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 $2\mathcal{F}_1$-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 [5], Lennon provided a general formula expressing the number of $\mathbb{F}_p$-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 [8], 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
characters of $\mathbb{F}_q^\times$, then $\binom{A}{B}$ is defined by

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

where $J(A, B)$ denotes the usual Jacobi sum and $B$ 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 $B_1, B_2, \ldots, B_n \in \mathbb{F}_q^\times$, the Gaussian hypergeometric series $n+1F_n$ is defined to be

$$
(1.2) \quad \binom{A_0, A_1, \ldots, A_n}{B_1, B_2, \ldots, B_n} := \frac{q}{q - 1} \sum_\chi \left( \frac{A_0}{\chi} \right) \left( \frac{A_1}{B_1 \chi} \right) \cdots \left( \frac{A_n}{B_n \chi} \right) \chi(x),
$$

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

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

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

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

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

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 $q \equiv 1 \pmod{6}$. In addition, let $a$ be non-zero and $(-a/3)$ be a quadratic residue modulo $q$. If $T \in \mathbb{F}_q^\times$ is a generator of the character group, then the trace of the Frobenius on $E_{a,b}$ can be expressed as

$$
 a_q(E_{a,b}) = -qt^{\frac{e-1}{2}}(-k) \binom{2F_1}{T^{\frac{e-1}{2}}, T^{\frac{3(e-1)}{2}} | -\frac{k^3 + ak + b}{4k^3}},
$$

where $e$ 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 $q \equiv 1 \pmod{4}$. Also assume that $x^3 + ax + b = 0$ has a non-zero solution in $\mathbb{F}_q$ and $T \in \mathbb{F}_q^\times$ is a generator of the character group. The trace of the Frobenius on $E_{a,b}$ can be expressed as

$$
 a_q(E_{a,b}) = -qt^{\frac{e-1}{2}}(6h)T^{\frac{e-1}{2}}(-1) \binom{2F_1}{T^{\frac{e-1}{2}}, T^{\frac{3(e-1)}{2}} | \frac{12h^2 + 4a}{9h^2}},
$$

where $e$ 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

$$
(2.1) \quad \theta(\alpha) = \zeta^{\text{tr}(\alpha)},
$$

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

$$
\text{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{e-1}}.
$$
For $A \in \hat{\mathbb{F}}_q^\times$, the Gauss sum is defined by
\begin{equation}
G(A) := \sum_{x \in \mathbb{F}_q} A(x) \zeta^{t(x)} = \sum_{x \in \mathbb{F}_q} A(x) \theta(x).
\end{equation}

We let $T$ denote a fixed generator of $\hat{\mathbb{F}}_q^\times$. 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 $\epsilon$ be the trivial character. Then
\begin{align}
& (1) \quad \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) \quad \sum_{n=0}^{q-2} T^n(x) = \begin{cases} q - 1 & \text{if } x = 1; \\ 0 & \text{if } x \neq 1. \end{cases}
\end{align}

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
\[ G_i G_{-i} = q T^i(-1). \]

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

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
\begin{equation}
E_1 : y^2 = x^3 + cx^2 + d,
\end{equation}
where $c \neq 0$. The trace of the Frobenius endomorphism on $E_1$ is given by
\begin{equation}
\alpha_q(E_1) = q + 1 - \#E_1(\mathbb{F}_q).
\end{equation}

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 $q \equiv 1 \pmod{6}$. If $T \in \hat{\mathbb{F}}_q^\times$ is a generator of the character group, then the trace of the Frobenius on $E_1$ is given by
\[ \alpha_q(E_1) = -q T^{\frac{q-1}{6}}(-3c) \ _2F_1\left( T^{\frac{2}{e}}, \ T^{\frac{5(q-1)}{6}} \epsilon \mid -\frac{27d}{4c^2} \right), \]
where $\epsilon$ 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 \( \#E_1(F_q) \) the number of points on the curve \( E_1 \) over \( F_q \) including the point at infinity. Then
\[ \#E_1(F_q) - 1 = \#\{(x, y) \in F_q \times F_q : P(x, y) = 0\}. \]
Using the elementary identity from [5],
\[ \sum_{z \in F_q} \theta(zP(x, y)) = \begin{cases} q & \text{if } P(x, y) = 0; \\ 0 & \text{if } P(x, y) \neq 0, \end{cases} \]
we obtain
\[ q \cdot (\#E_1(F_q) - 1) = \sum_{x, y, z \in F_q} \theta(zP(x, y)) \]
\[ = q^2 + \sum_{z \in F_q^\times} \theta(zd) + \sum_{y, z \in F_q^\times} \theta(zd)\theta(-zy^2) \]
\[ + \sum_{x, z \in F_q^\times} \theta(zd)\theta(zx^3)\theta(zcx^2)\theta(-zy^2) \]
\[ = q^2 + A + B + C + D. \] (3.4)
Now using Lemma 2.2 and then applying Lemma 2.1 repeatedly for each term of (3.4), we deduce that
\[ A = \frac{1}{q - 1} \sum_{z \in F_q^\times} \sum_{l=0}^{q-2} G_{-l}T^l(zd) = \frac{1}{q - 1} \sum_{l=0}^{q-2} G_{-l}T^l(d) \sum_{z \in F_q^\times} T^l(z) = G_0 = -1. \]
Similarly,
\[ B = \frac{1}{(q - 1)^2} \sum_{l, m=0}^{q-2} G_{-l}G_{-m}T^l(d)T^m(-1) \sum_{y \in F_q^\times} T^{2m}(y) \sum_{z \in F_q^\times} T^{l+m}(z) \]
\[ = 1 + G_{\frac{q-1}{2}} G_{-\frac{q-1}{2}} T^{\frac{q-1}{2}}(d)T^{\frac{q-1}{2}}(-1). \]
Using Lemma 2.3 for \( i = \frac{q-1}{2} \), we deduce that
\[ B = 1 + qT^{\frac{q-1}{2}}(-1)T^{\frac{q-1}{2}}(d)T^{\frac{q-1}{2}}(-1) \]
\[ = 1 + qT^{\frac{q-1}{2}}(d). \]
Expanding the next term, we have
\[ C = \frac{1}{(q - 1)^3} \sum_{l, m, n=0}^{q-2} G_{-l}G_{-m}G_{-n}T^l(d)T^n(c) \sum_{z \in F_q^\times} T^{l+m+n}(z) \sum_{x \in F_q^\times} T^{3m+2n}(x). \]
Finally,
\[
D = \frac{1}{(q - 1)^4} \sum_{l,m,n,k=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{-k} T^l(d) T^n(c) T^k(-1) \\
\times \sum_{z \in \mathbb{F}_q^*} T^{l+m+n+k}(z) \sum_{x \in \mathbb{F}_q^*} T^{3m+2n}(x) \sum_{z \in \mathbb{F}_q^*} T^{2k}(z).
\]

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
\[
D_{\frac{q-1}{2}} = \frac{1}{(q - 1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n} G_{\frac{q-1}{2}} T^l(d) T^n(c) T^2 \left( \frac{q-1}{2} \right) (-1) \\
\times \sum_{z \in \mathbb{F}_q^*} T^{l+m+n+\frac{q-1}{2}}(z) \sum_{x \in \mathbb{F}_q^*} T^{3m+2n}(x),
\]
which is zero unless \(m = -\frac{2}{3}n\) and \(n = -3l - \frac{3(q-1)}{2}\). Since \(G_{3l+3(q-1)} = G_{3l+\frac{q-1}{2}}\) and \(G_{-2l-(q-1)} = G_{-2l}\), we have
\[
D_{\frac{q-1}{2}} = \frac{1}{q - 1} \sum_{l=0}^{q-2} G_{-l} G_{-2l} G_{3l+\frac{q-1}{2}} G_{\frac{(q-1)}{6}} T^l(d) T^{-3l+\frac{q-1}{2}}(c) T^2 \left( \frac{q-1}{2} \right) (-1).
\]

Using the Davenport-Hasse relation (Lemma 2.4) for \(m = 2, \psi = T^{-1}\) and \(m = 3, \psi = T^{l+\frac{q-1}{2}}\) respectively, we deduce that
\[
G_{-2l} = \frac{G_{-l} G_{-l-\frac{q-1}{2}}}{G_{\frac{q-1}{2}} T^{l}(4)} \quad \text{and} \quad G_{3l+\frac{q-1}{2}} = \frac{G_{l+\frac{q-1}{2}} G_{l+\frac{q-1}{2}} G_{l+\frac{q-1}{6}}}{q T^{-l-\frac{q-1}{2}}(27)}.
\]

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

Now, if \(T^{m-n} \neq \epsilon\), then we have
\[
(3.5) \quad G_m G_{-n} = q \left( \frac{T^m}{T^n} \right) G_{m-n} T^n(-1).
\]

Replacing \(l\) by \(l-\frac{q-1}{2}\) and using (3.5), we obtain
\[
D_{\frac{q-1}{2}} = \frac{q T^{\frac{q-1}{2}}(-3c)}{q - 1} \sum_{l=0}^{q-2} G_{l} G_{-l} \left( \frac{T^{l-\frac{q-1}{2}}}{T^{l+\frac{q-1}{2}}} \right) G_{\frac{q-1}{6}} \left( \frac{T^{l+\frac{q-1}{2}}}{T^{l-\frac{q-1}{2}}} \right) G_{\frac{q-1}{6}} T^{l-\frac{q-1}{2}} \left( \frac{27d}{4c^3} \right).
\]
Plugging the facts that if \( l \neq 0 \), then \( G_l G_{-l} = q T^l (-1) \) and if \( l = 0 \), then \( G_l G_{-l} = q T^l (-1) - (q - 1) \) into the appropriate identities for each \( l \), we deduce that

\[
D_{2+1} = \frac{q^3 T^{2+1}_0 (-1) T^{2+1}_1 (3c)}{q - 1} \sum_{l=0}^{q-2} \left( \frac{T^{2+1}_1}{T^{2+1}_0} \right) \left( \frac{T^{2+1}_1 + \frac{q-1}{6}}{T^{2+1}_0} \right) T^{2+1}_1 \left( \frac{27d}{4c^3} \right) T^l (-1)
\]

\[
- q^2 T^{2+1}_1 (-1) T^{2+1}_2 (3c) \left( \frac{T^{2+1}_1 - 2 \frac{q-1}{6}}{T^{2+1}_2} \right) \left( \frac{T^{2+1}_1}{T^{2+1}_2} \right) T^{2+1}_2 \left( \frac{27d}{4c^3} \right).
\]

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

\[
D_{2+1} = \frac{q^3 T^{2+1}_0 (-3c)}{q - 1} \sum_{l=0}^{q-2} \left( \frac{T^{2+1}_1}{T^{2+1}_0} \right) \left( \frac{T^{2+1}_1 + \frac{5(q-1)}{6}}{T^{2+1}_0} \right) T^l \left( - \frac{27d}{4c^3} \right)
\]

\[
- q^2 T^{2+1}_1 (d) \frac{G^{2+1}_2 G^{2+1}_4 G^{2+1}_6 G^{2+1}_{5(q-1)}}{q^2 G^{2+1}_6 G^{2+1}_{5(q-1)}}
\]

\[
= q^2 T^{2+1}_1 (-3c) F_1 \left( \frac{T^{2+1}_1}{e}, \frac{T^{5(q-1)}_{27}}{e} \right) - \frac{27d}{4c^3} - q T^{2+1}_1 (d).
\]

Putting the values of \( A, B, C, D \) all together in \( \text{[3.1]} \) gives

\[
q \cdot \left( \#E_1(\mathbb{F}_q) - 1 \right) = q^2 + q^2 T^{2+1}_1 (-3c) F_1 \left( \frac{T^{2+1}_1}{e}, \frac{T^{5(q-1)}_{27}}{e} \right) - \frac{27d}{4c^3}.
\]

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

**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

\[
E_{a,b}' : y^2 = x^3 + 3kx^2 + (k^3 + ak + b).
\]

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. \( \square \)

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

**Theorem 3.2.** Let \( q = p^f, p > 0 \), be a prime and \( q \equiv 1 \pmod{4} \). 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 \( T \in \mathbb{F}_q^\times \) is a generator of the character group, then the trace of the Frobenius on \( E_2 \) is given by

\[
a_q(E_2) = -q T^{2+1}_1 (2f) T^{2+1}_2 (-1) F_1 \left( \frac{T^{2+1}_1}{e}, \frac{T^{5(q-1)}_{27}}{e} \right),
\]

where \( e \) 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

\[ q \cdot (\#E_2(\mathbb{F}_q) - 1) = \sum_{x, y, z \in \mathbb{F}_q^\times} \theta(zP(x, y)) = q^2 + \sum_{y, z \in \mathbb{F}_q^\times} \theta(0) + \sum_{x, z \in \mathbb{F}_q^\times} \theta(-zy^2) + \sum_{x, y \in \mathbb{F}_q^\times} \theta(zx^3)\theta(zf x^2)\theta(zgy) \]

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

\[ (3.7) \quad := q^2 + (q - 1) + A + B + C. \]

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

\[ A = -(q - 1), \]

\[ B = \frac{1}{(q - 1)^3} \sum_{l, m, n=0}^{q-2} G_{-l}G_{m}G_{-n}T^m(f)T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x), \]

\[ C = -\frac{1}{(q - 1)^3} \sum_{l, m, n=0}^{q-2} G_{-l}G_{m}G_{n}T^m(f)T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x) \]

\[ + \frac{1}{(q - 1)^3} \sum_{l, m, n=0}^{q-2} G_{-l}G_{m}G_{n}G_{\frac{1}{2}}T^m(f)T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+\frac{2}{x}}(z) \]

\[ \times \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x). \]

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

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

The Davenport-Hasse relation (Lemma 2.2) with \( m = 2, \psi = T^\frac{2}{x} \) yields

\[ (3.9) \quad G_{2l+\frac{2}{x}} = \frac{G_{l+\frac{q-1}{x}}G_{l+\frac{3(q-1)}{x}}}{G_{\frac{2}{x}}} T^{l+\frac{q-1}{x}}. \]

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

\[ q \cdot (\#E_2(\mathbb{F}_q) - 1) = q^2 + \frac{q^3T^{\frac{2}{x}}(2f)T^{\frac{2}{x}}(-1)}{q - 1} \sum_{l=0}^{q-2} \left( T^l+\frac{2}{x} \right) \left( T^{l+\frac{3(q-1)}{x}} \right) T^l \left( \frac{4g}{f^2} \right) \]

\[ = q^2 + q^2T^{\frac{2}{x}}(2f)T^{\frac{2}{x}}(-1)2F_1 \left( \frac{T^{\frac{2}{x}}}{\epsilon}, \frac{T^{\frac{3(q-1)}{x}}}{\epsilon} \right) \left( \frac{4g}{f^2} \right), \]

and then using the relation \( a_q(E_2) = q + 1 - \#E_2(\mathbb{F}_q) \), we complete the proof. \( \square \)
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
\[
E''_{a,b} : y^2 = x^3 + 3hx^2 + (3h^2 + a)x.
\]
(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. \( \square \)

References


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