CORRESPONDENCE BETWEEN ELLIPTIC CURVES IN EDWARDS-BERNSTEIN AND WEIERSTRASS FORMS

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF OTTAWA
SUPERVISOR: PROFESSOR MONICA NEVINS
STUDENT: DANG NGUYEN

Abstract. In this paper, we explore the birational equivalence between the elliptic curves in Edwards-Bernstein and Weierstrass forms and when it induces an isomorphism of the group structures.

1. Introduction

Edwards proposed in [2] a normal form of elliptic curve which is an affine curve with a group law given by a closed-form formula. He mysteriously referred to Gauss [3, p. 404] for the origins of the addition formula on this curve. In terms of the applications in cryptography, the Edwards curve has two advantages over an elliptic curve in Weierstrass form: 1) it is an affine curve (that is, we do not need the point at infinity as in the case of the Weierstrass curve) and 2) it has a closed (and symmetric) formula for addition. In 2007, Bernstein and Lange extended the class of Edwards curves and verified the validity of the addition formula on the resulting Edwards-Bernstein curve. Their paper has been cited extensively in the literature and has found many practical applications in cryptography.

The addition formula in Weierstrass form is given by a geometric argument as we recall in Section 2.2. We refer the interested reader to [4, Section 2.2] for the addition algorithm which considers several different cases. In contrast, the addition formula for Edwards-Bernstein curve has no special cases and has a simple formula as we recall in Section 5.

Our goal in this project report is to present the mathematical background to better understand the correspondence between the Weierstrass and Edwards-Bernstein curves and also to complete the proof of some results in Bernstein and Lange's paper. To this end, we define birational equivalence between curves and present several examples to illustrate the key concepts. One aspect that Bernstein and Lange pull out is the choice of parameter d that influences the birational equivalence between the curves and the completeness of the addition formula. We have synthesized this discussion and illustrated it with some examples. Our main original contribution is to explicitly verify that the addition law on an Edwards-Bernstein curve corresponds to the standard addition law on a Weierstrass curve.

This document is organised as follows. In Section 2 we recall some definitions: elliptic curves, Weierstrass equations, birational equivalence and isomorphism. In Section 3 we present the birational equivalence between an Edwards-Bernstein curve and an elliptic curve in Weierstrass form. The exceptional points of the birational

Date: November 30, 2017.

maps are studied in Section 4. We show in Section 5 that the group law of the Edwards-Bernstein curves corresponds to the standard addition law of the elliptic curves. We conclude this document with some examples in Section 6.

2. Background

Let K be a field. Denote $\overline{K}$ an algebraic closure of K. The polynomial $p(x, y) \in K[x, y]$ defines an affine curve C over K. C is an algebraic variety and is composed of points in $(x, y) \in \overline{K}^2$ satisfying the equation $p(x, y) = 0$. Also, denote by $C(K)$ the set of K-rational points of C, that is

$$C(K) = \{(x, y) \in K^2 \mid p(x, y) = 0\}.$$

Given a homogeneous polynomial $q(X, Y, Z) \in K[X, Y, Z]$, a projective curve C' is a projective variety that consists of points $(X : Y : Z) \in \mathbb{P}^2(\overline{K})$ such that $q(X, Y, Z) = 0$. If q is the *projectivization* of p, meaning $q(X, Y, Z) = Z^n p(X/Z, Y/Z)$ where $\deg(p) = n$, then we can think of C' as C together with zero or more "points at infinity", corresponding to the intersection of $Z = 0$ and C'. The curve C' is called the *projective completion* of C.

A point P on C (or C') is *singular* if the partial derivatives of the defining polynomial of C (respectively C') vanish at P; and it is called *smooth* otherwise. The curve C (or C') is called singular if it has a singular point; otherwise it is called smooth.

Example 2.1. Let K be a field with $\mathrm{char}(K) \neq 2, 3$. Consider

$$p(x, y) = x^2 + y^2 - 1 - 3x^2y^2.$$

Let C be the affine curve defined by $p(x, y) = 0$. Its projective completion is the curve defined by

$$X^2Z^2 + Y^2Z^2 = Z^4 + 3X^2Y^2.$$

If $Z = 0$ then $X^2Y^2 = 0$. Thus $(1 : 0 : 0)$ and $(0 : 1 : 0)$ are two points at infinity of C.

The singular points of C are all points $(x, y) \in \overline{K}^2$ such that

$$p(x, y) = 0 \quad \text{and} \quad \frac{\partial p}{\partial x} = \frac{\partial p}{\partial y} = 0,$$

that is points (x, y) such that

$$\begin{cases} x^2 + y^2 = 1 + 3x^2y^2 \quad \text{and} \\ 2x - 6xy^2 = 2y - 6x^2y = 0. \end{cases}$$

It follows that there is no such point, so C is a smooth curve. As for C' it can be verified that the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ satisfy

$$\begin{cases} 2XZ^2 - 6XY^2 = 0 \\ 2YZ^2 - 6X^2Y = 0 \\ 2X^2Z + 2Y^2Z - 4Z^3 = 0 \end{cases}$$

so they are both singular. The curve C' is a singular curve.

2.1. **Elliptic curves.**

Definition 2.2. In this document, an *elliptic curve defined over a field K* is a smooth affine curve defined by the polynomial

$$y^2 = x^3 + ax + b \tag{2.1}$$

where $a, b \in K$ and $\mathrm{char}(K) \neq 2$. We add to C a point at infinity denoted ∞.

We will use the term *elliptic curve* to designate both the affine curve and its projective completion. The distinction is usually clear from the context.

The equation (2.2) is called the Weierstrass equation of the curve C.

Remark 2.3. The curve defined by (2.1) is singular when $\mathrm{char}(K) = 2$. In this case ($\mathrm{char}(K) = 2$) we use the following equation, called the *generalized Weierstrass equation*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in K$. It is shown in [4, Section 2.1] that if $\mathrm{char}(K) \neq 2$ then there is a linear change of variables after which the generalized Weierstrass equation takes the form (2.1). We also use a the following equation for elliptic curves in this document:

$$y^2 = x^3 + a'x^2 + b'x. \tag{2.2}$$

For example, when $\mathrm{char}(K) \neq 3$, the following linear change of variables transforms (2.2) to (2.1):

$$\begin{aligned} x &\mapsto x - \frac{a'}{3} \\ y &\mapsto y. \end{aligned}$$

The reason we use (2.2) is because the point $(0, 0)$ belongs to the curve. This point helps simplify our calculations of a point of order 4 when considering the group law acting on $C(K)$ (see Section 2.2). Since the group law is compatible with this linear change of variables which preserves the $x-$axis, we have a group homomorphism.

Remark 2.4. The following more general definition of an elliptic curve can be found in [5, Section III.3]:

> An elliptic curve (E, O) is a smooth curve of genus one E with a specific point $O \in E$.

Denote by $E(K)$ the set of points of E having coordinates in K. The point $O \in E(K)$ can be chosen arbitrarily, each choice gives rise to an elliptic curve. Using the Riemann-Roch theorem, it is shown in [5, Section III.3.1] that E is isomorphic to a curve C defined by the generalized Weierstrass equation. The point $O \in E$ corresponds to the point ∞ of C.

2.2. **The group law.** The points on an elliptic curve C over K form a group. When C has the form (2.1) or (2.2), this group law is often described geometrically, as follows:

> Let P, Q be two points on C. Draw a line L through P and Q. If $P = Q$ then instead let L be the tangent of C at P. Then L intersects E at a third point R'. Reflect R' across the x-axis to give a point $R \in C$. We define
>
> $$P + Q = R$$
>
> The point ∞ of C acts as the neutral element of this group.

Remark 2.5. The proof that this geometric group law is well-defined is given in [4, Sections 2.2, 2.4]. We will not detail the proof in this document. The non-obvious part is to prove the associativity of the group operation $+$.

Remark 2.6. With the more general definition of an elliptic curve (E, O) as a smooth curve of genus one, the group law is induced by the algebraic group law from the degree-0 Picard group $\mathrm{Pic}^0(E)$ as follows:

$$\kappa : E \xrightarrow{\sim} \mathrm{Pic}^0(E)$$

which sends $P \in E$ to the divisor class of $(P) - (O)$ in $\mathrm{Pic}^0(E)$. If the curve E is given by a Weierstrass equation, then this group law coincides with the geometric group law acting on the points of the Weierstrass curve. The proof is given in [5, Section III.3.4].

2.3. **Birational equivalence.** Recall that a *function defined over* K on a curve C is an equivalence class of regular functions $f(x, y) \in K(x, y)$ that is defined for at least one point in C. That is, if $f = \frac{g}{h}$ then h does not vanish on all of C. In fact, there can only be finitely many points of C where f is not defined. Two regular functions $\frac{g_1}{h_1}$ and $\frac{g_2}{h_2}$ on C are equivalent if and only if $g_1h_2 - g_2h_1$ vanishes on all of C.

Example 2.7. Let C be the curve $v^2 = u^3+6u^2+u$ defined over $\mathbb{F}_{13}$. The functions

$$f(u, v) = \frac{-2u}{v} \quad \text{and} \quad g(u, v) = -\frac{1 + u}{1 - u}$$

are defined on C except for finitely many points (called *exceptional points*), specifically points $(u, v) \in C$ such that $v = 0$ or $u = 1$. Let us calculate those points:

- If $v = 0$ then $u = 0$ or $u^2 + 6u + 1 = 0$. But $u^2 + 6u + 1 = 0$ has no roots in $\mathbb{F}_{13}$, so we have one exceptional point $(0, 0)$.
- If $u = 1$ then $v^2 = 8$ which is not a square in $\mathbb{F}_{13}$. So there are no exceptional points with $u = 1$.

It follows that g is defined everywhere. As for f, notice that $\frac{u}{v} = \frac{v}{u^2+6u+1}$ so $f(0, 0) = 0$. Therefore, f can be extended to all of C.

Definition 2.8. Let C_1 and C_2 be two curves in $\overline{K}^2$. A *rational map defined over* K from C_1 to C_2 is a map of the form

$$\phi : C_1 \to C_2 \qquad \phi = (f, g)$$

where f, g are functions defined over K on C_1 such that for every point $P \in C_1$ at which both f, g are defined, $\phi(P) = (f(P), g(P)) \in C_2$.

Example 2.9. In example 2.7, we can check that $f^2 + g^2 = 1 + 2f^2g^2$ by directly verifying the following identity

$$\frac{4u^2}{v^2} + \left(\frac{1 + u}{1 - u}\right)^2 = 1 + \frac{8u^2}{v^2}\left(\frac{1 + u}{1 - u}\right)^2$$

on the curve defined by $v^2 = u^3 + 6u^2 + u$.

Thus, the map $\phi = (f, g)$ is a rational map from the elliptic curve

$$C : v^2 = u^3 + 6u^2 + u$$

to the Edwards-Bernstein curve

$$E : x^2 + y^2 = 1 + 2x^2y^2$$

defined over $\mathbb{F}_{13}$. To see where the point at infinity ∞ of C is sent, let us look at the projective completion

$$\mathcal{C} : V^2 Z = U^3 + 6U^2 Z + UZ^2.$$

The point at infinity of C is $(0 : 1 : 0)$ on $\mathcal{C}$. Extending the map ϕ to $\mathcal{C}$ gives

$$\phi(U : V : Z) = \left(\frac{-2U}{V}, \frac{U+Z}{U-Z}\right) = \left(\frac{-2U}{V}, \frac{1+Z/U}{1-Z/U}\right).$$

Since $\frac{Z}{U} = \frac{U^2+6UZ+Z^2}{V^2}$ which vanishes at $(0 : 1 : 0)$, we have $\phi(\infty) = (0, 1)$.

Definition 2.10. A rational map $\phi : C_1 \to C_2$ is called *birational* if there is a rational map $\sigma : C_2 \to C_1$ such that

$$\sigma \circ \phi = \mathrm{id}_{C_1} \quad \text{and} \quad \phi \circ \sigma = \mathrm{id}_{C_2}$$

in which case C_1 and C_2 are said to be *birationally equivalent.* Note that the equality above is defined up to a finite number of points.

Example 2.11. Continuing with example 2.9. Let $\sigma = (u, v)$ be defined over the Edwards curve $E : x^2 + y^2 = 1 + 2x^2y^2$ with

$$u = -\frac{1+y}{1-y} \quad \text{and} \quad v = \frac{2(1+y)}{x(1-y)}$$

for all $(x, y) \in E(\mathbb{F}_{13}) \setminus \{(0, 1)\}$ and $\sigma(0, 1) = \infty \in C(\mathbb{F}_{13})$. This is a rational map from E to C. The reader can check with the map ϕ above, that σ induces a birational equivalence between E and C.

Definition 2.12. A rational map defined over K that is regular everywhere (i.e. defined everywhere) is called a *morphism defined over K.* A birational morphism whose inverse is also a morphism is an *isomorphism.*

We also use the phrase *change of variables* to refer to an isomorphism or a birational equivalence.

Example 2.13. We have seen in example 2.7 that the rational map ϕ is a morphism. In fact, ϕ is an isomorphism because its inverse σ is also a morphism. The only point that remains to check is $\sigma(0, -1)$ is well-defined in example 2.11. $u(0, -1)$ is clearly defined. As for $v(0, -1)$, note that

$$\frac{1+y}{x} = \frac{x(1-2y^2)}{1-y}.$$

So $v(0, -1) = 0$ and the map σ is regular everywhere.

2.4. **Quadratic twists.** Some curves may not be isomorphic over some field K but they are over some extension of K.

Example 2.14. $x^2 = 1$ and $x^2 = -1$ are not isomorphic over $\mathbb{R}$. They are over $\mathbb{C}$ by the change of variable $u = ix$ in $\mathbb{C}[x]$.

Definition 2.15. A *quadratic twist* of an elliptic curve C defined over K is another elliptic curve C' isomorphic to C over some quadratic extension of K.

Example 2.16. Since 2 is a non-square in $\mathbb{F}_{13}$, the curve $v^2 = u^3 + 6u^2 + u$ is isomorphic to $2v'^2 = u'^3 + 6u'^2 + u'$ over the quadratic extension $\mathbb{F}_{13}(\sqrt{2})$ via the change of variables $u = u'$ and $v = \sqrt{2}v'$.

Remark 2.17. There is a connection between $\bar{K}$-isomorphism class of elliptic curves and their j-invariant. Specifically two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant (see proof in [5, Section III.1.4]). We do not need to calculate the j-invariants in this document since our isomorphisms can be made explicit by changes of variables.

2.5. **Edwards-Bernstein normal form.** Elliptic curves can have different forms. We concern ourselves in this document with the following normal form introduced by Edwards [2] and expanded by Bernstein and Lange [1]:

$$x^2 + y^2 = c^2(1 + dx^2y^2) \tag{2.3}$$

with $c \neq 0$ and $d \notin \{0, 1\}$.

We describe in the next section the birational equivalence between Weierstrass curves and Edwards-Bernstein curves.

3. Birational equivalence between Weierstrass and Edwards-Bernstein curves

This section reformulates the content of [1, Section 2]. Our objective is to establish a birational equivalence between a Weierstrass curve and an Edwards-Bernstein curve over some extension of the base field K. As we will see shortly, the key ingredient to this birational equivalence is a point of order 4 on the Weierstrass curves. Notice that if point P has order 4 then $2P$ has order 2. Therefore we will try to identify points of order 2 to deduce a point of order 4.

Proposition 3.1. *Let C be an elliptic curve defined over K. There exists an extension K' of K such that $C(K')$ has an element of order 4.*

Proof. Let $P = (x_P, y_P)$ be a point in $C(K)$ with $y_P \neq 0$. The equation of the tangent at P is

$$L : y - y_P = (x - x_P)\lambda$$

where $\lambda = \frac{\partial f/\partial x}{\partial f/\partial y}$ taken at point (x_P, y_P) is the slope of the tangent at P and f is the defining equation of C. Recall that f has the form (2.1) or (2.2), so any point $(x, 0) \in C$ has order 2. We would like the line L to intersect C at such a point $R = (x_R, 0)$, or equivalently $2P = R$ to have order 2. Note that there are at most three candidates for x_R in the algebraic closure of K that can satisfy $f(x_R, 0) = 0$.

So we have a system of two equations and two variables x_P, y_P:

$$\begin{cases} f(x_P, y_P) = 0 \\ y_P = (x_P - x_R)\lambda \end{cases}$$

Then K' is an extension of K in which the above system has a solution for x_P, y_P. □

Example 3.2. Consider the curve $C : y^2 = x^3 + 4x^2 + x$ defined over $\mathbb{F}_{13}$. Let $P = (x_P, y_P) \in C$. The tangent of C at P is

$$y - y_P = (x - x_P)\frac{3x_P^2 + 8x_P + 1}{2y_P}$$

Suppose that L intersects C at point $(0, 0) \in C$, meaning

$$2y_P^2 = 3x_P^3 + 8x_P^2 + x_P. \tag{3.1}$$

Since $P \in C$,

$$y_P^2 = x_P^3 + 4x_P^2 + x_P. \tag{3.2}$$

Subtracting (3.1) by twice (3.2) gives

$$x_P^3 - x_P = 0.$$

It follows that $x_P = 0, y_P = 0$ or $x_P = 1, y_P^2 = 6$ or $x_P = -1, y_P^2 = 2$. Since 2 and 6 are non-square in $\mathbb{F}_{13}$ the curve $C(\mathbb{F}_{13})$ has no points of order 4. If C is defined over $\mathbb{F}_{13}(\sqrt{2}) \simeq \mathbb{F}_{169}$ then the group $C(\mathbb{F}_{169})$ has a point of order 4.

For the rest of this section, we assume that the group $C(K)$ has an element P of order 4. The following proposition shows that we can always make a linear change of variables such that $2P = (0, 0)$.

Proposition 3.3. *Let C_0 be an elliptic curve defined over K such that the group $C_0(K)$ has a point P_0 of order 4. Then C_0 is isomorphic over K to an elliptic curve C of the form*

$$C : s^2 = r^3 + ar^2 + br$$

with $a, b \in K$. The corresponding point $P \in C(K)$ of P_0 has order 4 and satisfies $2P = (0, 0)$.

Proof. Let $f(x, y) = 0$ be the Weierstrass equation for C_0. Since $P_0 = (x_0, y_0)$ has order 4, $2P_0$ has order 2. So $2P_0 = (x_1, 0)$ for some $x_1 \in K$. Applying the translation $r = x - x_1$ and $s = y$ on C_0 gives the curve $C : s^2 = r^3 + ar^2 + br$ isomorphic to C_0, for some $a, b \in K$. The point $P = (x_0 - x_1, y_0) \in C(K)$ has order 4 by this isomorphism. We also have $2P = (0, 0)$. □

Proposition 3.4. *In the setting of Proposition 3.3, if $P = (r_1, s_1)$ then*

$$a = \frac{2r_1(1+d)}{1-d} \quad \text{and}$$
$$b = r_1^2$$

where $d = 1 - \frac{4r_1^3}{s_1^2}$.

Proof. Since $P \in C$, we have

$$s_1^2 = r_1^3 + ar_1^2 + br_1 \tag{3.3}$$

We have $s_1 \neq 0$ because P has order 4 and not 2. It follows that $r_1 \neq 0$. The line tangent to C at P is

$$y - s_1 = (x - r_1)\frac{3r_1^2 + 2ar_1 + b}{2s_1}$$

Suppose that this line goes through point $(x', y') \in C$. We then have $2P = (x', -y')$ by the standard addition law. But $2P = (0, 0)$ by Proposition 3.3. So $(x', y') = (0, 0)$, meaning

$$2s_1^2 = 3r_1^3 + 2ar_1^2 + br_1 \tag{3.4}$$

Combining (3.3) and (3.4) yields

$$a = \frac{s_1^2}{r_1^2} - 2r_1, \quad \text{and}$$
$$b = r_1^2$$

Put $d = 1 - \frac{4r_1^3}{s_1^2}$, then $a = \frac{2r_1(1+d)}{1-d}$. □

Note that $d \neq 1$ because $r_1 \neq 0$. Also $d \neq 0$, otherwise the Weierstrass equation defining C would be $y^2 = x(x + r_1)^2$ which is singular at $(-r_1, 0)$.

Corollary 3.5. *C is isomorphic over K to the curve*

$$C^* : \frac{1}{1-d}v^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

Proof. Putting $u = \frac{r}{r_1}$ and $v = \frac{2s}{s_1}$ in Proposition 3.4 yields the desired result. □

Theorem 3.6. *Let K be a non-binary field. Let C be an elliptic curve over K such that the group $C(K)$ has an element of order 4. Then there exists $d \in K - \{0, 1\}$ such that the curve $E : x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent over K to C.*

Proof. By Proposition 3.3, let $P = (r_1, s_1) \in C(K)$ be the point of order 4 and satisfy $2P = (0, 0)$. Put $d = 1 - \frac{4r_1^3}{s_1^2} \in K - \{0, 1\}$.

On the other hand, the rational map

$$(x, y) \mapsto (u, v) = \left(\frac{1+y}{1-y}, \frac{2(1+y)}{x(1-y)}\right)$$

transforms the curve

$$E : x^2 + y^2 = 1 + dx^2y^2$$

into the curve

$$C^* : \frac{1}{1-d}v^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

It is well-defined except for finitely many points (x, y) with $x(y - 1) = 0$.

Its inverse is the rational map

$$(u, v) \mapsto (x, y) = \left(\frac{2u}{v}, \frac{u-1}{u+1}\right)$$

This map is also well-defined except for finitely many points (u, v) such that $v(u + 1) = 0$.

These two rational maps establish the birational equivalence over K between the curves E and C^*. The theorem follows from Corollary 3.5. □

Note that in general the curve C^* defined over K is not necessarily an elliptic curve over K for parameter $d \in K$ chosen arbitrarily. Therefore, Theorem 3.6 does not imply a bijection between the sets of Edwards-Bernstein curves E defined over K and elliptic curves C defined over K birational equivalent to E. The next result states that if d is a non-square in a non-binary finite field K then the Edwards-Bernstein curve $E : x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to an elliptic curve C over K.

Corollary 3.7. *Let $K = \mathbb{F}_p$ where p is an odd prime. If d is a quadratic nonresidue in K then the curve $E : x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to an elliptic curve C over K.*

Proof. We have seen in Theorem 3.6 that E is birationally equivalent over K to the curve

$$C^* : \frac{1}{1-d}v^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

If $1-d$ is a square in K then this curve is isomorphic over K to the elliptic curve

$$C : v'^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

by the change of variables $u \mapsto u$, $v \mapsto \frac{v}{\sqrt{1-d}}$.

If $1-d$ is a non-square in K then $\frac{d}{1-d}$ is a square because d is also a non-square. Replace d by $\frac{1}{d}$ and u by $-u$ in C^* shows that E is birationally equivalent over K to the curve

$$\frac{d}{1-d}v^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

which is an elliptic curve defined over K by the change of variables $u \mapsto u$, $v \mapsto \sqrt{\frac{d}{1-d}}v$. □

We will discuss in the next section the exceptional points of the birational maps between the Edwards-Bernstein curve E and the curve C^*.

4. Exceptional points of the birational maps

As described in the previous section, Bernstein has introduced the birational maps between the Edwards-Bernstein curve

$$E : x^2 + y^2 = 1 + dx^2y^2$$

and the curve

$$C^* : \frac{1}{1-d}v^2 = u^3 + \frac{2(1+d)}{1-d}u^2 + u$$

for $d \neq 0, 1$, as follows:

$$\begin{array}{rrcl} \phi : & E & \to & C^* \\ & (x,y) & \mapsto & \left(\frac{1+y}{1-y}, \frac{2(1+y)}{x(1-y)}\right) \\ \sigma : & C^* & \to & E \\ & (u,v) & \mapsto & \left(\frac{2u}{v}, \frac{u-1}{u+1}\right) \end{array}$$

We now try to identify the exceptional points of E (resp. C^*) where the map ϕ (resp. σ) is not defined. We will refer to the result in [5, Proposition 2.1] which says that every rational map can be extended to all smooth points.

First, let us consider the map ϕ. It is defined everywhere except at points $(x,y) \in E(K)$ such that $x(1-y) = 0$. There are only two such points: $(0,1)$ and $(0,-1)$. Both points are smooth by the test

$$P \text{ is singular} \Leftrightarrow \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$$

where $f(x,y) = x^2 + y^2 - 1 - dx^2y^2$ is the defining equation of E. So, the map ϕ is also defined at these 2 points.

We would like to know which points on C^* they correspond to. We notice that

$$\frac{1+y}{x} = \frac{x(1-dy^2)}{1-y}.$$

So in fact an alternate expression for ϕ is

$$\phi(x,y) = \left(\frac{1+y}{1-y}, \frac{2x(1-dy^2)}{(1-y)^2}\right).$$

It follows that $\phi(0,-1) = (0,0)$, a smooth point. As for the point $(0,1)$, denote by $\mathcal{C}$ the projective completion of C^*:

$$\mathcal{C} : \frac{1}{1-d}V^2T = U^3 + \frac{2(1+d)}{1-d}U^2T + UT^2$$

Extending the map ϕ gives

$$\phi(x,y) = \left(\frac{1+y}{1-y} : \frac{2(1+y)}{x(1-y)} : 1\right) = (x(1+y) : 2(1+y) : x(1-y)).$$

So $\phi(0,1) = (0:1:0)$ is the point at infinity of the curve C^*, which is also smooth. It follows that ϕ is a morphism.

We now consider the inverse map σ. It is defined everywhere except at points (u,v) such that $v(u+1) = 0$. We obtain 5 points:

$$\begin{aligned}
&P_1 = (0,0),\\
&P_2 = \left(\frac{\sqrt{d}-1}{\sqrt{d}+1}, 0\right), \quad P_3 = \left(\frac{\sqrt{d}+1}{\sqrt{d}-1}, 0\right),\\
&P_4 = (-1, 2\sqrt{d}), \quad P_5 = (-1, -2\sqrt{d}).
\end{aligned}$$

Notice that points P_2, P_3, P_4 and P_5 only exist if d is a square in K. We can check that all these points are smooth on C^* using the partial derivative test as above. So the map σ is also defined at these 5 points.

We would like to know which points on E they correspond to. For $P_1 = (0,0)$, we notice that

$$\frac{u}{v} = \left(\frac{1}{1-d}\right)\frac{v}{u^2 + 2\left(\frac{1+d}{1-d}\right)u + 1}$$

So an alternate expression for σ is

$$\sigma(u,v) = \left(\left(\frac{2}{1-d}\right)\frac{v}{u^2 + 2\left(\frac{1+d}{1-d}\right)u + 1}, \frac{u-1}{u+1}\right)$$

It follows that $\sigma(0,0) = (0,-1)$ which is a smooth point. We conclude that if d is not a square in K then σ is a morphism.

Suppose now that d is a square in K. Let us consider the remaining 4 points. Let $\mathcal{E}$ be the projective completion of E:

$$\mathcal{E} : X^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2$$

Extending the map σ gives

$$\sigma(u,v) = \left(\frac{2u}{v} : \frac{u-1}{u+1} : 1\right) = (2u(u+1) : v(u-1) : v(u+1)).$$

It follows that $\sigma(P_2) = \sigma(P_3) = (1:0:0)$ and $\sigma(P_4) = \sigma(P_5) = (0:1:0)$ which are the two points at infinity of E.

Notice that those two points $(1:0:0), (0:1:0) \in \mathcal{E}$ are singular and their inverse images are 4 smooth points.

In summary, we have an isomorphism between the affine curve E and the projective curve $\mathcal{C}$ over K if and only if d is a non-square in K.

5. The group law on an Edwards-Bernstein curve

5.1. **The statement of the group law.** In [1, Section 3], the authors state that the group law on the points of an Edwards-Bernstein curve (2.3)

$$E : x^2 + y^2 = c^2(1 + dx^2y^2)$$

can be expressed as

$$(x_1, y_1) + (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right) \tag{5.1}$$

for any pair of points $(x_1, y_1), (x_2, y_2)$ on the curves where the above addition is defined. The point $(0, c)$ is the neutral element.

More specifically, Bernstein and Lange show that the group law (5.1) is well-defined, meaning:

(1) It is complete when d is a non-square in K (stated here in Theorem 5.1).
(2) It produces a point on the curve (Theorem 5.2 which we prove in Section 5.2).
(3) It corresponds to the standard addition law on the birationally equivalent Weierstrass curve (Theorem 5.3 in Section 5.3 where we complete the proof of [1, Theorem 3.2]).

A benefit of Edwards-Bernstein curves compared to its Weierstrass counterparts is the same formula works for the addition of two different points as well as for the point doubling.

In general the addition law (5.1) is not defined for all pairs of points on the curve (2.3). For example the addition is not defined for points $(x_1, y_1), (x_2, y_2)$ with $dx_1x_2y_1y_2 = \pm 1$. As we will see later in this section, if d is a non-square in K then (5.1) is complete, meaning it is defined for all pairs of points on the curve.

Note that the curve $\bar{E} : \bar{x}^2 + \bar{y}^2 = c^2(1 + \bar{d}\bar{x}^2\bar{y}^2)$ is isomorphic to the curve $E : x^2 + y^2 = 1 + dx^2y^2$ when $d = \bar{d}c^4$ by the change of variables $\bar{x} = cx$ and $\bar{y} = cy$. We assume that the Edwards-Bernstein curve takes the form of E (i.e. $c = 1$) to simplify the calculations in the rest of this section.

We start by quoting a theorem by Bernstein and Lange that says if d is a non-square in K then the addition law (5.1) is well-defined for all pairs of points on the Edwards-Bernstein curve. The addition law is then said *complete.* This result is due to Bernstein and Lange [1, Theorem 3.3].

Theorem 5.1. *Let d be a non-square in a non-binary field K. Define the Edwards-Bernstein curve over K*

$$E : x^2 + y^2 = 1 + dx^2y^2.$$

Let $x_1, y_1, x_2, y_2 \in K$ such that $(x_1, y_1), (x_2, y_2) \in E$. Then

$$dx_1x_2y_1y_2 \neq 1 \quad \text{and} \quad dx_1x_2y_1y_2 \neq -1.$$

Proof. The proof is given in [1, Proof of Theorem 3.3]. It is a proof by contradiction. The main idea is to show that the following identities hold, when $\epsilon = dx_1x_2y_1y_2 \in \{-1, 1\}$:

$$(x_1 + \epsilon y_1)^2 = dx_1^2y_1^2(x_2 + y_2)^2$$

and similarly

$$(x_1 - \epsilon y_1)^2 = dx_1^2y_1^2(x_2 - y_2)^2.$$

Therefore d must be a square, a contradiction. □

5.2. **Closure of the group law.** The next theorem shows that the addition law (5.1) produces a point on the curve E. This result is due to Bernstein and Lange [1, Theorem 3.1].

Theorem 5.2. *Let $d \neq 0, 1$ in a non-binary field K. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on the curve*

$$E : x^2 + y^2 = 1 + dx^2y^2$$

such that $dx_1x_2y_1y_2 \neq \pm 1$. Define

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1y_2x_2y_1} \quad \text{and} \quad y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}$$

Then $R = (x_3, y_3) \in E$.

Proof. The proof consists of verifying the following identity:

$$x_3^2 + y_3^2 - dx_3^2y_3^2 = 1.$$

or equivalently, upon clearing denominators and noting that $(1 + dx_1x_2y_1y_2)^2(1 - dx_1x_2y_1y_2)^2 = (1 - d^2x_1^2x_2^2y_1^2y_2^2)^2$, that

$$\begin{aligned}&(x_1y_2 + x_2y_1)^2(1 - dx_1x_2y_1y_2)^2 + (y_1y_2 - x_1x_2)^2(1 + dx_1x_2y_1y_2)^2\\&\quad - d(x_1y_2 + x_2y_1)^2(y_1y_2 - x_1x_2)^2\\&= (1 - d^2x_1^2x_2^2y_1^2y_2^2)^2.\end{aligned}$$

Let LHS (resp. RHS) be the left-hand (resp. right-hand) side expression. Expanding LHS gives

$$\begin{aligned}\text{LHS} =&x_1^2y_2^2 + x_2^2y_1^2 + d^2x_1^4x_2^2y_1^2y_2^4 + d^2x_1^2x_2^4y_1^4y_2^2 - 4dx_1^2x_2^2y_1^2y_2^2\\&+ x_1^2x_2^2 + y_1^2y_2^2 + d^2x_1^4x_2^4y_1^2y_2^2 + d^2x_1^2x_2^2y_1^4y_2^4 - dx_1^4x_2^2y_2^2\\&- dx_1^2x_2^4y_1^2 - dx_1^2y_1^2y_2^4 - dx_2^2y_1^4y_2^2.\end{aligned} \tag{5.2}$$

We now expand RHS and check that they are equal. First, since the points P, Q are on the curve, we have

$$\begin{aligned}x_1^2 + y_1^2 &= 1 + dx_1^2y_1^2\\&= 1 + (x_2^2 + y_2^2 - dx_2^2y_2^2)dx_1^2y_1^2\\&= (x_2^2 + y_2^2)dx_1^2y_1^2 + 1 - d^2x_1^2x_2^2y_1^2y_2^2.\end{aligned}$$

So

$$1 - d^2x_1^2x_2^2y_1^2y_2^2 = x_1^2 + y_1^2 - (x_2^2 + y_2^2)dx_1^2y_1^2$$

and similarly

$$1 - d^2x_1^2x_2^2y_1^2y_2^2 = x_2^2 + y_2^2 - (x_1^2 + y_1^2)dx_2^2y_2^2.$$

Thus,

$$\text{RHS} = (x_1^2 + y_1^2 - (x_2^2 + y_2^2)dx_1^2y_1^2)(x_2^2 + y_2^2 - (x_1^2 + y_1^2)dx_2^2y_2^2).$$

Expanding RHS gives an expression identical to (5.2), as claimed. □

The result presented in the next section will allow to conclude that the addition law (5.1) on the Edwards-Bernstein curve is well-defined.

5.3. **Equivalence with the standard addition law.** We begin by recalling some notations. Let $d \neq 0, 1$ in a non-binary field K such that the curve

$$C^* : \frac{1}{1-d} v^2 = u^3 + \frac{2(1+d)}{1-d} u^2 + u$$

is elliptic over K. Recall that the Edwards-Bernstein curve

$$E : x^2 + y^2 = 1 + dx^2y^2$$

is birationally equivalent to C^* via the map $\phi(x, y) = (u, v)$ with

$$u = \frac{1+y}{1-y} \quad \text{and} \quad v = \frac{2(1+y)}{x(1-y)}. \tag{5.3}$$

Let $x_1, y_1, x_2, y_2 \in K$ such that $(x_1, y_1) \in E$, $(x_2, y_2) \in E$ and $dx_1x_2y_1y_2 \neq \pm 1$. Let

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \quad \text{and} \quad y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}. \tag{5.4}$$

For $i \in \{1, 2, 3\}$, define P_i as follows:

- $P_i = \infty$ if $(x_i, y_i) = (0, 1)$.
- $P_i = (0, 0)$ if $(x_i, y_i) = (0, -1)$.
- $P_i = (u_i, v_i) = \phi(x_i, y_i)$ otherwise. Note that P_i is well-defined because $(x_i, y_i) \in E$ by the choice of x_1, x_2, y_1, y_2 and by Theorem 5.2 for x_3, y_3.

It follows that $P_i \in C^*(K)$.

The next theorem says that the group law (5.1) on the Edwards-Bernstein curve corresponds to the standard addition law on the Weierstrass curve. This implies that the group law is associative, has an identity element and the inverse elements exist. Hence the group law is well-defined.

Theorem 5.3. *$P_1 + P_2 = P_3$ according to the standard addition law on the elliptic curve C^*.*

There are several cases to consider. In [1, Proof of Theorem 3.2] the authors explicitly prove the following cases:

- $x_1 = 0$ or
- $x_2 = 0$ or
- $P_1, P_2 \in \{\infty, (0, 0)\}$ or
- $P_1 = -P_2$.

They refer to a SageMath script to verify the remaining two cases:

(a) $P_1 = P_2$, i.e. doubling a point.
(b) $P_1 \neq \pm P_2$, i.e. adding two different (and non-opposite) points.

We present here a direct verification of Cases (a) and (b). Note that $x_1 \neq 0$ and $x_2 \neq 0$ in both cases.

Proof of Case (a). Since $P_1 = P_2$ in this case and $P_1 \neq -P_2$, we have $v_1 \neq 0$ and P_3 is a finite point. The standard addition law on C^* states that the point $-P_3$ must be on the tangent line to C^* at P_1. Therefore, we must show that

$$-v_3 - v_1 = (u_3 - u_1)\lambda \tag{5.5}$$

holds, where λ is the slope of the tangent to C^* at P_1, given by

$$\lambda = \frac{3u_1^2 + 4\left(\frac{1+d}{1-d}\right)u_1 + 1}{\left(\frac{2}{1-d}\right)v_1}. \tag{5.6}$$

We will now find u_1, v_1, u_3, v_3 and check that equation (5.5) holds.

Since $x_1 = x_2$ and $y_1 = y_2$, (5.4) gives

$$(x_3, y_3) = \left(\frac{2x_1y_1}{1+dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1-dx_1^2y_1^2}\right) = \left(\frac{2x_1y_1}{x_1^2+y_1^2}, \frac{y_1^2-x_1^2}{2-(x_1^2+y_1^2)}\right). \tag{5.7}$$

We now consider separately the case $y_1 = 0$ (which produces an exceptional point (x_3, y_3)) and the case $y_1 \neq 0$.

Case $y_1 = 0$: Then $x_1^2 = 1$, which implies $u_1 = 1$ and $v_1^2 = 4$ by (5.3). Also, $(x_3, y_3) = (0, -1)$ by (5.7). So $(u_3, v_3) = (0, 0)$ (see exceptional points in Section 4). Equation (5.6) gives $\lambda = \frac{4}{v_1}$.

Since $v_1^2 = 4$, $(u_3 - u_1)\lambda = -\frac{4}{v_1} = -v_1 = v_3 - v_1$, so (5.5) holds.

Case $y_1 \neq 0$: Using (5.3) and (5.7) we write the coordinates of the points P_1, P_3 as follows:

$$u_1 = \frac{1+y_1}{1-y_1}, \quad v_1 = \frac{2(1+y_1)}{x_1(1-y_1)}, \tag{5.8}$$

$$u_3 = \frac{1+y_3}{1-y_3} = \frac{1-x_1^2}{1-y_1^2}, \quad v_3 = \frac{2u_3}{x_3} = \left(\frac{x_1^2+y_1^2}{x_1y_1}\right)\left(\frac{1-x_1^2}{1-y_1^2}\right). \tag{5.9}$$

Denote by LHS (resp. RHS) the left-hand (resp. right-hand) side expression of (5.5); we will show they are equal. Substituting v_1, v_3 from (5.8) and (5.9) in LHS gives

$$\text{LHS} = \frac{-x_1^2 - 5y_1^2 + x_1^4 - 2y_1 + x_1^2y_1^2 - 2y_1^3}{x_1y_1(1-y_1^2)}. \tag{5.10}$$

Using u_1, u_3 from (5.8) and (5.9) we have

$$u_3 - u_1 = -\frac{x_1^2 + y_1^2 + 2y_1}{1-y_1^2}. \tag{5.11}$$

Also, substituting u_1, u_3 in (5.6) gives

$$\lambda = \frac{2x_1 + x_1y_1 - dx_1y_1 - 2dx_1y_1^2}{1-y_1^2}. \tag{5.12}$$

Multiplying the numerator and denominator of λ in (5.12) by $x_1y_1 \neq 0$ and replacing $dx_1^2y_1^2 = x_1^2 + y_1^2 - 1$ give

$$\lambda = \frac{1 + 2y_1 - x_1^2 - y_1^2 - 2y_1^3 + x_1^2y_1^2}{x_1y_1(1-y_1^2)}. \tag{5.13}$$

It follows that from (5.11) and (5.13) that

$$\text{RHS} = (u_3 - u_1)\lambda = \frac{(-x_1^2 - 5y_1^2 + x_1^4 + x_1^2y_1^2 - 2y_1 - 2y_1^3)(1-y_1^2)}{x_1y_1(1-y_1^2)^2}. \tag{5.14}$$

Thus, LHS = RHS as claimed. □

We have just shown that doubling a point (of order different than 2) on the Edwards-Bernstein curve E corresponds to doubling the image point by ϕ on the elliptic curve C^*.

We now show that adding two different points (non-inverse of one another) on the Edwards-Bernstein curve E corresponds to adding the image points by ϕ on the elliptic curve C^*. More specifically, since P_i $i \in \{1, 2, 3\}$ denotes the image point on C^* for $i \in \{1, 2, 3\}$, showing $P_3 = P_1 + P_2$ amounts to show that the points P_1, P_2 and $-P_3$ are collinear.

Recall the following assumptions from the beginning of the section for this case:

- $x_1 \neq 0$, $x_2 \neq 0$.
- $P_1, P_2 \notin \{(0, 0), \infty\}$.
- $P_1 \neq \pm P_2$.

Proof of Case (b). First, note that P_1, P_2 and $-P_3$ will be collinear if and only if the following equation holds:

$$\frac{v_2 - v_1}{u_2 - u_1} = \frac{-v_3 - v_1}{u_3 - u_1} \tag{5.15}$$

which says that the slope of the line going through points P_1, P_2 must be the same as that of the line going through $P_1, -P_3$. Since $v_i = \frac{2u_i}{x_i}$, we can rewrite (5.15) as

$$(u_3 - u_1)\left(\frac{v_2 - v_1}{u_2 - u_1}\right) = -\frac{2u_3}{x_3} - \frac{2u_1}{x_1}$$

which gives

$$u_1\left(\lambda - \frac{2}{x_1}\right) = u_3\left(\lambda + \frac{2}{x_3}\right) \tag{5.16}$$

where

$$\begin{aligned}
\lambda &= \frac{v_2 - v_1}{u_2 - u_1} \\
&= \frac{\frac{2}{x_2}\left(\frac{1+y_2}{1-y_2}\right) - \frac{2}{x_1}\left(\frac{1+y_1}{1-y_1}\right)}{\left(\frac{1+y_2}{1-y_2}\right) - \left(\frac{1+y_1}{1-y_1}\right)} \\
&= \frac{x_1(1-y_1)(1+y_2) - x_2(1+y_1)(1-y_2)}{x_1x_2(y_2 - y_1)} \qquad (5.17)
\end{aligned}$$

Denote by LHS (resp. RHS) the left-hand (resp. right-hand) side expression of (5.16). Our goal is to show that they are equal. We first expand the LHS expression:

$$\begin{aligned}
\text{LHS} &= \left(\frac{1+y_1}{1-y_1}\right)\left(\lambda - \frac{2}{x_1}\right) \\
&= \left(\frac{1+y_1}{1-y_1}\right)\left(\frac{x_1(1-y_1)(1+y_2) - x_2(1+y_1)(1-y_2) - 2x_2(y_2 - y_1)}{x_1x_2(y_2 - y_1)}\right) \\
&= \left(\frac{1+y_1}{1-y_1}\right)\frac{(x_1 - x_2)(1-y_1)(1+y_2)}{x_1x_2(y_2 - y_1)} \\
&= \frac{(x_1 - x_2)(1+y_1)(1+y_2)}{x_1x_2(y_2 - y_1)}
\end{aligned}$$

Since the LHS expression does not contain any term with coefficient d, we will expand the RHS expression and use the equation of the curve E to eliminate any terms with coefficient d.

Before we fully expand the RHS expression, let us calculate

$$\begin{aligned}
&x_1x_2(y_2-y_1)(1+dx_1x_2y_1y_2) = x_1x_2(y_2-y_1) + dx_1^2x_2^2y_1y_2^2 - dx_1^2x_2^2y_1^2y_2\\
&\quad = x_1x_2(y_2-y_1) + x_1^2y_1(1-x_2^2-y_2^2) - x_2^2y_2(1-x_1^2-y_1^2)
\end{aligned}$$

Thus by using the expression of λ in (5.17) and that of x_3 in (5.4), we have:

$$\begin{aligned}
\lambda + \frac{2}{x_3} &= \frac{x_1(1-y_1)(1+y_2) - x_2(1-y_2)(1+y_1)}{x_1x_2(y_2-y_1)} + 2\frac{1+dx_1x_2y_1y_2}{x_1y_2+x_2y_1}\\
&= \frac{A}{x_1x_2(y_2-y_1)(x_1y_2+x_2y_1)}
\end{aligned}$$

where

$$\begin{aligned}
A = {} & x_1^2y_2 - x_2^2y_1 + x_1^2y_2^2 - x_2^2y_1^2 - x_1x_2y_1 + x_1x_2y_2 + x_1^2y_1y_2^2 - x_2^2y_1^2y_2\\
& - x_1^2y_1y_2 - x_1x_2y_1^2 + x_1x_2y_2^2 + x_2^2y_1y_2 - x_1x_2y_1^2y_2 + x_1x_2y_1y_2^2\\
& - 2x_1^2y_1 + 2x_2^2y_2 + 2x_1^2x_2^2y_1 - 2x_1^2x_2^2y_2.
\end{aligned}$$

The RHS expression of (5.16) becomes

$$\text{RHS} = \frac{u_3A}{x_1x_2(y_2-y_1)(x_1y_2+x_2y_1)}$$

where

$$\begin{aligned}
u_3 &= \frac{1+\left(\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right)}{1-\left(\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right)}\\
&= \frac{1-dx_1x_2y_1y_2+y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2-y_1y_2+x_1x_2}. \qquad (5.18)
\end{aligned}$$

Notice that both LHS and RHS expressions have the common factor $x_1x_2(y_2-y_1)\neq 0$, it follows that the identity LHS = RHS is equivalent to

$$(x_1y_2+x_2y_1)\text{Numerator(LHS)Denominator}(u_3) - \text{Numerator}(u_3)A = 0 \qquad (5.19)$$

Case $y_1 = 0$: Then $x_1^2 = 1$. We substitute this in LHS, u_3 and A. Notice that $x_1y_2(x_1-x_2) = y_2(1-x_1x_2)$. The left-hand side of (5.19) becomes

$$\begin{aligned}
&x_1y_2(x_1-x_2)(1+y_2)(1+x_1x_2) - (1-x_1x_2)y_2(1+x_1x_2)(1+y_2)\\
&= (1+y_2)(1+x_1x_2)(x_1y_2(x_1-x_2)-(1-x_1x_2)y_2)\\
&= 0.
\end{aligned}$$

So LHS = RHS, as claimed.

Case $y_1 \neq 0$: Multiplying both numerator and denominator of u_3 in (5.18) by $x_1 y_1 \neq 0$ gives

$$\begin{aligned}
u_3 &= \frac{x_1y_1 - dx_1^2y_1^2x_2y_2 + x_1y_1^2y_2 - x_1^2x_2y_1}{x_1y_1 - dx_1^2y_1^2x_2y_2 - x_1y_1^2y_2 + x_1^2x_2y_1} \\
&= \frac{x_1y_1 - x_2y_2(x_1^2 + y_1^2 - 1) + x_1y_1^2y_2 - x_1^2x_2y_1}{x_1y_1 - x_2y_2(x_1^2 + y_1^2 - 1) - x_1y_1^2y_2 + x_1^2x_2y_1}.
\end{aligned}$$

Making this substitution, we see that the left-hand side of (5.19) is a polynomial in x_1, x_2, y_1, y_2 and does not contain the coefficient d. After expanding, we notice that it is equal to

$$(x_1^2x_2 - x_2 - x_1 - x_2y_1 - x_1y_2 - x_1y_1y_2)B$$

with

$$\begin{aligned}
B &= x_1^2x_2^2y_1^2 + x_1^2y_1^2y_2^2 - x_1^2x_2^2y_2^2 - x_2^2y_1^2y_2^2 + x_2^2y_2^2 - x_1^2y_1^2 \\
&= x_1^2y_1^2(x_2^2 + y_2^2 - 1) - x_2^2y_2^2(x_1^2 + y_1^2 - 1) \\
&= dx_1^2y_1^2x_2^2y_2^2 - dx_2^2y_2^2x_1^2y_1^2 \\
&= 0.
\end{aligned}$$

So LHS = RHS as claimed. □

In conclusion, $P_1 + P_2 = P_3$ in every case. The group law (5.1) on the Edwards-Bernstein curve corresponds to the standard addition law on the birationally equivalent elliptic curve. Therefore, we conclude that if d is not a square in K, we have an isomorphism of groups.

6. Examples

We conclude this document with two examples of Edwards-Bernstein curves defined over a non-binary finite field. In the first example (Section 6.1), the coefficient d is chosen to be a non-square. Therefore we have an isomorphism between the Edwards-Bernstein curve and the elliptic curve. Also, the addition law (5.1) is defined everywhere in this example.

In the second example (Section 6.2), the coefficient d is chosen to be a square. We will see that the group law (5.1) is not defined for all pairs of points on the Edwards-Bernstein curve. Interestingly, it is still birationally equivalent to an elliptic curve defined over the base field.

6.1. **An example with d non-square.** Let $K = \mathbb{F}_7$. The curve

$$E : x^2 + y^2 = 1 + 3x^2y^2$$

is smooth since $dc^4 = 3 \neq 1(7)$. Note that $d = 3$ is a non-square in K.

E is birationally equivalent to the elliptic curve

$$C : v^2 = u^3 + 4u^2 + u$$

via the maps

$$\begin{aligned}
\sigma &: (x, y) \mapsto \left(-\frac{1+y}{1-y}, \frac{4(1+y)}{x(1-y)} \right) \\
\phi &: (u, v) \mapsto \left(-\frac{4u}{v}, -\frac{1+u}{1-u} \right)
\end{aligned}$$

There are four K-rational points on each of E and C. The correspondence between $E(K)$ and $C(K)$ is

(x, y)	(u, v)
(0,1)	∞
(0,-1)	(0,0)
(1,0)	(-1,-3)
(-1,0)	(-1,3)

The map σ is actually an isomorphism following the results from Section 4. The following table shows that the group law (5.1) in E (which is defined for all pairs of points in C and denoted $P + Q$) corresponds to the standard addition law in C (denoted by $\sigma(P) + \sigma(Q)$):

P	Q	$P + Q$	$\sigma(P)$	$\sigma(Q)$	$\sigma(P) + \sigma(Q)$
(0, 1)	(0, 1)	(0, 1)	∞	∞	∞
(0, 1)	(0, -1)	(0, -1)	∞	(0,0)	(0,0)
(0, 1)	(1, 0)	(1, 0)	∞	(-1,-3)	(-1,-3)
(0, 1)	(-1, 0)	(-1, 0)	∞	(-1,3)	(-1,3)
(0, -1)	(0, -1)	(0, 1)	(0,0)	(0,0)	∞
(0, -1)	(1, 0)	(-1, 0)	(0,0)	(-1,-3)	(-1,3)
(0, -1)	(-1, 0)	(1, 0)	(0,0)	(-1,3)	(-1,-3)
(1, 0)	(1, 0)	(0, -1)	(-1,-3)	(-1,-3)	(0,0)
(1, 0)	(-1, 0)	(0, 1)	(-1,-3)	(-1,3)	∞
(-1, 0)	(-1, 0)	(0, -1)	(-1, 3)	(-1, 3)	(0,0)

Point $(0, 0) \in C(K)$ is the unique point of order 2.

6.2. **An example with d square.** Let $K = \mathbb{F}_{11}$, the curve

$$E : x^2 + y^2 = 1 + 4x^2y^2$$

is smooth because $dc^4 = 4 \neq 1(11)$.

E is birational equivalent to

$$C : v^2 = u^3 - 4u^2 + u$$

via the maps:

$$\sigma : (x, y) \mapsto \left(-\frac{1 + y}{1 - y}, \frac{4(1 + y)}{x(1 - y)}\right)$$
$$\phi : (u, v) \mapsto \left(-\frac{4u}{v}, -\frac{1 + u}{1 - u}\right)$$

There are 12 K-rational points on E and 14 on $\mathcal{E}$ whereas C has 16 K-rational points. The correspondence between $\mathcal{E}(K)$ and $C(K)$ is:

(x, y)	(u, v)
(0,1)	∞
(0,-1)	(0,0)
(1,0)	(-1,4)
(-1,0)	(-1,-4)
(2,3)	(2,-4)
(-2,3)	(2,4)
(2,-3)	(-5,-1)
(-2,-3)	(-5,1)
(3,2)	(3,-4)
(-3,2)	(3,4)
(3,-2)	(4,2)
(-3,-2)	(4,-2)
∞_1	(1,3)
∞_1	(1,-3)
∞_2	(-4,0)
∞_2	(-3,0)

Note that ∞_1 and ∞_2 are the two points at infinity of E, as described in Section 4.

Most pairs of points in $E(K)$ are not addable using (5.1) because $4x_1x_2y_1y_2 = \pm 1$. For the addable pairs $(P, Q) \in E(K) \times E(K)$, the sum $R = P + Q$ is also a point in $E(K)$, for example:

$$(1, 0) + (3, 2) = (2, -3).$$

For every pair of point $(P, Q) \in E(K) \times E(K)$, the addition of the corresponding pair $(\sigma(P), \sigma(Q)) \in C(K) \times C(K)$ is always defined (using the standard addition law). Whenever the group law (5.1) is defined for (P, Q), it produces a point that corresponds via the map σ to the sum of the corresponding points in $C(K)$, that is

$$\sigma(P + Q) = \sigma(P) + \sigma(Q).$$

The left '+' sign denotes the group law (5.1). The right '+' sign denotes the standard addition law in $C(K)$. For example:

$$\sigma(1, 0) + \sigma(3, 2) = (-1, 4) + (3, -4) = (-5, -1) = \sigma(2, -3).$$

Note however that the addition (5.1) does not make σ a group homomorphism between $E(K)$ and $C(K)$, because it is not defined on many pairs of points. For example: doubling $(2, -3)$ in $E(K)$ cannot be done by (5.1).

References

[1] Daniel J. Bernstein, Tanja Lange. *Faster Addition and Doubling on Elliptic curves.* ASIACRYPT, 29-50, 2007.

[2] Harold M. Edwards. *A Normal Form for Elliptic Curves.* Bulletin of the American Mathematical Society 44, 393-422, 2007.

[3] Carl F. Gauss. *Werke.* K. Gesellschaft der Wissenschaften zu Göttingen, vol. 3, 1870.

[4] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, 2nd Edition.* CRC Press, 2008.

[5] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition.* Springer, 2008.

[6] SageMath. *http://www.sagemath.org/*

Department of Mathematics and Statistics, University of Ottawa