New Model of Binary Elliptic Curve

Demba Sow¹ & Djiby Sow¹

¹ Ecole Doctorale de Mathématiques et Informatique, Laboratoire d’Algèbre de Cryptologie de Géométrie Algébrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal

Correspondence: Demba Sow, Ecole Doctorale de Mathématiques et Informatique, Laboratoire d’Algèbre de Cryptologie de Géométrie Algébrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal. E-mail: sowdembis@yahoo.fr

Received: August 15, 2012  Accepted: September 13, 2012  Online Published: November 21, 2012
doi:10.5539/jmr.v4n6p34  URL: http://dx.doi.org/10.5539/jmr.v4n6p34

Abstract

In our paper we propose a new binary elliptic curve of the form \( a [x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] = 0. \) If \( m \geq 5 \) we prove that each ordinary elliptic curve \( y^2 + x y = x^3 + a x^2 + \beta, \beta \neq 0 \) over \( \mathbb{F}_{2^m} \), is birationally equivalent over \( \mathbb{F}_{2^m} \) to our curve. This paper also presents the formulas for the group law.

Keywords: elliptic curves, binary Edwards curves, binary fields, binary Huff curves

1. Introduction

Recently, many papers are written about binary elliptic curves such as Binary Edwards curves (Bernstein, Lange, & Farashahi, 2008) and Binary Huff curves (Devigne & Joye, 2011). In this paper, we introduce a new binary elliptic curve.

Let \( E \) be a projective curve of dimension one, defined over a field \( \mathbb{K} \). \( E \) is an elliptic curve if \( E \) is nonsingular (smooth), irreducible over \( \overline{\mathbb{K}} \) (algebraic closure), with genus 1 and has at least one rational point (over \( \mathbb{K} \)).

The affine version of elliptic curve in Weierstrass form is:

\[
E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6
\]

where the coefficients \( a_1, a_2, a_3, a_4, \text{ and } a_6 \) are in \( K \); with a special element denoted by \( \mathcal{O} \) and called the point at infinity.

An binary non supersingular elliptic curve \( E \) has the classical Weierstrass equation:

\[
y^2 + x y = x^3 + a x^2 + \beta \quad (\beta \neq 0).
\]

The group law of a binary elliptic curve is given by the following. Let \( P = (x_1, y_1) \) and \( Q = (x_2, y_2) \) be elements in \( E \) then we have the following:

- the neutral element is \( \mathcal{O} \) and the opposite of \( P \), is \( -P = (x_1, x_1 + y_1) \);
- if \( Q \neq -P \) then \( P + Q = (x_3, y_3) \):
  - if \( P \neq Q \) then \( x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \) and \( y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \) with \( \lambda = \frac{y_1 + y_2}{x_1 + x_2} \);
  - if \( P = Q \) then \( x_3 = \lambda^2 + \lambda + a \) and \( y_3 = x_1^2 + \lambda x_3 + x_3 \) with \( \lambda = x_1 + \frac{y_1}{x_1} \).

In section 2 we introduce a new binary curve and prove that it is a projective variety.

In section 3 we study the universality of the model and explain how to do the addition via a birational equivalence.

2. A New Binary Curve

In the following, we introduce a new curve and study its properties.

Definition 2.1 (New binary curve) Suppose that \( k \) is a field such that it’s characteristic is 2. Let \( a, b \) be elements of \( k \) with \( ab(a + b) \neq 0 \). The new binary curve with coefficients \( a \) and \( b \) is the affine curve

\[
E_{a,b} : a[x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] = 0.
\]
2.1 Varieties

**Proposition 2.2** The curve \( a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0 \) with \( ab(a + b) \neq 0 \) define over \( \mathbb{F}_{2^n} \) is absolutely irreducible in \( \mathbb{F}_{2^n} \).

*Proof.* Put \( H(x, y) = (a + (a + b)x)y + a(x^2 + 1) \) in \( \mathbb{F}_{2^n} \). Suppose that \( H \) is reducible i.e. there exist four non zero functions \( f, f', g, g' \) such that \( H(x, y) = [f(x) + (a + b)y][f'(x) + g'(x)y] = f(x)f'(x) + (f(x)g'(x) + g(x)f'(x))y + g(x)g'(x)y^2 \), by identification:

\[
\begin{align*}
\{ f(x)f'(x) &= a(x^2 + 1), \\
g(x)g'(x) &= (a + b)x + a, \\
f(x)g'(x) + g(x)f'(x) &= ax + (a + b)x^2, \\
\}
\]

- **1st case:** \( f = cste \) then (1) \( \Rightarrow f' = a(x^2 + 1) \), (2) \( \Rightarrow g = cste \) and (2) \( \Rightarrow g' = \frac{a + (a + b)x}{g} \). In (3) we have \( fg' + fg' = a\frac{g^2}{f}x^2 + (a + b)\frac{f}{g}x + a\left(\frac{f'}{g'} + \frac{g'}{f'}\right) \); by identification

\[
\begin{align*}
\{ a + b &= \frac{g}{f}, \\
a &= (a + b)\frac{f}{g'}, \\
\}
\]

(3') iff. \( \frac{b^2}{a + b} = 0 \) iff. \( b = 0 \) impossible because \( b \neq 0 \).

- **2nd case:** \( f' = cste \) then (1) \( \Rightarrow f = a(x^2 + 1) \), (3) \( \Rightarrow g' = cste \) and (2) \( \Rightarrow g = \frac{a + (a + b)x}{g'} \). In (3) we have \( fg' + fg' = a\frac{g'}{f'}x^2 + (a + b)\frac{f}{g'}x + a\left(\frac{f'}{g'} + \frac{g'}{f'}\right) \); by identification

\[
\begin{align*}
\{ a + b &= \frac{g'}{f'}, \\
a &= (a + b)\frac{f'}{g'}, \\
\}
\]

(3') iff. \( \frac{b^2}{a + b} = 0 \) iff. \( b = 0 \) impossible because \( b \neq 0 \).

- **3rd case:** \( \deg f = \deg f' = 1 \) then there exists \( a_1, a_2 \) such that \( f(x) = a_1(x + 1) \) and \( f'(x) = a_2(x + 1) \). Equation (2) implies that \( g = cste \) or \( g' = cste \). Suppose \( g = cste \) then \( g' = \frac{a + (a + b)x}{g} \). Equation (3) implies that \( fg' + fg' = a_1(x + 1) \left[ \frac{(a + (a + b)x + a)}{g} \right] + g a_2(x + 1) = x[(a + b)x + a] \) if \( x = 1 \) then \( (a + b) + a = 0 \) impossible.

2.2 Smooth Varieties

**Theorem 1.3 (Nonsingularity)** Each binary curve define over \( \mathbb{F}_{2^n} \) by \( a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0 \) is nonsingular.

*Proof.* It exists smooth variety if the following system assume solution:

\[
\begin{align*}
\{ H(x, y) &= y^2[a + (a + b)x] + y[a + (a + b)x^2] + a(x^2 + 1) = 0, \\
\frac{\partial H}{\partial x} &= (a + b)y^2 + ay = 0, \\
\frac{\partial H}{\partial y} &= (a + b)x^2 + ax = 0, \\
\}
\]

35
Equation (2) implies that $y = 0$ or $y = \frac{a}{a + b}$ and equation (3) implies that $x = 0$ or $x = \frac{a}{a + b}$.

If $x = \frac{a}{a + b}$, in (1) we have $a(\frac{a^2}{a^2 + b^2} + 1) = 0 \iff ab^2 = 0 \iff a = 0$ or $b = 0$, impossible because $ab \neq 0$. Thus $H$ is nonsingular.

2.3 Projective Form

2.3.1 Homogenous Equation

If we put $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we obtain the projective form of the curve $E_{a,b}$. Thus we have the following homogenous equation:

$$a[X^2Z + Y^2Z + XYZ + Z^3] + (a + b)[X^2Y + Y^2X] = 0.$$  

2.3.2 Infinites Points

$Z = 0$ implies that $(a + b)[X^2Y + Y^2X] = 0$ iff. $X = 0$ or $Y = 0$ or $X = Y$.

- $X = 0$, $(X : Y : 0) = (0 : 1 : 0)$;
- $Y = 0$, $(X : Y : 0) = (X : 0 : 0) = (1 : 0 : 0)$;
- $X = Y$, $(X : Y : 0) = (X : X : 0) = (1 : 1 : 0)$.

We have three points at infinity.

2.3.3 Singularity of Infinites Points

- $(1 : 0 : 0)$, $X = 1$ we have the following equation $T(Z, Y) = a[Z + Y^2Z + YZ + Z^3] + (a + b)[Y + Y^2]$. $\frac{\partial T}{\partial Y} = aZ + a + b$, $\frac{\partial T}{\partial Z}(0, 0) = a + b \neq 0$ thus the point $(1 : 0 : 0)$ is a nonsingular infinite point.

- $(0 : 1 : 0)$, $Y = 1$ we have the following equation $T(X, Z) = a[X^2Z + XZ + Z^3] + (a + b)[X^2 + X].$ $\frac{\partial T}{\partial X} = aZ + a + b$, $\frac{\partial T}{\partial X}(0, 0) = a + b \neq 0$ thus the point $(0 : 1 : 0)$ is a nonsingular infinite point.

- $(1 : 1 : 0)$, $X = Y = 1$ we have the following equation $T(Z) = a[Z + Z + Z^3] = aZ[1 + Z^2]$. $\frac{\partial T}{\partial Z} = a[1 + Z^2]$, $\frac{\partial T}{\partial Z}(0, 0) = a \neq 0$ thus the point $(1 : 1 : 0)$ is a nonsingular infinite point.

2.4 Birational Equivalence

**Theorem 2.4** Suppose that $k$ is a field such that it’s characteristic is 2 and $a$, $b \in k$. Each curve with affine equation $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ with $ab(a + b) \neq 0$ is equivalent in a birationally way to the curve $v^2 + v \left[\frac{1 + au}{a + b}\right] = u \left[\frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2\right]$ via the map $\varphi : (x, y) \longmapsto (u, v)$, with

$$\begin{align*}
\begin{cases}
u = \frac{y}{a + (a + b)x} \\
u = \frac{1}{a + (a + b)x} \\
u = \frac{1 + au}{(a + b)u}
\end{cases}
\end{align*}$$

Proof.

a) Assume that $v^2 + v \left[\frac{1 + au}{a + b}\right] = u \left[\frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2\right]$ and prove that $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$.

Let $H(x, y) = a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x]$. We obtain

$$H(x, y) = a \left[\frac{1 + a^2u^2}{(a^2 + b^2)u^2} + \frac{v(1 + au)}{(a + b)u^2 + 1} + (a + b) \frac{v(1 + a^2u^2)}{(a^2 + b^2)u^3} + \frac{v^2(1 + au)}{(a^2 + b^2)u^3}\right]$$

$$= a[1 + a^2u^2]u + au^2(a^2 + b^2) + auv(a + b)(1 + au) + u^3(a^2 + b^2) + (a + b)v(1 + a^2u^2) + v^2(a + b)(1 + au)]$$

$$= u(a + a^2u^2) + au(a + b) + u^2(1 + au) + v^2(a + b)(1 + au)$$

$$= v^2 + v \left[\frac{1 + au}{a + b}\right] + u \left[\frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2}\right]$$

$$= 0$$
b) Suppose that \( a[x^2 + y^2 + xy + 1] + (a+b)[x^2 y + y^2 x] = 0 \) and prove that \( v^2 + v \left( \frac{1 + au}{a + b} \right) = u \left( \frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2 \right) \).

Let \( G(u, v) = v^2 + v \left( \frac{1 + au}{a + b} \right) + u \left( \frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2 \right) \). We have the following

\[
G(u, v) = \frac{y^2}{[a + (a + b)x]^2} + \frac{y}{a + (a + b)x} \left[ \frac{1 + a(a + b)x}{a + b} \right] + \frac{1}{a + (a + b)x} \left[ \frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} \times \frac{1}{(a + (a + b)x)^2} \right]
\]

\[
\begin{align*}
&= y^2(a + (a + b)x) + y(a + (a + b)x) \left[ \frac{a + (a + b)x + a}{a + b} \right] + \left[ \frac{a(a^2 + (a + b)^2)x^2}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} \right] \\
&= ay^2 + (a + b)xy^2 + axy + (a + b)x^2y + a + ax^2 \\
&= a[x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] \\
&= 0
\end{align*}
\]

**Corollary 2.5 (Projective version)** Suppose that \( k \) is a field such that it’s characteristic is 2 and \( a, b \in k \). Each curve with projective equation \( a[X^2Z + Y^2Z + XYZ + Z^2] + (a+b)[X^2Y + Y^2X] = 0 \) with \( ab(a+b) \neq 0 \) is equivalent in a birationally way to the curve \( V^2W + VW^2 \left( \frac{W + au}{a + b} \right) = U \left[ \frac{aw^2}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} U^2 \right] \) by

\[
\begin{align*}
U &= \frac{Z}{a + b} \\
V &= \frac{Y}{a + b} \\
W &= X + \frac{aZ}{a + b}
\end{align*}
\]

**Proof.** Similarly to the above.

3. **Universality of the Model and Addition Law**

First of all let us recall the properties of trace function.

Let \( \mathbb{F}_q = \mathbb{F}_{p^r} \) be a field of \( q = p^r \) elements. The trace function denoted \( \text{Trace} \) is defined as follows: \( \text{Trace}(a) = a + a^p + \ldots + a^{p^{r-1}} \) for \( a \in \mathbb{F}_q \).

**Properties:**

1. \( \text{Trace}(\alpha) \in \mathbb{Z}/p\mathbb{Z} \);  
2. \( \text{Trace}(\alpha^p) = \alpha \);  
3. There exists \( \gamma \in \mathbb{F}_p \), with \( \text{Trace}(\gamma) \neq 0 \);  
4. if \( a \in \mathbb{Z}/p\mathbb{Z} \), then \( \text{Trace}(a) = na \);  
5. if \( a \in \mathbb{Z}/p\mathbb{Z} \), then \( \text{Trace}(a\alpha) = a\text{Trace}(\alpha) \);  
6. \( \text{Trace}(\alpha + \beta) = \text{Trace}(\alpha) + \text{Trace}(\beta) \);  
7. The polynomial \( x^p - x - \alpha \in \mathbb{F}_q[x] \) is
   
   (a) either irreducible;  
   (b) or a product of factors of degree 1.

8. The polynomial \( x^p - x - \alpha \in \mathbb{F}_q[x] \) is product of factors of degree 1 if and only if \( \text{Trace}(\alpha) = 0 \).

**Corollary:** \( \text{Trace function for binary fields} \) Let \( \alpha, \beta \in \mathbb{F}_{2^r} \)

1. \( \text{Trace}(\alpha^2) = \alpha \);  
2. The equation \( x^2 + ux + v = 0 \) with \( u, v \in \mathbb{F}_{2^r}[x], \) \( u \neq 0 \) has a solution if and only if \( \text{Trace}(\frac{u}{v}) = 0 \). Furthermore, for a solution \( x_0 \) the other is \( x_0 + u \).
Cardinality for elliptic curve

The cardinality of an elliptic curve $E$ over $\mathbb{F}_q$ is the number of $\mathbb{F}_q$-rational points. The theorem of Hasse-Weil relates the number of points to the field size.

**Theorem: (Hasse-Weil)** Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Then

$$|E(\mathbb{F}_q)| = q + 1 - t$$

and $|t| \leq 2 \sqrt{q}$.

### 3.1 Universality

When introducing a new form or elliptic curve, it is important to study how many "good" curve are isomorphic to the new model.

**Theorem 3.1** Over $\mathbb{F}_2$ with $l \geq 5$, the curves $y^2 = x^3 + ax^2 + xy + \beta$ for $\beta \neq 0$ and $a[x^2 + y^2 + xy + 1] + (a+b)[x^2y + y^2x] = 0$ are birationally equivalent.

**Proof.**

- $a[x^2 + y^2 + xy + 1] + (a+b)[x^2y + y^2x] = 0$ is equivalent in a birationally way over $\mathbb{F}_2$ to an elliptic curve in the form

$$y^2 + v \left( \frac{1 + au}{a + b} \right) = u \left[ \frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2 \right]$$

via the map $\varphi_1: (x, y) \rightarrow (u, v)$, with

$$\begin{aligned}
  u &= \frac{1}{a + (a+b)x} \\
  v &= \frac{y}{a + (a+b)x}
\end{aligned}$$

- We have also $v^2 + v \left( \frac{1 + au}{a + b} \right) = u \left[ \frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2 \right]$ is equivalent in a birationally way to $v^2 + a_1u'v' = u'^3 + a_2u'^2 + a_4u' + a_6$ with $a_1 = \frac{a}{c(a+b)}$, $a_2 = \frac{1}{a}$, $a_4 = \frac{1}{a^2} + \frac{1}{b^2}$ and $a_6 = \frac{1}{c(a^2 + b^2)} + \frac{1}{a^2}$ and $c^2 = \frac{ab^2}{a^2 + b^2}$, via the map $\varphi_2: (u, v) \rightarrow (u', v')$, with

$$\begin{aligned}
  u' &= \frac{1}{a} + u \\
  v' &= \frac{v}{c}
\end{aligned}$$

- Define change of variables, put

$$\begin{aligned}
  u &= \frac{1}{a} + u' \\
  v &= cv'
\end{aligned}$$

Then we have

$$u'^3 + a_2u'^2 + a_4u' + a_6$$

with $a_1 = \frac{a}{c(a+b)}$, $a_2 = \frac{1}{a}$, $a_4 = \frac{1}{a^2} + \frac{1}{c}$ and $a_6 = \frac{1}{c(a^2 + b^2)} + \frac{1}{a^2}$.

Define another the change of variables

$$\begin{aligned}
  u' &= a_2^T \\
  v' &= a_1^T (Z + sT + \lambda)
\end{aligned}$$

then we have

$$a_1^T (Z^2 + s^2T^2 + \lambda^2) + a_1^T (Z + sT + \lambda) = a_2^T Z^3 + a_4^T a_2 T^2 + a_1^T a_4 T + a_6 Z^2 + T_1 Z$$

$$= T^3 + T^2 \left( s^2 + s + \frac{a_2}{a_1} \right) + T \left( \lambda + \frac{a_4}{a_1} \right) + \lambda^2 + \frac{a_6}{a_1}.$$

By identification:

$$\begin{aligned}
  s^2 + s + \frac{a_2}{a_1} &= a_2' \\
  \lambda + \frac{a_4}{a_1} &= 0 \\
  \lambda^2 + \frac{a_6}{a_1} &= a_6' \Rightarrow a_6' = \frac{a_2^2}{a_1^2} + \frac{a_6}{a_1} = \frac{a_2^2 + a_1 a_6}{a_1^2}.
\end{aligned}$$
Define \( h^2 = \frac{a_2}{a_1} \implies h = \frac{a_1}{\sqrt{a_2}} \). Thus we have \( s^2 + s + a_2^2 + h^2 = 0 \), \( h^2 = \frac{a_2}{a_1^2} = \frac{c^2(a_2 + b_2)^2}{a_2^3} \), \( a_1^2 = \left( a_4 + a_1 \sqrt{a_2} \right) = \left( 1 + \frac{c^2(a_2 + b_2)^2}{a_2^3} \right) \left( 1 + \frac{c^2(a_2 + b_2)^2}{a_2^3} \right)^2 \left( 1 + \frac{h^2 + \sqrt{1 + h^2}}{a_2^3} \right) \implies h^2 \sqrt{a_6} = h^2 + h^{-1} \implies h^2 + h^{-2} + h^{-1} = 0.

Put \( t = h^{-1} \) thus \( t^2 + t + h^2 \sqrt{a_6} = 0 \).

Thus \( \begin{cases} s^2 + s + a_2^2 + h^2 = 0 \\ t^2 + t + h^2 \sqrt{a_6} = 0 \end{cases} \implies \begin{cases} \text{Trace}(a_2^2, h) = 0 \\ \text{Trace}(h^2 \sqrt{a_6}) = 0 \end{cases} \implies \begin{cases} \text{Trace}(h^{-1}) = \text{Trace}(h) \\ \text{Trace}(h \sqrt{a_6}) = 0 \end{cases} \).

For each \( \lambda, \pi \in \mathbb{F}_2 \), define

\[ L_{\lambda, \pi} = \{ h \in \mathbb{F}_2^\times : \text{Trace}(h^{-1}) = \lambda, \text{Trace}(h \sqrt{a_6}) = \pi \} \]

We define by \(|L|\) the cardinality of the set \( L \) and \(|E|\) the cardinality of \( E \). Since \( t^4 \sqrt{a_6} + t + 1 = 0 \) has at most 4 roots, we must prove that \( |L_{\text{Trace}(a_2^2), 0}| \) has at least 5 elements i.e. \(|L_{\text{Trace}(a_2^2), 0}| \geq 5 \) if \( l \geq 5 \).

Namely let at prove that \(|L_{0,0}| \geq 5 \) and \(|L_{1,0}| \geq 5 \) if \( l \geq 4 \).

We have \(|L_{0,0}| + |L_{1,0}| = 2^{t-1} - 1 \). Therefore, since \( h \) can take all values in \( \mathbb{F}_2^\times \), then \( h \sqrt{a_6} \) also take all values in \( \mathbb{F}_2^\times \). We deduce that \(|L_{0,0}| + |L_{1,0}| \) count the elements \( h \in \mathbb{F}_2^\times \) with \( \text{Trace}(h) = 0 \). Now, we have \(|L_{1,0}| + |L_{1,1}| = 2^{t-1} \). Therefore, similarly as above \(|L_{0,0}| + |L_{1,1}| \) count the elements \( h \in \mathbb{F}_2^\times \) with \( \text{Trace}(h) = 1 \). We have \(|L_{0,0}| + |L_{1,0}| = \frac{2^{t-1} - 1}{2} = 2^{t-2} - 1, |L_{1,0}| + |L_{1,1}| = \frac{2^{t-1} - 1}{2} = 2^{t-2} - 1 \).

Let us compute \(|L_{0,0}| + |L_{1,1}| \). We have the following:

\[ h \in L_{0,0} \cup L_{1,1} \iff \begin{cases} \text{Trace}(h^{-1}) = 0 = \text{Trace}(h \sqrt{a_6}) \\ \text{Trace}(h^{-1}) = 1 = \text{Trace}(h \sqrt{a_6}) \end{cases} \iff \text{Trace}(h^{-1}) = \text{Trace}(h \sqrt{a_6}) \iff \text{Trace}(h^{-1} + h \sqrt{a_6}) = 0 \iff \text{we have two possibilities for } x, \text{ namely } (x \text{ and } x + 1) \text{ such that } x^2 + x + h^{-1} + h \sqrt{a_6} = 0 \iff h^2 x^2 + h^2 x + h + h \sqrt{a_6} = 0 \iff (hx)^2 + h(hx) = h^3 + h \sqrt{a_6} + h \iff v^2 + uv = u^3 + h \sqrt{a_6} + u \text{ with } v = hx \text{ and } u = h. \]

Hasse’s theorem implies that it exists \( \delta = |E(\mathbb{F}_2^\times)| - 2^t - 1 \in [-2 \sqrt{2}, 2 \sqrt{2}] \), the point \((0, 0)\) and the infinite point do not verify the above equation and two points on the curve produce one \( h \).

Thus \( |L_{0,0}| + |L_{1,1}| = |E(\mathbb{F}_2^\times)| - 2^t - 1 \), \( |L_{0,0} + |L_{1,1}| = 2^{t-1} + \frac{\delta - 1}{2} \), \( |L_{1,0}| = 2(|L_{0,0}| + |L_{1,0}|) + 2(|L_{1,0}| + |L_{1,1}|) - 2(|L_{0,0}| + |L_{1,1}|) = 2^{t-1} - 1 + 2^{t-1} - 2(2^{t-1} - \frac{\delta - 1}{2}) = 2^t - (\delta + 1) \), \( |L_{0,0}| = 4(2^{t-1} - 1) - 4|L_{1,0}| = 4(2^{t-1} - 1) - (2^t - (\delta - 1)) = 2^t - 4 - 2^t + 6 + 1 = 2^t + 6 - 3 \), \( |L_{0,0}| \geq 2^t - 2 \sqrt{2} - 3 \implies |L_{0,0}| \geq \frac{2^t - 2 \sqrt{2} - 3}{4} \) and \( |L_{1,0}| \geq 2^t - 2 \sqrt{2} - 1 \implies |L_{1,0}| \geq \frac{2^t - 2 \sqrt{2} - 1}{4} \geq \frac{(\sqrt{2} - 1)^2 - 4}{4} \geq 11.25 \geq 5. \)

As final remark, in order to transform the curve \( z^2 + tz = t^3 + a_2 t^2 + a_6^2 \) with \( a_2^2 = \frac{b_2}{a_1} \) and \( a_6^2 = \frac{b_1}{a_2} \) via the map \( \psi : (x, y) \mapsto (t, z) \) with
Proof.

a) Suppose that \( z^2 + tz = t^3 + a'_2 t^2 + a'_6 \) and prove that \( a[x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] = 0 \).

Let \( H(x, y) = a[x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] \), we have the following:

\[
H(x, y) = a \left[ \frac{a^6}{(b^2 + a^2 t)^2} + \frac{a^6}{(b^2 + a^2 t)^2} + \frac{a^3}{a + b} \right] + 1
\]

\[
+ (a + b) \left[ \frac{a^3}{a + b} \right] \frac{a^3}{a + b} \frac{a + b}{b^2 + a^2 t^2}
\]

\[
= a[t^2(b^2 + a^2 t) + z^2(b^2 + a^2 t) + \frac{a^4}{a + b} b^4(b^2 + a^2 t) + zt(b^2 + a^2 t) + \frac{a^2}{a^2} b^2 t(b^2 + a^2 t)
\]

\[
+ \frac{a^2}{a^2} b^2 \left( b^2 + a^2 t^3 \right) + (a + b) \left[ t^2(a^2 + b^2) + \frac{a^3}{a + b} z^2 t + \frac{a^3}{a + b} b^2 t(b^2 + a^2 t) \right]
\]

\[
= z^2 + t z + t^3 + a'_2 t^2 + a'_6
\]

\[
= 0.
\]

b) Suppose that \( a[x^2 + y^2 + xy + 1] + (a + b)[x^2 y + y^2 x] = 0 \) and prove that \( z^2 + tz = t^3 + a'_2 t^2 + a'_6 \).

Let \( G(t, z) = z^2 + z t + t^3 + a'_2 t^2 + a'_6 \), we have the following:

\[
G(t, z) = \frac{b^2}{a^4} \left[ \frac{(a^2 + b^2) y^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2]}{(a + (a + b) x) y^2} \right]
\]

\[
+ \frac{b^2}{a^4} \frac{(a + a + b) x}{y} \left[ \frac{(a + a + b) y + \frac{a^3}{a^4} [a + (a + b) x]}{a + a + b) x} \right]
\]

\[
= a^2 + b^2) x^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2] \frac{a + (a + b) x}{a + (a + b) x} + x \frac{a + (a + b) x}{a^2} \left[ \frac{a^2 + b^2}{a^3} + \frac{1}{a^4} \right]
\]

\[
= a^2 + b^2) x^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2] \frac{a + (a + b) x}{a + (a + b) x} + x \frac{a + (a + b) x}{a^2} \left[ \frac{a^2 + b^2}{a^3} + \frac{1}{a^4} \right]
\]

\[
= a^2 + b^2) x^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2] \frac{a + (a + b) x}{a + (a + b) x} + x \frac{a + (a + b) x}{a^2} \left[ \frac{a^2 + b^2}{a^3} + \frac{1}{a^4} \right]
\]

\[
= a^2 + b^2) x^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2] \frac{a + (a + b) x}{a + (a + b) x} + x \frac{a + (a + b) x}{a^2} \left[ \frac{a^2 + b^2}{a^3} + \frac{1}{a^4} \right]
\]

\[
= a^2 + b^2) x^2 + \frac{a^4}{a^3} [a^2 + (a^2 + b^2) x^2] \frac{a + (a + b) x}{a + (a + b) x} + x \frac{a + (a + b) x}{a^2} \left[ \frac{a^2 + b^2}{a^3} + \frac{1}{a^4} \right]
\]

\[
= 0.
\]
Corollary 3.3 (Projective version) Suppose that \( k \) is a field such that it’s characteristic is 2 and \( a, b \in k \). Each curve with projective equation \( a[X^2Z + Y^2Z + XYZ + Z^3] + (a+b)[X^2Y + Y^2X] \) = 0 with \( ab(a+b) \neq 0 \) is equivalent in a birationally way to the curve \( V^2W + UVW = U^3 + a'_2U^2W + a'_6W^3 \) with \( a'_2 = \frac{b_2^2}{a^2} \) and \( a'_6 = \frac{a^4 + b_4^3}{a^8} b_4^3 + \frac{a^2 + b_2^3}{a^6} b_4^3 \) by

\[
\begin{align*}
U &= \frac{b_2^2(a+b)}{a^2} X \\
V &= \frac{b_2^2}{a^2} (a+b)Y + \frac{a_2^2 + b_2^3}{a^2}(aZ + (a+b)X) \\
W &= aZ + (a+b)X
\end{align*}
\]

\[
\begin{align*}
X &= \frac{a^3}{a+b} U \\
Y &= \frac{a^3}{a+b} V + \frac{a + b}{a} b_2^2 W \\
Z &= a^2 U + b_2^2 W
\end{align*}
\]

Proof. To refer to from above.

3.2 Addition Law

- **Neutral element:** In corollary 1.5, we have

\[
\begin{align*}
U &= \frac{Z}{a+b} \\
V &= \frac{Y}{a+b} \\
W &= X + \frac{aZ}{a+b}
\end{align*}
\]

and the point at infinity is \( P_\infty = (0 : 1 : 0) \) in the elliptic curve in form \( V^2W + VW = W + aU \infty = a^2 a_2 b_2 W^2 + \frac{ab^2}{a^2 + b_2^2} U^2 \).

The neutral element is the point \( \varphi^{-1}(P_\infty) = \varphi^{-1}(0 : 1 : 0) = (0 : a + b : 0) = (0 : 1 : 0) \).

- **Symmetrical element:** if \( P = (x, y) \) is a point over the curve. We have \( -P = \varphi^{-1}(\varphi(P)) \), and in the curve \( v^2 + \frac{1 + au}{a+b} = u \left[ \frac{a}{a^2 + b_2^2} + \frac{ab^2}{a^2 + b_2^2} u^2 \right] \), we have \( \varphi(P) = -(u,v) = \left( u, v + \frac{1 + au}{a+b} \right) \). Thus the symmetrical element is \( -P = (x, y + v) \).

- **Addition law:** let \( y = ax + \beta \) denote the line \( (PQ) \) where \( P = (x_P,y_P) \) and \( Q = (x_Q,y_Q) \) are in the curve \( E_{a,b} \). We define \( P + Q = R \) where \( R = (x_R,y_R) \) and \( -R = (x_R,x_R + y_R) \) is third intersection point between the line and the curve.

We have \( a(x^2 + \alpha x + \beta^2)^2 + x(ax + \beta) + 1 + (a+b)[x^2(ax + \beta) + (ax + \beta)^2 x] \) = 0, thus \( [(a+b)(\alpha + \alpha^2)]x^3 + [a(1 + \alpha + \alpha^2) + \beta(a + b)]x^2 + [ab + \beta^2(a + b)]x + a(\beta^2 + 1) = 0 \). Thus \( x_P + x_Q + x_R = \frac{a(1 + \alpha + \alpha^2) + \beta(a + b)}{(a+b)(\alpha + \alpha^2)} \).

Hence we have:

\[
\begin{align*}
x_R &= x_P + x_Q + \frac{a(1 + \alpha + \alpha^2) + \beta(a + b)}{(a+b)(\alpha + \alpha^2)} \\
y_R &= a x_R + \beta
\end{align*}
\]

with \( \alpha = \frac{y_P + y_Q}{x_P + x_Q} \) and \( \beta = y_P + ax_P \).

4. Conclusion

We have successfully proposed a new binary elliptic curve. For further works, one must study if the addition law is unified and complete.

References


