ON THE NUMBER OF POINTS ON $y^2 = x^3 - ax$ OVER $\mathbb{F}_q$.

Gautam Kalita*
Department of Mathematics, Indian Institute of Information Technology Guwahati, Guwahati-781001, Assam, INDIA
*For correspondence. (gautam.kalita@iiitg.ac.in)

Abstract: In [8, Chap. 18, Thm. 5], Rosen and Ireland express the number of $\mathbb{F}_p$ points on the family of elliptic curves $y^2 = x^3 - ax$ in terms of Jacobi sums using properties of character sums. In this paper we give an alternative proof of this result using Gaussian hypergeometric series and extend it to $\mathbb{F}_q$. Further if a is a quadratic residue in $\mathbb{F}_q$, then we find a similar results using another technique.

Keywords: elliptic curves; character; Gaussian hypergeometric function; traces of Frobenius endomorphism

2010 Mathematics Classification Numbers: 11T24, 11G20, 33C20

1. Introduction and statement of results:

Finding number of solutions of a polynomial equation over a finite field is a problem of interest to mathematicians for many years. Many mathematicians have found many interesting connections of different parameters of algebraic curves and other mathematical objects like characters, modular forms, hypergeometric functions.

Gauss introduced ${}_2F_1$ classical hypergeometric series. For a complex number a and a non-negative integer n, let $(a)_n$ denote the rising factorial defined by

$$(a)_0 := 1 \text{ and } (a)_n := a(a+1)(a+2)\cdots(a+n-1) \text{ for } n > 0.$$

Then, for complex numbers a_i, b_j, and z, with none of the b_j being negative integer or zero, the classical hypergeometric series is defined by

$${}_{r+1}F_r\left(\begin{matrix} a_0, & a_1, & \cdots, & a_r \\ & b_1, & \cdots, & b_r \end{matrix} \mid z\right) := \sum_{n=0}^{\infty} \frac{(a_0)_n(a_1)_n\cdots(a_r)_n}{(b_1)_n(b_2)_n\cdots(b_r)_n}\frac{z^n}{n!}.$$

The relations of classical hypergeometric series with number of points on algebraic curves have been investigated by many mathematicians. The period of an elliptic curve has close association with classical hypergeometric series. For details, see [13, 15, 5, 12, 1].

In 1980's, Greene [6] defined Gaussian hypergeometric function, which is finite field analogue of classical hypergeometric series. Let $q = p^e$ be a power of an odd prime and $\mathbb{F}_q$ the finite field of q elements. Let $\widehat{\mathbb{F}_q^{\times}}$ denote the group of multiplicative characters χ on $\mathbb{F}_q^{\times}$, extended to all of $\mathbb{F}_q$ by setting $\chi(0) := 0$. For $A, B \in \widehat{\mathbb{F}_q^{\times}}$, the binomial coefficient $\binom{A}{B}$ is defined by

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

where $J(A, B)$ denotes the usual Jacobi sum and $\overline{B}$ is the inverse of B. With this notation, for characters $A_0, A_1, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ of $\mathbb{F}_q$, the Gaussian hypergeometric series ${}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \cdots, & A_n \\ & B_1, & \cdots, & B_n \end{matrix} \mid x\right)$ over $\mathbb{F}_q$ is defined as

$${}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \cdots, & A_n \\ & B_1, & \cdots, & B_n \end{matrix} \mid x\right) := \frac{q}{q-1}\sum_{\chi}\binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\cdots\binom{A_n\chi}{B_n\chi}\chi(x), \tag{2}$$

where the sum is over all characters χ of $\mathbb{F}_q$. Gaussian hypergeometric series possess many interesting properties analogous to the classical hypergeometric series. This encourages mathematicians to find connection of certain parameters of algebraic curves with Gaussian hypergeometric function. Recently, Koike [9], Ono [14], Fuselier [7], Lennon [10, 11], Barman and the author [2, 3], and many more have deduced expressions of traces of Frobenius of certain families of elliptic curves in terms of special values of Gaussian hypergeometric functions.

For $a \in \mathbb{F}_q^\times$ we consider the elliptic curve E_a defined by the affine equation

$$E : y^2 = x^3 - ax$$

If we denote by $a_q(E_a)$ the trace of the Frobenius endomorphism on E_a,then

$$a_q(E_a) = q + 1 - \#E_a(\mathbb{F}_q), \tag{3}$$

where $\#E_a(\mathbb{F}_q)$ denotes the number of $\mathbb{F}_q$ -points on E_a including the point at infinity. Clearly the curve E has one point at infinity so that $\#E_a(\mathbb{F}_q) = 1 + N(y^2 = x^3 - ax)$. In [8], Rosen and Ireland deduced the following result regarding the number of $\mathbb{F}_q$-points on E_a.

Theorem 1.1. [8, Chap. 18, Thm. 5] *Suppose $p \neq 2$ and $p \nmid a$. Consider the elliptic curve $y^2 = x^3 - ax$ over $\mathbb{F}_q$. If $p \equiv 3$ (mod 4) then $\#E_a(\mathbb{F}_a) = p + 1$. If $p \equiv 1$ (mod 4), then*

$$\#E_a(\mathbb{F}_q) = p + 1 + \overline{\chi_4(-a)}J(\chi_4, \chi_4) + \chi_4(-a)\overline{J(\chi_4, \chi_4)},$$

where χ_4 is a character of order 4 on $\mathbb{F}_q$.

They use properties of characters to count the number of different order residues present in $\mathbb{F}_q$ together with a transformation of the elliptic curve to deduce the result. Here we give an alternative proof of the above theorem and extend the above result to $\mathbb{F}_q$.

Theorem 1.2. *Let $q = p^e$, $p > 0$ a prime number with $q \equiv 1$ (mod 4). For the elliptic curve*

$$E_a : y^2 = x^3 - ax,$$

the trace of Frobenius is given by

$$a_q(E_a) = -2Re\,\{\chi^3(-a)J(\chi_4, \chi_4)\},$$

where χ_4 is a character of order 4 on $\mathbb{F}_q$.
Further we proof the following theorem.

Theorem 1.3. *Let $q = p^e$, $p > 0$ a prime number and a is a quadratic residue in $\mathbb{F}_q^\times$. Then the trace of Frobenius of the elliptic curve*

$$E_a : y^2 = x^3 - ax$$

is given by

$$a_q(E_a) = \begin{cases} 0, & \text{if } q \equiv 3 \ (mod\ 4); \\ -2\sqrt{\phi}(-a)\,Re\ J(\sqrt{\phi}, \sqrt{\phi}), & \text{if } q \equiv 1 \ (mod\ 4). \end{cases}$$

2. Preliminaries:

In this section, we recall some basic terminologies and properties of characters as well as Gaussian hypergeometric function. We begin with the definition of additive character. The additive character $\theta : \mathbb{F}_q \to \mathbb{C}^\times$ is defined by

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

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

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

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

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

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. [8, Chap. 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. [7, 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 lemma gives a relation between Jacobi sum and Gauss sum.

Lemma 2.3. [7, Lemma 2.6] *If $T^{m-n} \neq \epsilon$, then*

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

Finally, we restate a results from [6].

Lemma 2.4. [6, (4.11)]

$${}_2F_1\left(\begin{matrix} A, & B \\ & AB \end{matrix} \mid -1\right) = \begin{cases} 0, & \text{if } B \text{ is not a square;} \\ \binom{C}{A} + \binom{\phi C}{A}, & \text{if } B = C^2. \end{cases}$$

3. Proof of the results:

Proof of Theorem 1.2 : Let $E_a(\mathbb{F}_q)$ denotes the $\mathbb{F}_q$ -points on the elliptic curve E_a including the point at infinity. Then

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

where,

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

Using the identity from [8]

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

We express the number of points as

$$\begin{aligned} q\cdot(\#E_a(\mathbb{F}_q)-1) &= \sum_{x,y,z\in\mathbb{F}_q}\theta(zP(x,y)) \\ &= q^2 + \sum_{z\in\mathbb{F}_q^{\times}}\theta(0) + \sum_{y,z\in\mathbb{F}_q^{\times}}\theta(zy^2) + \sum_{x,z\in\mathbb{F}_q^{\times}}\theta(-zx^3)\theta(zax) \\ &\quad + \sum_{x,y,z\in\mathbb{F}_q^{\times}}\theta(-zx^3)\theta(zax)\theta(zy^2) \\ &= q^2 + (q-1) + A + B + C. \end{aligned} \tag{4}$$

Now using Lemma 2.2 and Lemma 2.1 repeatedly for each term of (4), we deduce that

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

Expanding the next term, we obtain

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

Finally, the last term yields

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

The innermost sum is zero unless $l = 0$ or $\frac{q-1}{2}$. For these two values of l, the term reduces to

$$C = -B + C_{\frac{q-1}{2}},$$

where

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

Now, $C\underline{q-1}$ is nonzero for $n = -3m$ and m = (q-1)/4 or 3(q-1)/4. Using this and then Lemma 2.3, we obtain

$$\begin{aligned} C_{\frac{q-1}{2}} &= G_{-\frac{q-1}{2}}G_{-\frac{q-1}{4}}G_{-\frac{q-1}{4}}T^{\frac{q-1}{4}}(-a) + G_{-\frac{q-1}{2}}G_{\frac{q-1}{4}}G_{\frac{q-1}{4}}T^{-\frac{(q-1)}{4}}(-a) \\ &= G_{-\frac{q-1}{2}}G_{\frac{q-1}{2}}J(T^{-\frac{(q-1)}{4}},T^{-\frac{(q-1)}{4}})T^{\frac{q-1}{4}}(-a) + G_{-\frac{q-1}{2}}G_{\frac{q-1}{2}}J(T^{\frac{(q-1)}{4}},T^{\frac{(q-1)}{4}})T^{\frac{3(q-1)}{4}}(-a) \\ &= 2q \operatorname{Re}\{J(T^{\frac{(q-1)}{4}},T^{\frac{(q-1)}{4}})T^{\frac{3(q-1)}{4}}(-a)\}. \end{aligned} \qquad . \qquad (5)$$

The last equality follows from the fact that $G_{\frac{q-1}{2}} = \sqrt{q}$ for q ≡ 1 (mod 4). Finally, combining all values of A, B and C in (4), we have

$$q\cdot(\#E_1^a(\mathbb{F}_q)-1) = q^2 + 2q \operatorname{Re}\{J(T^{\frac{(q-1)}{4}},T^{\frac{(q-1)}{4}})T^{\frac{3(q-1)}{4}}(-a)\}.$$

From the relation $a_q(E_a) = 1 + q - \#E_a(\mathbb{F}_q)$, the proof follows.

Let p be a prime such that $p \equiv 1 \pmod 4$ and g be a primitive root modulo p. Then there exist non negative integers c, d such that $c^2 + d^2 = p$ with $c \equiv -\varphi(2) \pmod 4$ and $d \equiv c\, g^{(q-1)/4} \pmod p$. Hence values of Table 3.2.1 of [4, Chap. 3, pp. 108] yield the following corollary.

Corollary 3.1. *Let p be a prime number such that $p \equiv 1$ (mod 4). If a is quadratic residue in $\mathbb{F}_q^\times$, then the trace of Frobenius for the elliptic curve*

$$E_a : y^2 = x^3 - ax$$

is given by

$$a_q(E_a) = -2c\chi_4{}^3(a),$$

where c, d are non negative integers such that $c^2 + d^2 = p$ with $c \equiv -\varphi(2)$ (mod 4) and $d \equiv c\, g^{(q-1)/4}$ (mod p) with g being a primitive root in modulo p.

Proof of Theorem 1.3 : Since $a \in \mathbb{F}_q^\times$ is a quadratic residue, let $a = \alpha^2$. By definition, the trace of Frobenius for the elliptic curve E_a is given by

$$\begin{aligned} a_q(E_a) &= -\sum_{x\in\mathbb{F}_q} \phi(x^3 - ax) \\ &= -\sum_{x\in\mathbb{F}_q} \phi(x)\phi(x-\alpha)\phi(x+\alpha). \end{aligned} \qquad (6)$$

Again we have,

$${}_2F_1\left(\begin{matrix}\phi, & \phi \\ & \epsilon\end{matrix} \mid -1\right) = \frac{\phi(-1)}{q} \sum_{x\in\mathbb{F}_q} \phi(x)\phi(1-x)\phi(1+x).$$

Replacing x by x/α, we obtain

$${}_2F_1\left(\begin{matrix}\phi, & \phi \\ & \epsilon\end{matrix} \mid -1\right) = \frac{1}{q\phi(\alpha)}\sum_{x\in\mathbb{F}_q}\phi(x)\phi(x-\alpha)\phi(x+\alpha).$$

Using (6) and Lemma 2.4, we have

$$\begin{aligned}-\frac{a_q(E_a)}{q\phi(\alpha)} &= {}_2F_1\left(\begin{matrix}\phi, & \phi \\ & \epsilon\end{matrix} \mid -1\right)\\ &= \begin{cases} 0, & \text{if } q \equiv 3 \pmod 4; \\ \binom{\sqrt{\phi}}{\phi} + \binom{\phi\sqrt{\phi}}{\phi}, & \text{if } q \equiv 1 \pmod 4. \end{cases}\end{aligned} \tag{7}$$

The fact

$$\binom{\phi\sqrt{\phi}}{\phi} = \binom{\overline{\sqrt{\phi}}}{\phi} = \overline{\binom{\sqrt{\phi}}{\phi}}$$

yields that

$$\binom{\sqrt{\phi}}{\phi} + \binom{\phi\sqrt{\phi}}{\phi} = 2\ \mathrm{Re}\binom{\sqrt{\phi}}{\phi} = 2\ \mathrm{Re}\left(\frac{\sqrt{\phi}}{\sqrt{\phi}}\right) = \frac{2\sqrt{\phi}(-1)}{q}\ \mathrm{Re}\ \mathrm{J}(\sqrt{\phi}, \sqrt{\phi}).$$

Using this in (7), 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.

[2] R. Barman and G. Kalita, *Hypergeometric functions over* F$_q$ *and traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **141** (2013), no. 10, 3403–3410.

[3] R. Barman and G. Kalita, *Elliptic Curves and Special Values of Gaussian hypergeometric series*, J. Number Theory **133** (2013), no. 9, 3099–3111.

[4] B. C. Berndt, et al. *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, A Wiley-Interscience Publication, New York, 1997.

[5] F. Beukers, *Algebraic values of G-functions*, J. Reine Angew. Math. **434**, 45–65, 1993.

[6] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301**(1), 77–101, 1987.

[7] J. Fuselier, *Hypergeometric functions over* F$_p$ *and relations to elliptic curves and modular forms*, Proc. Amer. Math. Soc. **138** (2010), 109–123.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modarn Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[9] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22**, 461–467, 1992.

[10] C. Lennon, *Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **139**, 1931–938, 2011.

[11] C. Lennon, *Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold*, J. Number Theory **131**(12), 2320–2351, 2011.

[12] D. McCarthy, *F_2 Hypergeometric series and periods of elliptic curves*, Int. J. Number Theory, 6(3)(2010), 461-470.

[13] J. Rouse, *Hypergeometric function and elliptic curves*, Ramanujan J. **12** (2), 197–205, 2006.

[14] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350**(3), 1205–1223, 1998.

[15] P. F. Stiller, *Classical automorphic forms and hypergeometric functions*, J. Number Theory **28**(2), 219–232, 1988.