# A Note on Elliptic Curves and Gaussian Hypergeometric Series

Abhishek Juyal, Ankan Pal, and Bidisha Roy

Abstract. In this article, by defining trace of Edwards curves $E_{a,d} : x^2 + y^2 = a^2(1 + dx^2y^2)$ over finite field $\mathbb{F}_p$, we establish an interplay between *trace of* $E_{a,d}$ and *trace of a family of elliptic curves* $E : y^2 = x^3 - \frac{1 + a^4d}{a^2}x^2 + dx$. Moreover, we express number of points on the Edwards curves $E_{a,d}$ in terms of the Gaussian hypergeometric series ${}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix}\,\middle|\, 1 - a^4d\right)$, where $\epsilon_p$ and $\phi_p$ are trivial and quadratic characters over $\mathbb{F}_p$, respectively. As a corollary, we express Hasse-Weil $L$-function at $s = 1$ i.e. $L(E, 1)$ associated to $E$ involving the Gaussian hypergeometric series. Analogous to previous findings, for twisted Edwards curve $E'_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ and the family of elliptic curves $E' : y^2 = x(x - 1)\left(x - \frac{a}{d}\right)$, we also obtain similar results.

## 1. Introduction

One of the focus of this article is to express the number of points on the Edwards curves over a finite field in terms of Gaussian hypergeometric series. Another focus is to establish some relations between trace of Edwards curves and traces of certain elliptic curves. After introducing by H.M. Edwards in 2007, Edwards models of elliptic curves are gaining attention because of having simpler group law and has been used in many cryptographic applications. As our target is to obtain a new connection between Edwards curve and certain elliptic curves, here we start with an elementary definition of elliptic curves.

An elliptic curve $\mathcal{C}$ (defined over field $\mathbb{K}$) is a smooth projective curve of genus one, with a point at infinity $\mathcal{O}$. $\mathcal{C}$ can be described by a global minimal Weierstrass equation of the form,

$$\mathcal{C} : y^2 + a_1x + a_3xy + a_5y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i$ are elements in the field $\mathbb{K}$. Counting number of rational points on algebraic varieties has been a long standing fascination of mathematicians as early as the Gaussian era [SZ08]. For example, evaluation of the Hasse-Weil $L$-function at $s = 1$ can be simply reduced to a point counting problem and it provides a measure of the density of rational points of an elliptic curve [Ste68]. We have traced a long and arduous path from there, and in the recent times with the advent of fast algorithms for point counting, such as *Schoof-Elkies-Atkins* algorithm [Sch95], the study of evaluation of $L$-function has become computationally tractable.

We were drawn towards calculating the number of rational points through a particular characterization in terms of a particular *Gaussian hypergeometric series.* A rigorous mention of this topic can be found in the literature as early as 1656 (*Arithmetica Infinitorum*) [GG05, Chapter 2]. In the recent times, Greene elucidates the Gaussian hypergeometric series as a power series analogue over any finite field [Gre87]. An innovative way was found by Ono in [Ono98] to count number of points on an elliptic curve through use of the Gaussian hypergeometric series. Following similar motivation and using several identities from [Gre87], Sadek et. al. in [SES16] were able to count number of rational points on Edwards curves $E_{a,1} : x^2 + y^2 = a^2(1 + x^2y^2)$, and twisted Edwards curves $E'_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{F}_p$.

In this article, we follow similar rationale and extend this result for a generic case of Edwards curves $E_{a,d} : x^2 + y^2 = a^2(1 + dx^2y^2)$ in **Proposition** 3.2. After counting the number of rational points on the Edwards curves family, we connect it with the number of rational points of certain

2010 *Mathematics Subject Classification.* Primary 11G05, Secondary 11D59.

*Key words and phrases.* Finite Transformation Formulae, Edwards Curves, Legendre Symbol, Elliptic Curves, Hasse-Weil $L$-function, Gaussian Hypergeometric Series.

family of elliptic curves over $\mathbb{F}_p$. In section 3 we provide two formulas which illustrates the relationship between the trace of certain elliptic curve and trace of an Edwards curve over $\mathbb{F}_p$. Typically, isogenies of elliptic curves are used to estimate the number of rational points on alternate parametrization of elliptic curves. We use a very different technique i.e. William's transformation formulas [Wil70] to find a closed-form expression to estimate the number of rational points.

## 2. Main Results

We start by defining the following two families of elliptic curves which are the main objects of study in this article.

For two non-zero integers $a$ and $d$, we denote the following family of Weierstrass equations over $\mathbb{Q}$ as *Type-I.*

$$E : y^2 = x^3 - \frac{1 + a^4 d}{a^2} x^2 + dx. \qquad (\textbf{Type-I})$$

Correspondingly, for $a$ and $d$ an *Edwards curve* [Edw07] over $\mathbb{Q}$ characterized by the following equation.

$$E_{a,d} : x^2 + y^2 = a^2(1 + dx^2y^2). \qquad (1)$$

Moreover, for a prime $p$, the *mod* $p$ reduction of $E$ (respectively, $E_{a,d}$) is denoted by $E_p$ (respectively, $E_{a,d,p}$). In this article, for Edwards curves, we define;

$$tr(E_{a,d,p}) = p + 2 - \#E_{a,d}(\mathbb{F}_p).$$

Now we state the main result as follows.

**Theorem 2.1.** *Let $a, d$ be non-zero integers and $E$ be an elliptic curve defined as above* ***Type-I****. Let $p$ be an odd prime such that,*

(a) *$E$ and $E_{a,d}$ have good reduction at $p$.*
(b) *$a, d \not\equiv 0 \pmod p$ and $a^4 d \not\equiv 1 \pmod p$.*

*Then, we have*

$$tr(E_p) = \left(\frac{d}{p}\right) tr(E_{a,d,p}) - 1 \quad \text{and} \quad tr(E_{a,d,p}) = \phi_p(d) - p \; {}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \,\middle|\, 1 - a^4 d\right),$$

*where $\epsilon_p$ and $\phi_p$ are trivial and quadratic character over $\mathbb{F}_p$, respectively. Here ${}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \,\middle|\, x\right)$ denotes the Gaussian hypergeometric series defined in (5), $tr(\cdot)$ denotes the trace of the curve, and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.*

**Remark 1.** *Here we note that, finding examples for* ***Type-I*** *elliptic curves is a little difficult. If we consider $E : 900y^2 = 900x^3 - 4860001x^2 + 5400x$, it satisfies both relations obtained in Theorem 2.1, for only four primes out of the first hundred primes.*

**Remark 2.** [Dam12, Section 4.3] *We note that there exists a bi-rational equivalency between Edwards curve and elliptic curves in Weierstrass form. The corresponding Weierstrass equation for $E_{a,d}$ is,*

$$E_{W,a,d} : y^2 = x^3 + 2(a^4 d + 1)x^2 + (a^4 d - 1)^2 x.$$

Next, for two chosen non-zero integers $a$ and $d$, we frame the following equation in Legendre form as *Type-II*,

$$E' : y^2 = x(x - 1)\left(x - \frac{a}{d}\right). \qquad (\textbf{Type-II})$$

Correspondingly, for $a$ and $d$, we also define a *twisted Edwards curve* [BBJ$^+$08] over $\mathbb{Q}$ characterized by the following equation

$$E'_{a,d} : ax^2 + y^2 = 1 + dx^2y^2. \tag{2}$$

Similarly as above, for a prime $p$, the *mod* $p$ reduction of $E'$ (respectively, $E'_{a,d}$) is denoted by $E'_p$ (respectively, $E'_{a,d,p}$). The evaluation of number of rational points of $E'$ over $\mathbb{F}_p$ in terms of the hypergeometric series can be derived as a special case of [Ono04, Theorem 11.6] and [Gre87, Theorem 3.6]. This will again reappear in the final expression of the following theorem, though we use a different method to obtain it.

**Theorem 2.2.** *Let $a, d$ be non-zero integers and $E'$ be an elliptic curve defined as above **Type-II**. Let $p$ be an odd prime such that,*

(a) *$E'$ and $E'_{a,d}$ have good reduction at $p$,*
(b) *$a, d \not\equiv 0 \pmod p$.*

*Then, we have*

$$tr(E'_p) = \left(\frac{d}{p}\right) tr(E'_{a,d,p}) - \left(\frac{a}{p}\right).$$

**Remark 3.** *We found a typical example for **Type-II** elliptic curve, namely, $E : 4y^2 = 4x^3 - 21x^2 + 17x$. We note that, $E$ satisfies the above relation for $74$ primes, if we consider the first hundred primes.*

**Remark 4.** [BBJ$^+$08, Theorem 3.2] *It is interesting to mention that there exists a bi-rational equivalency (a well defined map $\psi$) between twisted Edwards curve and elliptic curves in Weierstrass form. The corresponding Weierstrass equation for $E'_{a,d}$ is,*

$$E'_{W,a,d} : y^2 = x^3 - \frac{1}{4}\left(\frac{1}{3}\left(\frac{a+d}{2}\right)^2 + ad\right)x + \frac{a+d}{27}\left(ad - \frac{1}{2}\left(\frac{a-d}{4}\right)^2\right). \tag{3}$$

**Corollary 2.3.** *For the aforementioned elliptic curves $E$ and $E'$, the Hasse-Weil $L-$functions at $s = 1$ can be expressed like;*

$$L(E', 1) = \prod_p \left[1 + \phi_p(-ad)\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \,\middle|\, a^{-1}d\right) + \frac{\phi_p(a)}{p}\right]^{-1}$$

*and*

$$L(E, 1) = \prod_p \left[\frac{p+1}{p} + \phi_p(d)\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \,\middle|\, 1 - a^4d\right)\right]^{-1},$$

*where $\epsilon_p$, $\phi_p$ and ${}_2F_1(\bullet)$ as mentioned in Theorem 2.1.*

**Remark 5.** *In* [BK13], *Barman and Kalita studied the relation between traces of certain elliptic curves and certain hypergeometric series. In that article, they considered those elliptic curves in terms of the Weierstrass model with some specific coefficients. However, their coefficients does not include the cases we are considering in this article as Type-I and Type-II.*

## 3. Preliminaries

In this section, we begin by introducing *trace of a given elliptic curve* which is one of the important objects in this article. Let $E_G$ be an elliptic curve defined over $\mathbb{Q}$, characterized by the global minimal Weierstrass equation,

$$E_G : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4}$$

and $\Delta$ be the discriminant of $E_G$. For each prime $p$, we denote $E_{G,p}$ as the reduction modulo $p$ of $E_G$ and we have the *trace*, $tr(E_{G,p})$, as

$$tr(E_{G,p}) = p + 1 - \#E_{G,p}(\mathbb{F}_p).$$

If $p|\Delta$, then $E_{G,p}$ has a singularity and,

$$tr(E_{G,p}) = \begin{cases} 0, & \text{for the case of a cusp,} \\ 1, & \text{for the case of a split node,} \\ -1, & \text{for the case of a non-split node.} \end{cases}$$

If $p \nmid \Delta$, then $E_G$ has good reduction at $p$ and we have, $tr(E_{G,p}) \le 2\sqrt{p}$, by the Hasse's theorem [Sil09].

Since we intend to connect number of points of Edwards curve with hypergeometric series, now, we briefly discuss hypergeometric series which will be useful to proceed towards the proof of the main results. Following [Gre87] and [SES16], the *Gaussian hypergeometric series* can be treated as a power series analogue in a finite field. For that purpose, choose $p$ is an odd prime and $A$, $B$ are two characters over $\mathbb{F}_p$. Then we define the Jacobi sum as,

$$J(A,B) = \sum_{x\in\mathbb{F}_p} A(x)B(1-x) \quad \text{and define the symbol} \quad \binom{A}{B} = \frac{B(-1)}{p} J\left(A, \frac{1}{B}\right).$$

Further, we assume that $\chi$ is a multiplicative character over $\mathbb{F}_p$. Then the *Gaussian hypergeometric series* for characters $A_i$ and $B_i$ is defined as

$$_{n+1}F_n\left(\begin{matrix} A_0 & A_1 & \dots & A_n \\ & B_1 & \dots & B_n \end{matrix} \middle| \, x\right) = \frac{p}{p-1} \sum_{\chi} \binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\dots\binom{A_n\chi}{B_n\chi}\chi(x). \tag{5}$$

Now, we turn our attention towards counting points on Edwards curves in terms of the *Gaussian hypergeometric series* in Proposition 3.2. For doing so, we collect some identities which are available in literature as follows.

**Lemma 3.0.1.** [Gre87] *For any character $A_p$, we have*

$$\bar{A}_p(1-x) = \delta_p(x) + \frac{p}{p-1}\sum_{\chi_p}\chi_p(x)\binom{A_p\chi_p}{\chi_p}, \qquad \text{where} \qquad \delta_p = \begin{cases} 1, & \text{if } x=0 \\ 0, & \text{otherwise} \end{cases},$$

*and the sum is over all multiplicative characters $\chi_p$ on $\mathbb{F}_p$.*

**Lemma 3.0.2.** [SES16, Lemma 4.1] *If $\chi_p$ is a multiplicative character and $\phi_p$ is a quadratic character over $\mathbb{F}_p$, then*

$$\sum_{y\in\mathbb{F}_p}\chi_p(y^2)\phi_p(1-y^2) = p\phi_p(-1)\left[\binom{\phi_p\chi_p}{\chi_p} + \binom{\chi_p}{\phi_p\chi_p}\right].$$

We prove an analogue of the above lemma in the following proposition.

**Proposition 3.1.** *If $\chi_p$ is a multiplicative character and $\phi_p$ is a quadratic character over $\mathbb{F}_p$, then*

$$\sum_{z\in\mathbb{F}_p}\chi_p(z^2)\phi_p(a^2-z^2) = p\phi_p(-1)\chi_p(a^2)\left[\binom{\phi_p\chi_p}{\chi_p} + \binom{\chi_p}{\phi_p\chi_p}\right].$$

*Proof.* In Lemma 3.0.2 we substitute $y = \frac{z}{a}$, and the proof follows. □

**Lemma 3.1.1.** [Gre87, Corollary 3.16(ii)] *If $\phi_p$ and $\epsilon_p$ are quadratic and trivial characters respectively over $\mathbb{F}_p$, then*

$$_2F_1\left(\begin{matrix}\phi_p & \epsilon_p \\ & \phi_p\end{matrix} \middle| \, a^4d\right) = -\frac{\phi_p(-1)}{p}\left[\phi_p(d^{-1})+1\right].$$

Now, we mention a functional property from [Gre87] of the *Gaussian hypergeometric series* $_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \middle| \, x\right)$.

**Lemma 3.1.2.** [Gre87, Theorem 4.4 (i)] *If $\phi_p$ and $\epsilon_p$ are quadratic and trivial characters respectively over $\mathbb{F}_p$ then,*

$$ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, x\right) = \phi_p(-1)\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, 1-x\right). $$

Now, we will count the number of points on Edwards curves $E_{a,d,p}$ through the *Gaussian hypergeometric series* using the following proposition.

**Proposition 3.2.** *Suppose $E_{a,d}$ is an Edwards curve as mentioned in* (1). *Let $p$ be a prime number which satisfies the conditions as in Theorem 2.1. If $\phi_p$ and $\epsilon_p$ are quadratic and trivial characters respectively over $\mathbb{F}_p$ then,*

$$ tr(E_{a,d,p}) = \phi_p(d^{-1}) - p\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, 1-a^4d\right). $$

*Proof.* We start by observing that,

$$ E_{a,d,p} : x^2 = \frac{y^2-a^2}{da^2y^2-1}\ . $$

For counting the number of points of $E_{a,d}$ modulo $p$, i.e., $\#E_{a,d,p}$, we invoke quadratic character $\phi_p$ as follows.

$$
\begin{aligned}
\#E_{a,d,p} &= 2+p+\sum_{y\in\mathbb{F}_p\setminus\{(a\sqrt{d})^{-1}\}} \phi_p\left(\frac{y^2-a^2}{da^2y^2-1}\right)\\
&= 2+p+\sum_{y}\phi_p(a^2-y^2)\bar{\phi_p}(1-da^2y^2)\\
&= 3+p+\sum_{y}\phi_p(a^2-y^2)\left[\frac{p}{p-1}\sum_{\chi_p}\chi_p(a^2dy^2)\binom{\phi_p\chi_p}{\chi_p}\right] \quad (\textit{Lemma } 3.0.1)\\
&= 3+p+\frac{p}{p-1}\sum_{\chi_p}\chi_p(a^2d)\binom{\phi_p\chi_p}{\chi_p}\left(\sum_{y}\chi_p(y^2)\phi_p(a^2-y^2)\right)\\
&= 3+p+\frac{p}{p-1}\sum_{\chi_p}\chi_p(a^2d)\binom{\phi_p\chi_p}{\chi_p}\left(p\phi_p(-1)\chi_p(a^2)\left[\binom{\phi_p\chi_p}{\chi_p}+\binom{\chi_p}{\phi_p\chi_p}\right]\right) \quad (\textit{Prop. } 3.1)\\
&= 3+p+p\phi_p(-1)\left\{\frac{p}{p-1}\sum_{\chi_p}\binom{\phi_p\chi_p}{\chi_p}\left[\binom{\phi_p\chi_p}{\chi_p}+\binom{\chi_p}{\phi_p\chi_p}\right]\chi_p(a^4d)\right\}\\
&= 3+p+p\phi_p(-1)\left[{}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, a^4d\right)+{}_2F_1\left(\begin{matrix}\phi_p & \epsilon_p\\ & \phi_p\end{matrix}\,\middle|\, a^4d\right)\right]\\
&= 2+p-\phi_p(d^{-1})+p\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, 1-a^4d\right) \quad (\textit{Lemma } 3.1.1 \textit{ and Lemma } 3.1.2)
\end{aligned}
$$

□

After taking $d=1$ in the above proposition, we conclude the following corollary which was proved in [SES16, Theorem 3.2].

**Corollary 3.3.** *Suppose $E_{a,1}=E_{a,d=1}$ is an Edwards curve as mentioned in* (1). *Let $p$ be a prime number which satisfies the conditions as in Theorem 2.1. If $\phi_p$ and $\epsilon_p$ are quadratic and trivial characters respectively over $\mathbb{F}_p$ then,*

$$ tr(E_{a,1,p}) = 1-p\ {}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\,\middle|\, 1-a^4\right). $$

The following lemma connects the number of points on a *twisted* Edwards curve modulo a prime and hypergeometric series.

**Lemma 3.3.1.** [SES16, Theorem 4.2] *Suppose $E'_{a,d}$ is an Edwards curve as mentioned in (2). Let $p$ be a prime number which satisfies the conditions as in Theorem 2.2. If $\phi_p$ and $\epsilon_p$ are quadratic and trivial characters over $\mathbb{F}_p$, then*

$$tr(E'_{a,d,p}) = \phi_p(d) - p\phi_p(-a)\,{}_2F_1\left(\begin{matrix}\phi_p & \phi_p \\ & \epsilon_p\end{matrix} \;\middle|\; a^{-1}d\right).$$

Till now, we have witnessed connection between number of points on Edwards curves and hypergeometric series. For proving main results, we have to connect number of Edwards curve with trace of certain families of elliptic curves. One of the main focus of this article is to observe number of points on certain curves through the *Williams transformation formula.*

For that purpose, *Williams transformation formula* will be used as a tool in Propositions 4.1 and 5.1. Prior to that, we note *Williams transformation formula* as follows.

**Definition 1.** *(Williams Transformation Formula)* [Wil70] *Let $\mathcal{F}$ be any complex valued periodic function with period $p$. For any integer $x$,*

$$\sum_{x=0}^{p-1} \mathcal{F}(x) = \sum_{x=0}^{p-1} \mathcal{F}(x^2) - \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \mathcal{F}(x), \tag{6}$$

*where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.*

Formula (6) was used by Williams in [Wil79] to derive the following,

$$\sum_{x=0}^{p-1} \mathcal{F}\left(\frac{a^*x^2+bx+c}{Ax^2+Bx+C}\right) = \sum_{x=0}^{p-1} \mathcal{F}(x) + \sum_{x=0}^{p-1} \left(\frac{Dx^2+\Delta x+d^*}{p}\right)\mathcal{F}(x) - \mathcal{F}\left(\frac{a^*}{A}\right), \tag{7}$$

where $a^*, b, c, A, B, C$ are integers and

$$D = B^2 - 4AC, \quad \Delta = 4a^*C - 2bB + 4cA, \quad d^* = b^2 - 4a^*c,$$

satisfying

$$\Delta^2 - 4Dd^* \not\equiv 0 \;\; (mod\ p) \quad \text{and} \quad Ax^2 + Bx + C \not\equiv 0 \; (mod\ p). \tag{8}$$

We know *Legendre symbol* is a complex valued function defined over integers and is also a periodic function on $\mathbb{F}_p$ with period $p$. Hence, we can consider $\mathcal{F}$ in (7) as the Legendre symbol and get,

$$\sum_{x=0}^{p-1} \left(\frac{\frac{a^*x^2+bx+c}{Ax^2+Bx+C}}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) + \sum_{x=0}^{p-1} \left(\frac{Dx^2+\Delta x+d^*}{p}\right)\left(\frac{x}{p}\right) - \left(\frac{\frac{a^*}{A}}{p}\right). \tag{9}$$

Next, we note that Legendre symbol is a multiplicative function and it satisfies $\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0.$ Using this, we can manipulate (9) to derive,

$$\sum_{x=0}^{p-1} \left(\frac{\frac{a^*x^2+bx+c}{Ax^2+Bx+C}}{p}\right) = \left(\frac{D}{p}\right) \sum_{x=0}^{p-1} \left(\frac{x^3 + \frac{\Delta}{D}x^2 + \frac{d^*}{D}x}{p}\right) - \left(\frac{a^*A}{p}\right). \tag{10}$$

## 4. Proof of Theorem 2.1

We prove the theorem through the following proposition.

**Proposition 4.1.** *Suppose $E$ is an elliptic curve as mentioned in* ***Type-I****. Also assume conditions as in Theorem 2.1. Then, the $tr(E_p)$ satisfies the following relation,*

$$tr(E_p) = \left(\frac{d}{p}\right) tr(E_{a,d,p}) - 1,$$

*where $E_{a,d}$ as mentioned in (1).*

*Proof.* We consider the *mod* $p$ reduction of the Edwards curve in (1) as,

$$E_{a,d,p} : x^2 + y^2 = a^2(1 + dx^2y^2),$$

which can be re-written as,

$$y^2 = \frac{x^2 - a^2}{a^2dx^2 - 1},$$

where, $a^2dx^2 - 1 \not\equiv 0$ $(mod\ p)$ (this condition is equivalent to equation (8)). We also consider the *mod* $p$ reduction of **Type-I** elliptic curves characterized by the following equation in Weierstrass form.

$$E : y^2 = x^3 - \frac{1 + a^4d}{a^2}x^2 + dx.$$

Now, using equation (10), we will relate the aforementioned *mod* $p$ reduction of the Edwards curves and elliptic curves of **Type-I**. In equation (10) we set,

$$a^* = 1; \quad b = 0; \quad c = -a^2 \quad \text{and} \quad A = a^2d; \quad B = 0; \quad C = -1.$$

Now, we compute,

$$D = 4a^2d; \quad \Delta = -4(1 + a^4d); \quad d^* = 4a^2$$

and

$$\Delta^2 - 4Dd^* = \left(4(a^4d - 1)\right)^2 \not\equiv 0 \pmod{p}.$$

An important aspect to note here is that the *non-zero* integers $a$ and $d$ are chosen so that the **Type-I** family of curves is *non-singular*. Also, $p$ is chosen under the conditions mentioned in Theorem 2.1. Substituting these values in (10), we have,

$$\sum_{x=0}^{p-1} \left(\frac{\frac{x^2-a^2}{a^2dx^2-1}}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{4a^2d}{p}\right)\left(\frac{x^3 - \frac{1+a^4d}{a^2}x^2 + dx}{p}\right) - \left(\frac{a^2d}{p}\right).$$

Note that $\sum_{x=0}^{p-1} \left(\frac{\frac{x^2-a^2}{a^2dx^2-1}}{p}\right) = \#E_{a,d}(\mathbb{F}_p) - p - 2$. Since, $\left(\frac{d}{p}\right) \not\equiv 0$, multiplying by $\left(\frac{d}{p}\right)$, we can substantiate our claim,

$$tr(E_p) = \left(\frac{d}{p}\right) tr(E_{a,d,p}) - 1.$$

□

The second desired relation has been obtained in the conclusion of Proposition 3.1. □

## 5. Proof of Theorem 2.2

Here we furnish the proof through the following proposition.

**Proposition 5.1.** *Suppose $E'$ is an elliptic curve as mentioned in* ***Type-II****. Also assume conditions as in Theorem 2.2. Then, $tr(E'_p)$ satisfies the following relation,*

$$tr(E'_p) = \left(\frac{d}{p}\right) tr(E'_{a,d,p}) - \left(\frac{a}{p}\right),$$

*where $E'_{a,d}$ as mentioned in equation (2).*

*Proof.* We consider the *mod p* reduction of the twisted Edwards curve (2) as,

$$E'_{a,d,p} : ax^2 + y^2 = 1 + dx^2y^2,$$

which can be re-written like,

$$E'_{a,d,p} : y^2 = \frac{ax^2-1}{dx^2-1}, \tag{11}$$

where, $dx^2 - 1 \not\equiv 0$ (*mod p*) (this condition is equivalent to equation (8)). We also consider the *mod p* reduction of **Type-II** elliptic curves characterized by the following equation in Legendre form.

$$E' : y^2 = x(x-1)\left(x - \frac{a}{d}\right). \tag{12}$$

Now, using equation (10), we will relate the aforementioned *mod p* reduction of the twisted Edwards curves and elliptic curves of **Type-II**. In equation (10) we set,

$$a^* = a; \quad b = 0; \quad c = -1 \quad \text{and} \quad A = d; \quad B = 0; \quad C = -1.$$

Thus, we compute,

$$D = 4d; \quad \Delta = -4(a+d); \quad d^* = 4a \quad \text{and} \quad \Delta^2 - 4Dd^* = (4(a-d))^2 \quad \not\equiv 0 \quad (mod\ p).$$

This is equivalent to $a \not\equiv d \not\equiv 0$ (*mod p*). An important aspect to note here is that the *non-zero* integers $a$ and $d$ are chosen so that the **Type-II** family of curves is *non-singular*. Also, $p$ is chosen under the conditions discussed in section 2. Thus, we are ready to substitute these values in (10). Hence, we have

$$\sum_{x=0}^{p-1} \left(\frac{\frac{ax^2-1}{dx^2-1}}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{4d}{p}\right) \left(\frac{x^3 - \frac{a+d}{d}x^2 + \frac{a}{d}x}{p}\right) - \left(\frac{ad}{p}\right).$$

Using basic properties of Legendre symbol, we obtain,

$$\sum_{x=0}^{p-1} \left(\frac{\frac{ax^2-1}{dx^2-1}}{p}\right) = \left(\frac{d}{p}\right) \sum_{x=0}^{p-1} \left(\frac{x(x-1)\left(x-\frac{a}{d}\right)}{p}\right) - \left(\frac{ad}{p}\right)$$

and this implies

$$-(p + 2 - \#E'_{a,d,p}(\mathbb{F}_p)) = -\left(\frac{d}{p}\right) tr(E'_p) - \left(\frac{ad}{p}\right).$$

To relate the trace of (11) and (12), we follow the similar notation as equation (2). Next, we multiply both sides by $\left(\frac{d}{p}\right)$ and derive the following,

$$-\left(\frac{d}{p}\right) tr(E'_{a,d,p}) = -tr(E'_p) - \left(\frac{a}{p}\right),$$

where $\left(\frac{d}{p}\right)$ and $\left(\frac{a}{p}\right)$ are *non-zero*, since $a$ and $d$ are *non-zero* and not divisible by $p$ and the proof follows. □

**Remark 6.** *If we choose $D, \Delta,$ and $d^*$, in such a way that, $x^3 + \frac{\Delta}{D}x^2 + \frac{d^*}{D}x$ is an elliptic curve over $\mathbb{Q}$ having complex multiplication, then the character sum $\sum_{x=0}^{p-1} \left(\frac{x^3 + \frac{\Delta}{D}x^2 + \frac{d^*}{D}x}{p}\right)$ can be explicitly evaluated using Deuring's Lifting Theorem* [Deu41].

## 6. Proof of Corollary 2.3

As we mentioned earlier, our another goal is to study the *Hasse-Weil L-function* at $s=1$ for certain families of elliptic curves. The *L-function associated to* $E_G$ (eq (4)) is defined by,

$$L(E_G,s)=\prod_{p\nmid\Delta}\left(1-\frac{tr(E_{G,p})}{p^s}+\frac{p}{p^{2s}}\right)^{-1}\prod_{p|\Delta}\left(1-\frac{tr(E_{G,p})}{p^s}\right)^{-1}. \tag{13}$$

The infinite product in (13) is absolutely convergent for $\Re(s)>3/2$, and it can be expanded into the Dirichlet series $L(E_G,s)=\sum_{n=1}^{\infty}a_n n^{-s}$. In general, the Euler product (13) for $L(E_G,s)$ may not converge at $s=1$, but formally evaluating (13) at $s=1$ gives,

$$L(E_G,1)=\prod_{p\nmid\Delta}\left(\frac{\#E_{G,p}}{p}\right)^{-1}.$$

Here the equality implies almost equal. Since, $\Delta$ is finite, thus there are only finite number of terms in the second product.

In equation (13), we have observed that for any elliptic curve $E_G$ over $\mathbb{Q}$, the Hasse-Weil $L$-function at $s=1$ can be written as

$$L(E_G,1)=\prod_{p}\frac{p}{p+1-tr(E_{G,p})}. \tag{14}$$

Now we are ready to give the proof of the Corollary.

*Proof of Corollary 2.3:* A relation between trace of **Type-I** elliptic curves and trace of Edwards curve (eq (1)) has been obtained in Proposition 4.1 like;

$$tr(E_p)=\left(\frac{d}{p}\right)tr(E_{a,d,p})-1. \tag{15}$$

For proving the first expression, we re-write equation (14) for the **Type-I** family of curves as

$$L(E,1)=\prod_{p}\frac{p}{p+1-tr(E_p)}.$$

Using equation (15), we obtain

$$L(E,1)=\prod_{p}\frac{p}{p-\left(\frac{d}{p}\right)tr(E_{a,d,p})+2}.$$

Now, we connect trace of the Edwards curve, $tr(E_{a,d,p})$, with hypergeometric series as obtained in Theorem 2.1. Using that, we get the following expression of $L$-function which concludes the proof of first part;

$$L(E,1)=\prod_{p}\left[\frac{p+1}{p}+\phi_p(d)\;{}_2F_1\left(\begin{matrix}\phi_p & \phi_p\\ & \epsilon_p\end{matrix}\;\middle|\;1-a^4d\right)\right]^{-1}.$$

For concluding the second statement, we use the relation proved in Proposition 5.1 as $tr(E'_p)=\left(\frac{d}{p}\right)tr(E'_{a,d,p})-\left(\frac{a}{p}\right)$. For the expression of $L(E',1)$, similar as above, we re-write equation (14) for **Type-II** elliptic curves to get

$$L(E',1)=\prod_{p}\frac{p}{p+1-tr(E'_p)}. \tag{16}$$

Invoking the aforementioned trace relation, we obtain

$$L(E',1)=\prod_{p}\frac{p}{p-\left(\frac{d}{p}\right)tr(E'_{a,d,p})+\left(\frac{a}{p}\right)+1}. \tag{17}$$

Now, we invoke Lemma 3.3.1 in equation (17) to determine $tr(E'_{a,d,p})$ in terms of hypergeometric series. Thus we obtain

$$L(E',1) = \prod_{p} \left[ 1 + \frac{\phi_p(a)}{p} + \phi_p(-ad) \left\{ {}_2F_1 \left( \begin{matrix} \phi_p & \phi_p \\ & \epsilon_p \end{matrix} \middle| \, a^{-1}d \right) \right\} \right]^{-1},$$

which concludes the proof of Theorem 2.2. □

## 7. Conclusion and Remarks

Our holistic objective was to conjoin two disparate transformation formulae ([Wil70] and [Gre87], the first one is obtained by purely algebraic means, whereas the second one is analytic). To the best of our knowledge, the literature is devoid of the reconciliation of these paradigms and techniques. In this article, we illustrated a method for the evaluation of the Hasse-Weil $L$-function at $s = 1$ for some families of elliptic curves, utilizing Edwards curve [Edw07], the Gaussian hypergeometric series [SES16], and finite transformation formula [Wil70].

One of the remark is about point counting on elliptic curves and their alternate parametrization. The Schoof-Elkies-Atkins **(SEA)** [Sch95] technique can be used to efficiently compute the trace of $E'_{a,d,p}$ or $E'_p$; once one of them is known, the other can be computed using Proposition 5.1. Similar argument follows for $E_{a,d,p}$ and $E_p$ from Proposition 4.1. In section 2, we mentioned the conditions for choosing the prime $p$. If we introduce one more condition that we will only consider those primes for which the bi-rational map between the twisted Edwards curve $E'_{a,d}$ (characterized by equation (2)) and the corresponding elliptic curve $E'_{W,a,d}$ in Weierstrass form (characterized by equation (3)), i.e.; $\psi : E'_{a,d} \to E'_{W,a,d}$ is invariant under *mod p* reduction; Then, for such primes $p$, proposition 5.1 can be expressed in terms of $E'_{W,a,d}$. Similar argument would follow for the **Type-I** elliptic curves too.

## 8. Acknowledgment

The authors thank the referee for suggestions and careful reading. All the authors are greatly indebted towards Prof. Mohammad Sadek for taking interest in this research work and directing it towards the *hypergeometric* way. The second author would like to thank Mr. Manoj Gyawali for describing the idea of homogenizing the Edwards curve, which simplified some computations in SAGE computer algebra system. The second author is grateful to Prof. Norberto Gavioli for his comments on the algebraic manipulations involving the Legendre symbol. The third author would like to thank Tata Institute of Fundamental Research for their kind support during her post-doctoral tenure.

## References

[BBJ+08] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted edwards curves*, International Conference on Cryptology in Africa, Springer, 2008, pp. 389–405.

[BK13] Rupam Barman and Gautam Kalita, *Elliptic curves and special values of gaussian hypergeometric series*, Journal of Number Theory **133** (2013), no. 9, 3099–3111.

[Dam12] MR Dam, *Edwards elliptic curves*, Ph.D. thesis, Faculty of Science and Engineering, 2012.

[Deu41] Max Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, vol. 14, Springer, 1941, pp. 197–272.

[Edw07] Harold Edwards, *A normal form for elliptic curves*, Bulletin of the American mathematical society **44** (2007), no. 3, 393–422.

[GG05] Ivor Grattan-Guinness, *Landmark writings in western mathematics 1640-1940*, Elsevier, 2005.

[Gre87] John Greene, *Hypergeometric functions over finite fields*, Transactions of the American Mathematical Society **301** (1987), no. 1, 77–101.

[Ono98] Ken Ono, *Values of gaussian hypergeometric series*, Transactions of the American Mathematical Society **350** (1998), no. 3, 1205–1223.

[Ono04] ———, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series: Arithmetic of the coefficients of modular forms and q-series*, no. 102, American Mathematical Soc., 2004.

[Sch95] René Schoof, *Counting points on elliptic curves over finite fields*, Journal de théorie des nombres de Bordeaux **7** (1995), no. 1, 219–254.

[SES16] Mohammad Sadek and Nermine El-Sissi, *Edwards curves and gaussian hypergeometric series*, Journal de Théorie des Nombres de Bordeaux **28** (2016), no. 1, 115–124.

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[Ste68] NM Stephens, *The diophantine equation $x^3+y^3 = dz^3$ and the conjectures of birch and swinnerton-dyer.*, Journal für die reine und angewandte Mathematik **231** (1968), 121–162.

[SZ08] Susanne Schmitt and Horst G Zimmer, *Elliptic curves: A computational approach*, vol. 31, Walter de Gruyter, 2008.

[Wil70] Kenneth Williams, *Finite transformation formulae involving the legendre symbol*, Pacific Journal of Mathematics **34** (1970), no. 2, 559–568.

[Wil79] Kenneth S Williams, *Evaluation of character sums connected with elliptic curves*, Proceedings of the American Mathematical Society **73** (1979), no. 3, 291–299.

Abhishek Juyal, Department of Mathematics, Hemwati Nandan Bahuguna (H.N.B.) Garhwal University, Srinagar Garhwal, Uttarakhand, 246175, India.

*Email address*: abhinfo1402@gmail.com

Ankan Pal, Department of Mathematics, University of L'Aquila, Via Vetoio, L'Aquila - 67100, Italy.

*Email address*: ankanpal100@gmail.com

Bidisha Roy, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai - 400005, India. **Current address:** Bidisha Roy, Scuola Normale Superiore di Pisa, Piazza dei Cavalieri 7, Pisa 56126, Italy

*Email address*: brroy123456@gmail.com