Edwards model of elliptic curves defined over any finite field

Oumar Diao[1] and Emmanuel Fouotsa[2]

[1]Université de Rennes I, Laboratoire IRMAR Campus de Beaulieu, 35042 Rennes Cedex, France, oumar.diao@univ-rennes1.fr
[2]Department of Mathematics, University of Bamenda, Higher Teacher Training College P.O. BOX 39, Bambili-Cameroon, emmanuelfouotsa@prmais.org

January 8, 2013

Abstract

In this paper, we present an Edwards model for elliptic curves which is defined over any perfect field and in particular over finite fields. This Edwards model is birationally equivalent to the well known Edwards model over non-binary fields and is ordinary over binary fields. For this, we use theta functions of level four to obtain an intermediate model that we call a level 4 theta model. This model enables us to obtain the new Edwards model with a complete and unified group law. Over binary fields, we present an efficient arithmetic of these curves. We also provide competitive differential addition formulas over any perfect field.

Keywords: Elliptic curve, level 4 theta model, Edwards model, efficient arithmetic, theta functions, Riemann relations.

1 Introduction

In [**Edw07**], Edwards has described the model $Ed_c : x^2 + y^2 = c^2(1 + x^2y^2)$ for elliptic curves over a non-binary field $\mathbb{K}$. The sum of two points (x_1, y_1) and (x_2, y_2) on this Edwards curve Ed_c is given by:

$$\left(\frac{x_1y_2 + x_2y_1}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)}\right). \tag{1}$$

The group law on Ed_c is unified, this means that the same formulas can be used to compute both the adition of two points and the doubling of a point. But this group law is not complete, i.e. it does not work for every pair of inputs. In fact, if $x \neq 0, y \neq 0$, and the point $(x, y) \in Ed_c$, then so are $(\pm 1/x, \pm 1/y)$. But we can not compute the sum of (x, y) and $(1/x, 1/y)$ because the denominator of the second coordinate of the sum vanishes.

To fill this gap, Bernstein and Lange introduced in [**BL08**] a more general model defined by $BL_{c,d} : x^2 + y^2 = c^2(1 + dx^2y^2)$ over non-binary fields $\mathbb{K}$. Using the birational map $(\overline{x}, \overline{y}) \mapsto (x, y) = (\overline{x}\sqrt[4]{d}, \overline{y}\sqrt[4]{d})$, one transforms the classical Edwards model $Ed_c : x^2 + y^2 = c^2(1 + x^2y^2)$ to the model $BL_{c,d} : \overline{x}^2 + \overline{y}^2 = \overline{c}^2(1 + d\overline{x}^2\overline{y}^2)$, where $\overline{c} = c/\sqrt[4]{d}$. One can then derive the group law formulas on $BL_{c,d}$. The formulas obtained are also unified and the addition law is complete if d is not a square in $\mathbb{K}$. But $BL_{c,d}$ and its twisted given by $ax^2 + y^2 = 1 + dx^2y^2$ in [**BBJLP08**] always give singular model over binary fields.

To resolve the problem in binary fields, Bernstein, Lange, and Farashahi introduced in [**BLF08**] the ordinary binary model defined by $E_{B,d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2$. Another binary model is introduced in [**Wu:2010:608**] but, the connection between these binary models [**BLF08**, **Wu:2010:608**] and the classical Edwards model Ed_c of [**Edw07**] has not been made explicit, to our knowledge. To solve this problem, Diao in his thesis [**Dphd10**] introduced a new binary Edwards model which is deduced from the well known Edwards model, but the addition law is not unified and not efficient.

Contribution of this paper: Our first contribution in this work is the introduction of an Edwards model for elliptic curves which is valid in all fields. For this, we use an intermediate model given by level 4 theta functions, that we call the level 4 theta model in this paper. We obtain unified addition formulas for addition law from Riemann theta relations.
Moreover, we prove that the group laws on these curves are complete over any finite field $\mathbb{F}_q$ of characteristic $p \geq 3$ where $q \equiv 3 \bmod 4$. Over non-binary field, if $q \not\equiv 3 \bmod 4$, then we show that, the group law is complete depending on the curve parameters. Over binary field, we show that there exists a subgroup of odd order such that addition laws are complete.

Over binary fields, addition formulas are competitive with the well known models of elliptic curve. The addition of two points requires $7M + 2S + 2m$ and $12M + 2S$, respectively, for the level 4 theta model and the Edwards model where M denote the multiplication, S the square and m the multiplication by a constant in the field $\mathbb{K}$.

Over non-binary fields, we provide competitive differential addition formulas. Indeed the computation of the point nP for an arbitrary integer n and a point P costs $4M + 3S + 4m$ and $5M + 5S + 2m$ per bits of n, respectively, for the level 4 theta model and the Edwards model.

Outline: The rest of the paper is organised as follows: In section 2, we briefly review the theory of theta functions. We define the level 4 theta model and present explicit formulas for point addition in section 3 . We use the results of this section to deduce the equation and the arithmetic of our Edwards model in section 4 . Section 5 deals with the differential addition on the curves mentioned above.

2 Theta functions

In this section, we briefly review some general results about theta functions. A more comprehensive understanding, and results in this section can be found in [**Mum74**, **Mum83**, **Cos11**, **RobPhD10**, **Dphd10**].

2.1 General definition

Let $\mathcal{H}_1$ be the upper-half space over $\mathbb{C}$ and $\omega \in \mathcal{H}_1$. Let $\Lambda_\omega := \omega\mathbb{Z} + \mathbb{Z}$ be a lattice of $\mathbb{C}$ and $a, b \in \mathbb{Q}$. The theta function with rational characteristics (a, b) is by definition an analytic function on $\mathbb{C} \times \mathcal{H}_1$ given by:

$$\theta_{a,b}(z,\omega) \quad = \quad \sum_{n\in\mathbb{Z}} \exp\left(i\pi(n+a)^2\omega + 2i\pi(n+a)(z+b)\right). \tag{2}$$

A function f defined on $\mathbb{C}$ is $\Lambda_\omega-$quasi-periodic of level $\ell \in \mathbb{N}^\star$ if for all $z \in \mathbb{C}$ and $m, n \in \mathbb{Z}$, we have $f(z + \omega m + n) = \exp\left(-i\ell\pi m^2\omega - 2i\ell\pi mz\right) f(z)$. For $\ell \in \mathbb{N}^\star$, the set $\mathcal{R}_{\ell,\omega}$ of $\Lambda_\omega-$quasi-periodic functions of level ℓ is a $\mathbb{C}-$vector space of dimension ℓ. For any $\ell \in \mathbb{N}^\star$, one basis of $\mathcal{R}_{\ell,\omega}$ is given by $\mathcal{B}_\ell := \left\{\theta_{0,b}(z, \ell^{-1}\omega), b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right\}$. If $\ell = k^2$, then an alternative basis of $\mathcal{R}_{\ell,\omega}$ is

$\mathcal{B}_{(k,k)} := \left\{\theta_{a,b}(kz,\omega), a, b \in \frac{1}{k}\mathbb{Z}/\mathbb{Z}\right\}$. The change of basis between $\mathcal{B}_\ell$ and $\mathcal{B}_{(k,k)}$ can be obtained by Koizumy formulas in [**Koizumi76**]:

$$\theta_{0,b}(z, \ell^{-1}\omega) = \sum_{\alpha \in \frac{1}{k}\mathbb{Z}/\mathbb{Z}} \theta_{\alpha,kb}(kz,\omega). \tag{3}$$

If $\ell \geq 3$, then we can consider the elements of the basis of $\mathcal{R}_{\ell,\omega}$ as projective coordinates of $\mathbb{P}^{\ell-1}$. And for $\ell = 2$, the image of $\mathcal{R}_{\ell,\omega}$ in $\mathbb{P}^{\ell-1}$ is the Kummer variety associated to E, which is the quotient of E by the automorphism -1. From now on, we are interested by the set of complex functions $\Lambda_\omega-$ quasi-periodic of level 4 denoted $\mathcal{R}_{4,\omega}$.

2.2 Riemann theta relations

Riemann theta relations give algebraic relations between theta functions. With these relations, one can derive the model and the addition law on elliptic curve. In the following theorem we recall that $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ can be seen as a subgroup of $\mathbb{Z}/4\mathbb{Z}$ via the map $n \longmapsto 4n$. To facilitate the writing and the reading, we set $\theta_i(z) := \theta_{0,i}(z, 4^{-1}\omega)$ for $i \in \mathbb{Z}/4\mathbb{Z}$.

Theorem 1 *Let i, j, k and l be in $\mathbb{Z}/4\mathbb{Z}$ such that $i' = (i+j+k+l)/2, j' = (i+j-k-l)/2, k' = (i-j+k-l)/2$ and $l' = (i-j-k+l)/2$ are in $\mathbb{Z}/4\mathbb{Z}$. Let z_1 and z_2 be elements in $\mathbb{C}$. The theta functions of level 4 satisfy:*

$$\begin{aligned}\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} &\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta}(0)\theta_{l+\eta}(0) \\ &= \sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2)\end{aligned} \tag{4}$$

Proof: Consider the particular case of [**LuRo10**] when $g = 1$. We replace $i+j, i-j, k+l$ and $k-l$ by i, j, k and l, respectively. We do the same for i', j', k' and l'. Then we have

$$\begin{aligned}&\left(\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\right)\left(\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0)\right) \\ &= \left(\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\right)\left(\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2)\right)\end{aligned} \tag{5}$$

These Riemann relations (5) can be rewritten in the form:

$$\begin{aligned}\sum_{\eta,\eta' \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} &\chi(\eta+\eta')\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta'}(0)\theta_{l+\eta'}(0) \\ &= \sum_{\eta,\eta' \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta+\eta')\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta'}(z_2)\theta_{l'+\eta'}(z_2).\end{aligned} \tag{6}$$

Then by summing under all characters χ on the dual $\widehat{\frac{1}{2}\mathbb{Z}/\mathbb{Z}}$, we obtain the desired result. □

Theta functions, or more precisely Riemann relations of theta functions, give a parametrisation of elliptic curves defined over $\mathbb{C}$. It is well known that elliptic curves over $\mathbb{C}$ are isomorphic to the torus $\mathbb{C}/\Lambda_\omega$. By the classical theory of theta functions, the isomorphism $E = \mathbb{C}/\Lambda_\omega$ gives an embedding into the projective space $\mathbb{P}^3$, for more details, see [**MumRedAb04**]. Moreover, Riemann relations satisfied by theta functions are defined over $\mathbb{C}$. According to Lefschetz principle [**Sil86**], these relations are also valid over any algebraically closed field of characteristic zero. But for characteristic $p > 0$, we consider an elliptic curve E defined by $f(x, y) = 0$ over a finite field $\mathbb{F}_q$ of characteristic p. We lift the coefficients of $f(x, y)$ over $\mathbb{Z}_q$, the valuation ring of $\mathbb{Q}_q$ which is an unramified extension of $\mathbb{Q}_p$. Let $E_{\mathbb{Z}_q}$ be the canonical lift of E over $\mathbb{Z}_q$ (i.e. $\mathrm{End}(E/\mathbb{F}_q) \simeq_p \mathrm{End}(E/\mathbb{Z}_q)$). We fix an embedding $\mathbb{Q}_q \hookrightarrow \mathbb{C}$ and an application of Lefschetz principle ensures that algebraic relations defined over $\mathbb{C}$ are also valid over an algebraic extension of $\mathbb{Q}_q$. We then use a reduction modulo p to obtain relations over $\mathbb{F}_q$.

3 Level 4 theta model

In this section, we define the level 4 theta model of elliptic curve, which is valid over any finite field. We take $z_2 = 0$ in formula (4) to obtain two equations that form an elliptic curve over $\mathbb{P}^3(\mathbb{C})$, that we call the level 4 theta model elliptic curve ([**Mum66Ab**]):

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right.$$

Where $X_u = \theta_u(z_1)$, $\lambda_1 = (a_0^2 + a_2^2)/(a_1^2)$ and $\lambda_2 = 2a_1^2/(a_0 a_2)$ with $a_i = X_i(0)$.
The point $[a_0 : a_1 : a_2 : a_3]$ is called the *theta null point*. The numbers $a_i = X_i(0), i = 0, 1, 2, 3$ are called *theta constants* and satisfy the ***Jacobi relation***

$$a_0 a_2 (a_0^2 + a_2^2) = 2a_1^4 \Longleftrightarrow \lambda_1 = \lambda_2. \tag{7}$$

We can show (see for example [**Car05**]) that $a_1 = a_3$ and we can set the common value equals 1.

3.1 Valid model over any finite field

Model over non-binary fields. Let $\mathbb{K}$ be a finite field of caracteristique $p \geq 3$. The Jacobi relation (7) is defined modulo p, then above coefficients λ_1 and λ_2 are defined over $\mathbb{K}$. Thus, in projective space $\mathbb{P}^3(\mathbb{K})$ with homogeneous coordinates $[X_0 : X_1 : X_2 : X_3]$, the curve given by $E_{\lambda_1,\lambda_2} : X_0^2 + X_2^2 = \lambda_1 X_1 X_3,\ X_1^2 + X_3^2 = \lambda_2 X_0 X_2$ defines an elliptic curve over the finite field $\mathbb{K}$.

Model over even characteristic. Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $\mathcal{W}(\mathbb{F}_q)$ the ring of Witt vectors with coefficients in $\mathbb{F}_q$, which is isomorphic to $\mathbb{Z}_q$, the valuation ring of the set of $2-$adic integers. So, to obtain the level 4 theta model in even characteristic, it suffices to compute the $2-$adic valuation of theta constants. Carls in [**Car05**] proves that on the canonical lift $E_{\mathcal{W}(\mathbb{F}_q)}$, we have for all $i \in \mathbb{Z}/4\mathbb{Z}$ the relations $a_i^2 = \alpha \sum_{j\in\mathbb{Z}/4\mathbb{Z}} \phi(a_{i+j})\phi(a_j)$ where ϕ is the lift of the Frobenius of $\mathbb{F}_q$ over $\mathcal{W}(\mathbb{F}_q)$ and $\alpha \in \mathbb{Z}_q$ is a non zero constant. Thus $\alpha(a_0 + a_2) = 1$ and $a_2 = 2\alpha a_0$. Applying the 2-adic valuation, v_2, to the both hand sides of these relations implies that $v_2(a_0) = 0$ and $v_2(a_2) = 1$. Then, there exists $c_0 \in \mathbb{Z}_q$ and $c_2 \in \mathbb{Z}_q$ such that $a_0 = c_0$ and $a_2 = 2c_2$. Finally we have $\lambda_1 = c_0^2 + 4c_2^2$ and $\lambda_2 = 1/(c_0 c_2)$. The equations of level 4 theta model of elliptic curve over the binary field $\mathbb{F}_q$ has a good reduction:

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right. , \text{ where } \lambda_i \in \mathbb{K}^\star.$$

We have $\lambda_1 = c_0^2$ and $\lambda_2 = 1/(c_0 c_2)$ and the Jacobi relation given by $\lambda_1 = \lambda_2$ is equivalent to $c_0^3 c_2 = 1$.

Valid model over any finite field. Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. Then a level 4 theta model is defined by the intersection of two equations:

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right. ,$$

where $\lambda_1 = c_0^2 + 4c_2^2$, $\lambda_2 = 1/(c_0 c_2) \in \mathbb{K}^\star$ and $c_0, c_2 \in \mathbb{K}^\star$ and $\lambda_1 = \lambda_2$. The Jacobi relation (7) becomes $c_0 c_2 (c_0^2 + 4c_2^2) = 1$ and the set of points $(c_0, c_2) \in \mathbb{A}^2(\mathbb{K})$ satisfying Jacobi relation is a curve C defined over $\mathbb{K}$. The number of rationals points of C is equal to the number of level 4 theta model defined over $\mathbb{K}$. In the above definitions, the condition $\lambda_1 \lambda_2 \neq 0$ ensures that the level 4 theta model E_{λ_1,λ_2} is not singular. Indeed, if we assume that $[X_0 : X_1 : X_2 : X_3]$ is a singular point, then the rank of the following matrix can not be two.

$$\begin{pmatrix} 2X_0 & -\lambda_1 X_3 & 2X_2 & -\lambda_1 X_1 \\ -\lambda_2 X_2 & 2X_1 & -\lambda_2 X_0 & 2X_3 \end{pmatrix}.$$

Observe that the model that we call level 4 theta model has been introcuced in 1966 by Mumford in non-binary fields [**Mum66Ab**]. Over binary fields, Carls [**Car05**] obtained the level 4 theta model but, he did not studied the arithmetic of this model. Recently, David Kohel [**Koh12**] studied the arthmetic of this model that he called a μ_4-normal form, but only in characteristic 2 and using a different approach than in our case.

3.2 Addition law on level 4 theta model

Our addition law come from Riemann theta relations, which are valid over any finite field.

Theorem 2 *Let $P_1 = [X_{1,0} : X_{1,1} : X_{1,2} : X_{1,3}]$ and $P_2 = [X_{2,0} : X_{2,1} : X_{2,2} : X_{2,3}]$ be two points on E_{λ_1,λ_2}. The coordinates of the sum $P_1 + P_2 = P_3$ are given by the following formulas:*

$$\begin{array}{rcl} X_{3,0} & = & (X_{1,0}^2 X_{2,0}^2 + X_{1,2}^2 X_{2,2}^2) - 4(c_2/c_0) X_{1,1} X_{1,3} X_{2,1} X_{2,3} \\ X_{3,1} & = & c_0(X_{1,0} X_{1,1} X_{2,0} X_{2,1} + X_{1,2} X_{1,3} X_{2,2} X_{2,3}) - 2c_2(X_{1,2} X_{1,3} X_{2,0} X_{2,1} + X_{1,0} X_{1,1} X_{2,2} X_{2,3}) \\ X_{3,2} & = & (X_{1,1}^2 X_{2,1}^2 + X_{1,3}^2 X_{2,3}^2) - 4(c_2/c_0) X_{1,0} X_{1,2} X_{2,0} X_{2,2} \\ X_{3,3} & = & c_0(X_{1,0} X_{1,3} X_{2,0} X_{2,3} + X_{1,1} X_{1,2} X_{2,1} X_{2,2}) - 2c_2(X_{1,0} X_{1,3} X_{2,1} X_{2,2} + X_{1,1} X_{1,2} X_{2,0} X_{2,3}) \end{array} . \quad (8)$$

In any finite field, the opposite of the point $P = [X_0 : X_1 : X_2 : X_3]$ is $-P = [X_0 : X_3 : X_2 : X_1]$ (the second coordinate and the fourth coordinate are permuted). The neutral element is $O_0 := [c_0 : 1 : 2c_2 : 1]$.

Proof: Consider $E_{\lambda_1,\lambda_2}/\mathbb{Z}_q$ the canonical lift of E_{λ_1,λ_2}. Then, an equation of $E_{\lambda_1,\lambda_2}/\mathbb{Z}_q$ is E_{λ_1,λ_2}. Let $\mathcal{B}(i', j', k', l') = \sum_{\beta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\beta}(z_1)\theta_{j'+\beta}(z_1)\theta_{l'+\beta}(z_2)\theta_{k'+\beta}(z_2)$, $\mathcal{Z}_{i,j} = \theta_i(z_1 + z_2)\theta_j(z_1 - z_2)$ and $\delta_{k,l} = \theta_k(0)\theta_l(0) = a_k a_l$. The equation (4) leads to a system of linear equations:

$$(S) \left\{ \begin{array}{rcl} \delta_{k,l}\mathcal{Z}_{i,j} + \delta_{k+2,l+2}\mathcal{Z}_{i+2,j+2} & = & \mathcal{B}(i', j', k', l') \\ \delta_{k+2,l}\mathcal{Z}_{i,j} + \delta_{k,l+2}\mathcal{Z}_{i+2,j+2} & = & \mathcal{B}(i', j', k' + 2, l') \end{array} \right.$$

The determinant of the system (S) is $\det(S) = a_l a_{l+2}(a_k^2 - a_{k+2}^2)$. To avoid a null determinant, we choose $k \notin \{1, 3\}$ since $a_1 = a_3$. The Cramer method to resolve the system (S) gives:

$$\begin{array}{rcl} \theta_i(z_1 + z_2)\theta_j(z_1 - z_2) & = & \dfrac{\delta_{k,l+2}\mathcal{B}(i', j', k', l') - \delta_{k+2,l+2}\mathcal{B}(i', j', k' + 2, l')}{\delta_{k,l}\delta_{k,l+2} - \delta_{k+2,l+2}\delta_{k+2,l}} \\ & = & \dfrac{a_k\mathcal{B}(i', j', k', l') - a_{k+2}\mathcal{B}(i', j', k' + 2, l')}{a_l(a_k^2 - a_{k+2}^2)}. \end{array} \quad (9)$$

We fix $k = 0$ and $l = i + j$. Then for $i \in \{0, 1, 2, 3\}$ we factorize (9) by $a_0^2 - a_2^2$ in projective coordinates to have:

$$\theta_i(z_1 + z_2)\theta_j(z_1 - z_2) \quad = \quad \frac{a_0\mathcal{B}(i', j', 0, i' + j') - a_2\mathcal{B}(i', j', 2, i' + j')}{a_{i+j}}. \tag{10}$$

In equation (10), if we fix j equal to $0, 1, 2$ and 3,respectively, then we obtain 16 formulas for $i \in \{0, 1, 2, 3\}$ which correspond to four different formulas for addition. Here we consider the case $j = 0$ which gives the addition law formulas in (8). We can factorize by $\theta_0(z_1 - z_2)$ since we are in projective coordinates. We obtain

$$\theta_i(z_1 + z_2)\theta_0(z_1 - z_2) \quad = \quad \frac{a_0\mathcal{B}(i', 0, 0, i') - a_2\mathcal{B}(i', 0, 2, i')}{a_i} \tag{11}$$

For $i \in \{0, 1, 2, 3\}$ and recalling that $c_i = a_i$ if $i \neq 2$, and $2c_2 = a_2$, we have:

$$\begin{aligned}
\theta_0(z_1 + z_2)\theta_0(z_1 - z_2) &= \frac{c_0\mathcal{B}(0, 0, 0, 0) - 2c_2\mathcal{B}(0, 0, 2, 0)}{c_0}, \\
\theta_1(z_1 + z_2)\theta_0(z_1 - z_2) &= \frac{c_0\mathcal{B}(1, 0, 0, 1) - 2c_2\mathcal{B}(1, 0, 2, 1)}{c_1}, \\
\theta_2(z_1 + z_2)\theta_0(z_1 - z_2) &= \frac{c_0\mathcal{B}(2, 0, 0, 2) - 2c_2\mathcal{B}(2, 0, 2, 2)}{2c_2}, \\
\theta_3(z_1 + z_2)\theta_0(z_1 - z_2) &= \frac{c_0\mathcal{B}(3, 0, 0, 3) - 2c_2\mathcal{B}(3, 0, 2, 3)}{c_3}.
\end{aligned}$$

If $l = i = 2$, the numerator and the denominator of (11) can be factorized by 2 before reducing modulo 2. Nevertheless one can avoid a_2 in the denominator by using this alternative relation

$$\theta_i(z_1 + z_2)\theta_0(z_1 - z_2) = \frac{a_0\mathcal{B}(i', 0, 0, i' + 2) - a_2\mathcal{B}(i', 0, 2, i' + 2)}{a_{i+2}},$$

which gives

$$\theta_2(z_1 + z_2)\theta_0(z_1 - z_2) = \frac{c_0\mathcal{B}(2, 0, 0, 0) - 2c_2\mathcal{B}(2, 0, 2, 0)}{c_0}.$$

Finally we have :

$$\textcircled{1}\left\{\begin{array}{rcl}
\theta_0(z_1 + z_2)\theta_0(z_1 - z_2) & = & \dfrac{c_0\Big(\theta_0^2(z_1)\theta_0^2(z_2) + \theta_2^2(z_1)\theta_2^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0}, \\
\theta_1(z_1 + z_2)\theta_0(z_1 - z_2) & = & c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big) \\
 & & -2c_2\Big(\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)\Big), \\
\theta_2(z_1 + z_2)\theta_0(z_1 - z_2) & = & \dfrac{-4c_2\theta_0(z_1)\theta_2(z_1)\theta_0(z_2)\theta_2(z_2) + c_0\Big(\theta_1^2(z_1)\theta_1^2(z_2) + \theta_3^2(z_1)\theta_3^2(z_2)\Big)}{c_0}, \\
\theta_3(z_1 + z_2)\theta_0(z_1 - z_2) & = & c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big) \\
 & & -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big).
\end{array}\right.$$

We set $X_{3,i} = \theta_i(z_1 + z_2), X_{1,i} = \theta_i(z_1)$ and $X_{2,i} = \theta_i(z_2)$. These relations are valid over $\mathbb{Q}_q$ according to Lefschetz principle and since they have a good reduction modulo p, this completes the proof. □

These relations give the theta of the sum $\theta_i(z_1 + z_2)$ in term of $\theta_i(z_1)$ and $\theta_i(z_2)$, and hence the addition formulas in any finite fields (see appendix B for a sage script for verification).

These formulas are valid modulo any prime p. In characteristic 2, the addition law formulas are given by:

$$\begin{array}{lcl} X_{3,0} & = & (X_{1,0}X_{2,0} + X_{1,2}X_{2,2})^2 \\ X_{3,1} & = & c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,1} + X_{1,2}X_{1,3}X_{2,2}X_{2,3}) \\ X_{3,2} & = & (X_{1,1}X_{2,1} + X_{1,3}X_{2,3})^2 \\ X_{3,3} & = & c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,3} + X_{1,1}X_{1,2}X_{2,1}X_{2,2}) \end{array}. \tag{12}$$

The neutral element becomes $0_0 := [c_0 : 1 : 0 : 1]$ over binary fields.
The additions laws (8) and (12) for non-binary and binary fields, respectively, are also valid for doubling: they are unified. More precisely, let $[X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}]$ be a point on E_{λ_1,λ_2}. The coordinates of $2[X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}] = [X_{5,0}, X_{5,1}, X_{5,2}, X_{5,3}]$ are:

$$\left\{\begin{array}{lcl} X_{5,0} & = & X_{1,0}^4 + X_{1,2}^4 - 4(c_2/c_0)X_{1,1}^2X_{1,3}^2 \\ X_{5,1} & = & c_0(X_{1,0}^2X_{1,1}^2 + X_{1,2}^2X_{1,3}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \\ X_{5,2} & = & X_{1,1}^4 + X_{1,3}^4 - (c_2/c_0)X_{1,0}^2X_{1,2}^2 \\ X_{5,3} & = & c_0(X_{1,0}^2X_{1,3}^2 + X_{1,1}^2X_{1,2}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \end{array}\right. \tag{13}$$

Denote by M, S and m the cost of a multiplication, a square and a multiplication by a constant, respectively, in the finite field $\mathbb{K}$. In characteristic 2, we have an efficient algorithm to compute point addition formulas (see section 4.3.2 for comparaison with previous work). The different costs are given in the following corollary.

Corollary 3 (Costs of addition) *The addition of two points on E_{λ_1,λ_2} can be done with:*

(a) $7M + 2S + 2m$, when $\mathbb{K}$ is a binary field;

(b) $11M + 8S + 6m$, when $\mathbb{K}$ is a non-binary field.

Proof: (a) In binary fields, the point addition formulas can be computed as follows:

$A := X_{1,0}{\cdot}X_{2,0};\ \ B := X_{1,1}{\cdot}X_{2,1};\ \ C := X_{1,2}{\cdot}X_{2,2};\ \ D := X_{1,3}{\cdot}X_{2,3};\ \ X_{3,0} := (A + C)^2;$
$X_{3,2} := (B + D)^2;\ \ X_{3,1} := c_0(A{\cdot}B + C{\cdot}D);\ \ X_{3,2} := X_{3,1} + c_0(A + C){\cdot}(B + D),$

which cost 7 multiplications and 2 squares and 2 multiplications by constant c_0.
(b) For efficiency in non-binary fields, a point $[X_0 : X_1 : X_2 : X_3]$ is represented as a seventuplet $(X_0, X_1, X_2, X_3, X_0X_1, X_2X_3)$. Thus the sum $(X_{3,0}, X_{3,1}, X_{3,2}, X_{3,3}, U_3, V_3)$ of the points represented by $(X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}, U_1, V_1)$ and $(X_{2,0}, X_{2,1}, X_{2,2}, X_{2,3}, U_2, V_2)$ where $U_1 = X_{1,0}X_{1,1}$; $V_1 = X_{1,2}X_{1,3}$ and $U_2 = X_{2,0}X_{2,1}$; $V_2 = X_{2,2}X_{2,3}$ can be computed with the algorithm:

$A := X_{1,0}{\cdot}X_{2,0};\ \ B := X_{1,1}{\cdot}X_{2,1};\ \ C := X_{1,2}{\cdot}X_{2,2};\ \ D := X_{1,3}{\cdot}X_{2,3};\ \ E := A^2;\ \ F := B^2;$
$G := C^2;\ \ H := D^2;\ \ X_{3,0} := E + G + 2(c_2/c_0)((B - D)^2 - F - H);$
$X_{3,2} := F + H + 2(c_2/c_0)((A - C)^2 - E - G);\ \ I := ((A + B)^2 - E - F)/2;$
$J := ((C + D)^2 - G - H)/2;\ \ K := (U_1 + V_1){\cdot}(U_2 + V_2) - I - J;$
$L := (A + C){\cdot}(B + D) - I - J;\ \ X_{3,1} := c_0(I + J) - 2c_2K;$
$E := (X_{1,0} + X_{1,2}){\cdot}(X_{1,3} + X_{1,1}) - U_1 - V_1;\ \ F := (X_{2,0} + X_{2,2}){\cdot}(X_{2,3} + X_{2,1}) - U_2 - V_2;$
$G := E{\cdot}F - L;\ \ X_{3,3} := c_0L - 2c_2G;\ \ U_3 := X_{3,0}{\cdot}X_{3,1};\ \ V_3 := X_{3,2}{\cdot}X_{3,3},$

This costs $11M + 8S + 6m$. □

Lemma 4 *Let E_{λ_1,λ_2} be the level 4 theta model of an elliptic curve over a finite field $\mathbb{K}$ of characteristic $p \geq 0$. Then E_{λ_1,λ_2} has a rational point of order 4.*

Proof: Let $\mathcal{S}_4$ be the group of permutation on $\{0,1,2,3\}$. Let $\sigma = (0,1,2,3)$ be the hull permutation of $\mathcal{S}_4$ and denote by $H_1 = \langle\sigma\rangle$ the subgroup of $\mathcal{S}_4$ generated by σ. Remark that if $P = [X_0 : X_1 : X_2 : X_3]$ is in E_{λ_1,λ_2}, then so are $[X_1 : X_2 : X_3 : X_0], [X_2 : X_3 : X_0 : X_1]$ and $[X_3 : X_0 : X_1 : X_2]$. There exists an action of H_1 on the points of E_{λ_1,λ_2} given by : $\sigma([X_0 : X_1 : X_2 : X_3]) = [X_{\sigma(0)} : X_{\sigma(1)} : X_{\sigma(2)} : X_{\sigma(3)}]$. Under this action, 4 divides the order of E_{λ_1,λ_2}. □

Over non-binary fields, apart from the neutral element $O_0 = [c_0 : 1 : 2c_2 : 1]$, the level 4 theta model has 3 points of order 2 namely: $\widetilde{O}_0 = [-c_0 : 1 : -2c_2 : 1], O_1 := [2c_2 : 1 : c_0 : 1]$ and $\widetilde{O}_1 := [-2c_2 : 1 : -c_0 : 1]$. The four points of order 4 are $A_1 := [1 : 2c_2 : 1 : c_0], \widetilde{A}_1 := [-1 : 2c_2 : -1, c_0], A_2 := [1 : c_0 : 1 : 2c_2]$ and $\widetilde{A}_2 := [-1 : c_0 : -1 : 2c_2]$. Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on level 4-theta model E_{λ_1,λ_2}, the actions of these rationals points of order 2 and 4 are:

$$\begin{aligned} P + O_0 &= [X_0 : X_1 : X_2 : X_3]\,, & P + \widetilde{O}_0 &= [-X_0 : X_1 : -X_2 : X_3]\,,\\ P + O_1 &= [X_2 : X_3 : X_0 : X_1]\,, & P + \widetilde{O}_1 &= [-X_2 : X_3 : -X_0 : X_1]\,,\\ P + A_1 &= [X_1 : X_2 : X_3 : X_0]\,, & P + \widetilde{A}_1 &= [-X_1 : X_2 : -X_3 : X_0]\,,\\ P + A_2 &= [X_3 : X_0 : X_1 : X_2]\,, & P + \widetilde{A}_2 &= [-X_3 : X_0 : -X_1 : X_2]\,. \end{aligned}$$

These formulas give: $P + \sigma^i(O_0) = \sigma^i(P)$ and $P + \tau^i(O_0) = \tau^i(P)$, from which we can deduce that $\sigma(P) + \sigma(Q) = P + Q + 2\sigma(O_0)$ and $\sigma(P) - \sigma(Q) = P - Q$.

Completness of group laws. A complete group law means that one can compute the addition of all pairs of input. This property is used to avoid some exceptional procedure attack on elliptic curve cryptosystems [**IzuTakEPA02**]. Let E_{λ_1,λ_2} defined over a non-binary $\mathbb{K}$.

Lemma 5 *Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on E_{λ_1,λ_2}. If $X_i = 0$, then we can write P in the form $\sigma^j([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon])$ for some $j = 0,1,2,3$ where $\varepsilon = \sqrt{-1}$.*

Proof: Without loss of generality, we can assume that $X_0 = 0$. If we have $X_j = 0$ for $j \neq 0$ then according to the equations of the curve, we obtain $P = [0 : 0 : 0 : 0] \notin \mathbb{P}^3$. Therefore $X_j \neq 0$ for $j \neq 0$. Assume also that $X_1 \neq 0$, then $X_2^2 = \lambda_1 X_1 X_3$ and $X_1^2 + X_3^2 = 0$ or equivalently $X_3 = \pm\sqrt{-1}X_1$ and $X_2^2 = \pm\sqrt{-1}\lambda_1 X_1^2$. Then over projective space, we have $P = \sigma^0([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon])$. Finally, it means that if $X_i = 0$ and $X_{i+1} \neq 0$ we have $P = \sigma^i([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon])$ □

Theorem 6 (completness) *The group law on E_{λ_1,λ_2} defined over $\mathbb{K}$ is complete if and only if one of the following conditions holds in $\mathbb{K}$:*

(1) -1 is not a square in $\mathbb{K}$, or

(2) $\sqrt{-1}\lambda_1$ is not a square in $\mathbb{K}$

Proof: For the first part, assume that these conditions do not hold, i.e. $\varepsilon = \sqrt{-1} \in \mathbb{K}$ and $\alpha = \sqrt{\varepsilon\lambda_1} \in \mathbb{K}$. We will prove that they are two points $P_1, P_2 \in E_{\lambda_1,\lambda_2}$ such that we can not add P_1 and P_2. Let $P_1 = [0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \varepsilon]$ be a point given by lemma 5 and consider the points $P_2 = [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$. By formulas in equation (8), the coordinate $X_{3,2}$ of $P_1 + P_2$ is equal to zero but $X_{3,1}^2 + X_{3,3}^2$ is not zero, according to the equation of the curve. Hence the group law is not complete. The converse is simple. Indeed, assume that one of the condition in the theorem holds. Then it is clear that the coordinates $X_{3,0}, X_{3,1}, X_{3,2}$ and $X_{3,3}$ of the sum $P_1 + P_2$ satisfy the equations of the curve. The only point (sum) that must be removed is $[0 : 0 : 0 : 0]$, but according to lemma 5 and by hypothesis, the sum of points can not give this point. So the group law is complete. □

The first sufficient condition of theorem 6 holds when $\mathbb{K}$ is a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$ such that $q \equiv 3 \bmod 4$. Notice that all points of the form $\sigma^i([\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1])$ given by theorem 6 have an even order, since their coordinates are given by theta constants. This implies that over any finite field (including binary fields), the addition law on the level 4 theta model E_{λ_1,λ_2} is complete in a subgroup of odd order.

4 Edwards model for elliptic curves

In [**Edw07**], Edwards gave a normal form for elliptic curves defined over non-binary fields with an unified addition law. From the level 4 theta model E_{λ_1,λ_2} elliptic curve, we derive an Edwards model which is defined over any finite field and which is birationally equivalent to this Edwards model over non binary fields.

4.1 Equation of the Edwards model

Theorem 7 *Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. The level 4 theta model E_{λ_1,λ_2} gives a normal form with equation: $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$, where $\lambda = \lambda_1\lambda_2 \in \mathbb{K}^\star$.*

Proof: Divide the first equation of E_{λ_1,λ_2} by X_0^2 and the second by X_1^2 and consider the following change of variables: $[X_0 : X_1 : X_2 : X_3] \longmapsto (x, y) = (X_2/X_0, X_3/X_1)$, we have:

$$1 + x^2 = \lambda_1 \frac{X_1X_3}{X_0^2} \quad \text{and} \quad y^2 + 1 = \lambda_2 \frac{X_0X_2}{X_1^2}.$$

Multiply the above two equations to have $(x^2 + 1)(1 + y^2) = \lambda_1\lambda_2 xy$, which can be written as $1 + x^2 + y^2 + x^2y^2 = \lambda_1\lambda_2 xy$. The change of variables gives the neutral element $O_0 := (2c_2/c_0, 1)$ which becomes $(0, 1)$ over binary fields. □

Theorem 8 *Let $\mathbb{K}$ be a non-binary field, then the model $\mathcal{E}_\lambda$, with the neutral element $O_0 := (2c_2/c_0, 1)$ is birationally equivalent to the well known Edwards model.*

Proof: Let $\mathcal{E}_\lambda/\mathbb{Z}_q$ be a canonical lift of $\mathcal{E}_\lambda$. Then $\mathcal{E}_\lambda/\mathbb{Z}_q$ comes from the model $E_{\lambda_1,\lambda_2}/\mathbb{Z}_q$ defined by the basis $\mathcal{B}_4 := \left\{\theta_{0,b}(z, 4^{-1}\omega), b \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}\right\}$. Consider the alternative basis $\mathcal{B}_{(2,2)} := \left\{\theta_{a,b}(2z, \omega), a, b \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}\right\}$. We recall that $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ can be identified to $\mathbb{Z}/2\mathbb{Z}$ via the map $n \longmapsto 2n$. The Koizumy formula (3) gives a change of basis:

$$\left\{\begin{array}{lcl} X_0(z) & = & \theta_{00}(z) + \theta_{10}(z) \\ X_1(z) & = & \theta_{01}(z) + \theta_{11}(z) \\ X_2(z) & = & \theta_{00}(z) - \theta_{10}(z) \\ X_3(z) & = & \theta_{01}(z) - \theta_{11}(z) \end{array}\right. \iff \left\{\begin{array}{lcl} \theta_{00}(z) & = & \frac{1}{2}\left(X_0(z) + X_2(z)\right) \\ \theta_{01}(z) & = & \frac{1}{2}\left(X_1(z) + X_3(z)\right) \\ \theta_{10}(z) & = & \frac{1}{2}\left(X_0(z) - X_2(z)\right) \\ \theta_{11}(z) & = & \frac{1}{2}\left(X_1(z) - X_3(z)\right) \end{array}\right.$$

The basis $\mathcal{B}_{(2,2)}$ gives an alternative model of elliptic curve defined over non-binary fields (see [**Mum83**] for more details):

$$\left\{\begin{array}{lcl} \theta_{00}^2(0)T_{00}^2 & = & \theta_{01}^2(0)T_{01}^2 + \theta_{10}^2(0)T_{10}^2 \\ \theta_{00}^2(0)T_{11}^2 & = & \theta_{10}^2(0)T_{01}^2 - \theta_{01}^2(0)T_{10}^2 \end{array}\right. , \text{ where } T_{ij} = \theta_{ij}(z) \tag{14}$$

Setting $x = \frac{T_{00}}{T_{10}}; y = \frac{T_{11}}{T_{01}}$ and $c = \theta_{10}(0)/\theta_{00}(0) = \frac{c_0 - 2c_2}{c_0 + 2c_2}$, the curve (14) is birationally equivalent to the well known Edwards model, for more details see [**Dphd10**], which ends the proof. □

According to Theorems 7 and 8, we have this definition:

Definition 1 Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. An Edwards model for elliptic curves is given by the equation:

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy, \text{ where } \lambda \in \mathbb{K}^\star.$$

Theorem 9 *Let $\mathbb{K}$ be a field of characteristic $p \geq 0$ and let $\lambda \in \mathbb{K}^\star$. Then the Edwards model defined over $\mathbb{K}$ is non-singular.*

Proof: Our Edwards model is birationally equivalent to the Edwards model $Ed_c : X^2 + Y^2 = c^2(1 + X^2Y^2)$ where $c = \frac{c_0-2c_2}{c_0+2c_2}$. The model Ed_c is non singular if and only if $c^4 \neq 1$ (see [**Edw07**]), i.e $(c_0 - 2c_2)^4 \neq (c_0 + 2c_2)^4$. This condition is equivalent to $c_0c_2(c_0^2 + 4c_2^2) \neq 0$ which is always true, according to Jacobi relation (7). □

Apart from the neutral element $O_0 := (2c_2/c_0, 1)$, the Edwards model $\mathcal{E}_\lambda : 1+x^2+y^2+x^2y^2 = \lambda xy$ has three 2−torsion rationals points: $P_2 = (1/\gamma, 1), P_3 = (-\gamma, -1)$ and $P_4 = (-1/\gamma, -1)$, where $\gamma = 2c_2/c_0$. The Edwards model $\mathcal{E}_\lambda$ also has four 4-torsion points which are rationals over $\mathbb{K}$: $Q_1 = (1, \gamma), Q_2 = (1, 1/\gamma), Q_3 = (-1, -\gamma)$ and $Q_4 = (-1, -1/\gamma)$. The actions of rationals points of order 2 and 4 are:

$$\begin{array}{ll} (x, y) + O = (x, y), & (x, y) + P_2 = (1/x, 1/y) \\ (x, y) + P_3 = (-x, -y), & (x, y) + P_4 = (-1/x, -1/y) \\ (x, y) + Q_1 = (1/y, x), & (x, y) + Q_2 = (y, 1/x) \\ (x, y) + Q_3 = (-1/y, -x), & (x, y) + Q_4 = (-y, -1/x) \end{array},$$

Remark 10 If $\mathbb{K}$ is a binary field, then $P_3 = O$, $P_4 = P_2$, $Q_3 = Q_1$ and $Q_4 = Q_2$. The number of rationals points of $\mathcal{E}_\lambda$ is then divisible by 4.

4.2 Birational equivalence with Weierstrass models

Theorem 11 *Let $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ be the Edwards model of elliptic curve defined over the finite field $\mathbb{K}$ of characteristic $p \geq 0$.*

(1) if $p \neq 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to a cubic Weierstrass model;

(2) if $p = 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to the Weierstrass model $v^2 + uv = u^3 + 1/\lambda^4$.

Proof: Theorem 8 gives the birational equivalence between $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ and the well known Edwards model $X^2 + Y^2 = c^2(1 + X^2Y^2)$. This well known Edwards model is birationally equivalent to the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$. Setting $X = 2c(u - c^4 - 1)/v$ and $Z = -c + uX^2/(2c)$, the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$ is birationally equivalent to the cubic Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$. This proves (1).
For fields of characteristic 2, the birational map and its inverse between Edwards model and Weierstrass model are

$$\begin{array}{lcl} (u, v) & \longmapsto & (x, y) = \left(\dfrac{1}{\lambda u}, \dfrac{\lambda^2 v + 1}{\lambda^2 u + \lambda^2 v + 1}\right) \text{ and } (0, 1) \mapsto [0 : 1 : 0] \\ (x, y) & \longmapsto & (u, v) = \left(\dfrac{1}{\lambda x}, \dfrac{\lambda y + x(y + 1)}{\lambda^2 x(y + 1)}\right) \text{ and } [0 : 1 : 0] \mapsto (0, 1). \end{array}$$

which ends the proof (see also [**Dphd10**]). □

Corollary 12 ($j-$Invariant) *Let $\mathbb{K}$ be a finite field and $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ the Edwards model over $\mathbb{K}$. The $j-$Invariant of $\mathcal{E}_\lambda$ is*

$$j = \frac{\left((c_0^4 - 4c_0^3c_2 + 8c_0^2c_2^2 + 16c_0c_2^3 + 16c_2^4)(c_0^4 + 4c_0^3c_2 + 8c_0^2c_2^2 - 16c_0c_2^3 + 16c_2^4)\right)^3}{\left(c_2c_0(c_0 - 2c_2)(c_0 + 2c_2)(c_0^2 + 4c_2^2)\right)^4}.$$

Over fields of characteristic 2*, the $j-$Invariant is* $\lambda^4 = j \bmod 2$.

Proof: Let $\mathbb{K}$ be a non-binary field. The $j-$Invariant of the Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$ over $\mathbb{K}$ is:

$$j_W = 2^4\frac{\left((c^4 - 2c^3 + 2c^2 + 2c + 1)(c^4 + 2c^3 + 2c^2 - 2c + 1)\right)^3}{\left(c(c-1)(c+1)(c^2+1)\right)^4}.$$

Since $c = (c_0 - 2c_2)/(c_0 + 2c_2)$, a straightforward calculation give the desired result. Notice that the expression of j is defined modulo any prime p then j is defined over field of any characteristic. Over fields of characteristic 2, we have $j \bmod 2 = (c_0/c_2)^4 = \lambda^4$ which is the $j-$Invariant of Weierstrass model $v^2 + uv = u^3 + 1/\lambda^4$ in theorem 11. □

4.3 Addition on the Edwards model

In [**Dphd10**], Diao uses formulas (1) on the known Edwards model [**Edw07**] to deduce an addition on his binary Edwards model. Over binary fields, the addition law in [**Dphd10**] is not unified and not efficient. However, to have an unified and more efficient addition law formulas we use the addition law on the level 4-theta model. More precisely we have:

Theorem 13 *Let (x_1, y_1) and (x_2, y_2) be two points of $\mathcal{E}_\lambda$. The coordinates of the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are given by:*

$$(x_3, y_3) = \left(\frac{c_0(x_1 + y_1x_2y_2) - 2c_2(y_1 + x_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)}, \frac{c_0(x_1x_2 + y_1y_2) - 2c_2(x_1y_2 + y_1x_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)}\right). \quad (15)$$

The opposite of the point is $-(x_1, y_1) = (x_1, 1/y_1)$ and the neutral element is $O_0 := (2c_2/c_0, 1)$.

One can verify the addition law on new Edwards model $\mathcal{E}_\lambda$ by this sage script [**Sage-4.8**]:

```
R.<c0,c2,x1,y1,x2,y2> = QQ[]
E1 = c0*c2*(x1^2 + y1^2 + 1 + x1^2*y1^2) - (c0^2 + 4*c2^2)*x1*y1
E2 = c0*c2*(x2^2 + y2^2 + 1 + x2^2*y2^2) - (c0^2 + 4*c2^2)*x2*y2
S = R.quo([E1,E2])
Nx3 = c0*(x1 + y1*x2*y2) - 2*c2*(y1 + x1*x2*y2)
Dx3 = c0*(y2 + x1*y1*x2) - 2*c2*(x2 + x1*y1*y2)
Ny3 = c0*(x1*x2 + y1*y2) - 2*c2*(x1*y2 + y1*x2)
Dy3 = c0*(1 + x1*x2*y1*y2) - 2*c2*(x1*y1 + x2*y2)
x3 = Nx3/Dx3; y3 = Ny3/Dy3

E3 = c0*c2*(x3^2 + y3^2 + 1 + x3^2*y3^2) - (c0^2 + 4*c2^2)*x3*y3
S(numerator(E3)) == 0
```

Over fields of characteristic 2, the coordinates of the sum of two points are obtained by a reduction modulo 2:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1y_1x_2y_2}\right). \quad (16)$$

Remark 14 Addition group law is unified over any fields, i.e. addition formulas are also valid for point doubling. The point doubling formulas can be written as follow:

$$2(x_1,y_1)=\left(\frac{c_0x_1(1+y_1^2)-2c_2y_1(1+x_1^2)}{c_0y_1(1+x_1^2)-2c_2x_1(1+y_1^2)},\frac{c_0(x_1^2+y_1^2)-4c_2x_1y_1}{c_0(1+x_1^2y_1^2)-4c_2x_1y_1}\right). \tag{17}$$

Over binary fields, the formulas (16) or (17) give the doubling formulas:

$$2(x_1,y_1)=\left(\frac{x_1(1+y_1)^2}{y_1(1+x_1)^2},\frac{(x_1+y_1)^2}{(1+x_1y_1)^2}\right). \tag{18}$$

According to theorems 6 and 7, the addition law on Edwards model $\mathcal{E}_\lambda$ is complete over any subgroup of $\mathcal{E}_\lambda$ of odd order.

4.3.1 Explicit formulas

Affine coordinates. Let (x_1,y_1) and (x_2,y_2) be two points on the Edwards model $\mathcal{E}_\lambda : 1+x^2+y^2+x^2y^2=\lambda xy$ defined the field $\mathbb{K}$. The following formulas compute the sum $(x_3,y_3)=(x_1,y_1)+(x_2,y_2)$, when it is defined:

$$\begin{array}{l} A=x_1{\cdot}y_1;\;\; B=x_2{\cdot}y_2;\;\; C=x_1+y_1{\cdot}B;\;\; D=y_1+x_1{\cdot}B;\;\; E=y_2+x_2{\cdot}A;\;\; F=x_2+y_2{\cdot}A;\\ G=A+B;\;\; H=(x_1+y_2){\cdot}(x_2+y_1)-G;\;\; I=(x_1+y_1){\cdot}(x_2+y_2)-H;\;\; J=1+A{\cdot}B;\\ x_3=(c_0{\cdot}C-2c_2{\cdot}D)/(c_0{\cdot}E-2c_2{\cdot}F);\qquad y_3=(c_0{\cdot}H-2c_2{\cdot}I)/(c_0{\cdot}J-2c_2{\cdot}G)\end{array}$$

These formulas cost $2I+9M+8m$ over non-binary fields and $2I+5M$ over binary fields, where I,M and m are the costs of a field inversion, a field multiplication and a field multiplication by a constant, respectively.

Remark that, the opposite of a point costs 1 inversion which is too expensive. Nevertheless the sum and the difference of two points (x_1,y_1) and (x_2,y_2) have the same complexity. Indeed, the following formula computes the difference $(x_5,y_5)=(x_1,y_1)-(x_2,y_2)$, if it is defined:

$$(x_5,y_5)=\left(\frac{c_0(x_1y_2+y_1x_2)-2c_2(x_1x_2+y_1y_2)}{c_0(1+x_1y_1x_2y_2)-2c_2(x_1y_1+x_2y_2)},\frac{c_0(y_1+x_1x_2y_2)-2c_2(x_1+y_1x_2y_2)}{c_0(y_2+x_1y_1x_2)-2c_2(x_2+x_1y_1y_2)}\right). \tag{19}$$

We retrieve the eight polynoms used to compute the sum: $F_1=x_1+y_1x_2y_2, F_2=y_1+x_1x_2y_2, F_3=y_2+x_1y_1x_2, F_4=x_2+x_1y_1y_2, F_5=x_1x_2+y_1y_2, F_6=x_1y_2+y_1x_2, F_7=1+x_1y_1x_2y_2$ and $F_8=x_1y_1+x_2y_2$. Therefore formulas (15) and (19) can be rewritten as follows:

$$\begin{aligned}(x_1,y_1)+(x_2,y_2)&=\left(\frac{c_0F_1-2c_2F_2}{c_0F_3-2c_2F_4},\frac{c_0F_5-2c_2F_6}{c_0F_7-2c_2F_8}\right),\\ (x_1,y_1)-(x_2,y_2)&=\left(\frac{c_0F_6-2c_2F_5}{c_0F_7-2c_2F_8},\frac{c_0F_2-2c_2F_1}{c_0F_3-2c_2F_4}\right).\end{aligned}$$

Projective coordinates. In this paragraph, we give projective coordinates over finite fields $\mathbb{K}$ of characteristic 2. To avoid inversions we can work in the projective space $\mathbb{P}^2(\mathbb{K})$. Let $x=X/Z$ and $y=Y/Z$, then the coordinates of the sum $[X_3:Y_3:Z_3]=[X_1:Y_1:Z_1]+[X_2:Y_2:Z_2]$ can be computed as follows:

$$\begin{array}{l} A=X_1{\cdot}X_2;\;\; B=Y_1{\cdot}Y_2;\;\; C=A{\cdot}B;\\ D=X_1{\cdot}Z_2;\;\; E=Y_2{\cdot}Z_1;\;\; Z=Z_1{\cdot}Z_2\\ F=E{\cdot}(C+D^2);\;\; G=D{\cdot}(C+E^2);\\ H=Z{\cdot}(A+B);\;\; I=C+Z^2;\\ X_3=F{\cdot}I;\;\; Y_3=H{\cdot}G;\;\; Z_3=G{\cdot}I\end{array}\quad .$$

The coordinates of a doubling $[X_4 : Y_4 : Z_4] = 2[X_1 : Y_1 : Z_1]$ can be computed as follows:

$$\begin{array}{l} A = (Y_1 + Z_1)^2; \quad B = (X_1 + Z_1)^2; \quad C = (Z_1 \cdot (X_1 + Y_1))^2; \\ D = A \cdot B + C; \quad E = X_1 \cdot A; \quad F = Y_1 \cdot B \\ X_4 = E \cdot D; \quad Y_4 = F \cdot C; \quad Z_4 = F \cdot D \end{array}.$$

Projective addition costs $12M + 3S$ and projective doubling costs $7M + 3S$ in the base field.

4.3.2 Comparisons of addition formulas with previous works

In this section, we compare our addition formulas in binary fields with other models of elliptic curves. As in theorems 7 and 11, we choose models that are birationally equivalent to the ordinary Weierstrass model $v^2 + uv = u^3 + b_2u + b_6$ where $b_2 = 0$ of Explicit-Formulas Database [**BL-EFD**]. Recall that M, S and m are the cost of multiplication, square and multiplication by a constant, respectively, over a finite field $\mathbb{K}$.

Models	Doubling	Addition
Weierstraß	$7M + 3S$	$14M + 1S$
Binary Edwards of [**BLF08**]	$4M + 4S + 1m$	$16M + 1S + 4m$
Hessian	$6M + 3S$	$12M + 6S$
Huff of [**DevJoyBinHuff11**]	$6M + 5S + 2m$	$13M + 2S + 2m$
Edwards model of [**Wu:2010:608**]	$3M + 3S + 1m$	$12M + 4S + 2m$
Level 4-theta model	$3M + 6S + 2m$	$7M + 2S + 2m$
Our Edwards model	$7M + 3S$	$12M + 3S$

Table 1: Comparisons of points operations in binary fields

We can observe that addition law on the level 4 theta model costs only $7M + 2S + 2m$, which is the fastest addition formulas among well known models of elliptic curves.

5 Differential addition on Kummer line

5.1 Differential addition on the level 4 theta model

This section is devoted to differential addition on Kummer line of elliptic curves. Let $\mathbb{K}$ be a field of characteristic $p \geq 0$ and let E_{λ_1,λ_2} be the level 4 theta model defined over the field $\mathbb{K}$. Let $[X_i] := [X_0 : X_1 : X_2 : X_3]$ be a point on E_{λ_1,λ_2}, the opposite of $[X_i]$ is $[X_0 : X_3 : X_2 : X_1]$. The set $\{X_0, X_2, X_1 + X_3\}$ is invariant under the action of opposite. Denote $W = X_1 + X_3$, an equation of Kummer line can be written as

$$\mathcal{K}_{E_{\lambda_1,\lambda_2}} : W^2 = \frac{2}{\lambda_1}(X_0^2 + X_2^2) + \lambda_2 X_0 X_2,$$

which become $W^2 = \lambda_2 X_0 X_2$ over binary fields. The addition on E_{λ_1,λ_2} does not induce an addition law on the corresponding Kummer line, but one can defined a differential addition on Kummer line. Let $[X_{1,i}] = [X_{1,0} : X_{1,1} : X_{1,2} : X_{1,3}]$ and $[X_{2,i}] = [X_{2,0} : X_{2,1} : X_{2,2} : X_{2,3}]$ be two points on E_{λ_1,λ_2} and let $[X_{3,i}] = [X_{1,i}] + [X_{2,i}]$, $[X_{4,i}] = [X_{1,i}] - [X_{2,i}]$ and $[X_{5,i}] = 2[X_{1,i}]$. For differential addition and differential doubling, we express the coordinates $X_{3,0}, X_{3,2}, X_{3,1} + X_{3,3}$ and $X_{5,0}, X_{5,2}, X_{5,1} + X_{5,3}$ in term of the coordinates of $X_{1,i}, X_{2,i}$ and $X_{4,i}$. Remark that the computation of $[X_{4,i}]$ is done using the addition formulas; that is by adding $[X_{1,i}]$ with the inverse of $[X_{2,i}]$. We have:

$$\begin{cases} X_{3,0} &= (X_{1,0}^2X_{2,0}^2 + X_{1,2}^2X_{2,2}^2) - 4(c_2/c_0)X_{1,1}X_{1,3}X_{2,1}X_{2,3} \\ X_{3,1} &= c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,1} + X_{1,2}X_{1,3}X_{2,2}X_{2,3}) - 2c_2(X_{1,0}X_{1,1}X_{2,2}X_{2,3} + X_{1,2}X_{1,3}X_{2,0}X_{2,1}) \\ X_{3,2} &= (X_{1,1}^2X_{2,1}^2 + X_{1,3}^2X_{2,3}^2) - 4(c2/c0)X_{1,0}X_{2,0}X_{1,2}X_{2,2} \\ X_{3,3} &= c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,3} + X_{1,1}X_{1,2}X_{2,1}X_{2,2}) - 2c_2(X_{1,0}X_{1,3}X_{2,1}X_{2,2} + X_{1,1}X_{1,2}X_{2,0}X_{2,3}) \end{cases}$$

$$\begin{cases} X_{4,0} &= (X_{1,0}^2X_{2,0}^2 + X_{1,2}^2X_{2,2}^2) - 4(c_2/c_0)X_{1,1}X_{1,3}X_{2,1}X_{2,3} \\ X_{4,1} &= c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,3} + X_{1,2}X_{1,3}X_{2,1}X_{2,2}) - 2c_2(X_{1,0}X_{1,1}X_{2,1}X_{2,2} + X_{1,2}X_{1,3}X_{2,0}X_{2,3}) \\ X_{4,2} &= (X_{1,1}^2X_{2,3}^2 + X_{1,3}^2X_{2,1}^2) - 4(c_2/c_0)X_{1,0}X_{1,2}X_{2,0}X_{2,2} \\ X_{4,3} &= c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,1} + X_{1,1}X_{1,2}X_{2,2}X_{2,3}) - 2c_2(X_{1,0}X_{1,3}X_{2,2}X_{2,3} + X_{1,1}X_{1,2}X_{2,0}X_{2,1}) \end{cases}$$

$$\begin{cases} X_{5,0} &= X_{1,0}^4 + X_{1,2}^4 - 4(c_2/c_0)X_{1,1}^2X_{1,3}^2 \\ X_{5,1} &= c_0(X_{1,0}^2X_{1,1}^2 + X_{1,2}^2X_{1,3}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \\ X_{5,2} &= X_{1,1}^4 + X_{1,3}^4 - (c_2/c_0)X_{1,0}^2X_{1,2}^2 \\ X_{5,3} &= c_0(X_{1,0}^2X_{1,3}^2 + X_{1,1}^2X_{1,2}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \end{cases}$$

A straightforward and easy calculation, while considering the equations of the curve, shows that:

$$\begin{cases} X_{3,0} &= X_{4,0} \\ X_{3,2} &= \dfrac{c_0^2 - 4c_2^2}{c_0c_2}X_{1,0}X_{2,0}{\cdot}X_{1,2}X_{2,2} - X_{4,2} \end{cases}, \tag{20}$$

$$\begin{cases} X_{5,0} &= \mu c_0(X_{1,0}^2 + X_{1,2}^2)^2 - 2X_{1,0}^2X_{1,2}^2 \\ X_{5,2} &= (c_2/c_0)X_{1,0}^2{\cdot}X_{1,2}^2 - 2\mu c_2(X_{1,0}^2 + X_{1,2}^2)^2 \end{cases}, \tag{21}$$

where $\mu = c_0/(c_0^2 + 4c_2^2)$. The cost of differential addition and doubling are $3M + 1m$ and $1M + 3S + 3m$ operations, respectively, over non-binary fields. Over binary fields, differential addition and doubling cost $3M + 1m$ and $1M + 3S + 1m$ operations, respectively. Notice that, moreover, we can also focus on the computation of the coordinates functions $W_i = X_{i,1} + X_{i,3}$ for $i = 1, 2, 3, 4, 5$, which give the addition law on the Kummer line $\mathcal{K}_{E_{\lambda_1,\lambda_2}} : W^2 = \dfrac{2}{\lambda_1}(X_0^2 + X_2^2) + \lambda_2X_0X_2,$. Finally we have:

$$\begin{aligned} W_3 &= W_1{\cdot}W_2{\cdot}\Big(c_0(X_{1,0}{\cdot}X_{2,0} + X_{1,2}{\cdot}X_{2,2}) - 2c_2(X_{1,0}X_{2,2} + X_{1,2}X_{2,0})\Big) - W_4 \\ W_5 &= \mu(c_0^2 - 4c_2^2)(X_{1,0}^2 + X_{1,2}^2){\cdot}(W_1^2 - 2c_0c_2(X_{1,0}^2 + X_{1,2}^2)) \end{aligned}$$

The computations cost $6M + 3m$ and $2M + 4S + 5m$ operations for differential addition and doubling, respectively, over non-binary fields. Over binary fields, these cost are $5M + 2m$ and $2M + 4S + 2m$ for differential addition and doubling, respectively.

5.2 Differential addition on the Edwards model over any finite field

Let $\mathcal{E}_\lambda$ be the Edwards model over the field $\mathbb{K}$ and let (x, y) be a point on $\mathcal{E}_\lambda$. The first coordinate of (x, y) is invariant under the negation action. For $i = 1, 2, 3, 4$, let (x_i, y_i) be a point on $\mathcal{E}_\lambda$ such that $(x_3, y_3) = (x_1, y_1) + (x_2, y_2), (x_4, y_4) = (x_1, y_1) - (x_2, y_2)$ and $(x_5, y_5) = 2(x_1, y_1)$. As in section 5.1, our goal is to express x_3 and x_5 in term of x_1, x_2 and x_4. We have $x_i = X_{i,2}/X_{i,0}$ for $i = 1, 2, 3, 4, 5$ where $[X_{i,0} : X_{i,1} : X_{i,2} : X_{i,3}]$ are points on the level 4 theta model. The first and second relation of (20) and (21) give, if they are defined:

$$x_3 + x_4 = \frac{(c_0^2 - 4c_2^2)x_1x_2}{c_0c_2(1 + x_1^2x_2^2)}, \tag{22}$$

$$x_5 = \frac{(c_2/c_0)x_1^2 - 2\mu c_2(1 + x_1^2)^2}{\mu c_0(1 + x_1^2)^2 - 2x_1^2}, \tag{23}$$

where $\mu = c_0/(c_0^2+4c_2^2)$. The computation of x_3 and x_5 costs $1I+1M+1S+1m$ and $1I+2S+3m$ operations,respectively. To avoid inversions, let $x_i = X_i/Z_i$ for $i = 1,2,3,4,5$ where $[X : Z]$ parametrizes the projective space $\mathbb{P}^1(\mathbb{K})$. Over any finite fields, formulas (22) and (23) become:

$$\left\{\begin{array}{lcl} X_3 & = & \frac{c_0^2-4c_2^2}{c_0c_2}Z_4X_1X_2Z_1Z_2 - X_4(X_1^2X_2^2+Z_1^2Z_2^2) \\ Z_3 & = & Z_4(X_1^2X_2^2+Z_1^2Z_2^2) \end{array}\right. , \tag{24}$$

$$\left\{\begin{array}{lcl} X_5 & = & (c_2/c_0)Z_1^2 \cdot X_1^2 - 2\mu c_2(Z_1^2+X_1^2)^2 \\ Z_5 & = & \mu c_0(Z_1^2+X_1^2)^2 - 2Z_1^2X_1^2 \end{array}\right. . \tag{25}$$

The computation of $[X_3 : Z_3]$ and $[X_5 : Z_5]$ costs $6M+2S+1m$ and $1M+3S+3m$ operations, respectively, over non-binary fields. The computational cost of the differential addition can be reduced to $4M+2S+1m$ if $Z_4 = 1$. Similarly, over fields of characteristic 2, formulas (22) and (23) become:

$$\left\{\begin{array}{lcl} X_3 & = & (c_0/c_2)Z_4X_1X_2Z_1Z_2 + X_4(X_1X_2+Z_1Z_2)^2 \\ Z_3 & = & Z_4(X_1X_2+Z_1Z_2)^2 \end{array}\right. , \tag{26}$$

$$\left\{\begin{array}{lcl} X_5 & = & (c_2/c_0)(Z_1 \cdot X_1)^2 \\ Z_5 & = & (Z_1+X_1)^4 \end{array}\right. . \tag{27}$$

The formulas (26) and (27) cost $6M+1S+1m$ and $1M+3S+1m$ operations, respectively, over fields of characteristic 2. If $Z_4 = 1$, formulas (26) can be reduced to $4M+1S+1m$ operations over binary fields. Formulas (26) correspond to Stam [**StamPKC02**] formulas and formulas (27) correspond to Gaudry and Lubicz formulas [**GauLubKummer09**].

5.3 Comparisons with previous work on differential addition

Over non-binary fields, Brier and Joye [**BJ02**] generalize the idea of Montgomerry [**MontECM87**] on general Weierstrass model $v^2 = u^3 + b_2u + b_6$. The method of [**BJ02**] uses $6M+2S+2m$ per bits for a scalar multiplication, i.e. multiply a point on Kummer line by a scalar. The best known formula, see table 2, uses $3M+6S+3m$ per bits and is due to Gaudry and Lubicz in [**GauLubKummer09**] on Kummer model of Legendre form $v^2 = u(u-1)(u-b)$. Our formula costs $4M+3S+4m$ on the level 4 theta model and $5M+5S+2m$ on the Edwards model. Over non-binary fields, we can assume that $S = M$ and consequently, our formula requires $7M+4m$ which is better than formula in [**GauLubKummer09**] which requires $9M+3m$. Moreover if we assume that $m = M$, then our method saves one multiplication.

model	differential doubling	differential addition	Total
Montgomerry [**MontECM87**]	$2M+2S+1m$	$3M+2S$	$5M+4S+1m$
Weierstraß	$4M+3S+2m$	$6M+2S+2m$	$10M+5S+4m$
Gaudry and Lubicz [**GauLubKummer09**]	$4S+2m$	$3M+2S+1m$	$3M+6S+3m$
Level 4-theta model	$1M+3S+3m$	$3M+1m$	$\mathbf{4M+3S+4m}$
Our Edwards model	$1M+3S+1m$	$4M+2S+1m$	$5M+5S+2m$

Table 2: Comparisons of differential addition over non-binary fields

Over binary fields, the best known formula, see table 3, due to Gaudry and Lubicz [**GauLubKummer09**] costs $5M+5S+1m$ on Kummer model of the ordinary elliptic curve $v^2+uv = u^3+b_6$. Our formulas requires $4M+3S+2m$ on the level 4 theta model and $5M+4S+2m$ on the Edwards model. The formulas on the level 4 theta model are the best to compute on Kummer line over binary fields.

model	differential doubling	differential addition	Total
Weierstraß of [**StamPKC02**]	$1M + 3S + 1m$	$4M + 1S$	$5M + 4S + 1m$
Binary Edwards of [**BLF08**]	$1M + 3S + 1m$	$4M + 1S + 1m$	$5M + 4S + 2m$
Huff of [**DevJoyBinHuff11**]	$1M + 3S + 1m$	$4M + 2S$	$5M + 5S + 1m$
Edwards model of [**Wu:2010:608**]	$1M + 4S + 1m$	$4M + 2S$	$5M + 6S + 1m$
Gaudry and Lubicz [**GauLubKummer09**]	$1M + 3S + 1m$	$4M + 2S$	$5M + 5S + 1m$
Level 4-theta model	$1M + 3S + 1m$	$3M + 1m$	$\mathbf{4M + 3S + 2m}$
Our Edwards model	$1M + 3S + 1m$	$4M + 1S + 1m$	$5M + 4S + 2m$

Table 3: Comparisons of differential addition over binary fields

6 Conclusion

We successfully introduced an Edwards model of elliptic curves defined over fields of all characteristic. We used a model of elliptic curve called level 4 theta model, comming from theta functions of level 4. We have shown that the group law on this theta model is complete and is the fastest in characteristic two, among common curves such as Weierstrass, Edwards, Huff and Hessian curves. As future work, one may compute pairings using theta functions in binary fields and Miller algorithm on these curves. Pairings computation over non-binary fields using theta funtions is published [**LuRo10**].

7 Acknowledgements

The authors are grateful to David Lubicz and Marc Joye for their helpful comments.

A Addition laws formulas on the level 4 theta model

The Riemann theta formulas give 16 relations that are classified according to j. Recall that $c_0 = a_0, c_2 = a_2/2 = \theta_2(0)/2$ and $a_3 = a_1 = 1$. Let $\mathbb{K}$ be field of characteristic $p \geq 0$ and let $c_0, c_2 \in \mathbb{K}^\star$ and let $E_{\lambda_1,\lambda_2} : X_0^2 + X_2^2 = \lambda_1 X_1 X_3, X_1^2 + X_3^2 = \lambda_2 X_0 X_2$ be the level 4 theta model defined over a field $\mathbb{K}$. The arithmetic (addition and doubling) on E_{λ_1,λ_2} is given by the following theta formulas:

$$\theta_i(z_1+z_2)\theta_j(z_1-z_2) = \frac{a_k \mathcal{B}(i',j',k',l') - a_{k+2}\mathcal{B}(i',j',k'+2,l')}{a_l}.$$

This formula give 4×4 formulas that give 4 equivalent group laws on E_{λ_1,λ_2}. The 4 group laws formulas are:

$$\begin{aligned}
\theta_i(z_1+z_2)\theta_0(z_1-z_2) &= \frac{a_0\mathcal{B}(i',0,0,i') - a_2\mathcal{B}(i',0,2,i')}{a_i},\\
\theta_i(z_1+z_2)\theta_1(z_1-z_2) &= \frac{a_0\mathcal{B}(i',1,0,i'+1) - a_2\mathcal{B}(i',1,2,i'+1)}{a_{i+1}},\\
\theta_i(z_1+z_2)\theta_2(z_1-z_2) &= \frac{a_0\mathcal{B}(i',2,0,i'+2) - a_2\mathcal{B}(i',2,2,i'+2)}{a_{i+2}},\\
\theta_i(z_1+z_2)\theta_3(z_1-z_2) &= \frac{a_0\mathcal{B}(i',3,0,i'+3) - a_2\mathcal{B}(i',3,2,i'+3)}{a_{i+3}}.
\end{aligned}$$

$$\text{①}\begin{cases}
\theta_0(z_1+z_2)\theta_0(z_1-z_2) = \dfrac{c_0\Big(\theta_0^2(z_1)\theta_0^2(z_2) + \theta_2^2(z_1)\theta_2^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0},\\
\theta_1(z_1+z_2)\theta_0(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big)\\
\qquad -2c_2\Big(\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)\Big),\\
\theta_2(z_1+z_2)\theta_0(z_1-z_2) = \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_0(z_2)\theta_2(z_2) - c_2\Big(\theta_1^2(z_1)\theta_3^2(z_2) + \theta_3^2(z_1)\theta_1^2(z_2)\Big)}{c_2},\\
\theta_3(z_1+z_2)\theta_0(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big)\\
\qquad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big).
\end{cases}$$

$$\text{②}\begin{cases}
\theta_0(z_1+z_2)\theta_1(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_3(z_2) + \theta_2(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)\Big)\\
\qquad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big),\\
\theta_1(z_1+z_2)\theta_1(z_1-z_2) = \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2) - c_2\Big(\theta_3^2(z_1)\theta_0^2(z_2) + \theta_2^2(z_1)\theta_1^2(z_2)\Big)}{c_2},\\
\theta_2(z_1+z_2)\theta_1(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_1(z_2)\Big)\\
\qquad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_2(z_2)\theta_3(z_2)\Big),\\
\theta_3(z_1+z_2)\theta_1(z_1-z_2) = \dfrac{c_0\Big(\theta_0^2(z_1)\theta_3^2(z_2) + \theta_2^2(z_1)\theta_1^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_0(z_2)\theta_2(z_2)}{c_0}.
\end{cases}$$

$$③\left\{\begin{array}{lcl}\theta_0(z_1+z_2)\theta_2(z_1-z_2) & = & \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2)-c_2\Big(\theta_1^2(z_1)\theta_1^2(z_2)+\theta_3^2(z_1)\theta_3^2(z_2)\Big)}{c_2}, \\ \theta_1(z_1+z_2)\theta_2(z_1-z_2) & = & c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big) \\ & & -2c_2\Big(\theta_0(z_1)\theta_3(z_2)\theta_0(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big), \\ \theta_2(z_1+z_2)\theta_2(z_1-z_2) & = & \dfrac{c_0\Big(\theta_0^2(z_1)\theta_2^2(z_2)+\theta_2^2(z_1)\theta_0^2(z_2)\Big)-4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0}, \\ \theta_3(z_1+z_2)\theta_2(z_1-z_2) & = & c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)\Big) \\ & & -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big).\end{array}\right.$$

$$④\left\{\begin{array}{lcl}\theta_0(z_1+z_2)\theta_3(z_1-z_2) & = & c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_2(z_2)\theta_3(z_2)\Big) \\ & & -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_1(z_2)\Big), \\ \theta_1(z_1+z_2)\theta_3(z_1-z_2) & = & \dfrac{c_0\Big(\theta_0^2(z_1)\theta_1^2(z_2)+\theta_2^2(z_1)\theta_3^2(z_2)\Big)-4c_2\theta_1(z_1)\theta_3(z_1)\theta_0(z_2)\theta_2(z_2)}{c_0}, \\ \theta_2(z_1+z_2)\theta_3(z_1-z_2) & = & c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_1(z_1)\theta_2(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2)\Big) \\ & & -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)\Big), \\ \theta_3(z_1+z_2)\theta_3(z_1-z_2) & = & \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2)-c_2\Big(\theta_1^2(z_1)\theta_0^2(z_2)+\theta_3^2(z_1)\theta_2^2(z_2)\Big)}{c_2}.\end{array}\right.$$

B Sage verification

This sage script verifies that addition formulas (8) are valid.

```
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
lbd1 = c0^2 + 4*c2^2; lbd2 = 1/(c0*c2)
LB = numerator(lbd1 - lbd2)

E1 = numerator(X0^2 + X2^2 - lbd1*X1*X3); E2 = numerator(X1^2 + X3^2 - lbd2*X0*X2)
F1 = numerator(Y0^2 + Y2^2 - lbd1*Y1*Y3); F2 = numerator(Y1^2 + Y3^2 - lbd2*Y0*Y2)

S = R.quo([E1,E2,F1,F2,LB])

Z0 = (X0^2*Y0^2 + X2^2*Y2^2) - 4*(c2/c0)*X1*X3*Y1*Y3
Z1 = c0*(X0*X1*Y0*Y1 + X2*X3*Y2*Y3) - 2*c2*(X2*X3*Y0*Y1 + X0*X1*Y2*Y3)
Z2 = (X1^2*Y1^2 + X3^2*Y3^2) - 4*(c2/c0)*X0*Y0*X2*Y2
Z3 = c0*(X0*X3*Y0*Y3 + X1*X2*Y1*Y2) - 2*c2*(X0*X3*Y1*Y2 + X1*X2*Y0*Y3)

G1 = Z0^2 + Z2^2 - lbd1*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd2*Z0*Z2
S(numerator(G1)) == 0; S(numerator(G2)) == 0
```