finite fields was developed in the mid-1980s by Greene. Since that time, connections between these functions and elliptic curves and modular forms have been investigated by mathematicians such as Ahlgren, Frechette, Koike, Ono, and Papanikolas. In this dissertation, we begin by giving a survey of these results and introducing hypergeometric functions over finite fields. We then focus on a particular family of elliptic curves whose j-invariant gives an automorphism of $\mathbb{P}^1$. We present an explicit relationship between the number of points on this family over $\mathbb{F}_p$ and the values of a particular hypergeometric function over $\mathbb{F}_p$. Then, we use the same family of elliptic curves to construct a formula for the traces of Hecke operators on cusp forms in level 1, utilizing results of Hijikata and Schoof. This leads to formulas for Ramanujan's τ-function in terms of hypergeometric functions.

ACKNOWLEDGMENTS

First and foremost, thanks to my advisor, Matt Papanikolas. Thank you for your patience, foresight, and encouragement through this process, from the beginning through to finding a job and completing my dissertation. I am proud to be the first in what is sure to be a long line of your students. Thanks also to the other members of my committee: Andreas Klappenecker, Peter Stiller, and Paula Tretkoff, for the advice and support you have so willingly given me along the way.

I would like to thank the many other excellent professors I have had in the math department at Texas A&M, especially Kirby Smith, Roger Smith, Carl Maxson, Jeff Morgan, Hal Schenck, and N. Sivakumar. As I develop as a teacher, I will be remembering the way you each taught me and hoping to emulate your care, precision, and enthusiasm.

A special thanks goes to all the girlfriends I met in graduate school, who have helped me keep my sanity and have made sure I take a break to have some fun every once in awhile: Alison Marr, Kendra Kilmer, Heather Ramsey, Archana Krishnagiri, Amy Collins, Lori Jones, Melanie Ledwig, Angie Allen, Lisa Abbott, and others.

To my parents John and Joy, thank you for teaching me to not give up on something I love, even when it is difficult, and thank you for always believing this day would come. To my sister Joanna, thank you for the infectious excitement you had after I completed my first proof. To my brother Justin, thank you for always offering to edit my writing, yet never making me feel ridiculous when you find my mistakes.

And finally, I must thank my husband Eddie. Without your constant support and unending confidence in me, I truly never would have made it to this day.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION AND HISTORY

I.1. General Introduction

Number theory is a broad branch of mathematics that encompasses topics from the study of integers to number fields to solutions of Diophantine equations. In this dissertation, we focus on relationships between three classes of objects: modular forms, elliptic curves, and hypergeometric functions over finite fields.

Modular forms are most easily viewed as holomorphic functions on the complex upper half plane which act in a nice way under various collections of transformations. The study of such functions and their properties encompasses a rich theory which includes the work of classical mathematicians such as Poincaré, Hecke, and Ramanujan, and yet remains an active field of research today, in number theory and other areas of mathematics.

Elliptic curves can be described as curves of genus 1, given by a cubic equation in two variables, together with a distinguished point, the *point at infinity*. These curves enjoy the special property of a group law, and they have relevance both to classical problems such as the congruent number problem (see [9]) and to current questions in cryptography, algebraic geometry, and more. Elliptic curves and modular forms have many known connections, perhaps most famously those brought to light in the proof of Fermat's Last Theorem.

Finally, we are interested in studying *hypergeometric functions over finite fields*. Classical hypergeometric functions have been studied for centuries and enjoy many beautiful symmetries and transformation identities (see, e.g. [18]). In the 1980s,

---

The journal model is International Mathematics Research Notices.

Greene [6] introduced a finite field analogue of such functions. He showed that these new functions also satisfy many transformations, in a completely analogous way to their classical counterparts. This dissertation focuses on connections the values of these hypergeometric functions have to both modular forms and counting points on elliptic curves over finite fields.

In the remaining section of this chapter, we give a brief survey of recent results which connect these objects. In Chapter II, we introduce the necessary preliminaries, including the definition of hypergeometric functions over $\mathbb{F}_p$ in Section II.2. Chapter III considers connections that hypergeometric functions over $\mathbb{F}_p$ have to a particular family of elliptic curves. Specifically, Theorem III.1.1 gives an explicit relationship between counting the number of points on a family of elliptic curves over $\mathbb{F}_p$ and the value of a certain hypergeometric function over $\mathbb{F}_p$. Then, relationships between hypergeometric functions over $\mathbb{F}_p$ and modular forms are studied in Chapter IV. We focus in particular on deriving a formula for the traces of Hecke operators on spaces of cusp forms in level 1, given in Theorem IV.1.1. This leads to formulas for Ramanujan's τ-function in terms of hypergeometric functions. Finally, in Chapter V, we summarize our work and provide avenues for future study.

I.2. Recent History

Classical hypergeometric series have been studied by mathematicians such as Euler, Vandermonde, and Kummer. An important example of these series is defined for $a, b, c \in \mathbb{C}$ as

$$ {}_2F_1[a, b; c; z] := \sum_{n=1}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n, $$

where $(w)_n = w(w+1)(w+2)\cdots(w+n-1)$.

In 1836, Kummer showed that the above series satisfies a well known second

order differential equation. The specialization ${}_2F_1[\frac{1}{2}, \frac{1}{2}; 1; t]$ has further interesting properties, as it is closely related to elliptic curves. In fact, it is a constant multiple of an elliptic integral which represents a period of the lattice associated to the Legendre family of elliptic curves $y^2 = x(x-1)(x-t)$.

At the start of the twentieth century, investigations into connections between classical hypergeometric functions and modular forms began. More recently, Stiller, Beukers, and others discovered new relationships between the two. In [19], Stiller constructed an isomorphism between the graded algebra generated by classical Eisenstein series E_4 and E_6 and one generated by powers and multiples of hypergeometric series of the form ${}_2F_1[\frac{1}{12}, \frac{5}{12}; \frac{1}{2}; t]$. Soon afterwards, Beukers [3] gave identifications between periods of families of elliptic curves and values of particular hypergeometric series. For example, he related a period of $y^2 = x^3 - x - t$ to the values ${}_2F_1[\frac{1}{12}, \frac{5}{12}; \frac{1}{2}; \frac{27}{4}t^2]$.

Meanwhile, in the mid-1980s, Greene [6] developed the theory of hypergeometric functions over finite fields. Let p be an odd prime, and let $\widehat{\mathbb{F}_p^\times}$ denote the group of multiplicative characters χ on $\mathbb{F}_p^\times$, extended to all of $\mathbb{F}_p$ by setting $\chi(0) = 0$. If $A, B \in \widehat{\mathbb{F}_p^\times}$ and J denotes the Jacobi sum, then define $\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B})$. Greene defined *hypergeometric functions over* $\mathbb{F}_p$, for $A_0, A_1, \ldots, A_n, B_1, B_2, \ldots, B_n \in \widehat{\mathbb{F}_p^\times}$ and $x \in \mathbb{F}_p$ by

$$ {}_{n+1}F_n\left(\left.\begin{matrix} A_0, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{matrix}\right| x\right) := \frac{p}{p-1} \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x), $$

where n is a positive integer. (See Section II.2 for more details.)

Greene explored the properties of these functions and showed that they satisfy many transformations analogous to those satisfied by their classical counterparts, such as an analogue to the classical integral representation of ${}_2F_1[a, b; c; z]$ (see Theorem II.2.3). The development of Greene's hypergeometric functions over $\mathbb{F}_p$ generated

interest in finding connections they may have with modular forms and elliptic curves. In recent years, many results have been proved in this direction.

Let ϕ and ε denote the unique quadratic and trivial characters, respectively, on $\mathbb{F}_p^\times$. Further, define two families of elliptic curves over $\mathbb{F}_p$ by

$$ {}_2E_1(t) : y^2 = x(x-1)(x-t)$$
$$ {}_3E_2(t) : y^2 = (x-1)(x^2+t).$$

Then, for odd primes p and $t \in \mathbb{F}_p$, define the traces of Frobenius on the above families by

$$ {}_2A_1(p,t) = p + 1 - \#{}_2E_1(t)(\mathbb{F}_p), \quad t \neq 0, 1$$
$$ {}_3A_2(p,t) = p + 1 - \#{}_3E_2(t)(\mathbb{F}_p), \quad t \neq 0, -1.$$

These families of elliptic curves are closely related to particular hypergeometric functions over $\mathbb{F}_p$. For example, ${}_2F_1[\phi, \phi, \varepsilon; t]$ arises in the formula for Fourier coefficients of a modular form associated to ${}_2E_1(t)$ ([10, 12]). Further, Koike and Ono, respectively, gave the following explicit relationships:

Theorem I.2.1 ((a) Koike [10], (b) Ono [12]). *Let p be an odd prime. Then*

(a) $$p\,{}_2F_1\left(\begin{matrix}\phi, \phi \\ \varepsilon\end{matrix}\middle| t\right) = -\phi(-1){}_2A_1(p,t), \quad t \neq 0, 1$$

(b) $$p^2\,{}_3F_2\left(\begin{matrix}\phi, \phi, \phi \\ \varepsilon, \varepsilon\end{matrix}\middle| 1 + \tfrac{1}{t}\right) = \phi(-t)({}_3A_2(p,t)^2 - p), \quad t \neq 0, -1.$$

Soon after, Ahlgren and Ono [2] and Ahlgren [1] exhibited formulas for the traces of Hecke operators on spaces of cusp forms in levels 8 and 4. Let $S_k(\Gamma_0(N))$ denote the vector space of cusp forms of weight k on the congruence subgroup $\Gamma_0(N)$ of $\Gamma = SL_2(\mathbb{Z})$. Let $\mathrm{Tr}_k(\Gamma_0(N), p)$ denote the trace of the Hecke operator $\mathrm{T}_k(p)$ on $S_k(\Gamma_0(N))$. (See Section IV.1 for more details.) Further, define polynomials $G_k(s,p)$

by

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

Theorem I.2.2 ((a) Ahlgren and Ono [2], (b) Ahlgren [1]). *Let p be an odd prime and $k \geq 4$ be an even integer. Then*

$$(a) \quad \mathrm{Tr}_k(\Gamma_0(8), p) = -4 - \sum_{t=2}^{p-2} G_k({}_2A_1(p, t^2), p)$$

$$(b) \quad \mathrm{Tr}_k(\Gamma_0(4), p) = -3 - \sum_{t=2}^{p-1} G_k({}_2A_1(p, t), p).$$

Ahlgren and Ono's methods involved combining the Eichler-Selberg trace formula [7] with a theorem given by Schoof [16]. In the proof of Theorem IV.1.1, given in Section IV.4, we use similar techniques to exhibit a formula in the level 1 setting. Recently, Frechette, Ono, and Papanikolas expanded the techniques of Ahlgren and Ono and obtained results in the level 2 case:

Theorem I.2.3 (Frechette, Ono, and Papanikolas [5]). *Let p be an odd prime and $k \geq 4$ be even. When $p \equiv 1 \pmod 4$, write $p = a^2 + b^2$, where a, b are nonnegative integers, with a odd. Then*

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

where

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

In addition, Frechette, Ono, and Papanikolas used relationships between counting points on varieties over $\mathbb{F}_p$ and hypergeometric functions over $\mathbb{F}_p$ to obtain further results for the traces of Hecke operators on spaces of newforms in level 8. Most recently, Papanikolas [13] used the results in [5] as a starting point to obtain a new formula for Ramanujan's τ function, as well as a new congruence for $\tau(p) \pmod{11}$.

CHAPTER II

PRELIMINARIES

II.1. Preliminaries on Characters

Let p be a prime and let $\widehat{\mathbb{F}_p^\times}$ denote the group of all multiplicative characters on $\mathbb{F}_p^\times$. Recall that χ is a *multiplicative character* on $\mathbb{F}_p^\times$ if $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a group homomorphism. We extend $\chi \in \widehat{\mathbb{F}_p^\times}$ to all of $\mathbb{F}_p$ by setting $\chi(0) = 0$. Throughout, we let ε denote the trivial character and ϕ denote the quadratic character (or Legendre symbol). Also, we denote $\zeta = e^{2\pi i/p}$.

Definition II.1.1. If $A, B \in \widehat{\mathbb{F}_p^\times}$, we define their *Jacobi sum* to be

$$J(A, B) = \sum_{x \in \mathbb{F}_p} A(x)B(1 - x).$$

Definition II.1.2. For $A \in \widehat{\mathbb{F}_p^\times}$, define the *Gauss sum* by

$$G(A) = \sum_{x \in \mathbb{F}_p} A(x)\zeta^x.$$

Also notice that since $\mathbb{F}_p^\times$ is a cyclic group, so is its group of multiplicative characters, $\widehat{\mathbb{F}_p^\times}$. Therefore, we let T denote a fixed generator of this group, i.e. $\langle T \rangle = \widehat{\mathbb{F}_p^\times}$. With this in mind, we often use the notation $G_m := G(T^m)$. Now, we give a few elementary properties of characters, as well as of Gauss and Jacobi sums. For proofs of these results, see Chapter 8 of [8]. First, we state the *orthogonality relations* for multiplicative characters.

Lemma II.1.3. *Let T be a generator for $\widehat{\mathbb{F}_p^\times}$. Then*

$$(a) \quad \sum_{x \in \mathbb{F}_p} T^n(x) = \begin{cases} p - 1 & \text{if } T^n = \varepsilon \\ 0 & \text{if } T^n \neq \varepsilon \end{cases}$$

$$(b) \quad \sum_{n=0}^{p-2} T^n(x) = \begin{cases} p-1 & \text{if } x = 1 \\ 0 & \text{if } x \neq 1. \end{cases}$$

The next result calculates the values of two particular Gauss sums, $G(\varepsilon)$ and $G(\phi)$.

Lemma II.1.4. $(a) \quad G(\varepsilon) = G_0 = -1$

$$(b) \quad G(\phi) = G_{\frac{p-1}{2}} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We now define an additive character $\theta : \mathbb{F}_p \to \mathbb{C}$ by $\theta(\alpha) = \zeta^\alpha$. Notice that we can write Gauss sums in terms of θ, as we have $G(A) = \sum_{x \in \mathbb{F}_p} A(x)\theta(x)$. In addition, we can write θ in terms of Gauss sums:

Lemma II.1.5. *For all* $\alpha \in \mathbb{F}_p^\times$,

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

Proof. We calculate the right-hand side and find that

$$\begin{aligned} \frac{1}{p-1} \sum_{m=0}^{p-2} G_{-m} T^m(\alpha) &= \frac{1}{p-1} \sum_{m=0}^{p-2} \sum_{x \in \mathbb{F}_p} T^{-m}(x)\theta(x) T^m(\alpha) \\ &= \frac{1}{p-1} \sum_{x \in \mathbb{F}_p} \theta(x) \sum_{m=0}^{p-2} T^{-m}\left(\frac{x}{\alpha}\right) \\ &= \frac{1}{p-1} \sum_{x=\alpha} \theta(x) \cdot (p-1) \quad \text{(Lemma II.1.3 (b))} \\ &= \theta(\alpha), \end{aligned}$$

as desired. □

II.2. Hypergeometric Functions over $\mathbb{F}_p$

In the mid 1980s, Greene [6] developed a theory of hypergeometric functions over finite fields. Let p be an odd prime, and as above, let $\widehat{\mathbb{F}_p^\times}$ denote the group of multiplicative characters on $\mathbb{F}_p$. If A, B are characters on $\mathbb{F}_p$, then define

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B}) = \frac{B(-1)}{p} \sum_{x \in \mathbb{F}_p} A(x)\overline{B}(1-x).$$

Greene defined *hypergeometric functions over* $\mathbb{F}_p$ in the following way:

Definition II.2.1 ([6] Defn. 3.10). If n is a positive integer, $x \in \mathbb{F}_p$, and $A_0, A_1, \ldots, A_n$, $B_1, B_2, \ldots, B_n \in \widehat{\mathbb{F}_p^\times}$, then define

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

It is important to note that Greene's definition holds for more general finite fields $\mathbb{F}_q$ where $q = p^k$, but for our purposes we focus on the case $q = p$. In his 1987 paper [6], Greene gave a comprehensive introduction to these functions and the many relations they satisfy. Some follow directly from his definitions, while others are far more subtle. We need a few of his results, which we now give below. First, we give a lemma which provides a formula for the multiplicative inverse of a Gauss sum.

Lemma II.2.2 ([6] Eqn. 1.12). *If $k \in \mathbb{Z}$ and $T^k \neq \varepsilon$, then*

$$G_k G_{-k} = pT^k(-1).$$

The following result was given by Greene as the definition of the hypergeometric function when $n = 1$. It provides an alternative to Definition II.2.1, and in particular, it allows us to write the ${}_2F_1$ hypergeometric function as a character sum.

Theorem II.2.3 ([6] Defn. 3.5). *If $A, B, C \in \widehat{\mathbb{F}_p^\times}$ and $x \in \mathbb{F}_p$, then*

$$ {}_2F_1\left(\begin{matrix} A, B \\ C \end{matrix}\middle| x\right) = \varepsilon(x)\frac{BC(-1)}{p}\sum_{y=0}^{p-1} B(y)\overline{B}C(1-y)\overline{A}(1-xy). $$

In [6], Greene presented many transformation identities satisfied by the hypergeometric functions he defined. The theorem below allows for the argument $x \in \mathbb{F}_p$ to be replaced by $1 - x$.

Theorem II.2.4 ([6] Theorem 4.4). *If $A, B, C \in \widehat{\mathbb{F}_p^\times}$ and $x \in \mathbb{F}_p \backslash \{0, 1\}$, then*

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

Finally, we recall a classical relationship between Gauss and Jacobi sums, but we write it utilizing Greene's definition for the binomial coefficient.

Lemma II.2.5. *If $T^{m-n} \neq \varepsilon$, then*

$$ \binom{T^m}{T^n} = \frac{G_m G_{-n} T^n(-1)}{G_{m-n} \cdot p}. $$

II.3. The Hasse-Davenport Relation

One relation between characters that is of particular interest to us is the *Hasse-Davenport relation.* The most general version of this relation involves an arbitrary additive character, and can be found in [11]. We require only the case when θ is taken as the additive character:

Theorem II.3.1 (Hasse-Davenport Relation [11]). *Let m be a positive integer and let p be a prime so that $p \equiv 1 \pmod{m}$. Let θ be the additive character on $\mathbb{F}_p$ defined by $\theta(\alpha) = \zeta^\alpha$, where $\zeta = e^{2\pi i/p}$. For multiplicative characters $\chi, \psi \in \widehat{\mathbb{F}_p^\times}$, we have*

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

Proof. See [11], page 61. □

We now look more closely at two instances of this relation.

Corollary II.3.2. *If* $p \equiv 1 \pmod 4$ *and* $k \in \mathbb{Z}$*,*

$$G_{-k}G_{-\frac{p-1}{2}-k} = \sqrt{p}\, G_{-2k}T^k(4).$$

Proof. We take $m = 2$ in Theorem II.3.1, since it follows that p is odd. Notice that there are precisely two characters having order dividing 2: ε and ϕ. Applying the Hasse-Davenport relation in this context and taking an arbitrary multiplicative character T^{-k}, we find that

$$G(T^{-k})G(\phi T^{-k}) = -G(T^{-2k})T^{-k}(2^{-2})G(\varepsilon)G(\phi).$$

Then, since $\phi = T^{\frac{p-1}{2}} = T^{-\frac{p-1}{2}}$, we have

$$G_{-k}G_{-\frac{p-1}{2}-k} = \sqrt{p}\, G_{-2k}T^k(4),$$

by Lemma II.1.4. □

Corollary II.3.3. *If* $k \in \mathbb{Z}$ *and* p *is a prime with* $p \equiv 1 \pmod 3$ *then*

$$G_kG_{k+\frac{p-1}{3}}G_{k+\frac{2(p-1)}{3}} = p\,T^{-k}(27)T^{\frac{p-1}{3}}(-1)G_{3k}.$$

Proof. Here, we take $m = 3$ in Theorem II.3.1. Notice that there are three multiplicative characters with order dividing 3, namely ε, $T^{\frac{p-1}{3}}$, and $T^{\frac{2(p-1)}{3}}$. Applying the Hasse-Davenport relation and taking an arbitrary multiplicative character T^k, we get

$$G\big(T^k\big)G\Big(T^{k+\frac{p-1}{3}}\Big)G\Big(T^{k+\frac{2(p-1)}{3}}\Big) = -G\big(T^{3k}\big)T^k(3^{-3})G(\varepsilon)G\Big(T^{\frac{p-1}{3}}\Big)G\Big(T^{\frac{2(p-1)}{3}}\Big).$$

Then, after simplifying and applying Lemma II.1.4 we have

$$G_k G_{k+\frac{p-1}{3}} G_{k+\frac{2(p-1)}{3}} = T^{-k}(27) G_{\frac{p-1}{3}} G_{\frac{2(p-1)}{3}} G_{3k}.$$

Because $T^{\frac{p-1}{3}}$ has order 3, we see that $\left(T^{\frac{p-1}{3}}\right)^2 = T^{\frac{2(p-1)}{3}} = \left(T^{\frac{p-1}{3}}\right)^{-1}$. Thus, since $T^{\frac{p-1}{3}} \neq \varepsilon$, Lemma II.2.2 implies that $G_{\frac{p-1}{3}} G_{\frac{2(p-1)}{3}} = p\, T^{\frac{p-1}{3}}(-1)$. Therefore, we have the desired result,

$$G_k G_{k+\frac{p-1}{3}} G_{k+\frac{2(p-1)}{3}} = p\, T^{-k}(27) T^{\frac{p-1}{3}}(-1) G_{3k}.$$

□

CHAPTER III

HYPERGEOMETRIC FUNCTIONS OVER $\mathbb{F}_p$ AND ELLIPTIC CURVES

III.1. Notation and Statement of Theorem

Throughout, we consider a family of elliptic curves having j-invariant $\frac{1728}{t}$. That is, for $t \in \mathbb{F}_p$, $t \neq 0, 1$ we let

$$E_t : y^2 = 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t}. \tag{1}$$

Further, we let $a(t,p)$ denote the trace of the Frobenius endomorphism on E_t. In particular, for $t \neq 0, 1$, we have

$$a(t,p) = p + 1 - \#E_t(\mathbb{F}_p),$$

where $\#E_t(\mathbb{F}_p)$ counts the number of solutions to $y^2 \equiv 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t} \pmod{p}$, including the point at infinity.

Henceforth, we let p be a prime number with $p \equiv 1 \pmod{12}$. With this in mind, we let $\xi \in \widehat{\mathbb{F}_p^\times}$ have order 12. Recall also that ε and ϕ denote the trivial and quadratic characters, respectively. The main theorem in this chapter explicitly relates the above trace of Frobenius and the values of a hypergeometric function over $\mathbb{F}_p$.

Theorem III.1.1. *Suppose p is a prime, $p \equiv 1 \pmod{12}$ and $\xi \in \widehat{\mathbb{F}_p^\times}$ has order 12. Then, if $t \in \mathbb{F}_p \backslash \{0, 1\}$ and notation is as above, we have*

$$p\,{}_2F_1\left(\left.\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\right| t\right) = \psi(t)a(t,p),$$

where $\psi(t) = -\phi(2)\xi^{-3}(1-t)$.

Notice that the hypergeometric function in the above theorem is a finite field analogue of the classical ${}_2F_1$ considered by Stiller in [19], as mentioned in Section

I.2. The proof of Theorem III.1.1 involves two main steps. First, we derive a formula for $a(t,p)$ in terms of Gauss sums, and then we write the hypergeometric function in terms of Gauss sums. The final proof follows from comparing the two.

III.2. Proof of Theorem III.1.1

We begin by deriving a formula for the trace of Frobenius in terms of Gauss sums.

Notation. • Let $s = \frac{p-1}{12}$.

• Let $P(x,y) = y^2 - 4x^3 + \frac{27}{1-t}x + \frac{27}{1-t}$.

Recall from the previous chapter that θ is the additive character on $\mathbb{F}_p$ given by $\theta(\alpha) = \zeta^\alpha$, where $\zeta = e^{2\pi i/p}$. Note that if $(x,y) \in \mathbb{F}_p^2$, then

$$\sum_{z\in\mathbb{F}_p} \theta(zP(x,y)) = \begin{cases} p & \text{if } P(x,y) = 0 \\ 0 & \text{if } P(x,y) \neq 0. \end{cases}$$

So we have

$$\begin{aligned} p\cdot(\#E_t(\mathbb{F}_p) - 1) &= \sum_{z\in\mathbb{F}_p}\sum_{x,y\in\mathbb{F}_p} \theta(zP(x,y)) \\ &= \sum_{x,y,\in\mathbb{F}_p} 1 + \sum_{z\in\mathbb{F}_p^\times}\sum_{x,y\in\mathbb{F}_p} \theta(zP(x,y)), \end{aligned}$$

after breaking apart the $z = 0$ contribution. Then, by separating the sums according to whether x and y are 0 and applying the additivity of θ, we have

$$\begin{aligned} p\cdot(\#E_t(\mathbb{F}_p) - 1) &= p^2 + \sum_{z\in\mathbb{F}_p^\times} \theta\left(z\frac{27}{1-t}\right) + \sum_{z\in\mathbb{F}_p^\times}\sum_{y\in\mathbb{F}_p^\times} \theta(zy^2)\theta\left(z\frac{27}{1-t}\right) \\ &\quad + \sum_{z\in\mathbb{F}_p^\times}\sum_{x\in\mathbb{F}_p^\times} \theta(-4zx^3)\theta\left(zx\frac{27}{1-t}\right)\theta\left(z\frac{27}{1-t}\right) + \sum_{x,y,z\in\mathbb{F}_p^\times} \theta(zP(x,y)) \\ &:= p^2 + A + B + C + D, \end{aligned}$$

where A, B, C, and D are set to be the four sums appearing in the previous line. We now compute A, B, C, and D using Lemmas II.1.3, II.1.4 and II.1.5 repeatedly. First, by Lemma II.1.5, we have

$$\begin{aligned} A = \sum_{z\in\mathbb{F}_p^\times} \theta\left(z\frac{27}{1-t}\right) &= \frac{1}{p-1}\sum_{z\in\mathbb{F}_p^\times}\sum_{m=0}^{p-2} G_{-m}T^m\left(z\frac{27}{1-t}\right) \\ &= \frac{1}{p-1}\sum_{m=0}^{p-2} G_{-m}T^m\left(\frac{27}{1-t}\right)\sum_{z\in\mathbb{F}_p^\times} T^m(z), \end{aligned}$$

after switching the order of summation. Then by Lemma II.1.3, $\sum_{z\in\mathbb{F}_p^\times} T^m(z)$ is only nonzero when $T^m = \varepsilon$, i.e. when $m = 0$. Thus, we have

$$A = G_0T^0\left(\frac{27}{1-t}\right) = G_0 = -1,$$

by Lemma II.1.4.

Now we compute B using similar techniques. First, we apply Lemma II.1.5 twice and follow by switching the order of summation so that all z terms appear in a single sum. We see that

$$\begin{aligned} B &= \frac{1}{(p-1)^2}\sum_{z\in\mathbb{F}_p^\times}\sum_{y\in\mathbb{F}_p^\times}\sum_{j,k=0}^{p-2} G_{-j}G_{-k}T^j(zy^2)T^k\left(z\frac{27}{1-t}\right) \\ &= \frac{1}{(p-1)^2}\sum_{y\in\mathbb{F}_p^\times}\sum_{j,k=0}^{p-2} G_{-j}G_{-k}T^j(y^2)T^k\left(\frac{27}{1-t}\right)\sum_{z\in\mathbb{F}_p^\times} T^{j+k}(z). \end{aligned}$$

By Lemma II.1.3, the final sum is nonzero only when $k = -j$, and in that case, it takes the value $p-1$. Making this substitution and pulling the y summation to the right gives

$$\begin{aligned} B &= \frac{1}{p-1}\sum_{j=0}^{p-2} G_{-j}G_jT^{-j}\left(\frac{27}{1-t}\right)\sum_{y\in\mathbb{F}_p^\times} T^{2j}(y) \\ &= G_0G_0T^0\left(\frac{27}{1-t}\right) + G_{-\frac{p-1}{2}}G_{\frac{p-1}{2}}T^{-\frac{p-1}{2}}\left(\frac{27}{1-t}\right). \end{aligned}$$

The second equality follows by Lemma II.1.3, since $T^{2j} = \varepsilon$ precisely when $j = 0$ or $j = \frac{p-1}{2}$. Thus, simplifying by Lemma II.1.4 and noting that $G_{-\frac{p-1}{2}} = G_{\frac{p-1}{2}} = \sqrt{p}$ provides

$$B = 1 + p\phi\left(\frac{27}{1-t}\right) = 1 + p\phi\left(\frac{3}{1-t}\right).$$

Next we compute C, beginning with three applications of Lemma II.1.5.

$$\begin{aligned} C &= \frac{1}{(p-1)^3} \sum_{z\in\mathbb{F}_p^\times} \sum_{x\in\mathbb{F}_p^\times} \sum_{j,k,m=0}^{p-2} G_{-j}G_{-k}G_{-m}T^j(-4zx^3)T^k\left(zx\frac{27}{1-t}\right)T^m\left(z\frac{27}{1-t}\right) \\ &= \frac{1}{(p-1)^3} \sum_{x\in\mathbb{F}_p^\times} \sum_{j,k,m=0}^{p-2} G_{-j}G_{-k}G_{-m}T^j(-4x^3)T^k\left(x\frac{27}{1-t}\right)T^m\left(\frac{27}{1-t}\right) \sum_{z\in\mathbb{F}_p^\times} T^{j+k+m}(z), \end{aligned}$$

by collecting all $T(z)$ terms into a single sum. Similar to the computation of B, we note that the final sum is only nonzero when $m = -j-k$, according to Lemma II.1.3. Making this substitution and rearranging terms yet again gives

$$\begin{aligned} C &= \frac{1}{(p-1)^2} \sum_{j,k=0}^{p-2} G_{-j}G_{-k}G_{j+k}T^j(-4)T^k\left(\frac{27}{1-t}\right)T^{-j-k}\left(\frac{27}{1-t}\right) \sum_{x\in\mathbb{F}_p^\times} T^{3j+k}(x) \\ &= \frac{1}{p-1} \sum_{j=0}^{p-2} G_{-j}G_{3j}G_{-2j}T^j(-4)T^{-j}\left(\frac{27}{1-t}\right). \end{aligned}$$

The last equality follows by substituting $k = -3j$, according to Lemma II.1.3. Finally, we compute D, which requires four applications of Lemma II.1.5 in the first step. We find that

$$\begin{aligned} D = \frac{1}{(p-1)^4} \sum_{x,y,z\in\mathbb{F}_p^\times} \sum_{j,k,\ell,m=0}^{p-2} & G_{-j}G_{-k}G_{-\ell}G_{-m}T^j(zy^2)T^k(-4zx^3) \\ & \cdot T^\ell\left(zx\frac{27}{1-t}\right)T^m\left(z\frac{27}{1-t}\right) \end{aligned}$$

$$= \frac{1}{(p-1)^4} \sum_{x,y \in \mathbb{F}_p^\times} \sum_{j,k,\ell,m=0}^{p-2} G_{-j} G_{-k} G_{-\ell} G_{-m} T^j(y^2) T^k(-4x^3) T^\ell \left(x \frac{27}{1-t} \right) \cdot T^m \left(\frac{27}{1-t} \right) \sum_{z \in \mathbb{F}_p^\times} T^{j+k+\ell+m}(z),$$

after simplifying to collect all $T(z)$ terms. As we have seen, Lemma II.1.3 implies the final sum is nonzero only when $m = -j-k-\ell$. Performing this substitution, together with collecting all $T(x)$ terms gives

$$\begin{aligned} D &= \frac{1}{(p-1)^3} \sum_{y \in \mathbb{F}_p^\times} \sum_{j,k,\ell=0}^{p-2} G_{-j} G_{-k} G_{-\ell} G_{j+k+\ell} T^j(y^2) T^k(-4) T^{-j-k} \left(\frac{27}{1-t} \right) \sum_{x \in \mathbb{F}_p^\times} T^{3k+\ell}(x) \\ &= \frac{1}{(p-1)^2} \sum_{j,k=0}^{p-2} G_{-j} G_{-k} G_{3k} G_{j-2k} T^k(-4) T^{-j-k} \left(\frac{27}{1-t} \right) \sum_{y \in \mathbb{F}_p^\times} T^{2j}(y), \end{aligned}$$

by applying the substitution $\ell = -3k$, according to Lemma II.1.3, and collecting all $T(y)$ terms. Finally, we note that, as in the computation of B, $T^{2j} = \varepsilon$ when $j = 0, \frac{p-1}{2}$. Accounting for both of these cases, we arrive at

$$\begin{aligned} D &= \frac{1}{p-1} \sum_{k=0}^{p-2} G_0 G_{-k} G_{3k} G_{-2k} T^k(-4) T^{-k} \left(\frac{27}{1-t} \right) \\ &\qquad + \frac{1}{p-1} \sum_{k=0}^{p-2} G_{-\frac{p-1}{2}} G_{-k} G_{3k} G_{\frac{p-1}{2}-2k} T^k(-4) T^{-k-\frac{p-1}{2}} \left(\frac{27}{1-t} \right) \\ &= \frac{1}{p-1} \sum_{k=0}^{p-2} G_{-k} G_{3k} T^k(-4) \left[-G_{-2k} T^{-k} \left(\frac{27}{1-t} \right) + \sqrt{p}\, G_{6s-2k} T^{-k-6s} \left(\frac{27}{1-t} \right) \right] \\ &= \frac{1}{p-1} \sum_{k=0}^{p-2} G_{-k} G_{3k} T^k(-4) T^{-k} \left(\frac{27}{1-t} \right) \left[-G_{-2k} + \sqrt{p}\, G_{6s-2k} \phi \left(\frac{3}{1-t} \right) \right], \end{aligned}$$

after collecting like terms and simplifying. Therefore, combining our calculations for A, B, C, and D, we see that

$$p \cdot (\#E_t(\mathbb{F}_p) - 1) = p^2 + A + B + C + D$$

$$= p^2 + p\phi\left(\frac{3}{1-t}\right) + \frac{\sqrt{p}}{p-1}\phi\left(\frac{3}{1-t}\right)\sum_{k=0}^{p-2} G_{-k}G_{3k}G_{6s-2k}T^k(-4)T^{-k}\left(\frac{27}{1-t}\right).$$

Now we compute the trace of Frobenius $a(t,p)$. Since $a(t,p) = p + 1 - \#E_t(\mathbb{F}_p)$, we have proved:

Proposition III.2.1. *If p is a prime, $p \equiv 1 \pmod{12}$, $s = \frac{p-1}{12}$, and E_t is as in (1), then*

$$a(t,p) = -\phi\left(\frac{3}{1-t}\right) - \frac{\phi\left(\frac{3}{1-t}\right)}{\sqrt{p}(p-1)}\sum_{k=0}^{p-2} G_{-k}G_{3k}G_{6s-2k}T^k(-4)T^{-k}\left(\frac{27}{1-t}\right).$$

Now that we have a formula for the trace of Frobenius on E_t in terms of Gauss sums, we must write our specialization of the ${}_2F_1$ hypergeometric function in similar terms. Recall that $s = \frac{p-1}{12}$ and T generates the character group $\widehat{\mathbb{F}_p^\times}$. Thus, we may take the character ξ of order 12 in the statement of Theorem III.1.1 to be T^s.

The next result gives an explicit formula for ${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)$ in terms of Gauss sums. In its proof, we make use of the specific cases of the Hasse-Davenport relation that we derived in Chapter II.

Proposition III.2.2. *For $t \in \mathbb{F}_p\backslash\{0,1\}$,*

$${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) = \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)}\sum_{k=0}^{p-2} G_{6s-2k}G_{3k}\frac{1}{G_k}T^k(4)T^{-k}\left(\frac{27}{1-t}\right).$$

Proof. By Theorem II.2.4,

$$\begin{aligned}
{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) &= \xi(-1){}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \xi^6\end{matrix}\middle| 1-t\right) \\
&= T^s(-1)\frac{p}{p-1}\sum_{\chi}\binom{\xi\chi}{\chi}\binom{\xi^5\chi}{\xi^6\chi}\chi(1-t) \qquad \text{(Definition II.2.1)} \\
&= T^s(-1)\frac{p}{p-1}\sum_{k=0}^{p-2}\binom{T^{s+k}}{T^k}\binom{T^{5s+k}}{T^{6s+k}}T^k(1-t),
\end{aligned}$$

as T generates the character group. Now we rewrite the product $\binom{T^{s+k}}{T^k}\binom{T^{5s+k}}{T^{6s+k}}$ of binomial coefficients in terms of Gauss sums, by way of Lemma II.2.5. Since $T^s = \xi$ and $T^{-s} = \xi^{-1}$ are not trivial, we have

$$\begin{aligned}\binom{T^{s+k}}{T^k}\binom{T^{5s+k}}{T^{6s+k}} &= \left[\frac{G_{s+k}G_{-k}T^k(-1)}{pG_s}\right]\cdot\left[\frac{G_{5s+k}G_{-6s-k}T^{6s+k}(-1)}{pG_{-s}}\right] \\ &= \frac{1}{p^3}G_{s+k}G_{-k}G_{5s+k}G_{-6s-k}T^{5s+2k}(-1),\end{aligned}$$

since $G_sG_{-s} = pT^s(-1)$ by Lemma II.2.2. Thus,

$$\begin{aligned}{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) &= \frac{T^s(-1)}{p^2(p-1)}\sum_{k=0}^{p-2} G_{s+k}G_{-k}G_{5s+k}G_{-6s-k}T^{5s+2k}(-1)T^k(1-t) \\ &= \frac{\phi(-1)}{p^2(p-1)}\sum_{k=0}^{p-2} G_{s+k}G_{-k}G_{5s+k}G_{-6s-k}T^k(1-t),\end{aligned}$$

since $T^sT^{5s} = \phi$ and $T^{2k}(-1) = 1$ for all k.

Now we apply the Hasse-Davenport relation (Corollary II.3.2) and make a substitution for $G_{-k}G_{-6s-k}$. We obtain

$${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) = \frac{\phi(-1)}{p^{\frac{3}{2}}(p-1)}\sum_{k=0}^{p-2} G_{s+k}G_{5s+k}G_{-2k}T^k(4)T^k(1-t).$$

Next, we let $k \mapsto k+3s$ and find

$$\begin{aligned}{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) &= \frac{\phi(-1)}{p^{\frac{3}{2}}(p-1)}\sum_{k=0}^{p-2} G_{4s+k}G_{8s+k}G_{-2k-6s}T^{k+3s}(4)T^{k+3s}(1-t) \\ &= \frac{\phi(-1)T^{4s}(-1)}{\sqrt{p}(p-1)}\sum_{k=0}^{p-2} G_{6s-2k}G_{3k}\frac{1}{G_k}T^{-k}(27)T^{k+3s}(4)T^{k+3s}(1-t),\end{aligned}$$

by applying the Hasse-Davenport relation (Corollary II.3.3) to make a substitution for $G_{4s+k}G_{8s+k}$, and by noting that $G_{-2k-6s} = G_{-2k+6s}$. Then, since $p \equiv 1 \pmod{12}$

implies $\phi(-1)T^{4s}(-1) = T^{10s}(-1) = 1$, we simplify to obtain

$$ {}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) = \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)} \sum_{k=0}^{p-2} G_{6s-2k}G_{3k}\frac{1}{G_k}T^k(4)T^{-k}\left(\frac{27}{1-t}\right), $$

as desired. □

We now have the necessary tools to complete the proof of Theorem III.1.1.

Proof of Theorem III.1.1. We combine the results of Propositions III.2.1 and III.2.2 with a bit of algebra to complete the proof. We begin by taking the formula for ${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)$ given in Proposition III.2.2, splitting off the $k = 0$ term in the sum and applying Lemma II.2.2 to the $k \geq 1$ terms, to move all Gauss sums to the numerator. We also simplify by noticing that $T^{-k}(-1) = T^k(-1)$ implies $T^{-k}(-1)T^k(4) = T^k(-4)$. We see that

$$\begin{aligned} {}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) &= \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)}\left[\sqrt{p} + \frac{1}{p}\sum_{k=1}^{p-2} G_{6s-2k}G_{3k}G_{-k}T^{-k}(-1)T^k(4)T^{-k}\left(\frac{27}{1-t}\right)\right] \\ &= \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)}\left[\sqrt{p} + \frac{1}{p}\sum_{k=1}^{p-2} G_{6s-2k}G_{3k}G_{-k}T^{k}(-4)T^{-k}\left(\frac{27}{1-t}\right)\right]. \end{aligned}$$

Next, we multiply by $\dfrac{\phi(3)T^{3s}(1-t)}{\phi(3)T^{3s}(1-t)}$ and rearrange, while recalling that $\phi = \phi^{-1}$. We obtain

$$\begin{aligned} {}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) &= -\frac{T^{3s}(4)}{\phi(3)T^{3s}(1-t)}\left[-\frac{1}{p-1}\phi\left(\frac{3}{1-t}\right)\right. \\ &\qquad \left. -\frac{1}{p^{\frac{3}{2}}(p-1)}\phi\left(\frac{3}{1-t}\right)\sum_{k=1}^{p-2} G_{6s-2k}G_{3k}G_{-k}T^{k}(-4)T^{-k}\left(\frac{27}{1-t}\right)\right] \\ &= -T^{3s}(4)\phi(3)T^{-3s}(1-t)\left[-\frac{\phi\left(\frac{3}{1-t}\right)}{p}\right. \\ &\qquad \left. -\frac{\phi\left(\frac{3}{1-t}\right)}{p^{\frac{3}{2}}(p-1)}\sum_{k=0}^{p-2} G_{6s-2k}G_{3k}G_{-k}T^{k}(-4)T^{-k}\left(\frac{27}{1-t}\right)\right]. \end{aligned}$$

The last equality follows by noting that the $k = 0$ term of the final sum is $-\frac{\phi\left(\frac{3}{1-t}\right)}{p(p-1)}$ and

$$-\frac{\phi\left(\frac{3}{1-t}\right)}{p-1} + \frac{\phi\left(\frac{3}{1-t}\right)}{p(p-1)} = -\frac{\phi\left(\frac{3}{1-t}\right)}{p}.$$

Recall now that Proposition III.2.1 provides that

$$-\phi\left(\frac{3}{1-t}\right) - \frac{\phi\left(\frac{3}{1-t}\right)}{\sqrt{p}(p-1)} \sum_{k=0}^{p-2} G_{6s-2k} G_{3k} G_{-k} T^k(-4) T^{-k}\left(\frac{27}{1-t}\right) = a(t,p).$$

Thus, we have

$$p\,{}_2F_1\left(\left.\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\right| t\right) = -T^{3s}(4)\phi(3)T^{-3s}(1-t)a(t,p),$$

so the proof is complete if $T^{3s}(4)\phi(3)T^{-3s}(1-t) = \phi(2)\xi^{-3}(1-t)$. Since $T^{3s} = \xi^3$ and $T^{-3s} = \xi^{-3}$, we need only show that

$$\xi^3(4)\phi(3) = \phi(2). \tag{2}$$

By multiplicativity, $\xi^3(4) = \xi^6(2) = \phi(2)$. Further, $\phi(3) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity, since $p \equiv 1 \pmod 4$. Also, since $p \equiv 1 \pmod 3$, we have $\phi(3) = \left(\frac{1}{3}\right) = 1$. This verifies (2), and hence completes the proof. □

We have proved two other results similar to Theorem III.1.1, but which apply to different families of elliptic curves. The particular families of elliptic curves were considered by Beukers in [3], where he related the periods of these families to values of classical hypergeometric functions. Our results are analogues involving hypergeometric functions over $\mathbb{F}_p$, and the characters which appear in our ${}_2F_1$ bear a striking resemblance to the parameters Beukers used in the classical case. We now state these results without proof, as they are proved following the same general steps given in the proof of Theorem III.1.1.

Proposition III.2.3. *Suppose p is a prime with $p \equiv 1 \pmod{12}$, and let $\xi \in \widehat{\mathbb{F}_p^\times}$ have order 12. Let $E_t : y^2 = x^3 + tx + 1$, and let $a(t,p) = p + 1 - \#E_t(\mathbb{F}_p)$. Then*

$$p\,{}_2F_1\left(\begin{matrix}\xi, \xi^7 \\ \xi^8\end{matrix}\middle| -\frac{4}{27}t^3\right) = \chi(t)a(t,p),$$

where $\chi(t) = -\xi^{-1}(-4)\xi^{-4}(\frac{t^3}{27})$.

Proposition III.2.4. *Suppose p is a prime with $p \equiv 1 \pmod{12}$, and let $\xi \in \widehat{\mathbb{F}_p^\times}$ have order 12. Let $E_t : y^2 = x^3 - x - t$, and let $a(t,p) = p + 1 - \#E_t(\mathbb{F}_p)$. Then*

$$p\,{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \phi\end{matrix}\middle| \frac{27}{4}t^2\right) = -\xi^3(-27)a(t,p).$$

It is interesting to note that in Proposition III.2.3, the values of the character $\chi(t)$, which appears as the coefficient of $a(t,p)$, are simply sixth roots of unity, and in Proposition III.2.4, the values of $\xi^3(-27)$ are simply ± 1. A priori, $\xi^3(-27) \in \{\pm 1, \pm i\}$, but in fact, we have $(\xi^3(-27))^2 = (\xi^3(-1)\xi^3(27))^2 = \phi(-1)\phi(27) = \phi(-1)\phi(3) = 1$. This follows since $p \equiv 1 \pmod{12}$ implies $\phi(-1) = 1$ and since $\phi(3) = 1$, as shown in the proof of Theorem III.1.1.

CHAPTER IV

HYPERGEOMETRIC FUNCTIONS AND MODULAR FORMS

IV.1. Introduction

In the previous chapters we introduced the notion of hypergeometric functions over a finite field and highlighted some connections these functions have to elliptic curves. Now we consider relationships between hypergeometric functions and modular forms. First, we recall some basic facts and notation. We follow the treatment of Koblitz, given in Chapter 3 of [9].

Let $\Gamma = SL_2(\mathbb{Z})$ be the special linear group, consisting of all invertible 2×2 matrices having entries in $\mathbb{Z}$ and determinant 1. Let $f(z)$ be a holomorphic function on the upper half plane $\mathbb{H}$ and let $k \in \mathbb{Z}$. Suppose that we have

$$f(\gamma z) = (cz + d)^k f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \tag{3}$$

Recall that f has a Fourier expansion of the form

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n \text{ where } q = e^{2\pi i z}, \tag{4}$$

and suppose that the above expansion satisfies $a_n = 0$ for all $n < 0$ (i.e. $f(z)$ is holomorphic at infinity). Then we say $f(z)$ is a *modular form of weight k for Γ*. We let $M_k := M_k(\Gamma)$ denote the set of all such functions.

If the Fourier expansion (4) of $f(z)$ has the additional property that $a_0 = 0$, then we say $f(z)$ is a *cusp form of weight k for Γ*, and we denote the set of these functions by $S_k := S_k(\Gamma)$.

Now, for a positive integer N, let $\Gamma_0(N)$ denote the congruence subgroup of Γ

defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| c \equiv 0 \pmod{N} \right\}.$$

One may generalize the type of relation given in (3) to define modular forms and cusp forms on such congruence subgroups of Γ. These modular forms are relevant to the results in [2], [1], and [5], mentioned in Section I.2. However, our interest lies only in the level one case, that is when $N = 1$ and we have $\Gamma_0(1) = \Gamma$, so we do not require such generalizations.

Further, we define the n^{th} *Hecke operator on* M_k by

$$\mathrm{T}_k(n) : M_k \to M_k,$$

where

$$(\mathrm{T}_k(n)f)(z) = n^{k-1} \sum_{\substack{ad=n \\ 0 \le b < d}} d^{-k} f\left(\frac{az+b}{d}\right).$$

Recall also that $\mathrm{T}_k(n)$ maps S_k to itself. We let $\mathrm{Tr}_k(\Gamma, n)$ denote the trace of the n^{th} Hecke operator on the space of cusp forms of weight k for Γ.

In this chapter, for primes $p \equiv 1 \pmod{12}$, we derive a formula for $\mathrm{Tr}_k(\Gamma, p)$ in terms of the number of points on the family

$$E_t : y^2 = 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t} \tag{5}$$

of elliptic curves from Chapter III. If we let $a(t,p) = p + 1 - \#E_t(\mathbb{F}_p)$ as before, we have the following theorem, whose proof we delay until Section IV.4.

Theorem IV.1.1. *Suppose p is a prime with $p \equiv 1 \pmod{12}$. Let $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ and $a + bi \equiv 1 \, (2+2i)$ in $\mathbb{Z}[i]$. Also, let $c, d \in \mathbb{Z}$ such that $p = c^2 - cd + d^2$*

and $c + d\omega \equiv 2\,(3)$ *in* $\mathbb{Z}[\omega]$, *where* $\omega = e^{2\pi i/3}$. *Then for even* $k \geq 4$,

$$\mathrm{Tr}_k(\Gamma, p) = -1 - \lambda(k, p) - \sum_{t=2}^{p-1} G_k(a(t, p), p),$$

where

$$\lambda(k, p) = \frac{1}{2}[G_k(2a, p) + G_k(2b, p)] + \frac{1}{3}[G_k(c + d, p) + G_k(2c - d, p) + G_k(c - 2d, p)]$$

and

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

IV.2. Theorems of Hasse, Schoof, and Hijikata

The proof of Theorem IV.1.1 utilizes three important results: a classical theorem of Hasse, a theorem of Schoof, and Hijikata's version of the Eichler-Selberg trace formula. In this section, we develop the context for these results and state the versions necessary for our proof.

The first result, proved by Hasse in the 1930s, gives an upper bound for the number of points on an elliptic curve defined over a finite field.

Theorem IV.2.1 (Hasse). *Let* E *be an elliptic curve defined over* $\mathbb{F}_p$, *where* p *is prime. Then*

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}.$$

Proof. See, for example, [17] page 131. □

The results of Schoof and Hijikata require some more notation. For both, we follow the treatment given in [5]. If $d < 0$, $d \equiv 0, 1 \pmod 4$, let $\mathcal{O}(d)$ denote the unique imaginary quadratic order in $\mathbb{Q}(\sqrt{d})$ having discriminant d. Let $h(d) = h(\mathcal{O}(d))$ be the order of the class group of $\mathcal{O}(d)$, and let $w(d) = w(\mathcal{O}(d))$ be half the

cardinality of the unit group of $\mathcal{O}(d)$. We then let $h^*(d) = h(d)/w(d)$. Further, if d is the discriminant of an imaginary quadratic order $\mathcal{O}$, let

$$H(d) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{max}} h(\mathcal{O}'), \tag{6}$$

where the sum is over all orders $\mathcal{O}'$ between $\mathcal{O}$ and $\mathcal{O}_{max}$, the maximal order. A complete treatment of the theory of orders in imaginary quadratic fields can be found in section 7 of [4].

Additionally, if K is a field, we define

$$Ell_K := \{[E]_K | E \text{ is defined over } K\},$$

where $[E]_K$ denotes the isomorphism class of E over K and $[E_1]_K = [E_2]_K$ if there exists an isomorphism $\beta : E_1 \to E_2$ over K. Now if p is an odd prime, define

$$I(s,p) := \{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} | \#E(\mathbb{F}_p) = p + 1 \pm s\}. \tag{7}$$

Schoof proved the following theorem, connecting the quantities in (6) and (7).

Theorem IV.2.2 (Schoof [16], Thm. 4.6). *If p is an odd prime and s is an integer with $0 < s < 2\sqrt{p}$, then*

$$\#I(s,p) = 2H(s^2 - 4p).$$

The final key ingredient to the proof of Theorem IV.1.1 is the Eichler-Selberg trace formula, which provides a starting point for calculating the trace of the p^{th} Hecke operator on S_k. We use Hijikata's version of this formula, which is found in [7], but we only require the level 1 formulation. Let $k \geq 2$ be an even integer, and let $p \equiv 1 \pmod{12}$ be prime.

Define

$$F_k(x,y) = \frac{x^{k-1} - y^{k-1}}{x - y}.$$

Then letting $x + y = s$ and $xy = p$ gives rise to polynomials $G_k(s,p) = F_k(x,y)$. These polynomials can be written alternatively as

$$G_k(s,p) = \sum_{j=0}^{\frac{k}{2}-1} (-1)^j \binom{k-2-j}{j} p^j s^{k-2j-2}, \tag{8}$$

as in the statement of Theorem IV.1.1. Note that when writing the polynomials $G_k(s,p)$, we take the convention $s^0 = 1$, so that the constant term of $G_k(s,p)$ is $(-p)^{\frac{k}{2}-1}$, for all values of s. Using this notation, the formulation given below is a straightforward reduction of Hijikata's trace formula in the level one case.

Theorem IV.2.3 (Hijikata [7], Thm. 2.2). *Let $k \geq 2$ be an even integer, and let $p \equiv 1 \pmod{12}$ be prime. Then*

$$\mathrm{Tr}_k(\Gamma, p) = -h^*(-4p)(-p)^{\frac{k}{2}-1} - 1 - \sum_{0<s<2\sqrt{p}} G_k(s,p) \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) + \delta(k),$$

where

$$\delta(k) = \begin{cases} p+1 & \text{if } k = 2 \\ 0 & \text{otherwise} \end{cases}$$

and where we classify integers s with $s^2 - 4p < 0$ by some positive integer ℓ and square-free integer m via

$$s^2 - 4p = \begin{cases} \ell^2 m, & 0 > m \equiv 1 \pmod 4 \\ \ell^2 4m, & 0 > m \equiv 2, 3 \pmod 4. \end{cases}$$

We end this section by recalling a result which relates isomorphism classes in

$Ell_{\overline{\mathbb{F}}_p}$ and $Ell_{\mathbb{F}_p}$. Define a map

$$\eta : Ell_{\mathbb{F}_p} \to Ell_{\overline{\mathbb{F}}_p}$$
$$[E]_{\mathbb{F}_p} \mapsto [E]_{\overline{\mathbb{F}}_p}.$$

Note that η is well defined since two curves which are isomorphic over $\mathbb{F}_p$ are necessarily isomorphic over $\overline{\mathbb{F}}_p$.

Lemma IV.2.4. *Let $p \geq 5$ be prime. Suppose $[E]_{\overline{\mathbb{F}}_p} \in \mathrm{Ell}_{\overline{\mathbb{F}}_p}$ and E is defined over $\mathbb{F}_p$. Then*

$$\#\eta^{-1}([E]_{\overline{\mathbb{F}}_p}) = \begin{cases} 2 & \text{if } j \neq 0, 1728 \\ 4 & \text{if } j = 1728 \\ 6 & \text{if } j = 0. \end{cases}$$

Proof. See Section X.5 of [17]. □

IV.3. Curves with j-invariant 1728 or 0

Among isomorphism classes of elliptic curves over $\mathbb{F}_p$, two are of particular interest to us: those having j-invariant 1728 and those having j-invariant 0. We devote this section to investigating certain properties of these curves. First, we must develop some notation.

Let m be a positive integer, and let $\zeta_m = e^{2\pi i/m}$ be a primitive m^{th} root of unity. Let $\mathbb{Q}(\zeta_m)$ denote the m^{th} cyclotomic field, and recall its ring of integers is $\mathbb{Z}[\zeta_m]$. (See, for example, pages 265-268 of [14].) For a prime ideal P in $\mathbb{Z}[\zeta_m]$, define

$$N(P) := |\mathbb{Z}[\zeta_m]/P| .$$

Definition IV.3.1. Let θ be a prime in $\mathbb{Z}[\zeta_m]$ with $\theta \nmid m$. Then, for $\alpha \in \mathbb{Z}[\zeta_m]$, define the *$m^{th}$-power residue symbol* $\left(\frac{\alpha}{\theta}\right)_m$ to be 0 if $\theta|\alpha$. Otherwise, define $\left(\frac{\alpha}{\theta}\right)_m$ to

be the unique m^{th} root of unity satisfying

$$\left(\frac{\alpha}{\theta}\right)_m \equiv \alpha^{\frac{N\theta-1}{m}} \pmod{\theta},$$

where $N\theta$ denotes the norm of the prime ideal generated by θ.

We specialize this definition for our purposes. In particular, we consider only $m = 2, 3, 4, 6$, where for $m = 2$, we get the usual quadratic character. Further, we need only consider the case when $\alpha \in \mathbb{Z}$. We notice the following properties in these particular cases:

- $\left(\frac{\alpha}{\theta}\right)_3 \in \{1, \omega, \omega^2\}$, where $\omega = e^{2\pi i/3}$.
- $\left(\frac{\alpha}{\theta}\right)_4 \in \{\pm 1, \pm i\}$.
- $\left(\frac{\alpha}{\theta}\right)_6 \in \{\zeta_6^j | j = 0, \ldots 5\}$, where $\zeta_6 = e^{2\pi i/6} = e^{\pi i/3}$.
- $\left(\frac{\alpha}{\theta}\right)_6^3$ is the quadratic character.
- $\left(\frac{\alpha}{\theta}\right)_6^2 = \left(\frac{\alpha}{\theta}\right)_3$.

Now we are ready to analyze our particular classes of curves. Throughout, we let p be a prime number with $p \equiv 1 \pmod{12}$. If E is any elliptic curve defined over $\mathbb{F}_p$, we let $a(E)$ be given by $a(E) = p+1-\#E(\mathbb{F}_p)$. We first focus on isomorphism classes of elliptic curves having j-invariant 1728, and then move to those having j-invariant 0.

Theorem IV.3.2 ([8], Ch. 18). *Let p be an odd prime with $p \equiv 1 \pmod{4}$, and let D be a nonzero integer. Suppose $p \nmid D$ and consider the elliptic curve $E : y^2 = x^3 - Dx$ over $\mathbb{F}_p$. Let $p = \theta\overline{\theta}$ where $\theta \in \mathbb{Z}[i]$ and $\theta \equiv 1 \,(2+2i)$. Then*

$$a(E) = \overline{\left(\frac{D}{\theta}\right)_4}\,\theta + \left(\frac{D}{\theta}\right)_4 \overline{\theta}.$$

We now use the above theorem to compute a formula for the sum of $a(E)^n$ over all curves E over $\mathbb{F}_p$ having j-invariant 1728.

Lemma IV.3.3. *Let $p \equiv 1 \pmod{12}$ and let $a, b \in \mathbb{Z}$ be such that $p = a^2 + b^2$ and $a + bi \equiv 1 \, (2 + 2i)$ in $\mathbb{Z}[i]$. Then for $n \geq 2$ even,*

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n = 2^{n+1}(a^n + b^n).$$

Proof. By Lemma IV.2.4, there are precisely four classes of elliptic curves to be included in the above sum. If $D \in \mathbb{F}_p^\times$ is not a square, we may take

$$E_0 : y^2 = x^3 - x \qquad E_2 : y^2 = x^3 - D^2x$$
$$E_1 : y^2 = x^3 - Dx \qquad E_3 : y^2 = x^3 - D^3x.$$

Notice that these curves are not isomorphic to one another over $\mathbb{F}_p$. Since $p \equiv 1 \pmod{4}$, we may apply Theorem IV.3.2 and we take $\theta = a + bi$. We use the theorem to compute $a(E_j)^n$ for each j. For E_0, we have $\left(\frac{1}{\theta}\right)_4 = 1$, and so

$$\begin{aligned} a(E_0)^n &= (\theta + \overline{\theta})^n \\ &= ((a + bi) + (a - bi))^n \\ &= (2a)^n. \end{aligned}$$

Now we apply Theorem IV.3.2 to the curve E_1 and have

$$\begin{aligned} a(E_1)^n &= \left(\overline{\left(\frac{D}{\theta}\right)}_4 \theta + \left(\frac{D}{\theta}\right)_4 \overline{\theta} \right)^n \\ &= \left(\overline{\left(\frac{D}{\theta}\right)}_4 (a + bi) + \left(\frac{D}{\theta}\right)_4 (a - bi) \right)^n. \end{aligned}$$

Since D is not a square in $\mathbb{F}_p^\times$, we have $\left(\frac{D}{\theta}\right)_4 = \pm i$, and so

$$\begin{aligned} a(E_1)^n &= \left((\mp i)(a+bi) + (\pm i)(a-bi) \right)^n \\ &= \left((\pm b \mp ai) + (\pm b \pm ai) \right)^n \\ &= (\pm 2b)^n \\ &= (2b)^n, \end{aligned}$$

since n is even. Next, for E_2 we have

$$\begin{aligned} a(E_2)^n &= \left(\overline{\left(\frac{D^2}{\theta}\right)}_4 \theta + \left(\frac{D^2}{\theta}\right)_4 \overline{\theta} \right)^n \\ &= \left(\overline{\left(\frac{D^2}{\theta}\right)}_4 (a+bi) + \left(\frac{D^2}{\theta}\right)_4 (a-bi) \right)^n. \end{aligned}$$

Notice that $\left(\frac{D^2}{\theta}\right)_4 = \left(\frac{D}{\theta}\right)_4^2 = \pm 1$, since $\left(\frac{D}{\theta}\right)_4 = \pm i$. Then we have

$$\begin{aligned} a(E_2)^n &= ((\pm 1)(a+bi) + (\pm 1)(a-bi))^n \\ &= ((\pm a \pm bi) + (\pm a \mp bi))^n \\ &= (\pm 2a)^n \\ &= (2a)^n, \end{aligned}$$

since n is even. Finally, for E_3 we have

$$\begin{aligned} a(E_3)^n &= \left(\overline{\left(\frac{D^3}{\theta}\right)}_4 \theta + \left(\frac{D^3}{\theta}\right)_4 \overline{\theta} \right)^n \\ &= (2b)^n, \end{aligned}$$

since $\left(\frac{D^3}{\theta}\right)_4 = \left(\frac{D}{\theta}\right)_4 \left(\frac{D^2}{\theta}\right)_4 = \pm i$ implies this is identical to the $a(E_1)^n$ computa-

tion. Therefore, adding these together, we have shown

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n = (2a)^n + (2b)^n + (2a)^n + (2b)^n = 2^{n+1}(a^n + b^n),$$

as desired. □

Now we look more closely at elliptic curves defined over $\mathbb{F}_p$ having j-invariant 0.

Theorem IV.3.4 ([8], Ch. 18). *Let p be an odd prime with $p \equiv 1 \pmod 3$ and let D be a nonzero integer. Suppose $p \nmid D$ and consider the elliptic curve $E : y^2 = x^3 + D$ over $\mathbb{F}_p$. Let $p = \theta\overline{\theta}$ where $\theta \in \mathbb{Z}[\omega]$ and $\omega = e^{2\pi i/3}$ and suppose $\theta \equiv 2 \,(3)$ in $\mathbb{Z}[\omega]$. Then*

$$a(E) = -\overline{\left(\frac{4D}{\theta}\right)_6}\,\theta - \left(\frac{4D}{\theta}\right)_6 \overline{\theta}.$$

We use the above theorem to compute a formula for the sum of $a(E)^n$ over all curves E over $\mathbb{F}_p$ having j-invariant 0.

Lemma IV.3.5. *Let $p \equiv 1 \pmod{12}$ and let $c, d \in \mathbb{Z}$ such that $p = c^2 - cd + d^2$ and $c + d\omega \equiv 2 \,(3)$ in $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Then for $n \geq 2$ even,*

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n = 2[(c+d)^n + (2c-d)^n + (c-2d)^n].$$

Proof. By Lemma IV.2.4, there are exactly six classes of elliptic curves to be included in the above sum. Suppose $D \in \mathbb{F}_p^\times$ is not a square or a cube. Then we may take

$$E_0' : y^2 = x^3 + 1 \qquad E_3' : y^2 = x^3 + D^3$$

$$E_1' : y^2 = x^3 + D \qquad E_4' : y^2 = x^3 + D^4$$

$$E_2' : y^2 = x^3 + D^2 \qquad E_5' : y^2 = x^3 + D^5.$$

Notice that these curves are not isomorphic to one another over $\mathbb{F}_p$. Since $p \equiv 1$

(mod 3), we may apply Theorem IV.3.4 and we take $\theta = c + d\omega$. Before we begin our computations, we make some observations.

- $\left(\frac{D}{\theta}\right)_6 = e^{\pm \pi i/3}$, since D is not a square or a cube.
- $\left(\frac{4}{\theta}\right)_6 = \left(\frac{2}{\theta}\right)_3 = 1, \omega,$ or ω^2.
- $\left(\frac{D}{\theta}\right)_3 \neq 1$ since $\left(\frac{D}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_6^2$. Thus, $\left(\frac{D}{\theta}\right)_3 = \omega$ or ω^2.
- $\left(\frac{D}{\theta}\right)_2 \neq 1$ since otherwise we have $\frac{x^2-D}{c+d\omega} = \frac{1}{p}(x^2 - D)(c + d\omega^2) \in \mathbb{Z}[\omega]$ which implies $p|(c + d\omega^2)$ since $D \notin \mathbb{F}_p^2$. Thus, $\left(\frac{D}{\theta}\right)_2 = -1$.
- $\omega + \omega^2 = -1$.

We now use Theorem IV.3.4 to compute $a(E'_j)$ for $j = 0, \ldots, 5$. In each computation, cases arise reflecting the value of $\left(\frac{D}{\theta}\right)_6$, $\left(\frac{2}{\theta}\right)_3$, and $\left(\frac{D}{\theta}\right)_3$, and we often make use of the observations made in the list above and the list following Definition IV.3.1. For each of $E'_0, \ldots, E'_5$, we show the explicit computation in one case. The other cases follow in a similar straightforward manner. We begin with E'_0 and find that

$$\begin{aligned} a(E'_0) &= -\overline{\left(\frac{4}{\theta}\right)}_6 \theta - \left(\frac{4}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2}{\theta}\right)}_3 (c + d\omega) - \left(\frac{2}{\theta}\right)_3 (c + d\omega^2). \end{aligned}$$

If $\left(\frac{2}{\theta}\right)_3 = 1$, we have

$$\begin{aligned} a(E'_0) &= -(c + d\omega) - (c + d\omega^2) \\ &= -2c - d(\omega + \omega^2) \\ &= -2c + d. \end{aligned}$$

The other two cases follow similarly, and we have

$$a(E_0') = \begin{cases} -2c+d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \\ c-2d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega \\ c+d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega^2. \end{cases} \tag{9}$$

Now we look at the curve E_1'. Applying Theorem IV.3.4 gives

$$\begin{aligned} a(E_1') &= -\overline{\left(\frac{4D}{\theta}\right)}_6 \theta - \left(\frac{4D}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_6 (c+d\omega) - \left(\frac{2}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_6 (c+d\omega^2), \end{aligned}$$

by the relation between the cubic and 6^{th} power residue symbols. Here, there are 6 cases to consider, according to the values of $\left(\frac{2}{\theta}\right)_3$ and $\left(\frac{D}{\theta}\right)_6$. For example, if $\left(\frac{2}{\theta}\right)_3 = 1$ and $\left(\frac{D}{\theta}\right)_6 = e^{\pi i/3}$, then

$$\begin{aligned} a(E_1') &= -e^{-\pi i/3}(c+d\omega) - e^{\pi i/3}(c+d\omega^2) \\ &= -c(e^{-\pi i/3} + e^{\pi i/3}) - d(\omega e^{-\pi i/3} + \omega^2 e^{\pi i/3}) \\ &= -c-d, \end{aligned}$$

since $e^{-\pi i/3} + e^{\pi i/3} = 1$. The other 5 cases follow in a similar manner, and we obtain

$$a(E_1') = \begin{cases} -c-d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{\pi i/3} \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{-\pi i/3} \\ -c+2d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{-\pi i/3} \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega^2 \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{\pi i/3} \\ 2c-d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{\pi i/3} \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega^2 \text{ and } \left(\frac{D}{\theta}\right)_6 = e^{-\pi i/3}. \end{cases} \tag{10}$$

Next, we look at E_2'. The theorem and our observations imply

$$\begin{aligned} a(E_2') &= -\overline{\left(\frac{4D^2}{\theta}\right)}_6 \theta - \left(\frac{4D^2}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_3 (c + d\omega) - \left(\frac{2}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_3 (c + d\omega^2). \end{aligned}$$

We again have 6 cases to consider here, depending on the values of $\left(\frac{2}{\theta}\right)_3$ and $\left(\frac{D}{\theta}\right)_3$. For example, if $\left(\frac{2}{\theta}\right)_3 = \omega^2 = \left(\frac{D}{\theta}\right)_3$, we have

$$\begin{aligned} a(E_2') &= -\omega\omega(c + d\omega) - \omega^2\omega^2(c + d\omega^2) \\ &= -c(\omega^2 + \omega) - d(1 + 1) \\ &= c - 2d. \end{aligned}$$

Computing the remaining cases gives

$$a(E_2') = \begin{cases} c - 2d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ c + d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega \\ -2c + d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega^2 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega. \end{cases} \tag{11}$$

Next, consider E_3'. Theorem IV.3.4 implies

$$\begin{aligned} a(E_3') &= -\overline{\left(\frac{4D^3}{\theta}\right)}_6 \theta - \left(\frac{4D^3}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_2 (c + d\omega) - \left(\frac{2}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_2 (c + d\omega^2) \\ &= \overline{\left(\frac{2}{\theta}\right)}_3 (c + d\omega) + \left(\frac{2}{\theta}\right)_3 (c + d\omega^2), \end{aligned}$$

since $\left(\frac{D}{\theta}\right)_2 = -1$ by the next to last observation we made at the start of the proof. Thus, here we have only three cases, representing the value of $\left(\frac{2}{\theta}\right)_3$. If $\left(\frac{2}{\theta}\right)_3 = \omega$, for instance, we have

$$\begin{aligned} a(E_3') &= \omega^2(c + d\omega) + \omega(c + d\omega^2) \\ &= c(\omega^2 + \omega) + d(1 + 1) \\ &= -c + 2d. \end{aligned}$$

Filling in the other two cases gives

$$a(E_3') = \begin{cases} 2c - d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \\ -c + 2d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega \\ -c - d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega^2. \end{cases} \tag{12}$$

Now, we move on to E_4' where the theorem and our observations imply

$$\begin{aligned} a(E_4') &= -\overline{\left(\frac{4D^4}{\theta}\right)}_6 \theta - \left(\frac{4D^4}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_3^2 (c + d\omega) - \left(\frac{2}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_3^2 (c + d\omega^2). \end{aligned}$$

Again we have 6 cases, according to the values of $\left(\frac{2}{\theta}\right)_3$ and $\left(\frac{D}{\theta}\right)_3$. If, for instance, $\left(\frac{2}{\theta}\right)_3 = \omega$ and $\left(\frac{D}{\theta}\right)_3 = \omega^2$, we have

$$\begin{aligned} a(E_4') &= -\omega^2\omega^2(c + d\omega) - \omega\omega(c + d\omega) \\ &= -c(\omega + \omega^2) - d(\omega^2 + \omega) \\ &= c + d. \end{aligned}$$

The other 5 calculations follow similarly, and we have

$$a(E_4') = \begin{cases} c+d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ c-2d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega^2 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega \\ -2c+d & \text{if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega^2. \end{cases} \tag{13}$$

Lastly, we compute $a(E_5')$. Theorem IV.3.2 provides

$$\begin{aligned} a(E_5') &= -\overline{\left(\frac{4D^5}{\theta}\right)}_6 \theta - \left(\frac{4D^5}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{4D^2}{\theta}\right)}_6 \overline{\left(\frac{D^3}{\theta}\right)}_6 \theta - \left(\frac{4D^2}{\theta}\right)_6 \left(\frac{D^3}{\theta}\right)_6 \overline{\theta} \\ &= -\overline{\left(\frac{2D}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_2 \theta - \left(\frac{2D}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_2 \overline{\theta}, \end{aligned}$$

by multiplicativity and by the last two observations made after Definition IV.3.1. Then, since $\left(\frac{D}{\theta}\right)_2 = -1$, as observed at the start of the proof, we have

$$a(E_5') = \overline{\left(\frac{2}{\theta}\right)}_3 \overline{\left(\frac{D}{\theta}\right)}_3 (c+d\omega) + \left(\frac{2}{\theta}\right)_3 \left(\frac{D}{\theta}\right)_3 (c+d\omega^2),$$

and we see that again, 6 cases arise. For example, if $\left(\frac{2}{\theta}\right)_3 = 1$ and $\left(\frac{D}{\theta}\right)_3 = \omega^2$, we obtain

$$\begin{aligned} a(E_5') &= \omega(c+d\omega) + \omega^2(c+d\omega^2) \\ &= c(\omega+\omega^2) + d(\omega^2+\omega) \\ &= -c-d. \end{aligned}$$

Computing the remaining 5 cases in a similar way, we find that

$$a(E_5') = \begin{cases} -c+2d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ -c-d & \text{if } \left(\frac{2}{\theta}\right)_3 = 1 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \left(\frac{D}{\theta}\right)_3 = \omega \\ 2c-d & \text{if } \left(\frac{2}{\theta}\right)_3 = \omega \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega^2 \\ & \textit{or if } \left(\frac{2}{\theta}\right)_3 = \omega^2 \text{ and } \left(\frac{D}{\theta}\right)_3 = \omega. \end{cases} \tag{14}$$

Now we are finally ready to compute the quantity

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n,$$

as the statement of our lemma requires. We must calculate this sum in 6 different cases, corresponding to the possibilities $\left(\frac{2}{\theta}\right)_3 \in \{1, \omega, \omega^2\}$, $\left(\frac{D}{\theta}\right)_3 \in \{\omega, \omega^2\}$, and $\left(\frac{D}{\pi}\right)_6 \in \{e^{\pm \pi i/3}\}$. We now work out the calculation in the case $\left(\frac{2}{\theta}\right)_3 = 1$, $\left(\frac{D}{\theta}\right)_3 = \omega$, and $\left(\frac{D}{\theta}\right)_6 = e^{\pi i/3}$. By consulting (9),...,(14) to find the appropriate value of $a(E_j')$ for each j in this case, we see that, for $n \geq 2$, even, we have

$$\begin{aligned} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n &= \sum_{j=0}^{5} a(E_j')^n \\ &= (-2c+d)^n + (-c-d)^n + (c-2d)^n + (2c-d)^n + (c+d)^n + (-c+2d)^n \\ &= 2(2c-d)^n + 2(c+d)^n + 2(c-2d)^n, \end{aligned}$$

since n is even. The calculation is equally straightforward in the remaining 5 cases,

and one sees that in each case, we arrive at

$$\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p}\\ j(E)=0}} a(E)^n = (-2c+d)^n + (-c-d)^n + (c-2d)^n + (2c-d)^n + (c+d)^n + (c-2d)^n$$

$$= 2[(c+d)^n + (2c-d)^n + (c-2d)^n],$$

as desired. □

IV.4. Proof of Theorem IV.1.1

Let $p \equiv 1 \pmod{12}$ be prime. As in (5), we define a family of elliptic curves over $\mathbb{F}_p$ by

$$E_t : y^2 = 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t}.$$

Further, for $t \in \mathbb{F}_p$, $t \neq 0, 1$, recall that

$$a(t,p) = p + 1 - \#E_t(\mathbb{F}_p).$$

As in Lemmas IV.3.3 and IV.3.5, we let integers a, b, c, and d be defined by $p = a^2 + b^2 = c^2 - cd + d^2$, where $a + bi \equiv 1\,(2+2i)$ in $\mathbb{Z}[i]$ and $c + d\omega \equiv 2\,(3)$ in $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Finally, we let h, h^*, w, and H be defined as in Section IV.2. We use this notation throughout the remainder of the chapter.

Lemma IV.4.1. *If $p \equiv 1 \pmod{12}$ is prime and notation is as above, then for $n \geq 2$ even,*

$$\sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2-4p}{f^2}\right) = \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) + \frac{1}{4}\sum_{\substack{[E]_{\mathbb{F}_p}\in \mathrm{Ell}_{\mathbb{F}_p}\\ j(E)=1728}} a(E)^n + \frac{1}{3}\sum_{\substack{[E]_{\mathbb{F}_p}\in \mathrm{Ell}_{\mathbb{F}_p}\\ j(E)=0}} a(E)^n,$$

where we classify integers s with $s^2 - 4p < 0$ by some positive integer ℓ and square-free

integer m via

$$s^2 - 4p = \begin{cases} \ell^2 m, & 0 > m \equiv 1 \pmod 4 \\ \ell^2 4m, & 0 > m \equiv 2, 3 \pmod 4). \end{cases}$$

Proof. First, notice that h and h^* agree unless the argument $\frac{s^2-4p}{f^2} = -3$ or -4, since in all other cases $w(d) = 1$. Thus, we have

$$\sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2-4p}{f^2}\right) = \sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2} \neq -3,-4}} h^*\left(\frac{s^2-4p}{f^2}\right) + \sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-4}} h(-4) + \sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-3}} h(-3).$$

When $\frac{s^2-4p}{f^2} = -4$, we have the maximal order $\mathbb{Z}[i]$ and $h^*(-4) = \frac{h(-4)}{w(-4)} = \frac{1}{2}$, so $h(-4) = h^*(-4) + \frac{1}{2}$. On the other hand, when $\frac{s^2-4p}{f^2} = -3$, we have the maximal order $\mathbb{Z}[\omega]$ and $h^*(-3) = \frac{h(-3)}{w(-3)} = \frac{1}{3}$, so $h(-3) = h^*(-3) + \frac{2}{3}$. Making these substitutions, we see that

$$\sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2-4p}{f^2}\right) = \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) + \frac{1}{2} \sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-4}} 1 + \frac{2}{3} \sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-3}} 1. \quad (15)$$

To complete the proof, we must verify that

$$\sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-4}} 1 = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n \quad (16)$$

and

$$\sum_{0<s<2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2}=-3}} 1 = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n. \tag{17}$$

First, we consider (16). Recall from the proof of Lemma IV.3.3 that $a(E) = \pm 2a, \pm 2b$ for all relevant E with j-invariant 1728. Also, it is easy to verify that $s = |2a|, |2b|$ satisfy $\frac{s^2-4p}{\ell^2} = -4$ (with $\ell = |b|, |a|$, respectively). Now, suppose $0 < s < 2\sqrt{p}$ satisfies $\frac{s^2-4p}{\ell^2} = -4$. Then $s^2 - 4p = -4\ell^2$ implies s is even, so we have $\left(\frac{s}{2}\right)^2 + \ell^2 = p$. Thus, it must be that $\frac{s}{2} = |a|, |b|$, since $\mathbb{Z}[i]$ is a UFD and $p = a^2 + b^2$. Since n is even, $(2a)^n = (-2a)^n$ and $(2b)^n = (-2b)^n$, so (16) follows.

Now, we prove (17) in a similar manner. Recall from the proof of Lemma IV.3.5 that $a(E) = \pm(c+d), \pm(2c-d), \pm(c-2d)$ for all relevant E with j-invariant 0. Also, $s = |c+d|$, $|2c-d|$, and $|c-2d|$ satisfy $\frac{s^2-4p}{\ell^2} = -3$ (by taking $\ell = |c-d|$, $|d|$, and $|c|$, respectively). Now, suppose $\frac{s^2-4p}{\ell^2} = -3$. Then in $\mathbb{Z}[\sqrt{-3}]$, we have

$$4p = (s + \sqrt{-3}\,\ell)(s - \sqrt{-3}\,\ell).$$

Since $-3 \equiv 5 \pmod 8$, 2 is inert in $\mathbb{Z}[\sqrt{-3}]$, so we must have $2|(s \pm \sqrt{-3}\,\ell)$. This implies

$$p = \left(\frac{s}{2} + \sqrt{-3}\,\frac{\ell}{2}\right)\left(\frac{s}{2} - \sqrt{-3}\,\frac{\ell}{2}\right) \tag{18}$$

in $\mathbb{Z}[\sqrt{-3}]$. Recall that we have $p = c^2 - cd + d^2$. In $\mathbb{Z}[\omega]$, we can write this as

$$\begin{aligned} p &= c^2 - cd + d^2 \\ &= (c + d\omega)(c + d\omega^2) && (19) \\ &= (d + c\omega)(d + c\omega^2) && (20) \\ &= (c\omega + d\omega^2)(c\omega^2 + d\omega). && (21) \end{aligned}$$

Since $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$, we can consider each of these factorizations in $\mathbb{Z}[\sqrt{-3}]$,

and each must be the same as (18), since $\mathbb{Z}[\sqrt{-3}]$ is a UFD. Making the substitution for ω into (19), (20), and (21) and comparing to (18) implies that $s = |2c - d|$, $|2d - c|$, and $|c + d|$, respectively. So in fact, $s = |2c - d|$, $|2d - c|$, $|c + d|$ are the only contributing s values to the sum on the left hand side of (17). Then since $a(E) = \pm(c + d), \pm(2c - d), \pm(c - 2d)$ and n is even, we have proved (17).

The lemma is finally proved by making the substitutions from (16) and (17) into (15). □

Proposition IV.4.2. *Let $p \equiv 1 \pmod{12}$ be prime and notation as above. Then for $n \geq 2$ even,*

$$\sum_{t=2}^{p-1} a(t,p)^n = \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) - 2^{n-1}(a^n + b^n) - \frac{1}{3}[(c+d)^n + (2c-d)^n + (c-2d)^n],$$

where we classify integers s with $s^2 - 4p < 0$ by some positive integer ℓ and square-free integer m via

$$s^2 - 4p = \begin{cases} \ell^2 m, & 0 > m \equiv 1 \pmod 4 \\ \ell^2 4m, & 0 > m \equiv 2, 3 \pmod 4. \end{cases}$$

Proof. Notice that for the given family of elliptic curves, $j(E_t) = \frac{1728}{t}$. Thus, as t ranges from 2 to $p - 1$, each E_t represents a distinct isomorphism class of elliptic curves in $Ell_{\overline{\mathbb{F}}_p}$. Moreover, since $j(E_t)$ gives an automorphism of $\mathbb{P}^1$, every j-invariant other than 0 and 1728 is represented precisely once. Thus, for even $n \geq 2$, we have

$$\sum_{t=2}^{p-1} a(t,p)^n = \sum_{\substack{[E]_{\overline{\mathbb{F}}_p} \in Ell_{\overline{\mathbb{F}}_p} \\ E/\mathbb{F}_p \\ j(E)\neq 0,1728}} a(E)^n.$$

For elliptic curves with j-invariant other than 0 and 1728, each class $[E] \in Ell_{\overline{\mathbb{F}}_p}$

gives rise to two distinct classes in $Ell_{\mathbb{F}_p}$ (see Lemma IV.2.4), represented by E and its quadratic twist E^{tw}. For such curves, $a(E)$ and $a(E^{tw})$ differ only by a sign, and so $a(E)^n = a(E^{tw})^n$, since n is even. Therefore, we have

$$\sum_{t=2}^{p-1} a(t,p)^n = \sum_{\substack{[E]_{\overline{\mathbb{F}}_p} \in Ell_{\overline{\mathbb{F}}_p} \\ E/\mathbb{F}_p \\ j(E)\neq 0,1728}} a(E)^n = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)\neq 0,1728}} a(E)^n.$$

Then, if we add and subtract the contributions from the classes $[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}$ with $j(E) = 0, 1728$, we have

$$\sum_{t=2}^{p-1} a(t,p)^n = \frac{1}{2}\left[\sum_{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}} a(E)^n - \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n \right]. \tag{22}$$

Now we look more closely at the sum $\sum_{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}} a(E)^n$. By Theorem IV.2.1, $Ell_{\mathbb{F}_p}$ is the the disjoint union

$$Ell_{\mathbb{F}_p} = \bigcup_{0 \le s < 2\sqrt{p}} I(s,p),$$

where $I(s,p)$ is defined as in (7). Then since $n \geq 2$ is even, we may write

$$\begin{aligned} \sum_{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}} a(E)^n &= \sum_{0 \le s < 2\sqrt{p}} \sum_{[E]_{\mathbb{F}_p} \in I(s,p)} s^n \\ &= \sum_{0 < s < 2\sqrt{p}} \#I(s,p) s^n, \end{aligned}$$

since $s = 0$ makes no contribution. Substituting this into (22) gives

$$\sum_{t=2}^{p-1} a(t,p)^n = \frac{1}{2} \sum_{0 < s < 2\sqrt{p}} \#I(s,p) s^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

Now we may apply Theorem IV.2.2 to obtain

$$\sum_{t=2}^{p-1} a(t,p)^n = \sum_{0<s<2\sqrt{p}} H(s^2-4p)s^n - \frac{1}{2}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

Recall from (6) that if d is the discriminant of an imaginary quadratic order $\mathcal{O}$,

$$H(d) := \sum_{\mathcal{O}\subseteq\mathcal{O}'\subseteq\mathcal{O}_{max}} h(\mathcal{O}'),$$

where the sum is over all orders between $\mathcal{O}$ and the maximal order. Then taking ℓ as defined as in the statement of the Proposition, we have

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

which gives

$$\sum_{t=2}^{p-1} a(t,p)^n = \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2-4p}{f^2}\right) - \frac{1}{2}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n. \tag{23}$$

To complete the proof, we apply Lemma IV.4.1 to the right side of (23), to replace h by h^*. Then, collecting terms gives

$$\begin{aligned}\sum_{t=2}^{p-1} a(t,p)^n &= \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) - \frac{1}{4}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{6}\sum_{\substack{[E]_{\mathbb{F}_p}\in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n \\ &= \sum_{0<s<2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2-4p}{f^2}\right) - 2^{n-1}(a^n+b^n) \\ &\quad - \frac{1}{3}[(c+d)^n + (2c-d)^n + (c-2d)^n],\end{aligned}$$

by Lemmas IV.3.3 and IV.3.5. This is the desired result. □

Proposition IV.4.2 and Theorem IV.2.3 give us the tools necessary to complete the proof of the main theorem in this chapter:

Proof of Theorem IV.1.1. By Theorem IV.2.3, we have for $k \geq 4$ even,

$$\begin{aligned}
\mathrm{Tr}_k(\Gamma, p) &= -1 - \frac{1}{2}h^*(-4p)(-p)^{\frac{k}{2}-1} - \sum_{0<s<2\sqrt{p}} G_k(s,p) \sum_f h^*\left(\frac{s^2-4p}{f^2}\right) \\
&= -1 - \frac{1}{2}h^*(-4p)(-p)^{\frac{k}{2}-1} - \sum_{0<s<2\sqrt{p}} \Bigg[(-p)^{\frac{k}{2}-1} \\
&\quad + \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j s^{k-2j-2}\Bigg] \sum_f h^*\left(\frac{s^2-4p}{f^2}\right) \\
&= -1 - \frac{1}{2}h^*(-4p)(-p)^{\frac{k}{2}-1} - (-p)^{\frac{k}{2}-1} \sum_{0<s<2\sqrt{p}} 1 \sum_f h^*\left(\frac{s^2-4p}{f^2}\right) \\
&\quad - \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \sum_{0<s<2\sqrt{p}} s^{k-2j-2} \sum_f h^*\left(\frac{s^2-4p}{f^2}\right),
\end{aligned}$$

after substituting in the definition of $G_k(s,p)$ and distributing. Now, note that taking $k = 2$ in Theorem IV.2.3 provides

$$0 = p - \frac{1}{2}h^*(-4p) - \sum_{0<s<2\sqrt{p}} 1 \sum_f h^*\left(\frac{s^2-4p}{f^2}\right).$$

We apply this, together with Proposition IV.4.2 and obtain

$$\begin{aligned}
\mathrm{Tr}_k(\Gamma, p) &= -1 - \frac{1}{2}h^*(-4p)(-p)^{\frac{k}{2}-1} + (-p)^{\frac{k}{2}-1}\left(\frac{1}{2}h^*(-4p) - p\right) \\
&\quad - \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \Bigg[\sum_{t=2}^{p-1} a(t,p)^{k-2j-2} + \frac{1}{2}\left[2^{k-2j-2}(a^{k-2j-2}+b^{k-2j-2})\right] \\
&\quad + \frac{1}{3}\left[(c+d)^{k-2j-2} + (2c-d)^{k-2j-2} + (c-2d)^{k-2j-2}\right]\Bigg] \\
&= -1 + (-p)^{\frac{k}{2}-1} \cdot (-p) - \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \sum_{t=2}^{p-1} a(t,p)^{k-2j-2} \\
&\quad - \frac{1}{2}\sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \left[(2a)^{k-2j-2} + (2b)^{k-2j-2}\right]
\end{aligned}$$

$$- \frac{1}{3}\sum_{j=0}^{\frac{k}{2}-2}(-1)^j\binom{k-2-j}{j}p^j\left[(c+d)^{k-2j-2}+(2c-d)^{k-2j-2}\right.$$
$$\left.+(c-2d)^{k-2j-2}\right],$$

after distributing once again. Now, we notice the simple fact that

$$(-p)^{\frac{k}{2}-1}\cdot(-p) = -(-p)^{\frac{k}{2}-1}(p-2) - 2\left(\frac{1}{2}(-p)^{\frac{k}{2}-1}\right) - 3\left(\frac{1}{3}(-p)^{\frac{k}{2}-1}\right).$$

Splitting up the factors of $(-p)^{\frac{k}{2}-1}$ in this way gives that

$$\begin{aligned}
\mathrm{Tr}_k(\Gamma,p) &= -1 - \frac{1}{2}\left[G_k(2a,p)+G_k(2b,p)\right] \\
&\quad - \frac{1}{3}\left[G_k(c+d,p)+G_k(2c-d,p)+G_k(c-2d,p)\right] \\
&\quad - (p-2)(-p)^{\frac{k}{2}-1} - \sum_{j=0}^{\frac{k}{2}-2}(-1)^j\binom{k-2-j}{j}p^j\sum_{t=2}^{p-1}a(t,p)^{k-2j-2} \\
&= -1-\lambda(k,p) - \sum_{t=2}^{p-1}(-p)^{\frac{k}{2}-1} - \sum_{t=2}^{p-1}\sum_{j=0}^{\frac{k}{2}-2}(-1)^j\binom{k-2-j}{j}p^j a(t,p)^{k-2j-2} \\
&= -1-\lambda(k,p) - \sum_{t=2}^{p-1}G_k(a(t,p),p),
\end{aligned}$$

according to the definitions of G_k and $\lambda(k,p)$ given in the statement of the theorem. This completes the proof of Theorem IV.1.1. □

Remark IV.4.3. According to Theorem III.1.1, we may rewrite $a(t,p)$ in terms of the hypergeometric function ${}_2F_1\left(\left.\begin{matrix}\xi,\xi^5\\ \varepsilon\end{matrix}\right|t\right)$. Thus, Theorem IV.1.1 can be reformulated to give Tr_k in terms of $\lambda(k,p)$ and $G_k\left(\psi^{-1}(t)p\,{}_2F_1\left(\left.\begin{matrix}\xi,\xi^5\\ \varepsilon\end{matrix}\right|t\right),p\right)$, where $\psi(t) = -\phi(2)\xi^{-3}(1-t)$.

Specializing to various values of k in Theorem IV.1.1, we arrive at more explicit formulas. In particular, taking $k = 12$, we obtain a formula for Ramanujan's τ-

function. Recall that we define $\tau(n)$ by

$$(2\pi)^{-12}\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

Also, recall that $\Delta(z)$ generates the one dimensional space S_{12}, and thus $\mathrm{Tr}_{12}(\Gamma, p) = \tau(p)$ for primes p. Then, taking $k = 12$ in the Theorem IV.1.1 gives the following:

Corollary IV.4.4. *Let a, b, c, and d be defined as above, and set $x = a^2b^2$ and $y = cd$. If p is a prime, $p \equiv 1(12)$, then*

$$\tau(p) = -1 - 8p^5 + 80p^3x - 256px^2 + 27y^2p^3 - 27y^3p^2 - \sum_{t=2}^{p-1} G_{12}(a(t,p),p),$$

where

$$G_{12}(s,p) = s^{10} - 9ps^8 + 28p^2s^6 - 35p^3s^4 + 15p^4s^2 - p^5.$$

Proof. First, one calculates easily from (8) in Section IV.2 that

$$G_{12}(s,p) = s^{10} - 9ps^8 + 28p^2s^6 - 35p^3s^4 + 15p^4s^2 - p^5.$$

To prove the corollary, we must show that

$$\lambda(12,p) = 8p^5 - 80p^3x + 256px^2 - 27y^2p^3 + 27y^3p^2, \tag{24}$$

where

$$\lambda(12,p) = \frac{1}{2}[G_{12}(2a,p) + G_{12}(2b,p)] + \frac{1}{3}[G_{12}(c+d,p) + G_{12}(2c-d,p) + G_{12}(c-2d,p)].$$

A tedious calculation by hand or an easy one with Maple, recalling that $p = a^2 + b^2 = c^2 - cd + d^2$, verifies this and hence completes the proof. □

As noted in IV.4.3, Corollary IV.4.4 can be reformulated in terms of the hypergeometric function ${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)$ considered in Chapter III. In fact, we can inductively

arrive at a formula for $\tau(p)$ in terms only of 10^{th} powers of this hypergeometric function.

Corollary IV.4.5. *Let $p \equiv 1 \pmod{12}$ be prime and let a, b, c, and d be defined as above. Let ξ be an element of order 12 in $\widehat{\mathbb{F}_p^\times}$. Then*

$$\begin{aligned}\tau(p) &= 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 - 2^9(a^{10} + b^{10}) \\ &\quad - \frac{1}{3}\left((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}\right) - \sum_{t=2}^{p-1} p^{10}\phi(1-t)\,{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)^{10}.\end{aligned}$$

Proof. Recall from the statement of Theorem IV.1.1 that we have

$$\lambda(k,p) = \frac{1}{2}[G_k(2a,p) + G_k(2b,p)] + \frac{1}{3}[G_k(c+d,p) + G_k(2c-d,p) + G_k(c-2d,p)],$$

where

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

Then, one can check by hand or with Maple that we have the following, recalling the relations $p = a^2 + b^2 = c^2 - cd + d^2$:

$$\begin{aligned}\lambda(4,p) &= 2p \\ \lambda(6,p) &= -4p^2 + 2^3(a^4 + b^4) \\ \lambda(8,p) &= -8p^3 + 2^5(a^6 + b^6) - 40p(a^4 + b^4) + \frac{1}{3}((c+d)^6 + (2c-d)^6 + (c-2d)^6) \\ \lambda(10,p) &= 52p^4 + 2^7(a^8 + b^8) - 224p(a^6 + b^6) + 120p^2(a^4 + b^4) \\ &\quad + \frac{1}{3}((c+d)^8 + (2c-d)^8 + (c-2d)^8) - \frac{7}{3}p((c+d)^6 + (2c-d)^6 + (c-2d)^6) \\ \lambda(12,p) &= -152p^5 + 2^9(a^{10} + b^{10}) - 1152p(a^8 + b^8) + 896p^2(a^6 + b^6) - 280p^3(a^4 + b^4) \\ &\quad + \frac{1}{3}((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}) \\ &\quad - 3p((c+d)^8 + (2c-d)^8 + (c-2d)^8) \\ &\quad + \frac{28}{3}p^2((c+d)^6 + (2c-d)^6 + (c-2d)^6).\end{aligned}$$

By using each successive formula for $G_k(a(t,p),p)$, together with Theorem IV.1.1 and the formulas for $\lambda(k,p)$ given above, we can compute $\sum_{t=2}^{p-1} a(t,p)^{k-2}$, for $k = 4,\ldots,12$. Now, we exhibit the computations in the cases $k=4$ and $k=6$, to give the idea of the technique. First, notice that $G_4(s,p) = s^2 - p$ and recall $\mathrm{Tr}_4(\Gamma,p) = 0$, as there are no cusp forms of weight 4 for Γ. Thus, Theorem IV.1.1 implies

$$\begin{aligned} 0 = \mathrm{Tr}_4(\Gamma,p) &= -1 - \lambda(4,p) - \sum_{t=2}^{p-1} G_4(a(t,p),p) \\ &= -1 - 2p - \sum_{t=2}^{p-1} (a(t,p)^2 - p) \\ &= -1 - 2p + p(p-2) - \sum_{t=2}^{p-1} a(t,p)^2. \end{aligned}$$

Thus, after simplifying, we see that

$$0 = p^2 - 4p - 1 - \sum_{t=2}^{p-1} a(t,p)^2. \tag{25}$$

Now, we utilize this computation to derive a formula for the sum of 4^{th} powers of $a(t,p)$. For $k=6$, we have $G_6(s,p) = s^4 - 3ps^2 + p^2$ and once again $\mathrm{Tr}_6(\Gamma,p) = 0$. Then, by Theorem IV.1.1 and the formula for $\lambda(6,p)$ given at the start of the proof, we see that

$$\begin{aligned} 0 = \mathrm{Tr}_6(\Gamma,p) &= -1 - \lambda(6,p) - \sum_{t=2}^{p-1} G_6(a(t,p),p) \\ &= -1 + 4p^2 - 2^3(a^4+b^4) - \sum_{t=2}^{p-1} (a(t,p)^4 - 3pa(t,p)^2 + p^2). \end{aligned}$$

We distribute the summation across the polynomial $G_6(a(t,p),p)$ and then make a substitution for $\sum_{t=2}^{p-1} a(t,p)^2$, according to (25). This gives

$$0 = \mathrm{Tr}_6(\Gamma,p) = 4p^2 - 1 - 2^3(a^4+b^4) - \sum_{t=2}^{p-1} a(t,p)^4 + 3p \sum_{t=2}^{p-1} a(t,p)^2 - p^2(p-2)$$

$$= 4p^2 - 1 - 2^3(a^4 + b^4) - \sum_{t=2}^{p-1} a(t,p)^4$$
$$+ 3p(-2p - 1 + p(p-2)) - p^2(p-2).$$

After simplifying, we arrive at

$$0 = 2p^3 - 6p^2 - 3p - 1 - \sum_{t=2}^{p-1} a(t,p)^4. \tag{26}$$

We continue this process, using successive formulas for $G_k(s,p)$ and $\lambda(k,p)$ and back-substituting previous results such as (25) and (26). We omit the tedious details of the next couple of cases, which result in the following:

$$\mathrm{Tr}_8(\Gamma,p) = 0 = 5p^4 - 9p^2 - 5p - 1 - 2^5(a^6 + b^6)$$
$$- \frac{1}{3}((c+d)^6 + (2c-d)^6 + (c-2d)^6) - \sum_{t=2}^{p-1} a(t,p)^6 \tag{27}$$

$$\mathrm{Tr}_{10}(\Gamma,p) = 0 = 14p^5 - 28p^3 - 20p^2 - 7p - 1 - 2^7(a^8 + b^8)$$
$$- \frac{1}{3}((c+d)^8 + (2c-d)^8 + (c-2d)^8) - \sum_{t=2}^{p-1} a(t,p)^8 \tag{28}$$

Now, we use (25),...,(28) together with the formula for $\lambda(12,p)$ from the beginning of the proof to compute a formula for $\tau(p)$. Since $G_{12}(s,p) = s^{10} - 9ps^8 + 28p^2s^6 - 35p^3s^4 + 15p^4s^2 - p^5$ and $\mathrm{Tr}_{12}(\Gamma,p) = \tau(p)$, Theorem IV.1.1 gives

$$\tau(p) = -1 - \lambda(12,p) - \sum_{t=2}^{p-1} G_{12}(a(t,p),p)$$
$$= -1 - \lambda(12,p) - \sum_{t=2}^{p-1} a(t,p)^{10} + 9p\sum_{t=2}^{p-1} a(t,p)^8 - 28p^2\sum_{t=2}^{p-1} a(t,p)^6$$
$$+ 35p^3\sum_{t=2}^{p-1} a(t,p)^4 - 15p^4\sum_{t=2}^{p-1} a(t,p)^2 + p^5(p-2)$$

$$
\begin{aligned}
&= -1 - \lambda(12,p) - \sum_{t=2}^{p-1} a(t,p)^{10} \\
&\quad + 9p\Big(14p^5 - 28p^3 - 20p^2 - 7p - 1 - 2^7(a^8 + b^8) \\
&\quad -\frac{1}{3}((c+d)^8 + (2c-d)^8 + (c-2d)^8)\Big) \\
&\quad - 28p^2\Big(5p^4 - 9p^2 - 5p - 1 - 2^5(a^6 + b^6) - \frac{1}{3}((c+d)^6 + (2c-d)^6 + (c-2d)^6)\Big) \\
&\quad + 35p^3(2p^3 - 6p^2 - 3p - 1) - 15p^4(p^2 - 4p - 1) + p^5(p-2),
\end{aligned}
$$

by (25), ...,(28). The substitution

$$
\begin{aligned}
\lambda(12,p) = &-152p^5 + 2^9(a^{10} + b^{10}) - 1152p(a^8 + b^8) + 896p^2(a^6 + b^6) - 280p^3(a^4 + b^4) \\
&+ \frac{1}{3}((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}) \\
&- 3p((c+d)^8 + (2c-d)^8 + (c-2d)^8) \\
&+ \frac{28}{3}p^2((c+d)^6 + (2c-d)^6 + (c-2d)^6).
\end{aligned}
$$

gives rise to many cancellations, and after simplifying, we find that

$$
\begin{aligned}
\tau(p) = 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 - 2^9(a^{10} + b^{10}) \\
- \frac{1}{3}((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}) - \sum_{t=2}^{p-1} a(t,p)^{10}. \quad (29)
\end{aligned}
$$

Finally, to complete the proof, we recall that Theorem III.1.1 implies

$$
p\,{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) = -\phi(2)\xi^{-3}(1-t)a(t,p)
$$

for $t \in \mathbb{F}_p \backslash \{0,1\}$. Thus,

$$
a(t,p)^{10} = \left(-p\phi(2)\xi^3(1-t)_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)\right)^{10} = p^{10}\phi(1-t)_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)^{10},
$$

since $\phi^{10} = \varepsilon$ and $\xi^{30} = \xi^6 = \phi$. This, together with (29), confirms the corollary. $\square$

The technique used in the proof of Corollary IV.4.5 can be extended one step further to arrive at yet another formula for $\tau(p)$:

Corollary IV.4.6. *Let $p \equiv 1 \pmod{12}$ be prime and let a, b, c, and d be defined as above. Let ξ be an element of order 12 in $\widehat{\mathbb{F}_p^\times}$. Then*

$$\tau(p) = 12p^6 - 27p^4 - 25p^3 - 14p^2 - \frac{54}{11}p - 1 - \frac{1}{11p} - \frac{2^{11}}{11p}(a^{12} + b^{12}) \\ - \frac{1}{33p}((c+d)^{12} + (2c-d)^{12} + (c-2d)^{12}) - \frac{1}{11}\sum_{t=2}^{p-1} p^{11}\, {}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)^{12}.$$

Proof. We continue the process used in the proof of Corollary IV.4.5 to consider the case $k = 14$. Using the notation from the statement of Theorem IV.1.1, one calculates that

$$G_{14}(s,p) = s^{12} - 11ps^{10} + 45p^2s^8 - 84p^3s^6 + 70p^4s^4 - 21p^5s^2 + p^6.$$

Now, since there are no cusp forms of level 14 for Γ, we have $\mathrm{Tr}_{14}(\Gamma, p) = 0$. Thus, Theorem IV.1.1 implies

$$\begin{aligned} 0 &= -1 - \lambda(14,p) - \sum_{t=2}^{p-1} G_{14}(a(t,p),p) \\ &= -1 - \lambda(14,p) - \sum_{t=2}^{p-1} a(t,p)^{12} + 11p\sum_{t=2}^{p-1} a(t,p)^{10} - 45p^2\sum_{t=2}^{p-1} a(t,p)^8 \\ &\quad + 84p^3\sum_{t=2}^{p-1} a(t,p)^6 - 70p^4\sum_{t=2}^{p-1} a(t,p)^4 + 21p^5\sum_{t=2}^{p-1} a(t,p)^2 - p^6(p-2). \end{aligned}$$

Next, we make a substitution for each $\displaystyle\sum_{t=2}^{p-1} a(t,p)^n$ for $n = 2, \ldots, 10$, according to (25),...,(29). Then we have

$$0 = -1 - \lambda(14,p) - \sum_{t=2}^{p-1} a(t,p)^{12} + 11p\Big(-\tau(p) + 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 \\ -2^9(a^{10} + b^{10}) - \frac{1}{3}((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10})\Big)$$

$$
\begin{aligned}
&- 45p^2\Big(14p^5 - 28p^3 - 20p^2 - 7p - 1 - 2^7(a^8 + b^8) \\
&- \frac{1}{3}((c+d)^8 + (2c-d)^8 + (c-2d)^8)\Big) \\
&+ 84p^3\Big(5p^4 - 9p^2 - 5p - 1 - 2^5(a^6 + b^6) - \frac{1}{3}((c+d)^6 + (2c-d)^6 + (c-2d)^6)\Big) \\
&- 70p^4(2p^3 - 6p^2 - 3p - 1) + 21p^5(p^2 - 4p - 1) - p^6(p-2).
\end{aligned}
$$

One may calculate, by hand or with the aide of Maple, that we have

$$
\begin{aligned}
\lambda(14,p) = {} & 338p^6 + 2^{11}(a^{12} + b^{12}) - 11 \cdot 2^9 p(a^{10} + b^{10}) + 45 \cdot 2^7 p^2(a^8 + b^8) \\
& - 84 \cdot 2^5 p^3(a^6 + b^6) + 70 \cdot 2^3 p^4(a^4 + b^4) \\
& + \frac{1}{3}((c+d)^{12} + (2c-d)^{12} + (c-2d)^{12}) \\
& - \frac{11}{3}p((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}) \\
& + 15p^2((c+d)^8 + (2c-d)^8 + (c-2d)^8) \\
& - 28p^3((c+d)^6 + (2c-d)^6 + (c-2d)^6).
\end{aligned}
$$

Making this substitution allows many cancellations, and after simplifying, we find that

$$
\begin{aligned}
0 = {} & 132p^7 - 297p^5 - 275p^4 - 154p^3 - 54p^2 - 1 - 11p - 11p\tau(p) - 2^{11}(a^{12} + b^{12}) \\
& - \frac{1}{3}((c+d)^{12} + (2c-d)^{12} + (c-2d)^{12}) - \sum_{t=2}^{p-1} a(t,p)^{12}. \quad (30)
\end{aligned}
$$

We now recall that Theorem III.1.1 implies

$$
p\,{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right) = -\phi(2)\xi^{-3}(1-t)a(t,p)
$$

for $t \in \mathbb{F}_p \backslash \{0,1\}$. Therefore,

$$
a(t,p)^{12} = \left(-p\phi(2)\xi^3(1-t){}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)\right)^{12} = p^{12}\,{}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)^{12},
$$

since ϕ has order 2 and ξ has order 12. Making this substitution into (30) and then solving for $\tau(p)$ gives the desired result.

□

CHAPTER V

CONCLUSIONS AND FUTURE RESEARCH

Throughout this dissertation, we focused on hypergeometric functions over $\mathbb{F}_p$ and connections they have to both elliptic curves and modular forms. We directed our attention to a particular family

$$E_t : y^2 = 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t}$$

of elliptic curves over $\mathbb{F}_p$, where $p \equiv 1 \pmod{12}$. Theorem III.1.1 exhibited a formula for the number of points on E_t over $\mathbb{F}_p$ in terms of the hypergeometric function ${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)$, where ξ is an element of order 12 in $\widehat{\mathbb{F}_p^\times}$. The proof of this theorem made use of repeated character sum manipulations, together with identities given by Greene [6]. We also applied two special cases of the Hasse-Davenport relation [11] to achieve the desired relationships between products of Gauss sums.

We then shifted our focus to modular forms. In particular, in Theorem IV.1.1 we gave a formula for the traces Tr_k of Hecke operators on S_k in terms of $\#E_t(\mathbb{F}_p)$. The main tools used in the proof of this theorem were Hijikata's version of the Eichler-Selberg trace formula [7] and a theorem of Schoof which relates counting isomorphism classes of elliptic curves to class numbers of imaginary quadratic fields [16].

Combining Theorems III.1.1 and IV.1.1 gave a way to write the traces $\mathrm{Tr}_k(\Gamma, p)$ in terms of ${}_2F_1\left(\begin{matrix}\xi, \xi^5 \\ \varepsilon\end{matrix}\middle| t\right)$, for primes $p \equiv 1 \pmod{12}$. In particular, taking $k = 12$ in Theorem IV.1.1 gave rise to various formulas for Ramanujan's τ-function, as described in Corollaries IV.4.4, IV.4.5, and IV.4.6.

We plan to continue the work of the previous chapters to future research. Various avenues for future study are listed below:

- Produce a recursive formula for Tr_k in terms of Tr_{2j}, $2j \leq k-2$, using combinatorial inverse pairs found in [15]. This will generalize the results in Corollaries IV.4.5 and IV.4.6.

- Investigate the questions considered in Chapters III and IV in the case that $p \equiv 1 \pmod{12}$ fails.

- Examine implications of Corollaries IV.4.4, IV.4.5, and IV.4.6 to various congruences of $\tau(p)$.

- Consider some generalizations of classical hypergeometric functions to higher dimensions and investigate appropriate extensions of these to the finite field setting.

REFERENCES

[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, *Modularity of a certain Calabi-Yau threefold*, Monatsh. Math. **129** (2000), no. 3, 177-190.

[3] F. Beukers, *Algebraic values of G-functions*, J. reine angew. Math. **434** (1993), 45-65.

[4] D.A. Cox, *Primes of the form x^2+ny^2. Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, New York, 1989.

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

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

[7] 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.

[8] 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.

[9] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.

[10] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), no. 3, 461-467.

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

[12] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205-1223.

[13] M. Papanikolas, *A formula and a congruence for Ramanujan's τ-function*, Proc. Amer. Math. Soc., **134** (2006), no. 2, 333-341.

[14] P. Ribenboim, *Algebraic Numbers*, John Wiley & Sons, New York, 1972.

[15] J. Riordan, *Combinatorial Identities*, John Wiley & Sons, New York, 1968.

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

[17] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[18] L. Slater, *Generalized Hypergeometric Functions*, Cambridge Univ. Press, Cambridge, 1966.

[19] P.F. Stiller, *Classical automorphic forms and hypergeometric functions*, J. Number Theory **28** (1988), no. 2, 219-232.

VITA

Jenny G. Fuselier was born in Augusta, Georgia on January 24, 1981. She received her Bachelor of Science in Mathematics from Texas A&M University in August, 2002. She then studied as a graduate assistant in the Department of Mathematics at Texas A&M University and completed her Ph.D. in August 2007. Her permanent address is 1063 Athena Court, Acworth, GA 30101, and her email address is jennyfuselier@gmail.com.