PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 10, October 2013, Pages 3403–3410
S 0002-9939(2013)11617-5
Article electronically published on June 21, 2013

HYPERGEOMETRIC FUNCTIONS OVER $\mathbb{F}_q$ AND TRACES OF FROBENIUS FOR ELLIPTIC CURVES

RUPAM BARMAN AND GAUTAM KALITA

(Communicated by Ken Ono)

Abstract. We present explicit relations between the traces of Frobenius endomorphisms of certain families of elliptic curves and special values of ${}_2F_1$-hypergeometric functions over $\mathbb{F}_q$ for $q \equiv 1 (\text{mod } 6)$ and $q \equiv 1 (\text{mod } 4)$.

1. Introduction and statement of results

In this paper, we consider the problem of expressing traces of Frobenius endomorphisms of certain families of elliptic curves in terms of hypergeometric functions over finite fields. In [4], Greene introduced the notion of hypergeometric functions over finite fields, or the *Gaussian hypergeometric series*, which are analogous to the classical hypergeometric series. Since then, many interesting relations between special values of these functions and the number of $\mathbb{F}_p$-points on certain varieties have been obtained. For example, Koike [6] and Ono [10] gave formulas for the number of $\mathbb{F}_p$-points on elliptic curves in terms of special values of the Gaussian hypergeometric series. Also, in [1, 2] the authors studied this problem for certain families of algebraic curves.

Recently in [3], Fuselier gave formulas for the trace of Frobenius of certain families of elliptic curves which involved the Gaussian hypergeometric series with characters of order 12 as parameters under the assumption that $p \equiv 1 (\text{mod } 12)$. In [8], Lennon provided a general formula expressing the number of $\mathbb{F}_q$-points of an elliptic curve E with $j(E) \neq 0, 1728$ in terms of values of Gaussian hypergeometric series for $q = p^e \equiv 1 (\text{mod } 12)$. In [9], for $q \equiv 1 (\text{mod } 3)$, Lennon also gave formulas for certain elliptic curves involving the Gaussian hypergeometric series with characters of order 3 as parameters.

We begin with some preliminary definitions needed to state our results. Let $q = p^e$ be a power of an odd prime and $\mathbb{F}_q$ the finite field of q elements. Extend each character $\chi \in \widehat{\mathbb{F}_q^\times}$ to all of $\mathbb{F}_q$ by setting $\chi(0) := 0$. If A and B are two

Received by the editors August 19, 2011 and, in revised form, December 21, 2011.

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

Key words and phrases. Gaussian hypergeometric series, elliptic curves, Frobenius endomorphisms.

The first author thanks the Mathematical Institute, University of Heidelberg and Mathematics Center Heidelberg (MATCH), where the majority of this research was conducted. He is grateful to John H. Coates, R. Sujatha, Otmar Venjakob, and Anupam Saikia for their encouragement.

The second author was partially supported by an INSPIRE Fellowship of the Department of Science and Technology, Goverment of India.

Finally, the authors thank Ken Ono and the referee for helpful comments.

characters of $\mathbb{F}_q^\times$, then $\binom{A}{B}$ is defined by

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

where $J(A, B)$ denotes the usual Jacobi sum and $\overline{B}$ is the inverse of B.

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 $A_0, A_1, \ldots, A_n$ and $B_1, B_2, \ldots, B_n \in \widehat{\mathbb{F}_q^\times}$, the Gaussian hypergeometric series ${}_{n+1}F_n$ is defined to be

(1.2)
$$ {}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \cdots, & A_n \\ & B_1, & \cdots, & B_n \end{matrix} \mid x \right) := \frac{q}{q-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x),$$

where the sum is over all characters χ of $\mathbb{F}_q^\times$.

Throughout the paper, we consider an elliptic curve $E_{a,b}$ over $\mathbb{F}_q$ in Weierstrass form as

$$E_{a,b} : y^2 = x^3 + ax + b. \tag{1.3}$$

If we denote by $a_q(E_{a,b})$ the trace of the Frobenius endomorphism on $E_{a,b}$, then

$$a_q(E_{a,b}) = q + 1 - \#E_{a,b}(\mathbb{F}_q), \tag{1.4}$$

where $\#E_{a,b}(\mathbb{F}_q)$ denotes the number of $\mathbb{F}_q$-points on $E_{a,b}$ including the point at infinity. In the following theorems, we express $a_q(E_{a,b})$ in terms of the Gaussian hypergeometric series.

Theorem 1.1. *Let $q = p^e$, $p > 0$, be a prime and $q \equiv 1$ (mod 6). In addition, let a be non-zero and $(-a/3)$ be a quadratic residue modulo q. If $T \in \widehat{\mathbb{F}_q^\times}$ is a generator of the character group, then the trace of the Frobenius on $E_{a,b}$ can be expressed as*

$$a_q(E_{a,b}) = -qT^{\frac{q-1}{2}}(-k)\ {}_2F_1 \left(\begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \epsilon \end{matrix} \mid -\frac{k^3 + ak + b}{4k^3} \right),$$

where ϵ is the trivial character of $\mathbb{F}_q$ and $k \in \mathbb{F}_q$ satisfies $3k^2 + a = 0$.

Theorem 1.2. *Let $q = p^e$, $p > 0$, be a prime, $q \neq 9$ and $q \equiv 1$ (mod 4). Also assume that $x^3 + ax + b = 0$ has a non-zero solution in $\mathbb{F}_q$ and $T \in \widehat{\mathbb{F}_q^\times}$ is a generator of the character group. The trace of the Frobenius on $E_{a,b}$ can be expressed as*

$$a_q(E_{a,b}) = -qT^{\frac{q-1}{2}}(6h)T^{\frac{q-1}{4}}(-1)\ {}_2F_1 \left(\begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ & \epsilon \end{matrix} \mid \frac{12h^2 + 4a}{9h^2} \right),$$

where ϵ is the trivial character of $\mathbb{F}_q$ and $h \in \mathbb{F}_q^\times$ satisfies $h^3 + ah + b = 0$.

2. Preliminaries

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

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

where $\zeta = e^{2\pi i/p}$ and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_q$ is the trace map given by

$$\mathrm{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{e-1}}.$$

For $A \in \widehat{\mathbb{F}_q^{\times}}$, the *Gauss sum* is defined by

$$G(A) := \sum_{x \in \mathbb{F}_q} A(x)\zeta^{\operatorname{tr}(x)} = \sum_{x \in \mathbb{F}_q} A(x)\theta(x). \tag{2.2}$$

We let T denote a fixed generator of $\widehat{\mathbb{F}_q^{\times}}$. We also denote by G_m the Gauss sum $G(T^m)$.

The *orthogonality relations* for multiplicative characters are listed in the following lemma.

Lemma 2.1 ([5], Chapter 8). *Let ϵ be the trivial character. Then*

(1) $\sum_{x \in \mathbb{F}_q} T^n(x) = \begin{cases} q-1 & \text{if } T^n = \epsilon; \\ 0 & \text{if } T^n \neq \epsilon. \end{cases}$

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

Using orthogonality, we have the following lemma.

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

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

The following two lemmas on the Gauss sum will be useful in the proof of our results.

Lemma 2.3 ([4], Eqn. 1.12). *If $i \in \mathbb{Z}$ and $T^i \neq \epsilon$, then*

$$G_i G_{-i} = qT^i(-1).$$

Lemma 2.4 (Davenport-Hasse Relation [7]). *Let m be a positive integer and let $q = p^e$ be a prime power such that $q \equiv 1 (mod\ m)$. For multiplicative characters $\chi, \psi \in \widehat{\mathbb{F}_q^{\times}}$, we have*

$$\prod_{\chi^m = 1} G(\chi\psi) = -G(\psi^m)\psi(m^{-m}) \prod_{\chi^m=1} G(\chi). \tag{2.3}$$

3. Proof of the results

Theorem 1.1 will follow as a consequence of the next theorem. We consider an elliptic curve E_1 over $\mathbb{F}_q$ in the form

$$E_1 : y^2 = x^3 + cx^2 + d, \tag{3.1}$$

where $c \neq 0$. The trace of the Frobenius endomorphism on E_1 is given by

$$a_q(E_1) = q + 1 - \#E_1(\mathbb{F}_q). \tag{3.2}$$

We express the trace of Frobenius on the curve E_1 as a special value of a hypergeometric function in the following way.

Theorem 3.1. *Let $q = p^e$, $p > 0$ a prime and $q \equiv 1$ $(mod\ 6)$. If $T \in \widehat{\mathbb{F}_q^{\times}}$ is a generator of the character group, then the trace of the Frobenius on E_1 is given by*

$$a_q(E_1) = -qT^{\frac{q-1}{2}}(-3c)\ {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \epsilon \end{matrix} \mid -\frac{27d}{4c^3} \right),$$

where ϵ is the trivial character of $\mathbb{F}_q$.

Proof. The method of this proof follows similarly to that given in [3]. Let

$$P(x,y)=x^3+cx^2+d-y^2$$

and denote by $\#E_1(\mathbb{F}_q)$ the number of points on the curve E_1 over $\mathbb{F}_q$ including the point at infinity. Then

$$\#E_1(\mathbb{F}_q)-1=\#\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q : P(x,y)=0\}.$$

Using the elementary identity from [5],

$$\sum_{z\in\mathbb{F}_q}\theta(zP(x,y))=\begin{cases} q & \text{if } P(x,y)=0;\\ 0 & \text{if } P(x,y)\neq 0,\end{cases}\tag{3.3}$$

we obtain

$$\begin{aligned}
&q\cdot(\#E_1(\mathbb{F}_q)-1)\\
&\quad=\sum_{x,y,z\in\mathbb{F}_q}\theta(zP(x,y))\\
&\quad=q^2+\sum_{z\in\mathbb{F}_q^\times}\theta(zd)+\sum_{y,z\in\mathbb{F}_q^\times}\theta(zd)\theta(-zy^2)\\
&\qquad+\sum_{x,z\in\mathbb{F}_q^\times}\theta(zd)\theta(zx^3)\theta(zcx^2)+\sum_{x,y,z\in\mathbb{F}_q^\times}\theta(zd)\theta(zx^3)\theta(zcx^2)\theta(-zy^2)\\
&\quad:=q^2+A+B+C+D. \qquad (3.4)
\end{aligned}$$

Now using Lemma 2.2 and then applying Lemma 2.1 repeatedly for each term of (3.4), we deduce that

$$A=\frac{1}{q-1}\sum_{z\in\mathbb{F}_q^\times}\sum_{l=0}^{q-2}G_{-l}T^l(zd)=\frac{1}{q-1}\sum_{l=0}^{q-2}G_{-l}T^l(d)\sum_{z\in\mathbb{F}_q^\times}T^l(z)=G_0=-1.$$

Similarly,

$$\begin{aligned}
B&=\frac{1}{(q-1)^2}\sum_{l,m=0}^{q-2}G_{-l}G_{-m}T^l(d)T^m(-1)\sum_{y\in\mathbb{F}_q^\times}T^{2m}(y)\sum_{z\in\mathbb{F}_q^\times}T^{l+m}(z)\\
&=1+G_{\frac{q-1}{2}}G_{-\frac{q-1}{2}}T^{\frac{q-1}{2}}(d)T^{\frac{q-1}{2}}(-1).
\end{aligned}$$

Using Lemma 2.3 for $i=\frac{q-1}{2}$, we deduce that

$$\begin{aligned}
B&=1+qT^{\frac{q-1}{2}}(-1)T^{\frac{q-1}{2}}(d)T^{\frac{q-1}{2}}(-1)\\
&=1+qT^{\frac{q-1}{2}}(d).
\end{aligned}$$

Expanding the next term, we have

$$C=\frac{1}{(q-1)^3}\sum_{l,m,n=0}^{q-2}G_{-l}G_{-m}G_{-n}T^l(d)T^n(c)\sum_{z\in\mathbb{F}_q^\times}T^{l+m+n}(z)\sum_{x\in\mathbb{F}_q^\times}T^{3m+2n}(x).$$

Finally,

$$D = \frac{1}{(q-1)^4} \sum_{l,m,n,k=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{-k}T^l(d)T^n(c)T^k(-1)$$
$$\times \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+k}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+2n}(x) \sum_{z \in \mathbb{F}_q^\times} T^{2k}(z).$$

The innermost sum of D is non-zero only when $k = 0$ or $k = \frac{q-1}{2}$. Using the fact that $G_0 = -1$, we obtain

$$D = -C + D_{\frac{q-1}{2}},$$

where

$$D_{\frac{q-1}{2}} = \frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{\frac{q-1}{2}}T^l(d)T^n(c)T^{\frac{q-1}{2}}(-1)$$
$$\times \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+\frac{q-1}{2}}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+2n}(x),$$

which is zero unless $m = -\frac{2}{3}n$ and $n = -3l - \frac{3(q-1)}{2}$. Since $G_{3l+\frac{3(q-1)}{2}} = G_{3l+\frac{q-1}{2}}$ and $G_{-2l-(q-1)} = G_{-2l}$, we have

$$D_{\frac{q-1}{2}} = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l}G_{-2l}G_{3l+\frac{q-1}{2}}G_{\frac{(q-1)}{2}}T^l(d)T^{-3l+\frac{q-1}{2}}(c)T^{\frac{q-1}{2}}(-1).$$

Using the Davenport-Hasse relation (Lemma 2.4) for $m = 2, \psi = T^{-l}$ and $m = 3, \psi = T^{l+\frac{q-1}{6}}$ respectively, we deduce that

$$G_{-2l} = \frac{G_{-l}G_{-l-\frac{q-1}{2}}}{G_{\frac{q-1}{2}}T^l(4)} \quad \text{and} \quad G_{3l+\frac{q-1}{2}} = \frac{G_{l+\frac{q-1}{6}}G_{l+\frac{q-1}{2}}G_{l+\frac{5(q-1)}{6}}}{qT^{-l-\frac{q-1}{6}}(27)}.$$

Therefore,

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(-3c)}{q(q-1)} \sum_{l=0}^{q-2} G_{-l}G_{-l}G_{-l-\frac{q-1}{2}}G_{l+\frac{q-1}{6}}G_{l+\frac{q-1}{2}}G_{l+\frac{5(q-1)}{6}}T^l\left(\frac{27d}{4c^3}\right).$$

Now, if $T^{m-n} \neq \epsilon$, then we have

$$G_mG_{-n} = q\binom{T^m}{T^n}G_{m-n}T^n(-1). \tag{3.5}$$

Replacing l by $l - \frac{q-1}{2}$ and using (3.5), we obtain

$$D_{\frac{q-1}{2}} = \frac{qT^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} G_lG_{-l}\binom{T^{l-\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}}G_{\frac{q-1}{6}}\binom{T^{l+\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}}G_{\frac{5(q-1)}{6}}T^{l-\frac{q-1}{2}}\left(\frac{27d}{4c^3}\right).$$

Plugging the facts that if $l \neq 0$, then $G_l G_{-l} = qT^l(-1)$ and if $l = 0$, then $G_l G_{-l} = qT^l(-1) - (q-1)$ into the appropriate identities for each l, we deduce that

$$\begin{aligned} D_{\frac{q-1}{2}} = {} & \frac{q^3 T^{\frac{q-1}{6}}(-1) T^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} \binom{T^{l-\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}} \binom{T^{l+\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}} T^{l-\frac{q-1}{2}}\left(\frac{27d}{4c^3}\right) T^l(-1) \\ & - q^2 T^{\frac{q-1}{6}}(-1) T^{\frac{q-1}{2}}(-3c) \binom{T^{\frac{2(q-1)}{3}}}{T^{\frac{q-1}{2}}} \binom{T^{\frac{q-1}{3}}}{T^{\frac{q-1}{2}}} T^{\frac{q-1}{2}}\left(\frac{27d}{4c^3}\right). \end{aligned}$$

Replacing l by $l + \frac{q-1}{2}$ in the first term and simplifying the second term, we obtain

$$\begin{aligned} D_{\frac{q-1}{2}} = {} & \frac{q^3 T^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} \binom{T^{l+\frac{q-1}{6}}}{T^l} \binom{T^{l+\frac{5(q-1)}{6}}}{T^l} T^l\left(-\frac{27d}{4c^3}\right) \\ & - q^2 T^{\frac{q-1}{2}}(d) \frac{G_{\frac{2(q-1)}{3}} G_{\frac{q-1}{2}} G_{\frac{q-1}{3}} G_{\frac{q-1}{2}}}{q^2 G_{\frac{q-1}{6}} G_{\frac{5(q-1)}{6}}} \\ = {} & q^2 T^{\frac{q-1}{2}}(-3c) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \epsilon \end{matrix} \mid -\frac{27d}{4c^3}\right) - qT^{\frac{q-1}{2}}(d). \end{aligned}$$

Putting the values of A, B, C, D all together in (3.4) gives

$$q \cdot (\#E_1(\mathbb{F}_q) - 1) = q^2 + q^2 T^{\frac{q-1}{2}}(-3c) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \epsilon \end{matrix} \mid -\frac{27d}{4c^3}\right).$$

Since $a_q(E_1) = q + 1 - \#E_1(\mathbb{F}_q)$, we have completed the proof of the theorem. □

Proof of Theorem 1.1. Since $a \neq 0$ and $(-a/3)$ is quadratic residue modulo q, we find $k \in \mathbb{F}_q^\times$ such that $3k^2 + a = 0$. A change of variables $(x, y) \mapsto (x + k, y)$ takes the elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ to

$$E'_{a,b} : y^2 = x^3 + 3kx^2 + (k^3 + ak + b). \tag{3.6}$$

Clearly $a_q(E_{a,b}) = a_q(E'_{a,b})$. Since $3k \neq 0$, using Theorem 3.1 for the elliptic curve $E'_{a,b}$, we complete the proof. □

We now prove a result for $q \equiv 1 (\text{mod } 4)$ similar to Theorem 3.1, and Theorem 1.2 will follow from this result.

Theorem 3.2. *Let $q = p^e$, $p > 0$, be a prime and $q \equiv 1$ $(mod\ 4)$. Let E_2 be an elliptic curve over $\mathbb{F}_q$ defined as*

$$E_2 : y^2 = x^3 + fx^2 + gx$$

such that $f \neq 0$. If $T \in \widehat{\mathbb{F}_q^\times}$ is a generator of the character group, then the trace of the Frobenius on E_2 is given by

$$a_q(E_2) = -qT^{\frac{q-1}{2}}(2f) T^{\frac{q-1}{4}}(-1) {}_2F_1\left(\begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ & \epsilon \end{matrix} \mid \frac{4g}{f^2}\right),$$

where ϵ is the trivial character of $\mathbb{F}_q$.

Proof. We have

$$\#E_2(\mathbb{F}_q) - 1 = \#\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x, y) = 0\},$$

where

$$P(x, y) = x^3 + fx^2 + gx - y^2.$$

Using (3.3), we express the number of points as

$$\begin{aligned} q\cdot(\#E_2(\mathbb{F}_q)-1) &= \sum_{x,y,z\in\mathbb{F}_q}\theta(zP(x,y)) \\ &= q^2+\sum_{z\in\mathbb{F}_q^\times}\theta(0)+\sum_{y,z\in\mathbb{F}_q^\times}\theta(-zy^2)+\sum_{x,z\in\mathbb{F}_q^\times}\theta(zx^3)\theta(zfx^2)\theta(zgx) \\ &\quad+\sum_{x,y,z\in\mathbb{F}_q^\times}\theta(zx^3)\theta(zfx^2)\theta(zgx)\theta(-zy^2) \\ &:= q^2+(q-1)+A+B+C. \end{aligned} \tag{3.7}$$

Now, following the same procedure as in the proof of Theorem (3.1), we deduce that

$$\begin{aligned} A &= -(q-1), \\ B &= \frac{1}{(q-1)^3}\sum_{l,m,n=0}^{q-2}G_{-l}G_{-m}G_{-n}T^m(f)T^n(g)\sum_{z\in\mathbb{F}_q^\times}T^{l+m+n}(z)\sum_{x\in\mathbb{F}_q^\times}T^{3l+2m+n}(x), \\ C &= -\frac{1}{(q-1)^3}\sum_{l,m,n=0}^{q-2}G_{-l}G_{-m}G_{-n}T^m(f)T^n(g)\sum_{z\in\mathbb{F}_q^\times}T^{l+m+n}(z)\sum_{x\in\mathbb{F}_q^\times}T^{3l+2m+n}(x) \\ &\quad+\frac{1}{(q-1)^3}\sum_{l,m,n=0}^{q-2}G_{-l}G_{-m}G_{-n}G_{\frac{q-1}{2}}T^m(f)T^n(g)\sum_{z\in\mathbb{F}_q^\times}T^{l+m+n+\frac{q-1}{2}}(z) \\ &\quad\times\sum_{x\in\mathbb{F}_q^\times}T^{3l+2m+n}(x). \end{aligned}$$

Substituting the values of A, B, C all together in (3.7) and simplifying after using Lemma 2.1, we obtain

$$q\cdot(\#E_2(\mathbb{F}_q)-1)=q^2+\frac{G_{\frac{q-1}{2}}T^{\frac{q-1}{2}}(f)}{q-1}\sum_{l=0}^{q-2}G_{-l}G_{2l+\frac{q-1}{2}}G_{-l}T^l\left(\frac{g}{f^2}\right). \tag{3.8}$$

The Davenport-Hasse relation (Lemma 2.4) with $m=2,\psi=T^{l+\frac{q-1}{4}}$ yields

$$G_{2l+\frac{q-1}{2}}=\frac{G_{l+\frac{q-1}{4}}G_{l+\frac{3(q-1)}{4}}}{G_{\frac{q-1}{2}}}T^{l-\frac{q-1}{4}}(4). \tag{3.9}$$

Using (3.9) and then (3.5) in (3.8), we have

$$\begin{aligned} q\cdot(\#E_2(\mathbb{F}_q)-1) &= q^2+\frac{q^3T^{\frac{q-1}{2}}(2f)T^{\frac{q-1}{4}}(-1)}{q-1}\sum_{l=0}^{q-2}\binom{T^{l+\frac{q-1}{4}}}{T^l}\binom{T^{l+\frac{3(q-1)}{4}}}{T^l}T^l\left(\frac{4g}{f^2}\right) \\ &= q^2+q^2T^{\frac{q-1}{2}}(2f)T^{\frac{q-1}{4}}(-1)\,{}_2F_1\left(\begin{matrix}T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ & \epsilon\end{matrix}\mid\frac{4g}{f^2}\right), \end{aligned}$$

and then using the relation $a_q(E_2)=q+1-\#E_2(\mathbb{F}_q)$, we complete the proof. □

Proof of Theorem 1.2. Since $x^3 + ax + b = 0$ has a non-zero solution in $\mathbb{F}_q$, let $h \in \mathbb{F}_q^\times$ be such that $h^3 + ah + b = 0$. A change of variables $(x, y) \mapsto (x + h, y)$ takes the elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ to

$$E''_{a,b} : y^2 = x^3 + 3hx^2 + (3h^2 + a)x. \tag{3.10}$$

Since $a_q(E_{a,b}) = a_q(E''_{a,b})$ and $3h \neq 0$, using Theorem 3.2 for the elliptic curve $E''_{a,b}$, we complete the proof. □

References

1. R. Barman and G. Kalita, *Hypergeometric functions and a family of algebraic curves*, Ramanujan J. **28** (2012), no. 2, 175–185. MR2925173
2. R. Barman and G. Kalita, *Certain values of Gaussian hypergeometric series and a family of algebraic curves*, Int. J. Number Theory **8** (2012), no. 4, 945–961. MR2926554
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 (2011c:11068)
4. J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77–101. MR879564 (88e:11122)
5. 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)
6. M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), 461-467. MR1194045 (93i:11146)
7. S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990. MR1029028 (91c:11001)
8. C. Lennon, *Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **139** (2011), 1931–1938. MR2775369
9. C. Lennon, *Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold*, J. Number Theory **131** (2011), no. 12, 2320–2351. MR2832827
10. K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205–1223. MR1407498 (98e:11141)

Department of Mathematical Sciences, Tezpur University, Napaam-784028, Sonitpur, Assam, India

E-mail address: rupamb@tezu.ernet.in

Department of Mathematical Sciences, Tezpur University, Napaam-784028, Sonitpur, Assam, India

E-mail address: gautamk@tezu.ernet.in