TRACES OF HECKE OPERATORS IN LEVEL 1 AND
GAUSSIAN HYPERGEOMETRIC FUNCTIONS

JENNY G. FUSELIER

(Communicated by Ken Ono)

Abstract. We provide formulas for traces of $p^{th}$ Hecke operators in level 1 in terms of values of finite field $2F_1$-hypergeometric functions, extending previous work of the author to all odd primes $p$ instead of only those $p \equiv 1 \pmod{12}$. We first give a general level 1 trace formula in terms of the trace of Frobenius on a family of elliptic curves, and then we draw on recent work of Lennon to produce level 1 trace formulas in terms of hypergeometric functions for all primes $p > 3$.

1. Introduction

In recent years, relationships between traces of Hecke operators and counting points on families of varieties have been explored. For example, Ahlgren and Ono [2] described traces of $p^{th}$ Hecke operators in weight 4 and level 8 in terms of the number of $\mathbb{F}_p$-points on a Calabi-Yau threefold, while in [1], Ahlgren related traces of Hecke operators in weight 6 and level 4 to counting $\mathbb{F}_p$-points on the Legendre family of elliptic curves. The level 2 formula (for all weights) was made explicit in terms of the number of $\mathbb{F}_p$-points on a family of elliptic curves by Frechette, Ono, and Papanikolas in [5]. In [7], the author considered the level 1 case and provided a formula in terms of the number of $\mathbb{F}_p$-points on a one-parameter family of elliptic curves for primes $p \equiv 1 \pmod{12}$. Most recently, Lennon [11] considered the levels 3 and 9 scenarios. Earlier work of Ihara [10] and Birch [4] gave reason to believe such formulas were possible.

Interestingly, these trace formulas also have a link to finite field hypergeometric functions introduced by Greene in the 1980s [8]. Various authors [3, 5, 12] have used relations between values of Greene’s hypergeometric functions and counting $\mathbb{F}_p$-points on varieties to produce trace formulas in terms of hypergeometric functions. In [7, Thm. 1.2], the author proved an explicit relationship between counting $\mathbb{F}_p$-points on a one-parameter family of elliptic curves and the values of a particular $2F_1$ function over $\mathbb{F}_p$, which led to a level 1 trace formula in terms of hypergeometric functions. However, this formula was only proved for primes $p \equiv 1 \pmod{12}$. Recently, Lennon [11] Thms. 1.1 and 2.1] has removed this restriction on the congruence class of $p$ to produce formulas that relate $\#E(\mathbb{F}_q)$ to values of a $2F_1$ function over $\mathbb{F}_q$ for any $q = p^e$ where $q \equiv 1 \pmod{12}$.

In this paper, we provide a level 1 trace formula that holds for all $p > 3$. Then, we use Lennon’s result to produce formulas for traces of Hecke operators in level 1 in terms of finite field hypergeometric functions.

Received by the editors September 15, 2011.

2010 Mathematics Subject Classification. Primary 11F30; Secondary 11T24, 11G20, 33C99.

©2012 American Mathematical Society
Reverts to public domain 28 years from publication

1871
2. Statement of main results

Let \( p > 3 \) be prime and let \( k \geq 2 \) be an even integer. 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

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

Throughout, results will depend on the congruence class of \( p \) mod 12. As such, we set up some notation for various congruence classes of \( p \) to be used throughout the remainder of the paper. Whenever \( p \equiv 1 \pmod{4} \), we let \( a, b \in \mathbb{Z} \) be such that \( p = a^2 + b^2 \) and \( a + bi \equiv 1 (2 + 2i) \) in \( \mathbb{Z}[i] \). In that case, we define

\[
\mu_k(p) = \frac{1}{2} [G_k(2a, p) + G_k(2b, p)].
\]

Similarly, whenever \( p \equiv 1 \pmod{3} \), we let \( c, d \in \mathbb{Z} \) be such that \( p = c^2 - cd + d^2 \) and \( c + d\omega \equiv 2 (3) \pmod{\mathbb{Z}[\omega]} \), where \( \omega = e^{2\pi i/3} \). In this case, we define

\[
\nu_k(p) = \frac{1}{3} [G_k(c + d, p) + G_k(2c - d, p) + G_k(c - 2d, p)].
\]

We consider a one-parameter family of elliptic curves having \( j \)-invariant \( \frac{1728}{t} \). Specifically, for \( t \in \mathbb{F}_p \setminus \{0, 1\} \), we let

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

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

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

Let \( \Gamma = SL_2(\mathbb{Z}) \) and let \( M_k \) and \( S_k \), respectively, denote the spaces of modular forms and cusp forms of weight \( k \) for \( \Gamma \). Further, let \( \text{Tr}_k(\Gamma, p) \) denote the trace of the Hecke operator \( T_k(p) \) on \( S_k \). Our first main result completely classifies the traces of cusp forms in level 1:

**Theorem 2.1.** Let \( p > 3 \) be prime. Then for even \( k \geq 4 \),

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

where

\[
\lambda(k, p) = \begin{cases} 
\mu_k(p) + \nu_k(p) & \text{if } p \equiv 1 \pmod{12}, \\
\mu_k(p) + (-p)^{\frac{k}{2}-1} & \text{if } p \equiv 5 \pmod{12}, \\
\nu_k(p) + (-p)^{\frac{k}{2}-1} & \text{if } p \equiv 7 \pmod{12}, \\
2(-p)^{\frac{k}{2}-1} & \text{if } p \equiv 11 \pmod{12}.
\end{cases}
\]

Next, we move to results which link these traces of Hecke operators in level 1 with hypergeometric functions over finite fields. We begin with some preliminaries. Let \( p \) be a prime and let \( q = p^\epsilon \). Let \( \mathbb{F}_q^\times \) denote the group of all multiplicative characters on \( \mathbb{F}_q^\times \). We extend \( \chi \in \mathbb{F}_q^\times \) to all of \( \mathbb{F}_q \) by setting \( \chi(0) = 0 \). We let \( \epsilon \)
denote the trivial character. For $A, B \in \mathbb{F}_p^\times$, let $J(A, B)$ denote the usual Jacobi symbol and define

$$\begin{align*}
\binom{A}{B} := \frac{B(-1)^{n\frac{p-1}{2}}}{q^2} J(A, B) = \frac{B(-1)^{n\frac{p-1}{2}}}{q^2} \sum_{x \in \mathbb{F}_q^\times} A(x) B(1 - x).
\end{align*}$$

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

**Definition 2.2** ([8], Defn. 3.10). If $n$ is a positive integer, $x \in \mathbb{F}_q^\times$, and $A_0, A_1, \ldots, A_n, B_1, B_2, \ldots, B_n \in \mathbb{F}_q^\times$, then define

$$F_{n+1}^\chi \left( \begin{matrix} A_0, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{matrix} \big| x \right)_q := \frac{q^{n+1}}{q - 1} \sum_{\chi \in \mathbb{F}_q^\times} \left( \begin{matrix} A_0 \chi \\ B_1 \chi \\ \vdots \\ A_n \chi \end{matrix} \right) \chi(x).$$

In [7, Thm. 1.2], the author proved a formula giving an explicit relationship between $a(t, p)$ and a $2F_1$-hypergeometric function over $\mathbb{F}_p$, but required that $p \equiv 1$ (mod 12). In this case, the result of Theorem 2.1 can be rewritten to be in terms of a hypergeometric function over $\mathbb{F}_p$. However, [7] did not address the other classes of primes mod 12. Notice that either $p \equiv 1$ (mod 12) or, if not, then $p^2 \equiv 1$ (mod 12). With this in mind, for the remainder of the paper we define $q = p^{e(p)}$, where

$$e(p) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{12}, \\
2 & \text{if } p \not\equiv 1 \pmod{12}.
\end{cases}$$

We consider the same family of elliptic curves $E_t$, as defined in [4], but now over $\mathbb{F}_q$, and with $a(t, q) = q + 1 - \#E_t(\mathbb{F}_q)$. Thanks to Lennon’s results [11] and an inverse pair given in [13], we can now describe the traces of Hecke operators in level 1 in terms of a $2F_1$ function over $\mathbb{F}_q$ for the other classes of primes mod 12:

**Theorem 2.3.** Let $p > 3$ be prime such that $p = 5, 7, 11$ (mod 12) with $q = p^{e(p)}$ and $T$ a generator of $\mathbb{F}_q^\times$. Let $k \geq 4$ be even and $m = \frac{k}{2} - 1$. Define $H_m(x) := \sum_{i=0}^m \binom{m+i}{m} x^i$. Then

$$\begin{align*}
\text{Tr}_k(\Gamma, p) &= -1 - \lambda(k, p) \\
&\quad - \sum_{i=2}^{p-1} (-p)^m H_m \left( p T^{\frac{a+1}{2}} (2) T^{\frac{a+1}{4}} (1 - t) 2 F_1 \left( \begin{array}{c} T^{\frac{a+1}{4}} \\ \frac{a+1}{2} \\ \frac{a+1}{4} \\ 2 \end{array} \right) \right),
\end{align*}$$

where $\lambda(k, p)$ is as in Theorem 2.1.

Our final result is a generalization of [7, Thm. 1.4], giving a recursive formula for traces of Hecke operators in level 1 in terms of hypergeometric functions, now for all primes $p > 3$:

**Theorem 2.4.** Let $p > 3$ be prime, and $q = p^{e(p)}$. Let $k \geq 4$ be even, and $m = \frac{k}{2} - 1$. Further, let $T$ be a generator of $\mathbb{F}_q^\times$ and $b_i = p^{m-i} \left[ \binom{2m}{m} - \binom{2m}{m-1} \right]$. 

Then
\[ \text{Tr}_{2(m+1)}(\Gamma, p) = -1 - \lambda(2m + 2, p) + b_0(p - 2) \]
\[ - \sum_{i=1}^{m-1} b_i \cdot (\text{Tr}_{2i+2}(\Gamma, p) + 1 + \lambda(2i + 2, p)) \]
\[ - \sum_{t=2}^{p-1} \left( \psi(t, q) \frac{T^{\frac{s(q-1)}{4}}}{\varepsilon} \right) + 2p(e(p) - 1) \frac{2m}{\pi(p)}, \]
where
\[ \psi(t, q) = -qT^{\frac{s}{2}}(2)T^{\frac{s}{4} - \frac{1}{2}}(1 - t) \]
and \( \lambda(k, p) \) is as in Theorem 2.1

3. Proof of Theorem 2.1

To prove Theorem 2.1 we begin with Hijikata’s version of the Eichler-Selberg trace formula [9]. The statement of this theorem requires some notation. 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 \( h^*(d) = h(d)/w(d). \) The following theorem is the level 1 formulation of Hijikata’s version of the Eichler-Selberg trace formula for any odd prime.

**Theorem 3.1.** Let \( p \) be an odd prime and \( k \geq 2 \) be even. Then
\[ \text{Tr}_k(\Gamma, p) = -1 - \frac{1}{2} \beta(p)(-p)^{\frac{k}{2} - 1} - \sum_{0 < s < 2\sqrt{p}} G_k(s, p) \sum_{f|\ell} h^* \left( \frac{s^2 - 4p}{f^2} \right) + \delta(k), \]
where
\[ \beta(p) = \begin{cases} h^*(-4p) & \text{if } p \equiv 1 \pmod{4}, \\ h^*(-4p) + h^*(-p) & \text{if } p \equiv 3 \pmod{4}, \end{cases} \]
\[ \delta(k) = p + 1 \text{ if } k = 2 \text{ and } 0 \text{ otherwise, and where we classify integers } s \text{ with } s^2 - 4p < 0 \text{ by some positive integer } \ell \text{ and square-free integer } m \text{ via} \]
\[ s^2 - 4p = \begin{cases} \ell^2 m, & 0 < m \equiv 1 \pmod{4}, \\ \ell^2 4m, & 0 < m \equiv 2, 3 \pmod{4}. \end{cases} \]

To link Theorem 3.1 to \( a(t, p), \) we need to consider all isomorphism classes of elliptic curves over \( \mathbb{F}_p. \) If \( E \) is any elliptic curve defined over \( \mathbb{F}_p, \) let \( a(E) = p + 1 - \#E(\mathbb{F}_p). \) Additionally, for a perfect field \( K, \) we define
\[ E_{\ell K} := \{ [E]_K : E \text{ is defined over } K \}, \]
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 \( K. \) We first address the cases \( j(E) = 1728 \) and \( j(E) = 0. \)

**Lemma 3.2.** Let \( p \) be an odd prime. Whenever \( p \equiv 1 \pmod{4}, \) define \( a, b \in \mathbb{Z} \) to be such that \( p = a^2 + b^2 \) and \( a + bi = 1(2 + 2i) \) in \( \mathbb{Z}[i]. \) Then, for \( n \geq 2 \) even,
\[ \sum_{[E]_{\ell K} \in \text{Ell}_p \atop j(E) = 1728} a(E)^n = \begin{cases} 2^{n+1}(a^n + b^n) & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \]
Proof. The case $p \equiv 1 \pmod{4}$ was proved by the author in [6, Lemma IV.3.3]. If $p \equiv 0 \pmod{4}$ and $[E]_{E_p} \in Ell_{E_p}$, then $\#E(\mathbb{F}_p) = p + 1$, so $a(E) = 0$. \hfill \Box

**Lemma 3.3.** Let $p > 3$ be prime. Whenever $p \equiv 1 \pmod{3}$, we let $c, d \in \mathbb{Z}$ be such that $p = c^2 - cd + d^2$ and $c + d \equiv 2 \pmod{3}$ in $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Then, for $n \geq 2$ even,

$$\sum_{[E]_{E_p} \in Ell_{E_p} \atop j(E) = 0} a(E)^n = \begin{cases} 2((c + d)^n + (2c - d)^n + (c - 2d)^n) & \text{if } p \equiv 1 \pmod{3}, \\ 0 & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

Proof. The case $p \equiv 1 \pmod{3}$ was proved by the author in [6, Lemma IV.3.5]. If $p \equiv 0 \pmod{3}$ and $[E]_{E_p} \in Ell_{E_p}$, then $\#E(\mathbb{F}_p) = p + 1$, so $a(E) = 0$. \hfill \Box

The proof of Theorem 2.1 proceeds along the same line as the proof of the $p \equiv 1 \pmod{12}$ case proved by the author in [7]. In particular, we begin with the following extension of [7, Lemma 5.3].

**Lemma 3.4.** Let $p > 3$ be prime. Then for $n \geq 2$ even,

$$\sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right) = \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^\ast\left(\frac{s^2 - 4p}{f^2}\right) + \frac{1}{4} \sum_{[E]_{E_p} \in Ell_{E_p} \atop j(E) = 1728} a(E)^n + \frac{1}{3} \sum_{[E]_{E_p} \in Ell_{E_p} \atop j(E) = 0} a(E)^n.$$

Proof. The proof for primes $p \equiv 1 \pmod{12}$ is provided in [7, Lemma 5.3]. It can be adapted to hold for all $p > 3$ once one verifies that the following two identities remain true:

$$\sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right) = \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^\ast\left(\frac{s^2 - 4p}{f^2}\right)$$

$$\sum_{[E]_{E_p} \in Ell_{E_p} \atop j(E) = 1728} a(E)^n = \frac{1}{2} \sum_{[E]_{E_p} \in Ell_{E_p} \atop j(E) = 0} a(E)^n.$$

First consider (7). The proof given in [7] holds for all primes $p \equiv 1 \pmod{4}$. In light of Lemma 3.2, we must verify that if $p \equiv 3 \pmod{4}$, then

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

We verify this by proving that no $s, f$ exist to contribute to the sums. For, suppose $s, f \in \mathbb{Z}$ such that $0 < s < 2\sqrt{p}$ and $\frac{s^2 - 4p}{f^2} = -4$. Then $4|s^2$, so $s$ must be even. Substituting $s = 2r$ and rearranging gives $r^2 + f^2 = p$, which is not possible since $p \equiv 3 \pmod{4}$. This verifies (7) for the remaining primes.
We handle (8) in a similar way. The proof in [7] verifies the equation for \( p \equiv 1 \) (mod 3). Keeping in mind Lemma [3.3] we must prove that if \( p \equiv 2 \) (mod 3), then
\[
\sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell \atop \frac{s^2 - 4p}{f^2} = -3} 1 = 0.
\]
Suppose then that we have \( s, f \in \mathbb{Z} \) such that \( 0 < s < 2\sqrt{p} \) and \( \frac{s^2 - 4p}{f^2} = -3 \). Then \( 4p = 3f^2 + s^2 \) and hence \( p \equiv 2 \equiv s^2 \) (mod 3). However, since \( \left( \frac{3}{p} \right) = -1 \), this is impossible. This verifies (8) for the remaining primes and completes the proof of the lemma. \( \square \)

The following proposition generalizes [7, Prop. 5.4] by removing the restriction on the congruence class of \( p \) (mod 12).

**Proposition 3.5.** Let \( p > 3 \) be prime and \( n \geq 2 \) be even. Then
\[
\sum_{t=2}^{p-1} a(t, p)^n = \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^* \left( \frac{s^2 - 4p}{f^2} \right) - \alpha(n, p) - \gamma(n, p),
\]
where
\[
\alpha(n, p) = \begin{cases} 2^{n-1}(a^n + b^n) & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}, \end{cases}
\]
\[
\gamma(n, p) = \begin{cases} \frac{3}{2} [(c + d)^n + (2c - d)^n + (c - 2d)^n] & \text{if } p \equiv 1 \pmod{3}, \\ 0 & \text{if } p \equiv 2 \pmod{3}, \end{cases}
\]
and \( a, b, c, d \) are defined as in the statements of Lemmas [3.2] and [3.3].

**Proof.** The bulk of the proof the author provides for the \( p \equiv 1 \) (mod 12) case in [7, Prop. 5.4] holds for the other congruence classes of \( p \), so we give an outline here. Since \( j(E_2) = \frac{1728}{1} \), we have that
\[
\sum_{t=2}^{p-1} a(t, p)^n = \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; E/\mathbb{Q}_p \atop j(E) \neq 0, 1728} a(E)^n
\]
\[
= \frac{1}{2} \left[ \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 1728} a(E)^n - \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 0} a(E)^n \right].
\]
Regardless of the congruence class of \( p \) (mod 12), the first sum in the last line above can still be written in terms of class numbers by combining Hasse’s theorem with a theorem of Schoof [14, Thm. 4.6]. This results in
\[
\sum_{t=2}^{p-1} a(t, p)^n = \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^* \left( \frac{s^2 - 4p}{f^2} \right) - \frac{1}{2} \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 1728} a(E)^n - \frac{1}{2} \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 0} a(E)^n
\]
\[
= \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^* \left( \frac{s^2 - 4p}{f^2} \right) - \frac{1}{4} \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 1728} a(E)^n - \frac{1}{6} \sum_{[E]_{\mathbb{Q}_p} \in \mathcal{Ell}_{\mathbb{Q}_p}; j(E) = 0} a(E)^n.
\]
by Lemma \[\text{Lemma 3.4}\] One now applies Lemmas \[\text{3.2 and 3.3}\] in each appropriate congruence class to obtain the result.

With these tools in place, we now complete the proof of Theorem \[\text{2.1}\].

**Proof of Theorem 2.1** The proof proceeds in a similar fashion to the author’s proof of the \( p \equiv 1 \pmod{12} \) case in [7, Thm. 1.3], with a few modifications. We still begin with an application of Theorem \[\text{3.1}\] and then substitute the definition of \( G_k(s, p) \). This gives

\[
\begin{align*}
\text{Tr}_k(\Gamma, p) &= -1 - \frac{1}{2} \beta(p)(-p)^{\frac{k}{2} - 1} - (-p)^{\frac{k}{2} - 1} \sum_{0 < s < 2\sqrt{p}} 1 \sum_{f | \ell} h^s \left( \frac{s^2 - 4p}{f^2} \right) \\
&\quad - \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \sum_{0 < s < 2\sqrt{p}} s^{k - 2j} \sum_{f | \ell} h^s \left( \frac{s^2 - 4p}{f^2} \right).
\end{align*}
\]

Now, notice that the \( k = 2 \) case of Theorem \[\text{3.1}\] gives

\[
0 = p - \frac{1}{2} \beta(p) - \sum_{0 < s < 2\sqrt{p}} 1 \sum_{f | \ell} h^s \left( \frac{s^2 - 4p}{f^2} \right).
\]

Substituting and applying Proposition \[\text{3.5}\] with \( n = k - 2j - 2 \) gives

\[
\begin{align*}
\text{Tr}_k(\Gamma, p) &= -1 + (-p)^{\frac{k}{2} - 1} \cdot (-p) - \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \sum_{t=2}^{p-1} a(t, p)^{k-2j-2} \\
&\quad - \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \alpha(k - 2j - 2, p) \\
&\quad - \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \gamma(k - 2j - 2, p).
\end{align*}
\]

To complete the proof, we distribute the copies of \( (-p)^{\frac{k}{2} - 1} \) to the three summations in a specific way. Notice that

\[
(-p)^{\frac{k}{2} - 1}(-p) = -(-p)^{\frac{k}{2} - 1}(p - 2) - (-p)^{\frac{k}{2} - 1} - (-p)^{\frac{k}{2} - 1}.
\]

First, since \( G_2 = 1 \), we see that

\[
(-p)^{\frac{k}{2} - 1}(p - 2) - \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \sum_{t=2}^{p-1} a(t, p)^{k-2j-2} = - \sum_{t=2}^{p-1} G_k(a(t, p), p).
\]

A straightforward calculation for each of the congruence classes of \( p \pmod{12} \) verifies

\[
\lambda(k, p) = (-p)^{\frac{k}{2} - 1} + \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \alpha(k - 2j - 2, p) \\
+ (-p)^{\frac{k}{2} - 1} + \sum_{j=0}^{\frac{k}{2} - 2} (-1)^j \binom{k - 2 - j}{j} p^j \gamma(k - 2j - 2, p).
\]
4. Trace Formulas in Terms of Hypergeometric Functions

We now prove Theorems 2.3 and 2.4. As mentioned before, one essential tool is a theorem of Lennon, which writes the trace of Frobenius of any elliptic curve in Weierstrass form in terms of a finite field hypergeometric function:

**Theorem 4.1** ([11] Thm. 2.1). Let \( q = p^e \), where \( p > 3 \) is prime and \( q \equiv 1 \pmod{12} \). Let \( E : y^2 = x^3 + ax + b \) be an elliptic curve over \( \mathbb{F}_q \) in Weierstrass form with \( j(E) \neq 0, 1728 \). Then the trace of the Frobenius map on \( E \) can be expressed as

\[
a(E(\mathbb{F}_q)) = -q \cdot T^{\frac{q-1}{4}} \left( \frac{a^3}{27} \right) \cdot 2F1 \left( \frac{T^{\frac{q-1}{12}}}{2}, \frac{T^{\frac{5(q-1)}{12}}}{\varepsilon} \mid -\frac{27b^2}{4a^3} \right).
\]

We now specify this theorem to our family of curves.

**Corollary 4.2.** Let \( p > 3 \) be prime and \( q = p^e(p) \), where \( e(p) \) is defined as in (8). Then

\[
a(t, q) = -qT^{\frac{q-1}{4}}(2)T^{\frac{q-1}{4}}(1 - t)2F1 \left( \frac{T^{\frac{q-1}{12}}}{2}, \frac{T^{\frac{5(q-1)}{12}}}{\varepsilon} \mid t \right).
\]

To prove this corollary, we require a transformation law proved by Greene:

**Theorem 4.3** ([8] Thm 4.4(i)). If \( A, B, C \in \mathbb{F}^\times_q \) and \( x \in \mathbb{F}_q \setminus \{0, 1\} \), then

\[
2F1 \left( \frac{A}{B}, \frac{C}{x} \bigg| x \right)_q = A(-1)2F1 \left( \frac{A}{AB}, \frac{B}{ABC} \bigg| 1 - x \right)_q.
\]

**Proof of Corollary 4.2**. After putting \( E_t \) into Weierstrass form, we have \( a = b = \frac{-27}{4(1-t)} \) in Theorem 4.1. Then \( a^3 = \frac{-3^6}{4^3(1-t)^3} \) and \( -27b^2 = 1 - t \). Combining these simplifications with Greene’s theorem above gives

\[
(12) \quad a(t, q) = -qT^{\frac{q-1}{4}} \left( \frac{-3^6}{4^3(1-t)^3} \right) T^{\frac{q-1}{12}}(-1)T^{\frac{5(q-1)}{12}}(1 - t)2F1 \left( \frac{T^{\frac{q-1}{12}}}{2}, \frac{T^{\frac{5(q-1)}{12}}}{\varepsilon} \mid t \right).
\]

Now, using multiplicity and the fact that \( T \) has order \( q - 1 \), we have

\[
T^{\frac{q-1}{4}} \left( \frac{-3^6}{4^3(1-t)^3} \right) = T^{\frac{3(q-1)}{4}} \left( \frac{-9}{4(1-t)} \right) = T^{\frac{q-1}{4}} \left( \frac{4(1-t)}{-9} \right).
\]

\[
= T^{\frac{q-1}{4}}(2)T^{\frac{q-1}{4}}(1-t)T^{\frac{q-1}{4}}(-1)T^{\frac{5(q-1)}{12}}(3) = T^{\frac{q-1}{4}}(2)T^{\frac{q-1}{4}}(1-t)T^{\frac{q-1}{4}}(-1),
\]

since \( T^{\frac{q-1}{4}} \) is its own inverse and \( q \equiv 1 \pmod{12} \). The proof is completed by making this substitution for \( T^{\frac{q-1}{4}} \left( \frac{-3^6}{4^3(1-t)^3} \right) \) into (12) and noting that \( T^{\frac{q-1}{4}}(-1)T^{\frac{5(q-1)}{12}}(-1) = T^{\frac{q-1}{4}}(-1) = 1 \), since \(-1 = (-1)^3\) and \( T^{\frac{q-1}{4}} \) has order 3.

**Remark 4.4.** If \( e(p) = 1 \) (i.e. \( q = p \)), the above corollary precisely matches the author’s result ([7] Thm. 1.3).

**Remark 4.5.** Lennon gives another way of writing the trace of Frobenius in terms of a \( 2F1 \) function in ([11] Thm. 1.1), using the \( j \)-invariant and discriminant of \( E \). We use Lennon’s Theorem 2.1 because it leads to a simpler hypergeometric function in this instance.
We require two more tools to prove our trace theorems. First, note that whenever $e(p) = 2$ (i.e. $q = p^2$), Theorem 4.1 relates $a(t, p^2)$ to a hypergeometric function over $\mathbb{F}_{p^6}$. Even though our trace formula, Theorem 2.1, is in terms of $a(t, p)$, we can still gain new information, since

$$a(t, p^2)^2 = a(t, p^2) + 2p.$$  

The last tool is an inverse pair given in [13]. As in the statement of Theorems 2.3 and 2.4 we let $m = \frac{q}{2} - 1$ and also define $H_m(x) := \sum_{i=0}^{m} (\frac{m+i}{m-i}) x^i$. Then, as in [7], notice that

$$G_k(s, p) = (-p)^m H_m \left( \frac{-s^2}{p} \right).$$

Consider the inverse pair [13] p. 67 given by

$$\rho_n(x) = \sum_{k=0}^{n} \left( \frac{n+k}{n-k} \right) x^n, \quad x^n = \sum_{k=0}^{n} (-1)^{k+n} \left[ \binom{2n}{n-k} - \binom{2n}{n-k-1} \right] \rho_k(x).$$

Applying this to the definition of $H_m$, we see that

$$x^m = \sum_{i=0}^{m} (-1)^{i+m} \left[ \binom{2m}{m-i} - \binom{2m}{m-i-1} \right] H_i(x).$$

By combining (14) with the choice $x = \frac{-s^2}{p}$, we have

$$s^{2m} = \sum_{i=0}^{m} b_i G_{2i+2}(s, p),$$

where $b_i = p^{m-i} \left[ \binom{2m}{m-i} - \binom{2m}{m-i-1} \right]$. We may now prove Theorems 2.3 and 2.4

**Proof of Theorem 2.3** Recall that in the statement of this theorem, $p \equiv 5, 7, 11 \pmod{12}$, so $q = p^2$. By (14) and (13), we have

$$G_k(a(t, p), p) = (-p)^m H_m \left( \frac{-a(t, p)^2}{p} \right)$$

$$= (-p)^m H_m \left( \frac{-a(t, p^2)}{p} - 2 \right)$$

$$= (-p)^m H_m \left( \frac{pT^\frac{q-1}{2} T^\frac{q-1}{4} (1-t)q_2F_1 \left( T^\frac{q-1}{4}, \frac{T^\frac{q-1}{12}}{\varepsilon} | t \right)}{q} - 2 \right),$$

by Corollary 4.2. Combining this with Theorem 2.1 completes the proof.

**Proof of Theorem 2.4** Recall that $p > 3$ is any prime and $q = p^{e(p)}$, where $e(p)$ is defined as in [15]. The proof begins along the same lines as the proof of [7] Thm. 1.4. Beginning with Theorem 2.1 we have

$$\text{Tr}_{2(m+1)}(\Gamma, p) = -1 - \lambda(2m + 2, p) - \sum_{t=2}^{p-1} G_{2m+2}(a(t, p), p).$$

Now, (16) implies that

$$s^{2m} = \sum_{i=0}^{m} b_i G_{2i+2}(s, p) = G_{2m+2}(s, p) + \sum_{i=0}^{m-1} b_i G_{2i+2}(s, p).$$

We isolate $G_{2m+2}(s, p)$ and take $s = a(t, p)$. Substituting into (17) gives

$$\text{Tr}_{2(m+1)}(\Gamma, p) = -1 - \lambda(2m + 2, p) - \sum_{t=2}^{p-1} \left( a(t, p)^{2m} - \sum_{i=0}^{m-1} b_i G_{2i+2}(a(t, p), p) \right)$$

$$= -1 - \lambda(2m + 2, p) - \sum_{t=2}^{p-1} a(t, p)^{2m} + b_0(p - 2)$$

$$+ \sum_{i=1}^{m-1} b_i \sum_{t=2}^{p-1} G_{2i+2}(a(t, p), p)$$

$$= -1 - \lambda(2m + 2, p) - \sum_{t=2}^{p-1} a(t, p)^{2m} + b_0(p - 2)$$

$$- \sum_{i=1}^{m-1} b_i (\text{Tr}_{2i+2}(\Gamma, p) + 1 + \lambda(2i + 2, p)),$$

since $G_2 = 1$ and by again applying Theorem 2.1 for the last equality. To complete the proof, we consider $a(t, p)^{2m}$. If $e(p) = 1$ (i.e. $q = p$), then using either Corollary 4.2 or [7] Thm. 1.2, we have

$$a(t, p)^{2m} = \left( -q T^{\frac{r-1}{2}}(2) T^{\frac{s-1}{2}}(1 - t) \binom{2m}{T^{\frac{n-1}{12}} \binom{a}{12}}{t} \right),$$

so our result matches [7] Thm. 1.4 in this case.

If $e(p) = 2$ (i.e. $q = p^2$), then [13] gives

$$a(t, p)^{2m} = (a(t, p)^2)^m = (a(t, p^2) + 2p)^m$$

$$= \left( -q T^{\frac{r-1}{2}}(2) T^{\frac{s-1}{2}}(1 - t) \binom{2m}{T^{\frac{n-1}{12}} \binom{a}{12}}{t} + 2p \right)^m,$$

by Corollary 4.2.

The final statement of the theorem combines these two cases together, completing our proof. \qed

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. MR1872789 (2002h:11056)

[2] S. Ahlgren and K. Ono, Modularity of a certain Calabi-Yau threefold, Monatsh. Math. 129 (2000), no. 3, 177-190. MR1746757 (2001b:11059)

[3] S. Ahlgren and K. Ono, A Gaussian hypergeometric series evaluation and Apéry number congruences, J. reine angew. Math. 518 (2000), 187-212. MR1739404 (2001e:11057)

[4] B.J. Birch, How the number of points of an elliptic curve over a fixed prime field varies, J. London Math. Soc. 43 (1968), 57-60. MR0230682 (37:6242)

[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. MR2096220 (2006a:11055)

[6] J.G. Fuselier, Hypergeometric functions over finite fields and relations to modular forms and elliptic curves, Ph.D. Thesis, Texas A&M University, 2007. MR2710790

[7] J.G. Fuselier, Hypergeometric functions over $\mathbb{F}_p$ and relations to elliptic curves and modular forms. Proc. Amer. Math. Soc. 138 (2010), no. 1, 109-123. MR2550175 (2011c:11068)

[8] J. Greene, Hypergeometric functions over finite fields, Trans. Amer. Math. Soc. 301 (1987), no. 1, 77-101. MR879564 (88e:11122)
[9] 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 pp. MR 960090 (90d:11056)

[10] Ihara, Y., *Hecke Polynomials as congruence \( \zeta \) functions in elliptic modular case*, Ann. of Math. (2) **85** (1967), 267–295. MR 0207655 (34:7470)

[11] Lennon, C., *Gaussian hypergeometric evaluations and traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **139** (2011), no. 6, 1931-1938. MR 2775369 (2012c:11260)

[12] Lennon, C., *A Trace Formula for Certain Hecke Operators and Gaussian Hypergeometric Functions*, http://arxiv.org/abs/1003.1157v8.

[13] J. Riordan, *Combinatorial Identities*, John Wiley & Sons, New York, 1968. MR 0231725 (38:53)

[14] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory, Ser. A **46** (1987), no. 2, 183-211. MR 0914657 (88k:14013)

Department of Mathematics and Computer Science, High Point University, High Point, North Carolina 27262

*E-mail address*: jfuselie@highpoint.edu