JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Mohammad SADEK et Nermine EL-SISSI

Edwards Curves and Gaussian Hypergeometric Series

Tome 28, n° 1 (2016), p. 115-124.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_1_115_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 115–124

Edwards Curves and Gaussian Hypergeometric Series

par Mohammad SADEK et Nermine EL-SISSI

Résumé. Soit E une courbe elliptique décrite par un modèle d'Edwards ou un modèle d'Edwards tordu sur $\mathbb{F}_p$, à savoir, E est définie par une des équations suivantes $x^2+y^2 = a^2(1+x^2y^2)$, $a^5-a \not\equiv 0 \bmod p$, ou, $ax^2+y^2 = 1+dx^2y^2$, $ad(a-d) \not\equiv 0 \bmod p$, respectivement. Nous représentons le nombre de points rationnels de E sur $\mathbb{F}_p$ en utilisant la série hypergéométrique de Gauss ${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\middle| x\right)$ où ϵ et ϕ sont les caractères trivial et quadratique sur $\mathbb{F}_p$, respectivement. Cette représentation nous permet d'évaluer $|E(\mathbb{F}_p)|$ pour certaines courbes elliptiques E, et de démontrer l'existence d'isogénies entre E et des courbes elliptiques de Legendre sur $\mathbb{F}_p$.

Abstract. Let E be an elliptic curve described by either an Edwards model or a twisted Edwards model over $\mathbb{F}_p$, namely, E is defined by one of the following equations $x^2+y^2 = a^2(1+x^2y^2)$, $a^5-a \not\equiv 0 \bmod p$, or, $ax^2+y^2 = 1+dx^2y^2$, $ad(a-d) \not\equiv 0 \bmod p$, respectively. We express the number of rational points of E over $\mathbb{F}_p$ using the Gaussian hypergeometric series ${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\middle| x\right)$ where ϵ and ϕ are the trivial and quadratic characters over $\mathbb{F}_p$ respectively. This enables us to evaluate $|E(\mathbb{F}_p)|$ for some elliptic curves E, and prove the existence of isogenies between E and Legendre elliptic curves over $\mathbb{F}_p$.

1. Introduction

In [4] Greene initiated the study of Gaussian hypergeometric series over finite fields. These series are analogous to the classical hypergeometric series. Several authors managed to find congruence relations satisfied by special values of these series, see [6]. Many special values of these series were determined.

One of the striking aspects of hypergeometric series is that some of their special values are linked to the number of rational points on some families

Manuscrit reçu le 27 novembre 2013, accepté le 15 mars 2015.
Mathematics Subject Classification. 11T24, 14H52.
Mots-clefs. Edwards Curves, Gaussian Hypergeometric Series, Finite Fields.

of algebraic curves over finite fields. Two families of elliptic curves were discussed in [5]. The number of rational points of an elliptic curve E described by a Legendre model, namely, $y^2 = x(x-1)(x-\lambda)$, $\lambda(\lambda-1) \not\equiv 0 \bmod p$, over the finite field $\mathbb{F}_p$ satisfies the following identity

$$|E(\mathbb{F}_p)| = 1 + p + p\phi(-1) \cdot {}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\Big|\lambda\right)$$

where ϵ and ϕ are the trivial and quadratic characters over $\mathbb{F}_p$ respectively. The latter identity was used to evaluate the hypergeometric series ${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\Big|\lambda\right)$ when $\lambda \in \{-1, 1/2, 2\}$. If E is defined by a Clausen model, $y^2 = (x-1)(x^2+\lambda), \lambda(\lambda+1) \not\equiv 0 \bmod p$, then

$$(1 + p - |E(\mathbb{F}_p)|)^2 = p + p^2\phi(\lambda+1) \cdot {}_3F_2\left(\begin{matrix}\phi & \phi & \phi \\ & \epsilon & \epsilon\end{matrix}\Big|\frac{\lambda}{\lambda+1}\right).$$

Again this was exploited in order to evaluate the hypergeometric series ${}_3F_2\left(\begin{matrix}\phi & \phi & \phi \\ & \epsilon & \epsilon\end{matrix}\Big|\frac{\lambda}{\lambda+1}\right)$ at some specific values of λ.

More Gaussian hypergeometric series appear in formulas describing the number of rational points on higher genus curves over finite fields. Some of these formulas can be found in [1] where the following family of algebraic curves are discussed

$$y^l = x(x-1)(x-\lambda),\ \lambda(\lambda-1) \not\equiv 0 \bmod p,\ l \geq 2.$$

In this note we are interested in elliptic curves described by Edwards models or twisted Edwards models, namely

$$\begin{aligned} x^2 + y^2 &= a^2(1 + x^2y^2),\ a^5 - a \not\equiv 0 \bmod p; \\ ax^2 + y^2 &= 1 + dx^2y^2,\ ad(a-d) \not\equiv 0 \bmod p \end{aligned}$$

respectively.

Edwards models of elliptic curves were proposed in [3] and have been used since then in many cryptographic applications. The main advantage enjoyed by these curves is that the group law is simpler to state than on other models representing elliptic curves. In addition, any elliptic curve defined over an algebraically closed field k can be expressed in the form $x^2+y^2 = a^2(1+x^2y^2)$. Twisted Edwards models appeared for the first time in [2] to express more elliptic curves over finite fields with the addition law being easily formulated.

We show that the number of rational points on an Edwards curve E over a finite field $\mathbb{F}_p$ can be written in terms of the Gaussian hypergeometric series ${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\Big|x\right)$. Consequently, we evaluate $|E(\mathbb{F}_p)|$ for some E. Then we prove that every Edwards curve is isogenous to a Legendre curve over $\mathbb{F}_p$. Finally, it turns out that the number of rational points on a twisted

Edwards curve E is described using special values of the hypergeometric series ${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\middle| x\right)$. This sets the stage for evaluating $|E(\mathbb{F}_p)|$ for some twisted Edwards curves E.

2. Gaussian hypergeometric series

Throughout the note p will be an odd prime unless otherwise stated. We extend multiplicative characters χ defined over $\mathbb{F}_p^\times$ to $\mathbb{F}_p$ by setting $\chi(0) = 0$. We write $\overline{\chi}$ to denote $1/\chi$. The trivial and quadratic characters will be denoted by ϵ and ϕ respectively. Let $J(A, B)$ denote the Jacobi sum

$$J(A, B) = \sum_{x \in \mathbb{F}_p} A(x)B(1 - x)$$

where A and B are characters over $\mathbb{F}_p$. Let $A_0, A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ be characters defined over $\mathbb{F}_p$. The *Gaussian hypergeometric series* is

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

where the sum is over all characters over $\mathbb{F}_p$ and

$$\binom{A}{B} := \frac{B(-1)}{p}J(A, \overline{B}) = \frac{B(-1)}{p}\sum_{x \in \mathbb{F}_p} A(x)\overline{B}(1 - x).$$

The following properties of the symbol $\binom{A}{B}$ can be found in [4].

Lemma 2.1. *For any characters A and B over $\mathbb{F}_p$, one has:*

a) $A(1 + x) = \delta(x) + \frac{p}{p-1}\sum_{\chi}\binom{A}{\chi}\chi(x)$ *where* $\delta(x) = 1$ *if* $x = 0$ *and* $\delta(x) = 0$ *if* $x \neq 0$;

b) $\overline{A}(1-x) = \delta(x) + \frac{p}{p-1}\sum_{\chi}\binom{A\chi}{\chi}\chi(x)$ *where* $\delta(x) = 1$ *if* $x = 0$ *and* $\delta(x) = 0$ *if* $x \neq 0$;

c) $\binom{A}{B} = \binom{A}{A\overline{B}}$;

d) $\binom{A}{B} = \binom{B\overline{A}}{B}B(-1)$;

e) $\binom{A}{\epsilon} = \binom{A}{A} = -\frac{1}{p} + \frac{p-1}{p}\delta(A)$ *where* $\delta(A) = 1$ *if* $A = \epsilon$ *and* $\delta(A) = 0$ *otherwise;*

f) $$\begin{pmatrix} B^2\chi^2 \\ \chi \end{pmatrix} = \begin{pmatrix} \phi B\chi \\ \chi \end{pmatrix}\begin{pmatrix} B\chi \\ B^2\chi \end{pmatrix}\begin{pmatrix} \phi \\ \phi B \end{pmatrix}^{-1} B\chi(4).$$

3. Rational points on Edwards curves

Let E be an elliptic curve over a field k with $\operatorname{char} k \neq 2$ defined by an Edwards model

$$x^2 + y^2 = a^2(1 + x^2y^2), \text{ where } a^5 - a \neq 0.$$

Such an elliptic curve will be called an *Edwards curve*. If (x_1, y_1) and (x_2, y_2) are two points on E, then these two points add up to

$$x_3 = \frac{1}{a} \cdot \frac{x_1y_2 + x_2y_1}{1 + x_1x_2y_1y_2}, \; y_3 = \frac{1}{a} \cdot \frac{y_1y_2 - x_1x_2}{1 - x_1x_2y_1y_2}.$$

There are two points at infinity, namely if we homogenize the defining equation, we get

$$x^2z^2 + y^2z^2 = a^2(z^4 + x^2y^2)$$

and the points at infinity are $(x : y : z) \in \{(1 : 0 : 0), (0 : 1 : 0)\}$.

We will need the following lemma to count rational points on an Edwards curve.

Lemma 3.1. *Let A be a character on $\mathbb{F}_p$ and $a \in {\mathbb{F}_p}^\times$. The following identities hold:*

a) $$\begin{pmatrix} A^2 \\ A \end{pmatrix} = \begin{cases} \binom{\phi A}{A} A(4) & \text{if } A \neq \epsilon \\ \frac{p-2}{p} & \text{if } A = \epsilon \end{cases}$$

b) $$\sum_{x \in \mathbb{F}_p} A(a^2 - x^2) = pA(4a^2)\begin{pmatrix} \overline{A}^2 \\ \overline{A} \end{pmatrix} = \begin{cases} pA(a^2)\binom{\phi\overline{A}}{\overline{A}} & \text{if } A \neq \epsilon \\ p - 2 & \text{if } A = \epsilon \end{cases}$$

Proof. a) In Lemma 2.1 f), put $B = \epsilon$ and $\chi = A$. This yields

$$\begin{pmatrix} A^2 \\ A \end{pmatrix} = \begin{pmatrix} \phi A \\ A \end{pmatrix}\begin{pmatrix} A \\ A \end{pmatrix}\begin{pmatrix} \phi \\ \phi \end{pmatrix}^{-1} A(4).$$

According to Lemma 2.1 e), the product above is $\begin{pmatrix} \phi A \\ A \end{pmatrix} A(4)$ if $A \neq \epsilon$, and it is $(2 - p)\begin{pmatrix} \phi A \\ A \end{pmatrix} A(4)$ if $A = \epsilon$.

To prove b), we notice that

$$\sum_{x \in \mathbb{F}_p} A(a^2 - x^2) = A\left(4a^2\right) \sum_{x \in \mathbb{F}_p} A\left(\frac{1}{2} - \frac{x}{2a}\right) A\left(\frac{1}{2} + \frac{x}{2a}\right)$$

Setting $u = \frac{1}{2} - \frac{x}{2a}$, the above sum becomes

$$\sum_{x\in\mathbb{F}_p} A(a^2-x^2) = A\left(4a^2\right)\sum_{u\in\mathbb{F}_p} A(u)A(1-u)$$
$$= A(4a^2)J(A,A) = pA(-4a^2)\left(\frac{A}{\overline{A}}\right).$$

Using Lemma 2.1 d), one has $\left(\frac{A}{\overline{A}}\right) = \left(\frac{\overline{A}^2}{\overline{A}}\right)\overline{A}(-1)$. Part b) now follows from a). □

The following theorem relates the number of rational points on an Edwards curve over $\mathbb{F}_p$ to a Gaussian hypergeometric series.

Theorem 3.2. *Let $E/\mathbb{F}_p$ be described by $x^2+y^2 = a^2(1+x^2y^2)$ where $a^5 \not\equiv a \bmod p$, p is an odd prime. Then*

$$|E(\mathbb{F}_p)| = 1 + p + p\cdot {}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big| 1-a^4\right).$$

Proof. The defining equation of E can be written as:

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

Bearing in mind that there are two points at infinity, one has

$$|E(\mathbb{F}_p)| = 2 + p + \sum_{x\in\mathbb{F}_p\setminus\{\pm a^{-1}\}} \phi\left(\frac{a^2-x^2}{1-a^2x^2}\right)$$
$$= 2 + p + \sum_{x\in\mathbb{F}_p\setminus\{\pm a^{-1}\}} \phi\left(1+\frac{a^2-a^{-2}}{a^{-2}-x^2}\right)$$
$$= 2 + p + \sum_{x\in\mathbb{F}_p\setminus\{\pm a^{-1}\}} \Big[\delta\left(\frac{a^2-a^{-2}}{a^{-2}-x^2}\right) + \frac{p}{p-1}\sum_{\chi}\binom{\phi}{\chi}\chi\left(\frac{a^2-a^{-2}}{a^{-2}-x^2}\right)\Big]$$
$$= 2 + p + \frac{p}{p-1}\sum_{x\in\mathbb{F}_p\setminus\{\pm a^{-1}\}}\sum_{\chi}\binom{\phi}{\chi}\chi\left(\frac{a^2-a^{-2}}{a^{-2}-x^2}\right)$$
$$= 2 + p + \frac{p}{p-1}\sum_{\chi}\binom{\phi}{\chi}\chi\left(a^2-a^{-2}\right)\sum_{x\in\mathbb{F}_p}\overline{\chi}(a^{-2}-x^2).$$

The third equality follows from Lemma 2.1 a). Now we use Lemma 3.1 b) to obtain the following identity:

$$|E(\mathbb{F}_p)| = 2+p+\frac{p}{p-1}\Big[p\sum_{\chi\neq\epsilon}\binom{\phi}{\chi}\binom{\phi\chi}{\chi}\overline{\chi}\left(a^{-2}\right)\chi\left(a^2-a^{-2}\right)+\binom{\phi}{\epsilon}(p-2)\Big].$$

Lemma 2.1 d) gives $\binom{\phi}{\chi} = \binom{\overline{\phi}\chi}{\chi}\chi(-1) = \binom{\phi\chi}{\chi}\chi(-1)$, thus

$$\begin{aligned}|E(\mathbb{F}_p)| &= 2+p+\frac{p^2}{p-1}\Big[\sum_{\chi\neq\epsilon}\binom{\phi\chi}{\chi}\binom{\phi\chi}{\chi}\chi\left(1-a^4\right)+\frac{2-p}{p^2}\Big]\\ &= 2+p+\frac{p^2}{p-1}\Big[\sum_{\chi}\binom{\phi\chi}{\chi}\binom{\phi\chi}{\chi}\chi\left(1-a^4\right)-\binom{\phi}{\epsilon}^2+\frac{2-p}{p^2}\Big]\\ &= 1+p+p\cdot{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|1-a^4\right).\end{aligned}$$

□

The Legendre family of elliptic curves is the one defined by

$$E_\lambda : y^2 = x(x-1)(x-\lambda),\ \lambda(\lambda-1)\not\equiv 0 \bmod p.$$

Theorem 1 in [5] states that $|E_\lambda(\mathbb{F}_p)| = 1+p+p\,\phi(-1)\cdot{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|\lambda\right)$. Since two elliptic curves over $\mathbb{F}_p$ are isogenous if and only if they have the same number of rational points, comparing $|E_\lambda(\mathbb{F}_p)|$ to the number of rational points of an Edwards curve E over $\mathbb{F}_p$ defined by $x^2+y^2 = a^2(1+x^2y^2)$, see Theorem 3.2, yields that E is isogenous to the Legendre elliptic curve E_{1-a^4} if $p\equiv 1 \bmod 4$. In fact, every Edwards curve is isogenous to a Legendre curve over $\mathbb{F}_p$.

Corollary 3.3. *Let E be defined by $x^2+y^2 = a^2(1+x^2y^2)$ over $\mathbb{F}_p$, where p is an odd prime and $a^5\not\equiv a \bmod p$. Then E is isogenous to the Legendre elliptic curve $E_{a^4} : y^2 = x(x-1)(x-a^4)$.*

Proof. According to Theorem 1 in [5],

$$|E_{a^4}(\mathbb{F}_p)| = 1+p+p\phi(-1)\cdot{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|a^4\right).$$

The following identity is Theorem 4.4 (i) of [4]

$${}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|x\right) = \phi(-1)\cdot{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|1-x\right).$$

Now set $x = a^4$ and use Theorem 3.2. Consequently, E and E_{a^4} have the same number of rational points over $\mathbb{F}_p$. It follows that they are isogenous over $\mathbb{F}_p$. □

We recall the following Proposition which can be found as Theorem 2 in [5].

Proposition 3.4. *Let p be an odd prime. If $\lambda \in \{-1, 1/2, 2\}$, then*

$$ {}_2F_1\left(\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\middle|\lambda\right) = \begin{cases} 0 & \text{if } p \equiv 3 \bmod 4, \\ \frac{2x\cdot(-1)^{(x+y+1)/2}}{p} & \text{if } p \equiv 1 \bmod 4, x^2+y^2 = p, x \text{ is odd.} \end{cases} $$

Corollary 3.5. *Let $E/\mathbb{F}_p$ be defined by $x^2+y^2 = a^2(1+x^2y^2)$ where $a^5 \not\equiv a \bmod p$. If $a^4 \in \{-1, 1/2, 2\}$, then*

$$ |E(\mathbb{F}_p)| = \begin{cases} 1+p & \text{if } p \equiv 3 \bmod 4, \\ 1+p+2x\cdot(-1)^{(x+y+1)/2} & \text{if } p \equiv 1 \bmod 4, x^2+y^2 = p, x \text{ is odd.} \end{cases} $$

Proof. This follows immediately from Corollary 3.3. □

4. Rational points on twisted Edwards curves

Twisted Edwards curves were introduced in [2] as generalizations of Edwards curves. These curves include more elliptic curves over finite fields than Edwards curves do. A twisted Edwards curve is an elliptic curve defined by the following *twisted Edwards model*

$$ ax^2 + y^2 = 1 + dx^2y^2 $$

where $ad(a-d) \neq 0$. For any field k with $\mathrm{char}(k) \neq 2$, any elliptic curve over k with three k-rational points of order 2 is 2-isogenous over k to a twisted Edwards curve, see Theorem 5.1 of [2], hence they have the same number of rational points over $\mathbb{F}_p$.

Lemma 4.1. *The following equality holds for any character A over $\mathbb{F}_p$*

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

Proof. We recall that the number of solutions of the equation $z^2 = a \bmod p$ is given by $N_a = \phi(a)+1$. In fact $N_a = 2$ if $a \in {\mathbb{F}_p}^2, a \neq 0$, $N_0 = 1$, and $N_a = 0$ otherwise. We consider the following sum:

$$ \begin{aligned} \sum_x \chi(x)\phi(x)\phi(1-x) &= \sum_x \chi(x)\phi(1-x)\,(N_x - 1) \\ &= \sum_x \chi(x)\phi(1-x)N_x - \sum_x \chi(x)\phi(1-x) \\ &= 2\sum_{x\in\mathbb{F}_p^2} \chi(x)\phi(1-x) - \sum_x \chi(x)\phi(1-x) \\ &= \sum_x \chi(x^2)\phi(1-x^2) - \sum_x \chi(x)\phi(1-x). \end{aligned} $$

Therefore,

$$\sum_x \chi(x^2)\phi(1-x^2) = J(\phi\chi,\phi) + J(\chi,\phi)$$
$$= p\phi(-1)\left[\binom{\phi\chi}{\phi} + \binom{\chi}{\phi}\right].$$

Using Lemma 2.1 c), one has $\binom{\phi\chi}{\phi} = \binom{\phi\chi}{\chi}$, similarly $\binom{\chi}{\phi} = \binom{\chi}{\phi\chi}$. □

Theorem 4.2. *Let $E/\mathbb{F}_p$ be described by $ax^2 + y^2 = 1 + dx^2y^2$ where $ad(a-d) \not\equiv 0$ mod p, p is an odd prime. Then*

$$|E(\mathbb{F}_p)| = 2 + p + \phi(a) + p\phi(-a)\left[{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big| a^{-1}d\right) + {}_2F_1\left(\begin{matrix}\phi & \epsilon\\ & \phi\end{matrix}\Big| a^{-1}d\right)\right].$$

In particular,

$$|E(\mathbb{F}_p)| = 2 + p - \phi(d) + p\phi(-a)\cdot {}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big| a^{-1}d\right).$$

Proof. We observe that we can write the above twisted Edwards model as

$$x^2 = \frac{1-y^2}{a-dy^2}.$$

We set $b = a^{-1}d$. The number of rational points of E over $\mathbb{F}_p$ is given by

$$|E(\mathbb{F}_p)| = 2 + p + \sum_{y\in\mathbb{F}_p\setminus\{\sqrt{ad^{-1}}\}} \phi\left(\frac{1-y^2}{a-dy^2}\right)$$
$$= 2 + p + \sum_{y\in\mathbb{F}_p} \phi\left(1-y^2\right)\phi\left(a-dy^2\right)$$
$$= 2 + p + \phi(a)\sum_{y\in\mathbb{F}_p} \phi(1-y^2)\phi(1-by^2)$$
$$= 2 + p + \phi(a)\sum_{y\in\mathbb{F}_p} \phi(1-y^2)\left[\delta(by^2) + \frac{p}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\chi(by^2)\right].$$

The last equality follows from Lemma 2.1 b). According to Lemma 4.1, one obtains

$$\begin{aligned}|E(\mathbb{F}_p)| &= 2+p+\phi(a)+\frac{p\phi(a)}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\chi(b)\sum_{y\in\mathbb{F}_p}\chi(y^2)\phi(1-y^2)\\ &= 2+p+\phi(a)+\frac{p^2\phi(-a)}{p-1}\sum_{\chi}\binom{\phi\chi}{\chi}\left[\binom{\phi\chi}{\chi}+\binom{\chi}{\phi\chi}\right]\chi(b)\\ &= 2+p+\phi(a)+p\phi(-a)\left[{}_2F_1\left(\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}\Big|a^{-1}d\right)+{}_2F_1\left(\begin{matrix}\phi & \epsilon\\ & \phi\end{matrix}\Big|a^{-1}d\right)\right].\end{aligned}$$

However, Corollary 3.16 in [4] indicates that

$$\begin{aligned}{}_2F_1\left(\begin{matrix}\phi & \epsilon\\ & \phi\end{matrix}\Big|a^{-1}d\right) &= \binom{\phi}{\phi}\phi(-a^{-1}d)\epsilon(1-a^{-1}d)-\frac{1}{p}\phi(-1)\epsilon(a^{-1}d)\\ &\quad+\frac{p-1}{p}\phi(-1)\delta(1-a^{-1}d)\delta(\epsilon)\\ &= -\frac{1}{p}\phi(-a^{-1}d)-\frac{1}{p}\phi(-1).\end{aligned}$$

This proves the theorem. □

Corollary 4.3. *Let p be an odd prime. Let $E/\mathbb{F}_p$ be defined by $ax^2+y^2=1+dx^2y^2$ where $ad(a-d)\not\equiv 0$ mod p. If $\lambda := a^{-1}d \in \{-1, 1/2, 2\}$, then*

$$|E(\mathbb{F}_p)| = \begin{cases}2+p-\phi(d) & \text{if } p\equiv 3 \bmod 4,\\ 2+p-\phi(d)+2x\cdot\phi(a)\cdot(-1)^{(x+y+1)/2} & \\ & \text{if } p\equiv 1 \bmod 4, x^2+y^2=p, x \text{ is odd.}\end{cases}$$

Proof. This follows from Theorem 4.2 and Proposition 3.4. □

We remark that any Legendre curve is isogenous to a twisted Edwards curve over $\mathbb{F}_p$. Indeed, any elliptic curve E with three $\mathbb{F}_p$-rational points of order 2 defined by $y^2=x(x-a)(x-b)$ is isogenous to the twisted Edwards curve $4ax^2+y^2=1+4bx^2y^2$, see Theorem 5.1 in [2]. Thus the formula for the number of rational points on a Legendre elliptic curve over $\mathbb{F}_p$, Theorem 1 of [5], follows as a special case from Theorem 4.2.

References

[1] R. Barman & G. Kalita, "Hypergeometric functions and a family of algebraic curves", *Ramanujan J.* **28** (2012), no. 2, p. 175-185.

[2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange & C. Peters, "Twisted Edwards curves", in *Progress in cryptology—AFRICACRYPT 2008*, Lecture Notes in Comput. Sci., vol. 5023, Springer, Berlin, 2008, p. 389-405.

[3] H. M. Edwards, "A normal form for elliptic curves", *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), no. 3, p. 393-422 (electronic).

[4] J. Greene, "Hypergeometric functions over finite fields", *Trans. Amer. Math. Soc.* **301** (1987), no. 1, p. 77-101.
[5] K. Ono, "Values of Gaussian hypergeometric series", *Trans. Amer. Math. Soc.* **350** (1998), no. 3, p. 1205-1223.
[6] R. Osburn & C. Schneider, "Gaussian hypergeometric series and supercongruences", *Math. Comp.* **78** (2009), no. 265, p. 275-292.

Mohammad Sadek
Department of Mathematics and Actuarial Science
American University in Cairo
74 S El-Teseen St, New Cairo
Cairo Governorate 11835
EGYPT
E-mail: mmsadek@aucegypt.edu

Nermine El-Sissi
Department of Mathematics and Actuarial Science
American University in Cairo
74 S El-Teseen St, New Cairo
Cairo Governorate 11835
EGYPT
E-mail: nelsissi@aucegypt.edu