PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 6, June 2011, Pages 1931–1938
S 0002-9939(2010)10609-3
Article electronically published on November 3, 2010

GAUSSIAN HYPERGEOMETRIC EVALUATIONS OF TRACES OF FROBENIUS FOR ELLIPTIC CURVES

CATHERINE LENNON

(Communicated by Matthew A. Papanikolas)

Abstract. We present here a formula for expressing the trace of the Frobenius endomorphism of an elliptic curve E over $\mathbb{F}_q$ satisfying $j(E) \neq 0, 1728$ and $q \equiv 1 \pmod{12}$ in terms of special values of Gaussian hypergeometric series. This paper uses methods introduced by Fuselier for one-parameter families of curves to express the trace of Frobenius of E as a function of its j-invariant and discriminant instead of a parameter, which are more intrinsic characteristics of the curve.

1. Introduction

Gaussian hypergeometric series were first defined by Greene in [4] as finite field analogues of the classical hypergeometric series. Since then, they have been shown to possess interesting arithmetic properties; in particular, special values of these functions can be used to express the number of $\mathbb{F}_p$-points on certain varieties. For example, results in [8] and [12] presented formulas expressing the number of $\mathbb{F}_p$-points of elliptic curves in certain families as special values of Gaussian hypergeometric series. These formulas, however, only used trivial and quadratic characters as parameters, and the task remained to find some expressions with parameters that were characters of higher orders [11].

Recently in [3], Fuselier provided formulas for certain families of elliptic curves which involved Gaussian hypergeometric series with characters of order 12 as parameters, under the assumption that $p \equiv 1 \pmod{12}$ (which is necessary to assure that characters of order 12 exist). In [10], we provide a formula for the trace of Frobenius for curves with 3-torsion and j-invariant not equal to 0, 1728 using characters of order three. Again, we must assume that $p \equiv 1 \pmod 3$.

In all of the previous results, the character parameters in the hypergeometric series depended on the family of curves considered. In addition, the values at which the hypergeometric series were evaluated were functions of the coefficients and so depended on the model used. Here, we give a general formula expressing the number of $\mathbb{F}_p$-points of an elliptic curve in terms of more intrinsic properties of the curve. Consequently, this characterization is coordinate-free and can be used to describe the number of points on any elliptic curve $E(\mathbb{F}_{p^e})$, with $j(E) \neq 0, 1728$ and

Received by the editors March 22, 2010 and, in revised form, May 28, 2010.

2010 *Mathematics Subject Classification.* Primary 11T24, 11G20.

This work was supported by the Department of Defense (DoD) through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program.

$p^e \equiv 1 \pmod{12}$ without having to put the curve in a specific form. In particular, the formula holds over $\mathbb{F}_{p^2}$ for all odd p whenever $j \neq 0, 1728$.

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

$$\binom{A}{B} := \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x)\bar{B}(1-x) = \frac{B(-1)}{q} J(A, \bar{B}), \tag{1.1}$$

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

Recall the definition of the *Gaussian hypergeometric series over* $\mathbb{F}_q$ first defined by Greene in [4]. For any positive integer n and characters $A_0, A_1, ..., A_n$ and $B_1, B_2, ..., B_n \in \widehat{\mathbb{F}_q^*}$, the Gaussian hypergeometric series ${}_{n+1}F_n$ is defined to be

(1.2)
$${}_{n+1}F_n\left(\begin{matrix} A_0 & A_1 & ... & A_n \\ & B_1 & ... & B_n \end{matrix} \,\middle|\, x\right)_q := \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x).$$

See also Katz [7] (in particular Section 8.2) for more information on how these sums naturally arise as the traces of Frobenius at closed points of certain ℓ-adic hypergeometric sheaves.

If we let $a(E(\mathbb{F}_q))$ denote the trace of the Frobenius endomorphism on E, then

$$a(E(\mathbb{F}_q)) = q + 1 - |E(\mathbb{F}_q)|$$

and the following theorem expresses this value, and therefore also $|E(\mathbb{F}_q)|$, in terms of Gaussian hypergeometric series.

Theorem 1.1. *Let $q = p^e$, $p > 0$ a prime and $q \equiv 1 \pmod{12}$. In addition, let E be an elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$ and $T \in \widehat{\mathbb{F}_q^*}$ a generator of the character group. The trace of the Frobenius map on E can be expressed as*

$$a(E(\mathbb{F}_q)) = -q \cdot T^{\frac{q-1}{12}}\left(\frac{1728}{\Delta(E)}\right) \cdot {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{12}} & T^{\frac{q-1}{12}} \\ & T^{\frac{2(q-1)}{3}} \end{matrix} \,\middle|\, \frac{j(E)}{1728}\right)_q, \tag{1.3}$$

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

Remark 1.2. It should be noted that the discriminant of the curve, $\Delta(E)$, appears in the formula for the trace of Frobenius above. Although the discriminant itself depends on the Weierstrass model, isomorphic curves will differ by a twelfth power of an element of $\mathbb{F}_q$. Since the discriminant only appears as the argument of a character of order 12, the discriminants of isomorphic curves will output the same value, so the formula is indeed independent of the Weierstrass model.

Remark 1.3. When $p \not\equiv 1 \pmod{12}$, information about $a(E(\mathbb{F}_p))$ can still be gained from Theorem 1.1. Because $p^2 \equiv 1 \pmod{12}$ for all $p > 3$, Theorem 1.1 applies with $q = p^2$. Using the relationship

$$a(E(\mathbb{F}_p))^2 = a(E(\mathbb{F}_{p^2})) + 2p,$$

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

2. Proof of Theorem 1.1

2.1. **Elliptic curves in Weierstrass form.** Theorem 1.1 will follow as a consequence of the next proposition after applying transformation laws for Gaussian hypergeometric series. Recall that in characteristic not 2 or 3 an elliptic curve can be written in Weierstrass form as

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

We prove the following theorem:

Theorem 2.1. *Let $q = p^e$, $p > 3$ a prime and $q \equiv 1 \pmod{12}$. Let $E(\mathbb{F}_q)$ 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*

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

This theorem extends Proposition III.2.4 of [2] to elliptic curves in the form given above, and the method of proof follows similarly to that given in [3].

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

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

then $|E(\mathbb{F}_q)|$ may be expressed as

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

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

$$\theta(\alpha) = \zeta^{\operatorname{tr}(\alpha)} \tag{2.1}$$

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

$$G_m := G(T^m) = \sum_{x \in \mathbb{F}_q} T^m(x)\theta(x). \tag{2.2}$$

As in [3], we begin by repeatedly using the elementary identity from [6],

$$\sum_{z \in \mathbb{F}_q} \theta(zP(x, y)) = \begin{cases} q & \text{if } P(x, y) = 0, \\ 0 & \text{if } P(x, y) \neq 0, \end{cases} \tag{2.3}$$

to express the number of points as

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

We will evaluate each of these labeled terms using the following lemma from [3].

Lemma 2.2 ([3, Lemma 3.3])**.** *For all $\alpha \in \mathbb{F}_q^*$,*

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

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

Since Lemma 2.2 holds only when the parameter is nonzero, we require that $a \neq 0$ and $b \neq 0$, or equivalently $j(E) \neq 0, 1728$. For A we have

$$A = \frac{1}{q-1}\sum_i G_{-i}T^i(b)\sum_z T^i(z) = G_0 = -1,$$

where the second equality follows from the fact that the innermost sum is 0 unless $i = 0$, at which it is $q-1$. Similarly,

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

and the inner sums here are nonzero only when $2j = 0$ and $j = -i$. Plugging in these values gives

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

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

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

Finally, we expand D:

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

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

$$\frac{1}{(q-1)^3}\sum_{i,j,k} G_{-i}G_{-j}G_{-k}G_0T^j(a)T^k(b)\sum_z T^{i+j+k}(z)\sum_x T^{3i+j}(x),$$

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

$$D_{\frac{q-1}{2}} := \frac{1}{q-1}\sum_i G_{-i}G_{3i}G_{-\frac{q-1}{2}-2i}G_{\frac{q-1}{2}}T^{-3i}(a)T^{\frac{q-1}{2}+2i}(b)T^{\frac{q-1}{2}}(-1), \tag{2.4}$$

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

$$q(|E(\mathbb{F}_q)| - 1) = q^2 + q \cdot T^{\frac{q-1}{2}}(b) + \frac{\sqrt{q}}{q-1}\sum_i G_{-i}G_{3i}G_{-\frac{q-1}{2}-2i}T^{-3i}(a)T^{\frac{q-1}{2}+2i}(b). \tag{2.5}$$

Now we expand G_{3i} and $G_{-\frac{q-1}{2}-2i} = G_{-2(\frac{q-1}{4}+i)}$ using the Davenport-Hasse relation from [9].

Theorem 2.3 (Davenport-Hasse Relation [9])**.** *Let m be a positive integer and let $q = p^e$ be a prime power such that $q \equiv 1 \pmod{m}$. Let θ be the additive character on $\mathbb{F}_q$ defined by $\theta(\alpha) = \zeta^{tr\alpha}$, where $\zeta = e^{2\pi i/p}$. For multiplicative characters $\chi, \psi \in \widehat{\mathbb{F}}_q^*$ we have*

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

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

Theorem 2.4 (Davenport-Hasse for $q \equiv 1 \pmod 3$)**.** *If $k \in \mathbb{Z}$ and q satisfies $q \equiv 1 \pmod 3$, then*

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

Theorem 2.5 (Davenport-Hasse for $q \equiv 1 \pmod 2$)**.** *If $k \in \mathbb{Z}$ and q satisfies $q \equiv 1 \pmod 2$, then*

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

We may then write

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

Plugging this into (2.4) gives

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

In order to write $a(E(\mathbb{F}_q))$ as a finite field hypergeometric function, we use the fact that if $T^{m-n} \neq \epsilon$, then

$$\binom{T^m}{T^n} = \frac{G_m G_{-n} T^n(-1)}{G_{m-n}q}. \tag{2.6}$$

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

Now use (2.6) to write

$$G_{i+\frac{q-1}{3}}G_{-i-\frac{q-1}{4}} = \binom{T^{i+\frac{q-1}{3}}}{T^{i+\frac{q-1}{4}}} G_{\frac{q-1}{12}} qT^{i+\frac{q-1}{4}}(-1), \tag{2.7}$$

$$G_{i+\frac{2(q-1)}{3}}G_{-i-\frac{3(q-1)}{4}} = \binom{T^{i+\frac{2(q-1)}{3}}}{T^{i+\frac{3(q-1)}{4}}} G_{-\frac{q-1}{12}} qT^{i+\frac{3(q-1)}{4}}(-1), \tag{2.8}$$

and plugging in (2.7), (2.8) gives

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

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

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

Next, we eliminate the G_iG_{-i} term. If $i \neq 0$, then $G_iG_{-i} = qT^i(-1)$, and if $i = 0$, then $G_iG_{-i} = 1 = qT^i(-1) - (q-1)$. Plugging in the appropriate identities for each i we may write (2.4) as

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

By (2.6) we have

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

and so the second term reduces to $-\frac{T^{\frac{q-1}{2}}(b)T^{\frac{q-1}{4}}(-1)q}{T^{\frac{q-1}{4}}(4)}$. Equation (2.4) becomes

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

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

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

Putting this all together then gives

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

Equivalently,

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

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

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

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

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

2.2. **Hypergeometric transformation laws and the proof of Theorem 1.1.** We now prove Theorem 1.1 as a consequence of Theorem 2.1 and the following transformation laws found in [4] given here for the special case of ${}_2F_1$ functions.

Theorem 2.6 ([4, Theorem 4.4(i)]). *For characters A, B, C of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$, $x \neq 0, 1$,*

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

Theorem 2.7 ([4, Theorem 4.2(ii)]). *For characters A, B, C of $\mathbb{F}_q$ and $x \in \mathbb{F}_q^*$,*

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

Proof of Theorem 1.1. We begin by noting that we may apply Theorem 2.6 to the expression in Theorem 2.1 because the parameter $-\frac{27b^2}{4a^3}$ will equal 1 if and only if the discriminant of E is 0, which we exclude. Similarly, it will equal 0 if and only if $b = 0$, in which case $j = 1728$, and we exclude this case as well. So we begin by applying Theorem 2.6 to obtain the expression

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

Applying Theorem 2.7 to this then gives

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

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

References

1. 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)
2. J. Fuselier, *Hypergeometric functions over finite fields and relations to modular forms and elliptic curves*, Ph.D. thesis, Texas A&M University, 2007.
3. J. Fuselier, *Hypergeometric functions over $\mathbb{F}_p$ and relations to elliptic curves and modular forms*, Proc. Amer. Math. Soc. **138** (2010), 109-123. MR2550175
4. J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77-101. MR879564 (88e:11122)
5. Y. Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case*, Ann. of Math. **85** (1967), no. 2, 267-295. MR0207655 (34:7470)
6. 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. MR1070716 (92e:11001)
7. N. Katz, *Exponential Sums and Differential Equations*, Princeton University Press, Princeton, NJ, 1990. MR1081536 (93a:14009)
8. M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. **25** (1995), no. 1, 43-52. MR1322601 (96b:11079)
9. S. Lang, *Cyclotomic Fields. I and II*, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990. MR1029028 (91c:11001)
10. C. Lennon, *A Trace Formula for Certain Hecke Operators and Gaussian Hypergeometric Functions*, http://arxiv.org/abs/1003.1157.
11. K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS, 102, Amer. Math. Soc., Providence, RI, 2004. MR2020489 (2005c:11053)
12. K. Ono, *Values of Gaussian Hypergeometric Series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205-1223. MR1407498 (98e:11141)
13. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139

E-mail address: `clennon@math.mit.edu`