Universiteit Leiden
The Netherlands

Edwards Curves

Nifterik, Line van

Citation
Nifterik, L. van. (2023). *Edwards Curves*.

Version:	Not Applicable (or Unknown)
License:	License to inclusion and publication of a Bachelor or Master Thesis, 2023
Downloaded from:	https://hdl.handle.net/1887/3663214

Note: To cite this publication please use the final published version (if applicable).

L.D.V. van Nifterik

Edwards curves

Master thesis

14 August 2023

Thesis supervisor: Prof. dr. R.M. van Luijk

Leiden University
Mathematical Institute

Contents

Introduction

Edwards curves, named after Harold Edwards who studied them in 2007, are a family of elliptic curves. They are mostly used in cryptography since curves of Edwards form provide some advantages over curves in Weierstraß form, mostly in terms of computational speed. Indeed, one of the most time-consuming processes in elliptic curve cryptography is adding points on the curve and Edwards curves provide a more convenient formula for the group law which enables that process to be done faster, without compromising any security. For this reason, public-key signatures such as the EdDSA, which are based on Edwards curves, were developed in the last decade by mathematicians such as Tanja Lange or Daniel J. Bernstein.
Because of their wide use in cryptography, most papers on Edwards curves focus on their role in cryptography and are usually quite computational. The goal of this thesis is to study Edwards curves in a more abstract way, focusing on their arithmetic properties.
We will start by stating some characteristics and properties of Edwards curves. In particular, we will give explicit formulas for the group law on Edwards curves (see Theorem 1.42). Then, in the second section, we will show that Edwards curves correspond to elliptic curves admitting a 4-torsion point (see Corollary 2.15 and Corollary 2.16). In the third section, we will perform descent by 2-isogeny on Edwards curves and show that the Edwards form of the curve allows some computations to be done more quickly than when performing descent on general elliptic curves (see Theorem 3.11). Finally, we will in the last section explicitly construct a 4-isogeny from a general Edwards curve to a related Edwards curve as well as its dual (see Theorem 4.1 and Theorem 4.10).

1 Introduction to Edwards curves: definition and characteristics.

In this section, we will define the concept of an Edwards curve and study some of its characteristics.

Definition 1.1. Let k be a field with $\mathrm{char}(k) \neq 2$. An open twisted Edwards curve E over the field k is a curve in $\mathbb{A}^2(x, y)$ defined by an equation of the form

$$x^2 + ay^2 = a + dx^2y^2$$

for some elements d in $k \setminus \{0, 1\}$ and a in k^*, together with a point O given by the coordinates $(0, 1)$.

Remark. When $a = 1$, we call such a curve an open Edwards curve.

Here are some examples of open twisted Edwards curves.

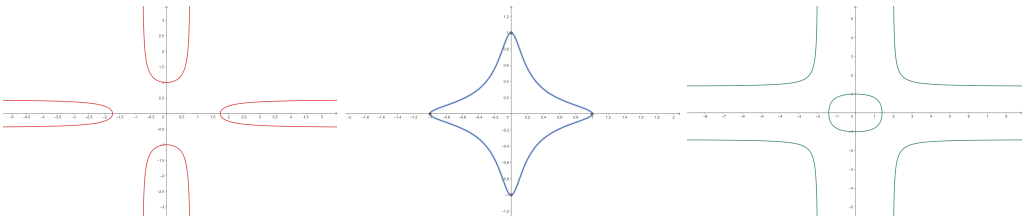


Figure 1: *Open twisted Edwards curves over* $\mathbb{R}$ *with* $a = 3$ *and* $d = 5$ *(red),* $a = 1$ *and* $d = -50$ *(blue) and* $a = 2$ *and* $d = 0.5$ *(green).*

Consider now an open twisted Edwards curve $E^0 \colon x^2 + ay^2 = a + dx^2y^2$ over a perfect field k with $\mathrm{char}(k) \neq 2$. Let δ be a root of the polynomial $X^2 - d$ and α a root of the polynomial $X^2 - a$. It is then clear that the point $(\alpha, 0)$ is on the twisted Edwards curve E^0. This point $(\alpha, 0)$ will be denoted by T.
We will start by studying the points at infinity of open twisted Edwards curves. To do so, we consider the natural completion of E^0 in $\mathbb{P}^2(X, Y, Z)$ where we identify $\mathbb{A}^2(x, y)$ with the standard affine part of $\mathbb{P}^2(X, Y, Z)$ given by $Z \neq 0$, through $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$.

Theorem 1.2. *The natural completion of* E^0 *in* $\mathbb{P}^2(X, Y, Z)$ *has two points at infinity given by the coordinates* $(1 : 0 : 0)$ *and* $(0 : 1 : 0)$ *and those are singular points.*

Proof. By embedding $\mathbb{A}^2(x, y)$ into $\mathbb{P}^2(X, Y, Z)$ through $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, the equation of E^0 becomes

$$Z^2X^2 + aZ^2Y^2 = aZ^4 + dX^2Y^2.$$

Now, define the homogeneous polynomial $F(X, Y, Z) = Z^2X^2 + aZ^2Y^2 - aZ^4 - dX^2Y^2$. At infinity the coordinate Z is equal to 0 and setting $Z = 0$ yields $F(X, Y, 0) = -dX^2Y^2$. Moreover a point $(X : Y : 0)$ is on the curve if and only if $F(X, Y, O) = 0$, i.e., if and only if $X = 0$ or $Y = 0$, since $d \neq 0$. Therefore the points at infinity on the curve are given by $(0 : 1 : 0)$ and $(1 : 0 : 0)$.
We now want to know if those points are singular or not. We start with the point $(0 : 1 : 0)$. In this case we have that $Y \neq 0$. As such we can consider the affine patch with variables $x' = \frac{X}{Y}$

and $z' = \frac{Z}{Y}$. In this patch, the point at infinity becomes $(0,0)$ and the equation of the curve is given by

$$z'^2x'^2 + az'^2 = az'^4 + dx'^2.$$

Let $f(x', z') = z'^2x'^2 + az'^2 - az'^4 - dx'^2$ and consider the derivatives

$$\frac{\partial f}{\partial x'} = 2z'^2x' - 2dx',$$
$$\frac{\partial f}{\partial z'} = 2x'^2z' + 2az' - 4az'^3.$$

At the point $(0,0)$, both derivatives are zero, meaning that the point $(0:1:0)$ at infinity is a singular point of the curve. For the point at infinity $(1:0:0)$, we have $X \neq 0$ so this time we will work in the affine patch with variables $\tilde{y} = \frac{Y}{X}$ and $\tilde{z} = \frac{Z}{X}$. In this patch, the point at infinity becomes $(0,0)$ and the equation of the curve is given by

$$\tilde{z}^2 + a\tilde{z}^2\tilde{y}^2 = a\tilde{z}^4 + d\tilde{y}^2.$$

Let $g(\tilde{y}, \tilde{z}) = \tilde{z}^2 + a\tilde{z}^2\tilde{y}^2 - a\tilde{z}^4 - d\tilde{y}^2$ and consider the derivatives

$$\frac{\partial g}{\partial \tilde{y}} = 2a\tilde{z}^2\tilde{y} - 2d\tilde{y},$$
$$\frac{\partial g}{\partial \tilde{z}} = 2\tilde{z} + 2a\tilde{y}^2\tilde{z} - 4a\tilde{z}^3.$$

Again, at the point $(0,0)$, both derivatives are zero, so the point $(1:0:0)$ at infinity is also a singular point of the curve. □

Hence the completion in $\mathbb{P}^2$ of a general open twisted Edwards curve has two singular points at infinity. The following theorem shows us that those points are the only singular points of such a curve.

Theorem 1.3. *The open twisted Edwards curve $E^0 \subset \mathbb{A}^2(x,y)$ is smooth.*

Proof. Consider the function $F(x,y) = x^2 + ay^2 - a - dx^2y^2$ and the derivatives

$$\frac{\partial F}{\partial x} = 2x - 2dy^2x$$
$$\frac{\partial F}{\partial y} = 2ay - 2dx^2y$$

We have $\frac{\partial F}{\partial x} = 0$ if and only if $x = 0$ or $1 - dy^2 = 0$, i.e., if and only if $x = 0$ or $y^2 = \frac{1}{d}$, and we have $\frac{\partial F}{\partial y} = 0$ if and only if $y = 0$ or $x^2 = \frac{a}{d}$.
Therefore, the only points to check for smoothness are the points $(0,0)$ and $\left(\pm\frac{\alpha}{\delta}, \pm\frac{1}{\delta}\right)$. It is quite clear that the point $(0,0)$ is not on the Edwards curve. Now, for the points $\left(\pm\frac{\alpha}{\delta}, \pm\frac{1}{\delta}\right)$, we see that

$$\left(\pm\frac{\alpha}{\delta}\right)^2 + a\left(\pm\frac{1}{\delta}\right)^2 = a + d\left(\pm\frac{\alpha}{\delta}\right)^2\left(\pm\frac{1}{\delta}\right)^2 \iff \frac{a}{d} + \frac{a}{d} = a + \frac{a}{d} \iff \frac{a}{d} = a \iff d = 1.$$

Since $d \neq 1$, the points $\left(\pm\frac{\alpha}{\delta}, \pm\frac{1}{\delta}\right)$ can therefore not be on the curve, and so we get that E^0 is smooth.

□

Hence E^0 is smooth on the affine plane but has a singularity at the points of infinity when completed in $\mathbb{P}^2(X, Y, Z)$.

Theorem 1.4. *The completion of E^0 in $\mathbb{P}^1(X_1, X_2) \times \mathbb{P}^1(Y_1, Y_2)$, where we put $x = \frac{X_1}{X_2}$ and $y = \frac{Y_1}{Y_2}$, is smooth.*

Proof. The equation of this completion of the curve E^0 is

$$X_1^2 Y_2^2 + a Y_1^2 X_2^2 = a X_2^2 Y_2^2 + d X_1^2 Y_1^2.$$

Let now $P = ((p_1 : p_2), (q_1 : q_2))$ be a point on $\mathbb{P}^1 \times \mathbb{P}^1$. If $p_1 = 0$ and $q_2 = 0$, then P is the point $((0 : 1), (1 : 0))$ which is not on the curve since we have then

$$p_1^2 q_2^2 + a q_1^2 p_2^2 = a q_1^2 p_2^2 \neq 0$$

but

$$a p_2^2 q_2^2 + d p_1^2 q_1^2 = 0.$$

If $q_1 = 0$ and $p_2 = 0$, then P is the point $((1 : 0), (0 : 1))$ which is also not on the curve since we have then

$$p_1^2 q_2^2 + a q_1^2 p_2^2 = 1$$

but

$$a p_2^2 q_2^2 + d p_1^2 q_1^2 = 0.$$

Hence if $P = ((p_1 : p_2), (q_1 : q_2))$ is a point on the curve then we have either $p_1 \neq 0$ and $q_1 \neq 0$, or $p_2 \neq 0$ and $q_2 \neq 0$.
Consider the case where $p_1 \neq 0$ and $q_1 \neq 0$. We then look at the affine part $\mathbb{A}^2(x', y') \subset \mathbb{P}^1(X_1, X_2) \times \mathbb{P}^1(Y_1, Y_2)$ where $x' = \frac{X_2}{X_1}$ and $y' = \frac{Y_2}{Y_1}$. By rescaling, we may assume $p_1 = q_1 = 1$. This yields

$$q_2^2 + a p_2^2 - a p_2^2 q_2^2 - d = 0$$

Define now the function $f_1(p_2, q_2) := q_2^2 + a p_2^2 - a p_2^2 q_2^2 - d$ and consider the derivatives

$$\frac{\partial f_1}{\partial p_2} = 2 a p_2 - 2 a p_2 q_2^2$$
$$\frac{\partial f_1}{\partial q_2} = 2 q_2 - 2 a q_2 p_2^2$$

For such a point $((1 : p_2), (1 : q_2))$ to be singular, we need both derivatives to be zero. This yields the equations $p_2(q_2^2 - 1) = 0$ and $q_2(a p_2^2 - 1) = 0$. Hence the possible singular points are given here by $((1 : 0), (1 : 0))$ and $(\alpha : \pm 1), ((1 : \pm 1))$. But the first point is not on the curve because $d \neq 0$ and the other points are not on the curve because $d \neq 1$.
Now, if we are in the case $p_2 \neq 0$ and $q_2 \neq 0$, then we already know by Theorem 1.3 that E^0 is smooth at the point P.
Hence the closure of the curve is smooth in $\mathbb{P}^1 \times \mathbb{P}^1$. □

We see that the natural completion of an open (twisted) Edwards curve E^0 in $\mathbb{P}^2$ is singular but that the completion of such a curve E^0 in $\mathbb{P}^1 \times \mathbb{P}^1$ as given in the previous theorem is smooth. This leads to the following definition.

Definition 1.5. The completion of a (twisted) open Edwards curve over k in $\mathbb{P}^1(X_1, X_2) \times \mathbb{P}^1(Y_1, Y_2)$ as defined in Theorem 1.4 is called a (twisted) Edwards curve over k.

From now on, we will denote by E the completion of E^0 in $\mathbb{P}^1(X_1, X_2) \times \mathbb{P}^1(Y_1, Y_2)$.

Lemma 1.6. *The only points which are on E but not on E^0 are the points given by $((1:0),(1:\pm\delta))$ and $((\pm\alpha:\delta),(1:0))$.*

Proof. The points which are on E but not on E^0 are the points at infinity, i.e., the points where $X_2 = 0$ or $Y_2 = 0$. The equation of E is given by

$$X_1^2Y_2^2 + aY_1^2X_2^2 = aX_2^2Y_2^2 + dX_1^2Y_1^2.$$

If $X_2 = 0$, then this equation becomes

$$X_1^2Y_2^2 = dX_1^2Y_1^2.$$

Because $X_2 = 0$, we necessarily have $X_1 \neq 0$ and so we get

$$Y_2^2 = dY_1^2.$$

Because $d \neq 0$, neither Y_1 nor Y_2 can be zero and so we may assume $Y_1 = 1$. This gives the points $((1:0),(1:\delta))$ and $((1:0),(1:-\delta))$.
If $Y_2 = 0$, then the equation of E becomes

$$aY_1^2X_2^2 = dX_1^2Y_1^2.$$

Since $Y_1 \neq 0$, this yields

$$aX_2^2 = dX_1^2.$$

Because neither a nor d are equal to 0, we must have $X_1 \neq 0$ and $X_2 \neq 0$ and so we may assume $X_1 = 1$. This gives the points $((\alpha:\delta),(1:0))$ and $((-\alpha:\delta),(1:0))$. □

Because those points will often be used, we introduce the following notation.

Definition 1.7. We denote the points $((1:0),(1:\delta))$ and $((1:0),(1:-\delta))$ on E by $\infty_{x,+}$ and $\infty_{x,-}$, respectively, and the points $((\alpha:\delta),(1:0))$ and $((-\alpha:\delta),(1:0))$ on E by $\infty_{y,+}$ and $\infty_{x,-}$, respectively.

We will now compute the divisors of x and y.

Definition 1.8. Let C be a curve over a field k. Let $D = \sum_{P \in C(\bar{k})} n_P(P)$ be a divisor on C. We say that D is effective if $n_P \geq 0$ for all P on C. We denote it by $D \geq 0$.

Definition 1.9. Let C be a curve over a field k. Let D be a divisor on C. We say that D is principal when $D = \mathrm{div}(f)$ for some function f in $\kappa(C)$.

Theorem 1.10. *Let D be a principal divisor on a smooth projective curve C. Then the degree of D is equal to 0.*

Proof. See [6, Chapter II, Proposition 3.1].

Theorem 1.11. *The divisors of $x = \frac{X_1}{X_2}$ and $y = \frac{Y_1}{Y_2}$ are given by*

$$\mathrm{div}(x) = (O) + ((0,-1)) - (\infty_{x,+}) - (\infty_{x,-})$$
$$\mathrm{div}(y) = (T) + ((-\alpha,0)) - (\infty_{y,+}) - (\infty_{y,-}).$$

Proof. We will first compute the divisor of x. We can easily check, using the equation of the curve that the only points on E satisfying $x = 0$ are $O = (0,1)$ and $(0,-1)$. Let us first compute

the order of x at O: the maximal ideal of the local ring corresponding to the point O is given by $\mathfrak{m}_O = (x, y-1)$. On the curve we have

$$x^2 + ay^2 = a + dx^2y^2$$

so we have

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

Since $d \neq 1$ and $a \neq 0$ both $dy^2 - 1$ are $a(y+1)$ are units here, hence $(y-1) \subseteq (x^2)$ in the local ring. Therefore $\mathfrak{m}_O = (x)$, meaning that x is a uniformiser at that point. Hence, $\mathrm{ord}_O(x) = 1$. With a similar argument, using the maximal ideal $\mathfrak{m}_{(0,-1)} = (x, y+1)$ and the fact that

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

we also have $\mathrm{ord}_{(0,-1)}(x) = 1$.
Now, the poles of the function x are given by the points where $X_2 = 0$ which correspond to the point $\infty_{x,+}$ and $\infty_{x,-}$ as seen in the proof of Lemma 1.6. Since we must have $\deg(\mathrm{div}(x)) = 0$ and $\mathrm{ord}_O(x) = 1$ and $\mathrm{ord}_{(0,-1)}(x) = 1$, the divisor of x must be given by

$$\mathrm{div}(x) = (O) + ((0,-1)) - (\infty_{x,+}) - (\infty_{x,-}).$$

For the function y, we can see, by using the equation of the curve, that its zeroes are given by the points $T = (\alpha, 0)$ and $(-\alpha, 0)$. Let us first have a look at the order of y at the point T. The maximal ideal corresponding to the point T is $\mathfrak{m}_T = (x - \alpha, y)$. The equation of the curve yields

$$x^2 + ay^2 = a + dx^2y^2$$

which implies

$$x - \alpha = \frac{y^2(dx^2 - a)}{x + \alpha}$$

and since $d \neq 1$ and $\alpha \neq 0$, we have that $dx^2 - a$ and $x + \alpha$ are units here, so $\mathfrak{m}_T = (y)$. Hence y is a uniformiser at T, so $\mathrm{ord}_T(y) = 1$. For the point $(-\alpha, 0)$, we can use a similar reasoning by rewriting the equation of the curve as

$$x + \alpha = \frac{y^2(dx^2 - a)}{x - \alpha}$$

which again yields $\mathfrak{m}_{(-\alpha,0)} = (y)$, so we get $\mathrm{ord}_{(-\alpha,0)}(y) = 1$ as well. The poles of y are given by the points where $Y_2 = 0$ which correspond to the point $\infty_{y,+}$ and $\infty_{y,-}$ as seen in the proof of Lemma 1.6. We must have $\deg(\mathrm{div}(y)) = 0$ and we know that $\mathrm{ord}_O(x) = 1$ and $\mathrm{ord}_{(0,-1)}(x) = 1$. Hence

$$\mathrm{div}(y) = (T) + ((-\alpha, 0)) - (\infty_{y,+}) - (\infty_{y,-})$$

which completes the proof. □

Remark. Even though the points $\infty_{x,+}$, $\infty_{x,-}$, $\infty_{y,+}$ and $\infty_{y,-}$ depend on the choice of α of δ, the divisors $(\infty_{x,+}) + (\infty_{x,-})$ and $(\infty_{y,+}) + (\infty_{x,-})$ do not since the points would just be permuted for different choices of α and δ.

Similarly we also get the following.

Lemma 1.12. *On E, we have*

$$\begin{aligned}\operatorname{div}(x-\alpha) &= 2(T) - (\infty_{x,+}) - (\infty_{x,-}),\\ \operatorname{div}(x+\alpha) &= 2(-\alpha,0) - (\infty_{x,+}) - (\infty_{x,-})\\ \operatorname{div}(y-1) &= 2(O) - (\infty_{y,+}) - (\infty_{y,-}).\end{aligned}$$

Proof. The only point on the curve with $x = \alpha$ is the point $T = (\alpha, 0)$ and so the point T is the only zero of $x - \alpha$. The equation of the curve yields

$$x - \alpha = \frac{y^2(dx^2 - a)}{x + \alpha}.$$

The maximal ideal corresponding to the point T is given by $\mathfrak{m}_T = (x - \alpha, y)$. Because $a \neq 0$ and $d \neq 1$, both $x + \alpha$ and $dx^2 - a$ are units here and so we see that $\mathfrak{m}_T = (x - \alpha, y) = (y)$. Hence $\operatorname{ord}_T(x - \alpha) = 2$. Moreover, the function $x - \alpha$ and x have the same poles, so

$$\operatorname{div}(x - \alpha) = 2(T) - (\infty_{x,+}) - (\infty_{x,-}).$$

The reasoning is similar for $x + \alpha$: the only point on the curve with $x = \alpha$ is the point $(-\alpha, 0)$. The maximal ideal at that point is $\mathfrak{m}_{(-\alpha,0)} = (x + \alpha, y)$ and we have

$$x + \alpha = \frac{y^2(dx^2 - a)}{x - \alpha}.$$

Because $a \neq 0$ and $d \neq 1$, both $x - \alpha$ and $dx^2 - a$ are units and so y is a uniformiser and $\operatorname{ord}_{(-\alpha,0)}(x + \alpha) = 2$. Since the function $x + \alpha$ has also the same poles as x, we therefore get

$$\operatorname{div}(x + \alpha) = 2((-\alpha, 0)) - (\infty_{x,+}) - (\infty_{x,-}).$$

Finally, the equation of the curve also yields

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

The maximal ideal corresponding to the point O is the ideal $\mathfrak{m}_O = (x, y - 1)$. Since $a \neq 0$ and $d \neq 1$, both $a(y + 1)$ and $dy^2 - 1$ are units and so we have $\mathfrak{m}_O = (x)$. Hence $\operatorname{ord}_O(y - 1) = 2$. Moreover, the function $y - 1$ has the same poles as the function y and so we get

$$\operatorname{div}(y - 1) = 2(O) - (\infty y, +) - (\infty_{y,-}).$$

□

We want in this section to give the group law on E. We will do so by using the Riemann-Roch theorem which we will restate here together with the necessary definitions.

Definition 1.13. Let C be a smooth projective curve over a field k and D a divisor on C. Then the Riemann-Roch space of D is defined as

$$L(D) = \{f \in \kappa(C)^* : \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

It is a finite-dimensional k-vector space and its dimension is denoted by

$$l(D) = \dim_k(L(D)).$$

Lemma 1.14. *Let C be a smooth projective curve over a field k. Then $l(0) = 1$.*

Proof. Let f be in $\kappa(C)^*$. Since $\deg(\mathrm{div}(f)) = 0$, we have that f is either constant or admits at least one pole. If f has a pole then $\mathrm{div}(f)$ is not effective and so f is not in $L(0)$. Hence f is in $L(0)$ if and only f is constant. Therefore $l(0) = \dim_k(L(0)) = 1$. □

Definition 1.15. Let C be a smooth projective curve over a field k and K_C a canonical divisor on C. The genus of the curve C is defined as the integer $g = l(K_C)$.

Theorem 1.16. *(Riemann-Roch theorem) Let C be a smooth projective curve over a field k and K_C a canonical divisor on C. Then for any divisor D on C, we have*

$$l(D) - l(K_C - D) = \deg(D) - g + 1$$

where g denotes the genus of the curve C.

Proof. See for instance [2, Chapter IV, Theorem 1.3]. □

From the theorem, we can deduce the following useful lemma.

Lemma 1.17. *Let C be a curve of genus 1 and D a divisor on C such that $\deg(D) > 0$. Then*

$$l(D) = \deg(D).$$

Proof. Let K_C be a canonical divisor on C. The Riemann-Roch theorem yields

$$l(K_c) - l(K_C - K_C) = \deg(K_C) - g + 1$$

with $g = l(K_C)$ the genus of the curve. Here we have $g = l(K_C) = 1$ so this equation becomes

$$1 - l(0) = \deg(K_C).$$

Lemma 1.14 gives us that $l(0) = 1$ and so we have $\deg(K_C) = 0$. Because $\deg(D) > 0$, this implies in particular

$$\deg(K_C - D) < 0.$$

So by definition 1.13, we must have $l(K_C - D) = 0$ since $\deg(\mathrm{div}(f)) = 0$ for all $f \in \kappa(\bar{C})$. The Riemann-Roch theorem now yields

$$l(D) - 0 = \deg(D) - 1 + 1$$

and so we see

$$l(D) = \deg(D).$$

□

Lemma 1.18. *The genus of E is equal to 1.*

Proof. Let g be the genus of E. Since E is a smooth curve in $\mathbb{P}^1 \times \mathbb{P}^1$ of type $(2, 2)$, we have by [2, Chapter V, Example 1.5.2] that its genus is equal to

$$g = (2 - 1)(2 - 1) = 1.$$

□

Lemma 1.19. *The curve E together with the point O is an elliptic curve.*

Proof. This follows immediately from Theorem 1.4 and Lemma 1.18.

A consequence of the above lemmas is the following corollary.

Corollary 1.20. *Let D_x be the divisor $(\infty_{x,+}) + (\infty_{x,-})$ on E and D_y the divisor $(\infty_{y,+}) + (\infty_{y,-})$. Then $L(D_x + D_y) = \langle 1, x, y, xy \rangle$.*

Proof. By Lemma 1.17 and 1.18, we have

$$l(D_x + D_y) = \deg(D_x + D_y) = 4.$$

Moreover, it is clear that $\langle 1, x, y, xy \rangle \subseteq L(D_x + D_y)$ since

$$\operatorname{div}(x) = (O) + ((0, -1)) - D_x$$

and

$$\operatorname{div}(y) = (T) + ((-\alpha, 0)) - D_y.$$

We are therefore only left to prove that the functions 1, x, y and xy are linearly independent. Suppose that c_1, c_2, c_2, c_4 are constants such that

$$c_1 + c_2 x + c_3 y + c_4 xy = 0. \tag{1}$$

Then, in particular

$$c_1 + c_2 x(O) + c_3 y(O) + c_4 (xy)(O) = 0.$$

This yields the equation $c_1 + c_3 = 0$ for $O = (0, 1)$. Now, evaluating (1) at the point $(0, -1)$ also yields $c_1 - c_3 = 0$. We conclude $c_1 = c_3 = 0$. Finally, evaluating (1) at the point $T = (\alpha, 0)$ gives us the equation $c_2 \alpha = 0$ which implies $c_2 = 0$ since $\alpha \neq 0$. But then, necessarily, we also have $c_4 = 0$ which completes the proof. □

Definition 1.21. Let C be a smooth curve over a perfect field k. Write $\operatorname{Div}^0(C)$ for the group of divisors on C over $\bar{k}$ of degree 0 and $\operatorname{PDiv}(C)$ for the group of principal divisors on C. We define the group $\operatorname{Pic}^0(C)$ as the quotient

$$\operatorname{Pic}^0(C) = \operatorname{Div}^0(C)/\operatorname{PDiv}(C).$$

With this definition, we can now state the following theorem.

Theorem 1.22. *There is a one-to-one correspondence between E and $Pic^0(E)$ given by*

$$P \mapsto [(P) - (O)].$$

Proof. This follows from Lemma 1.19 and [2, Chapter IV, Example 1.3.7]. □

This theorem shows that we can endow the curve with a group structure where the point O acts as the identity element.

Lemma 1.23. *Let C be an elliptic curve and $D = \sum_{P \in C(\bar{k})} n_P (P)$ be a divisor of C. Then D is a principal divisor if and only if*

$$\sum_{P \in C(\bar{k})} n_P = 0 \quad \textit{and} \quad \sum_{P \in C(\bar{k})} n_P P = 0.$$

Proof. See [6, Chapter III, Corollary 3.5]. □

We can now use the divisors computed in Theorem 1.11 and Lemma 1.12 to find out how maps like the translation by T or the $[-1]$-map sending a point P on E to its opposite $-P$ are given on coordinates.

Theorem 1.24. *The map $\iota\colon E \to E$ given by $(x, y) \mapsto (-x, y)$ corresponds to the automorphism $P \mapsto -P$.*
The map $\tau_T\colon E \to E$ defined by $(x, y) \mapsto \left(\alpha y, -\frac{x}{\alpha}\right)$ corresponds to the automorphism $P \mapsto P+T$.
The map $\rho\colon E \to E$ given by $(x, y) \mapsto (x, -y)$ corresponds to the automorphism $P \mapsto 2T - P$.
Moreover, the point T is a point of order 4 and the coordinates of the points $2T$ and $-T$ are respectively given by $(0, -1)$ and $(-\alpha, 0)$.

Proof. We know by Theorem 1.11 that

$$\operatorname{div}(y) = (T) + (-\alpha, 0) - (\infty_{y,+}) - (\infty_{y,-})$$

and by Lemma 1.12 that

$$\operatorname{div}(y - 1) = 2(O) - (\infty_{y,+}) - (\infty_{y,-}).$$

Hence, we have

$$\operatorname{div}\left(\frac{y}{y-1}\right) = (T) + (-\alpha, 0) - 2(O)$$

so by Lemma 1.23, on the curve, we get

$$T + (-\alpha, 0) = 2O$$

which implies

$$-T = (-\alpha, 0).$$

Together with Lemma 1.12, this implies

$$\begin{aligned}\operatorname{div}(x - \alpha) &= 2(T) - (\infty_{x,+}) - (\infty_{x,-})\\ \operatorname{div}(x + \alpha) &= 2(-T) - (\infty_{x,+}) - (\infty_{x,-}).\end{aligned}$$

Hence

$$\operatorname{div}\left(\frac{x-\alpha}{x+\alpha}\right) = 2(T) - 2(-T).$$

On the curve this yields

$$2T - (-2T) = O$$

which implies

$$4T = O$$

and $2T \neq O$, since $T \neq -T$, so T has order 4.
Consider now the map $\iota\colon E \to E$ given by $(x, y) \mapsto (-x, y)$. This map is well-defined for x only occurs in the equation of the curve to an even power. Let $P = (p, q)$ be a point on the curve. The zeroes of the function $y - q$ are clearly (p, q) and $(-p, q)$ and its poles are the same as those of y so we get

$$\begin{aligned}\operatorname{div}(y - q) &= ((p, q)) + ((-p, q)) - (\infty_{y,+}) - (\infty_{y,-})\\ &= (P) + (\iota(P)) - (\infty_{y,+}) - (\infty_{y,-})\end{aligned}$$

since $\deg(\operatorname{div}(y-q))$ must be equal to zero. Hence

$$\operatorname{div}\left(\frac{y-q}{y-1}\right) = (P) + (\iota(P)) - 2(O)$$

which, on the curve, implies

$$(P) + (\iota(P)) = 0$$

giving us in turn

$$\iota(P) = -P.$$

Therefore ι must be the map that sends a point P on the curve to its opposite $-P$. Now, since T has order 4, we know that $2T$ must be equal to $-2T$, in other words we have $2T = \iota(2T)$. This implies that x_{2T} must be equal to 0. By using the equation of the curve, we then see that y_{2T} can only be either 1 or -1, and since $2T$ can not be O, the only possibility left is $2T = (0, -1)$. Consider now the map $s\colon E \to E$ given by $(x, y) \mapsto \left(\alpha y, \frac{x}{\alpha}\right)$. It is well defined since

$$\begin{aligned}(\alpha y)^2 + a\left(\frac{x}{\alpha}\right)^2 &= x^2 + ay^2 \\ &= a + dx^2y^2 \\ &= a + d\left(\frac{x}{\alpha}\right)^2(\alpha y)^2.\end{aligned}$$

Let now $P = (p, q)$ be a point on the curve which is neither $O, T, 2T$ nor $-T$ and define

$$f = (xy - pq) + c(x + \alpha y - (p + \alpha q))$$

where $c = \frac{pq}{\alpha - (p+\alpha q)}$. It is quite clear that both $P = (p, q)$ and $s(P) = \left(\alpha q, \frac{p}{\alpha}\right)$ are zeroes of f. Moreover, we see that

$$\begin{aligned}f(O) &= -pq + c(\alpha - (p + \alpha q)) \\ &= -pq + \frac{pq}{\alpha - (p + \alpha q)}(\alpha - (p + \alpha q)) \\ &= 0\end{aligned}$$

and

$$\begin{aligned}f(T) &= -pq + c(\alpha - (p + \alpha q)) \\ &= -pq + \frac{pq}{\alpha - (p + \alpha q)}(\alpha - (p + \alpha q)) \\ &= 0.\end{aligned}$$

Now, since f is a polynomial that is linear in x and linear in y, we know that it has simple poles at $\infty_{x,+}$, $\infty_{x,-}$, $\infty_{y,+}$ and $\infty_{y,-}$. Hence the multiplicities of f at the points O, T, P and $s(P)$ are all equal to 1 and

$$\operatorname{div}(f) = (O) + (T) + (P) + (s(P)) - (\infty_{x,+}) - (\infty_{x,-}) - (\infty_{y,+}) - (\infty_{y,-}).$$

So we get on the curve

$$T + P + s(P) = \infty_{x,+} + \infty_{x,-} + \infty_{y,+} + \infty_{y,-}.$$

But since $\operatorname{div}(x) = (O) + (2T) - (\infty_{x,+}) - (\infty_{x,-})$ and $\operatorname{div}(y) = (T) + (-T) - (\infty_{y,+}) - (\infty_{y,-})$, we know that $\infty_{x,+} + \infty_{x,-} = 2T$ and $\infty_{y,+} + \infty_{y,-} = O$, so eventually we have

$$T + P + s(P) = 2T$$

which implies

$$s(P) = T - P.$$

Since any rational map from a smooth projective curve to itself extends uniquely to a morphism we have $s(P) = T - P$ for all P on E. This means in particular that the map $s \circ \iota$ sends a point P to $s(-P) = P + T$ and therefore corresponds to the translation by T. We will therefore from now on denote this map by τ_T. By the definition of ι and s on the coordinates of points of the curve, we see that $\tau_T \colon E \to E$ is given by

$$(x, y) \mapsto \left(\alpha y, -\frac{x}{\alpha}\right).$$

Finally, the map $\rho \colon E \to E$ sending a point P on the curve to $2T - P$ is equal to the composite $\tau_T^2 \circ \iota$ and so we have

$$\rho(x, y) = \tau_T^2((-x, y)) = \tau_T\left(\alpha y, \frac{x}{\alpha}\right) = (x, -y).$$

□

Corollary 1.25. *We have*

$$\infty_{y,+} = \infty_{x,+} + T,$$
$$\infty_{x,-} = \infty_{x,+} + 2T,$$

and

$$\infty_{y,-} = \infty_{x,+} - T.$$

Proof. The point $\infty_{x,+}$ is given by $((1 : 0), (1 : \delta))$. Applying τ_T yields

$$\tau_T((1 : 0), (1 : \delta)) = ((\alpha : \delta), (1 : 0)) = \infty_{y,+}.$$

Now, applying τ_T to $\infty_{y,+}$ yields

$$\tau_T((\alpha : \delta), (1 : 0) = ((\alpha : 0), (-1 : \delta)) = ((1 : 0), (-1 : \delta)) = \infty_{x,-}.$$

Finally

$$\tau_T(\infty_{x,-}) = \tau_T((1 : 0), (-1 : \delta)) = ((-\alpha : \delta), (1 : 0)) = \infty_{y,-}.$$

□

Moreover, we can also state the following.

Lemma 1.26. *We have*

$$\infty_{x,+} + \infty_{x,-} = 2T$$

and

$$\infty_{y,+} + \infty_{y,-} = O.$$

Proof. By Theorem 1.11, we have

$$\operatorname{div}(x) = (O) + (2T) - (\infty_{x,+} + \infty_{x,-})$$

and

$$\operatorname{div}(y) = (T) + (-T) - (\infty_{y,+} + \infty_{y,-}).$$

By Theorem 1.22, this yields on the curve

$$O + 2T = \infty_{x,+} + \infty_{x,-}$$

and

$$T - T = \infty_{y,+} + \infty_{y,-}.$$

Hence, we have indeed

$$\infty_{x,+} + \infty_{x,-} = 2T$$

and

$$\infty_{y,+} + \infty_{y,-} = O.$$

□

Corollary 1.27. *The points $\infty_{x,+}$ and $\infty_{x,-}$ have order 2.*

Proof. Lemma 1.26 yields

$$\infty_{x,+} + \infty_{x,-} = 2T$$

and by Corollary 1.25, we have

$$\infty_{x,-} = \infty_{x,+} + 2T.$$

Hence, when put together, those results yield

$$\infty_{x,+} + \infty_{x,+} + 2T = 2T$$

and

$$\infty_{x,-} - 2T + \infty_{x,-} = 2T.$$

This in turn directly implies

$$2\infty_{x,+} = 0$$

and

$$2\infty_{x,-} = 0$$

since T has order 4. □

We want to give a general formula for the sum of two points on the curve in terms of their coordinates. To do so, we will first state the following lemma.

Lemma 1.28. *Given P, Q in $E(k)$, there exists, up to scalar multiplication, a unique function f contained in $\langle 1, x, y, xy \rangle$ such that the divisor*

$$\operatorname{div}(f) - ((P) + (Q) + (O)) + D_x + D_y$$

is effective. Moreover, there is a unique $R \in E(k)$ such that

$$\operatorname{div}(f) = (P) + (Q) + (O) + (R) - D_x - D_y$$

and this R satisfies $2T - R = P + Q$.

Proof. Consider the Riemann-Roch space $L(D_y + D_x - (P) - (Q) - (O))$. Because the degree of the divisor $D_y + D_x - (P) - (Q) - (O)$ is one, we get by Lemma 1.17 that this space has dimension one. In other words there exists a unique f (up to scaling) such that

$$\operatorname{div}(f) - (P) - (Q) - (O) + D_x + D_y \geq 0.$$

Now we also have

$$\deg(\operatorname{div}(f) - (P) - (Q) - (O) + D_x + D_y) = 0 - 3 + 4 = 1$$

so there is a point R such that $\operatorname{div}(f) - (P) - (Q) - (O) + D_x + D_y = (R)$. In other words there exists a unique f (up to scaling) such that

$$\operatorname{div}(f) = (P) + (Q) + (O) + (R) - D_x - D_y.$$

By Theorem 1.22, this gives on the curve

$$P + Q + R + O = \infty_{x,+} + \infty_{x,-} + \infty_{y,+} + \infty_{y,-}$$

which by Lemma 1.26 implies

$$P + Q = 2T - R.$$

Moreover, since f is contained in $L(D_y + D_x - (P) - (Q) - (O))$, it is in particular contained in $L(D_y + D_x)$ which we have proven in Corollary 1.20 to be equal to $\langle 1, x, y, xy\rangle$. Hence f is contained in $\langle 1, x, y, xy\rangle$. □

We now have the necessary tools to give the formula in terms of the coordinates for the group law of the curve.

Theorem 1.29. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be two points on E^0 such that $a+dx_0x_1y_0y_1 \neq 0$ and $a - dx_0x_1y_0y_1 \neq 0$. Then their sum $P + Q$ is given by*

$$P + Q = \left(\frac{a(x_0y_1 + x_1y_0)}{a + dx_0x_1y_0y_1}, \frac{ay_0y_1 - x_0x_1}{a - dx_0x_1y_0y_1}\right).$$

Proof. By Lemma 1.28, we know that for points P and Q in $E(k)$ there exists, up to a scalar, a unique function f such that

$$\operatorname{div}(f) = (P) + (Q) + (O) + (R) - D_x - D_y$$

for some point R in $E(k)$ which then satisfies

$$R = 2T - (P + Q).$$

This means that finding this function f would enable us to find the point $P + Q$. Moreover, we also know by Lemma 1.28 that this function f is of the form

$$f = \beta + \gamma x + \lambda y + \mu xy$$

for some constants β, γ, λ and μ. To find those constants, we need to use the facts that O, P and Q are zeroes of f. This gives us the following equations

$$\begin{aligned} \beta + \lambda &= 0 \\ \beta + \gamma x_0 + \lambda y_0 + \mu x_0y_0 &= 0 \\ \beta + \gamma x_1 + \lambda y_1 + \mu x_1y_1 &= 0. \end{aligned}$$

The first equation yields $\lambda = -\beta$, so the two others equations become

$$\begin{aligned} \beta + \gamma x_0 - \beta y_0 + \mu x_0y_0 &= 0 \\ \beta + \gamma x_1 - \beta y_1 + \mu x_1y_1 &= 0. \end{aligned}$$

There are four cases.

- Suppose first that $P \neq \pm Q$, and suppose that P and Q are not equal to O, T, $2T$ or $-T$. If $\beta = 0$, then there is no solution to the system of equations. Indeed this would gives us the system

$$\begin{cases} x_0(\gamma + \mu y_0) & = 0 \\ x_1(\gamma + \mu y_1) & = 0. \end{cases}$$

Now, since P and Q are not equal to O or $2T$, we have $x_0 x_1 \neq 0$ and so this would imply $\mu(y_0 - y_1) = 0$. Because $P \neq -Q$, we also have $y_0 \neq y_1$ and so we get $\mu = 0$ and therefore also $\gamma = 0$. Hence $\beta \neq 0$. Moreover, we can scale the constants β, γ and μ and so we take β to be the non-zero constant given by $x_0 x_1(y_0 - y_1)$. The equations $f(P) = 0$ and $f(Q) = 0$ are distinct in this case and, when substituting the expression $\beta = x_0 x_1(y_0 - y_1)$ into those equations, they become

$$\begin{cases} x_0 x_1(y_0 - y_1) + \gamma x_0 - x_0 x_1(y_0 - y_1)y_0 + \mu x_0 y_0 & = 0 \\ x_0 x_1(y_0 - y_1) + \gamma x_1 - x_0 x_1(y_0 - y_1)y_1 + \mu x_1 y_1 & = 0. \end{cases} \qquad (\star)$$

The first equation yields

$$x_0 y_0 \mu = x_0 x_1(y_1 - y_0) - \gamma x_0 + y_0 x_0 x_1(y_0 - y_1).$$

Subtracting $x_1 y_1$ times the first equation in $(\star)$ from $x_0 y_0$ times the second equation yields

$$\begin{aligned} 0 = {} & x_0^2 y_0 x_1(y_0 - y_1) + \gamma x_0 x_1(y_0 - y_1) - x_0^2 y_0 x_1 y_1(y_0 - y_1) \\ & + x_0 x_1^2 y_1(y_1 - y_0) + y_0 x_0 x_1^2 y_1(y_0 - y_1). \end{aligned}$$

By dividing by $\beta = x_0 x_1(y_0 - y_1) \neq 0$, we then get

$$\gamma = x_1 y_1 - x_0 y_0 + y_0 y_1(x_0 - x_1)$$

which in turn yields

$$x_0 y_0 \mu = x_0 x_1(y_1 - y_0) - x_0(x_1 y_1 - x_0 y_0 + y_0(x_0 y_1 - x_1 y_1)) + y_0 x_0 x_1(y_0 - y_1)$$

and so we have

$$\mu = x_0 - x_1 + x_1 y_0 - x_0 y_1$$

since $x_0 y_0$ is non zero when P is not in $\langle T \rangle$. Hence when $P \neq \pm Q$ and P and Q are not in $\langle T \rangle$, the function f can be given by

$$f = x_0 x_1(y_0 - y_1) + [x_1 y_1 - x_0 y_0 + y_0 y_1(x_0 - x_1)]x - [x_0 x_1(y_0 - y_1)]y + [x_0 - x_1 + x_1 y_0 - x_0 y_1]xy.$$

Let S be the point given by the coordinates

$$\left(\frac{a(x_0 y_1 + x_1 y_0)}{a + d x_0 x_1 y_0 y_1}, \frac{a y_0 y_1 - x_0 x_1}{a - d x_0 x_1 y_0 y_1} \right)$$

as stated in the theorem. By Lemma 1.28, we are now left to check that $f(R)$ is indeed equal to 0, where $R = 2T - S$. Now, by theorem 1.24, the map $\kappa : E \to E, P \mapsto 2T - P$ is given on the coordinates by $(x, y) \mapsto (x, -y)$, therefore the coordinates of the point R are

$$\left(\frac{a(x_0 y_1 + x_1 y_0)}{a + d x_0 x_1 y_0 y_1}, \frac{x_0 x_1 - a y_0 y_1}{a - d x_0 x_1 y_0 y_1} \right).$$

We are now left to check that $f(R)$ is equal to 0, so we must compute

$$\begin{aligned} f(R) &= x_0x_1(y_0-y_1) + [x_1y_1 - x_0y_0 + y_0y_1(x_0-x_1)]\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1} \\ &\quad + x_0x_1(y_0-y_1)\frac{ay_0y_1 - x_0x_1}{a-dx_0x_1y_0y_1} \\ &\quad + [x_0 - x_1 + x_1y_0 - x_0y_1]\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}\frac{x_0x_1 - ay_0y_1}{a-dx_0x_1y_0y_1}. \end{aligned}$$

We want to prove that the numerator of this expression is indeed zero. We will therefore first multiply the entire expression by the non-zero factor $(a+dx_0x_1y_0y_1)(a-dx_0x_1y_0y_1)$. This gives us

$$\begin{aligned} f(R)(a+dx_0x_1y_0y_1)(a-dx_0x_1y_0y_1) &= a^2x_0x_1y_0 - a^2x_0x_1y_1 - d^2x_0^3x_1^3y_0^3y_1^2 + d^2x_0^3x_1^3y_0^2y_1^3 \\ &\quad + a^2x_0x_1y_1^2 + a^2x_1^2y_0y_1 - a^2x_0^2y_0y_1 - a^2x_0x_1y_0^2 \\ &\quad + a^2x_0^2y_0y_1^2 + a^2x_0x_1y_0^2y_1 - a^2x_0x_1y_0y_1^2 - a^2x_1^2y_0^2y_1 \\ &\quad - adx_0^2x_1^2y_0y_1^3 - adx_0x_1^3y_0^2y_1^2 + adx_0^3x_1y_0^2y_1^2 \\ &\quad + adx_0^2x_1^2y_0^3y_1 - adx_0^3x_1y_0^2y_1^3 + adx_0x_1^3y_0^3y_1^2 \\ &\quad + a^2x_0x_1y_0^2y_1 - ax_0^2x_1^2y_0 - a^2x_0x_1y_0y_1^2 + ax_0^2x_1^2y_1 \\ &\quad - dx_0^3x_1^3y_0^2y_1 + dx_0^3x_1^3y_0y_1^2 + ax_0^3x_1y_1 - ax_0^2x_1^2y_1 \\ &\quad - ax_0^3x_1y_1^2 + ax_0^2x_1^2y_0 - ax_0x_1^3y_0 + ax_0x_1^3y_0^2 \\ &\quad - a^2x_0^2y_0y_1^2 + a^2x_0x_1y_0y_1^2 + a^2x_0^2y_0y_1^3 - a^2x_0x_1y_0^2y_1 \\ &\quad + a^2x_1^2y_0^2y_1 - a^2x_1^2y_0^3y_1. \end{aligned}$$

We now make use of the equations $dx_0^2y_0^2 = x_0^2 + ay_0^2 - a$ and $dx_1^2y_1^2 = x_1^2 + ay_1^2 - a$. This indeed yields

$$\begin{aligned}
f(R)(a+dx_0x_1y_0y_1)(a-dx_0x_1y_0y_1) &= a^2x_0x_1y_0 - a^2x_0x_1y_1 - x_0^3x_1^3y_0 - ax_0^3x_1y_0y_1^2 \\
&+ ax_0^3x_1y_0 - ax_0x_1^3y_0^3 - a^2x_0x_1y_0^3y_1^2 + a^2x_0x_1y_0^3 \\
&+ ax_0x_1^3y_0 + a^2x_0x_1y_0y_1^2 - a^2x_0x_1y_0 + x_0^3x_1^3y_1 \\
&+ ax_0^3x_1y_1^3 - ax_0^3x_1y_1 + ax_0x_1^3y_0^2y_1 + a^2x_0x_1y_0^2y_1^3 \\
&- a^2x_0x_1y_0^2y_1 - ax_0x_1^3y_1 - a^2x_0x_1y_1^3 + a^2x_0x_1y_1 \\
&+ a^2x_0x_1y_1^2 + a^2x_1^2y_0y_1 - a^2x_0^2y_0y_1 - a^2x_0x_1y_0^2 \\
&+ a^2x_0^2y_0y_1^2 + a^2x_0x_1y_0^2y_1 - a^2x_0x_1y_0y_1^2 - a^2x_1^2y_0^2y_1 \\
&- ax_0^2x_1^2y_0y_1 - a^2x_0^2y_0y_1^3 + a^2x_0^2y_0y_1 - ax_0x_1^3y_0^2 \\
&- a^2x_0x_1y_0^2y_1^2 + a^2x_0x_1y_0^2 + ax_0^3x_1y_1^2 + a^2x_0x_1y_0^2y_1^2 \\
&- a^2x_0x_1y_1^2 + ax_0^2x_1^2y_0y_1 + a^2x_1^2y_0^3y_1 - a^2x_1^2y_0y_1 \\
&- ax_0^3x_1y_1^3 - a^2x_0x_1y_0^2y_1^3 + a^2x_0x_1y_1^3 + ax_0x_1^3y_0^3 \\
&+ a^2x_0x_1y_0^3y_1^2 - a^2x_0x_1y_0^3 + a^2x_0x_1y_0^2y_1 - ax_0^2x_1^2y_0 \\
&- a^2x_0x_1y_0y_1^2 + ax_0^2x_1^2y_1 - x_0^3x_1^3y_1 - ax_0x_1^3y_0^2y_1 \\
&+ ax_0x_1^3y_1 + x_0^3x_1^3y_0 + ax_0^3x_1y_0y_1^2 - ax_0^3x_1y_0 \\
&+ ax_0^3x_1y_1 - ax_0^2x_1^2y_1 - ax_0^3x_1y_1^2 + ax_0^2x_1^2y_0 \\
&- ax_0x_1^3y_0 + ax_0x_1^3y_0^2 - a^2x_0^2y_0y_1^2 + a^2x_0x_1y_0y_1^2 \\
&+ a^2x_0^2y_0y_1^3 - a^2x_0x_1y_0^2y_1 + a^2x_1^2y_0^2y_1 - a^2x_1^2y_0^3y_1 \\
&= 0.
\end{aligned}$$

- Suppose now that $P = Q$ and $P \neq O, T, 2T, -T$. We need to prove

$$2P = \left(\frac{2ax_0y_0}{a+dx_0^2y_0^2}, \frac{ay_0^2 - x_0^2}{a-dx_0^2y_0^2}\right).$$

Let us again denote the point given by those coordinates by S.
We have again $f(O) = 0$ and $f(P) = 0$ which gives us the following equations

$$\begin{aligned}
\beta + \lambda &= 0 \\
\beta + \gamma x_0 + \lambda y_0 + \mu x_0 y_0 &= 0.
\end{aligned}$$

But here we have that P must be a zero of f with multiplicity 2, hence we also get the equation

$$\left(\frac{dy}{dx}\right)_E (P) = \left(\frac{dy}{dx}\right)_f (P).$$

Let F denote the function that defines the curve E, i.e. we have $F = a + dx^2y^2 - x^2 - ay^2$. Then $\left(\frac{dy}{dx}\right)_E (P)$ can be rewritten as

$$\left(\frac{dy}{dx}\right)_E (P) = -\left(\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}}\right)(P) = \left(\frac{2x - 2dxy^2}{-2ay + 2dx^2y}\right)(P) = \frac{x_0(1-dy_0^2)}{y_0(dx_0^2 - a)}$$

Similarly, we have

$$\left(\frac{dy}{dx}\right)_f (P) = -\left(\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}\right)(P) = -\frac{\gamma + \mu y_0}{\lambda + \mu x_0}$$

So the equation $\left(\frac{dy}{dx}\right)_E(P) = \left(\frac{dy}{dx}\right)_f(P)$ becomes

$$\lambda x_0(dy_0^2 - 1) + \mu(ay_0^2 - x_0^2) + \gamma y_0(a - dx_0^2) = 0.$$

Using the fact $\lambda = -\beta$, the equation $f(P) = 0$ yields the following expression for μ in β and γ

$$\mu = \frac{\beta(y_0 - 1) - \gamma x_0}{x_0 y_0}.$$

Together with the equation $\lambda x_0(dy_0^2 - 1) + \mu(ay_0^2 - x_0^2) + \gamma y_0(a - dx_0^2) = 0$, we get the following expression for γ in terms of β

$$\gamma = \frac{\beta(ay_0^2 + dx_0^2 y_0^3 - x_0^2 - ay_0^3)}{x_0^3(1 - dy_0^2)}.$$

We see that if β is zero, then γ and λ is also zero and so we have $\beta = \gamma = \mu = \lambda = 0$. Therefore, β is non-zero and since we can scale the constants $\beta, \gamma\mu$ and λ, we now take β to be the non-zero constant $x_0^3(1 - dy_0^2)$. It is non-zero because the equation of the curve yields $x_0^3(a - dy_0^2) = ax_0(1 - y_0^2)$ and $ax_0(1 - y_0^2) \neq 0$, for P is neither O nor $2T$. We then get

$$\gamma = ay_0^2 + dx_0^2 y_0^3 - x_0^2 - ay_0^3 = ay_0^2 + y_0(x_0^2 + ay_0^2 - a) - x_0^2 - ay_0^3 = (x_0^2 + ay_0)(y_0 - 1)$$

since P is on the curve. For the same reason, we can also rewrite β as

$$\beta = x_0^3 - x_0(x_0^2 + ay_0^2 - a) = ax_0(1 - y_0^2)$$

Using those expressions of γ and β, we get for μ

$$\begin{aligned}\mu &= \frac{-ax_0 + ax_0y_0^2 + 2ax_0y_0 - ax_0y_0^3 - x_0^3y_0 - ax_0y_0^2 + x_0^3}{x_0y_0} \\ &= \frac{x_0^2 - a}{y_0} + 2a - x_0^2 - ay_0^2.\end{aligned}$$

Hence, the function f is given by

$$f(x,y) = ax_0(1 - y_0^2) + (x_0^2 + ay_0)(y_0 - 1)x + ax_0(y_0^2 - 1)y + \left(\frac{x_0^2 - a}{y_0} + 2a - x_0^2 - ay_0^2\right)xy$$

We are left to show that $f(R) = 0$ for

$$R = 2T - S = \left(\frac{2ax_0y_0}{a + dx_0^2y_0^2}, \frac{x_0^2 - ay_0^2}{a - dx_0^2y_0^2}\right) = \left(\frac{2ax_0y_0}{x_0^2 + ay_0^2}, \frac{x_0^2 - ay_0^2}{2a - x_0^2 - ay_0^2}\right).$$

Since we assume $a + dx_0^2y_0^2 \neq 0$ and $a - dx_0^2y_0^2 \neq 0$, in particular, we also have $x_0^2 + ay_0^2 \neq 0$ and $2a - x_0^2 - ay_0^2 \neq 0$. We get

$$\begin{aligned}f(R) = {} & ax_0(1 - y_0^2) + (x_0^2 + ay_0)(y_0 - 1)\frac{2ax_0y_0}{x_0^2 + ay_0^2} + ax_0(y_0^2 - 1)\frac{x_0^2 - ay_0^2}{2a - x_0^2 - ay_0^2} \\ & + \left(\frac{x_0^2 - a}{y_0} + 2a - x_0^2 - ay_0^2\right)\frac{2ax_0y_0}{x_0^2 + ay_0^2}\frac{x_0^2 - ay_0^2}{2a - x_0^2 - ay_0^2}.\end{aligned}$$

This gives us

$$\begin{aligned}(x_0^2+ay_0^2)(2a-x_0^2-ay_0^2)f(R) &= 2a^2x_0^3 - ax_0^5 - 4a^2x_0^3y_0^2 + 2a^3x_0y_0^2 - 3a^3x_0y_0^4 \\ &+ ax_0^5y_0^2 + 2a^2x_0^3y_0^4 + a^3x_0y_0^6 + 4a^2x_0^3y_0^2 - 2ax_0^5y_0^2 \\ &- 2a^2x_0^3y_0^4 + 4a^3x_0y_0^3 - 2a^3x_0y_0^5 - 4a^2x_0^3y_0 + 2ax_0^5y_0 \\ &- 4a^3x_0y_0^2 + 2a^2x_0^3y_0^2 + 2a^3x_0y_0^4 + ax_0^5y_0^2 - ax_0^5 \\ &- a^3x_0y_0^6 + a^3x_0y_0^4 + 2ax_0^5 - 2a^2x_0^3y_0^2 - 2a^2x_0^3 \\ &+ 2a^3x_0y_0^2 + 4a^2x_0^3y_0 - 4a^3x_0y_0^3 - 2ax_0^5y_0 + 2a^3x_0y_0^5 \\ &= 0.\end{aligned}$$

So we have indeed

$$2P = \left(\frac{2ax_0y_0}{a+dx_0^2y_0^2}, \frac{ay_0^2-x_0^2}{a-dx_0^2y_0^2}\right)$$

for $P \neq 0, T, 2T, -T$.

- If $P = -Q$ then the sum $P+Q$ must be equal to $O = (0,1)$. If $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ then we know by Theorem 1.24 that $x_1 = -x_0$ and $y_1 = y_0$. Now we have

$$\left(\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}, \frac{ay_0y_1-x_0x_1}{a-dx_0x_1y_0y_1}\right) = \left(\frac{a(x_0y_0-x_0y_0)}{a-dx_0^2y_0^2}, \frac{ay_0^2+x_0^2}{a+dx_0^2y_0^2}\right) = (0,1)$$

since $x_0^2 + ay_0^2 = a + dx_0^2y_0^2$. Hence the formula holds for $P = -Q$.

- For $P \in \{O, T, 2T, -T\}$, we have the following.
If $P = O$, we know that for all points $Q = (x_1, y_1)$ on E the sum $O + Q$ must be equal to Q itself. Now, for $P = (x_0, y_0) = O = (0,1)$ and $Q = (x_1, y_1)$, we have

$$\left(\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}, \frac{ay_0y_1-x_0x_1}{a-dx_0x_1y_0y_1}\right) = \left(\frac{ax_1}{a}, \frac{ay_1}{a}\right) = (x_1, y_1) = Q$$

so the formula holds for $P = O$.
If $P = T$, we know by Theorem 1.24 that for every point $Q = (x_1, y_1)$ on E, we must have that $T + Q = \left(\alpha y_1, -\frac{x_1}{\alpha}\right)$. On the other hand when we have $P = (x_0, y_0) = (\alpha, 0) = T$, then

$$\left(\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}, \frac{ay_0y_1-x_0x_1}{a-dx_0x_1y_0y_1}\right) = \left(\frac{a(\alpha y_1)}{a}, \frac{-\alpha x_1}{a}\right) = \left(\alpha y_1, -\frac{x_1}{\alpha}\right)$$

which proves the statement of the theorem for $P = T$.
Similarly, if $P = 2T$, then we know by Theorem 1.24 that the coordinates of P are given by $(0, -1)$. Hence

$$\left(\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}, \frac{ay_0y_1-x_0x_1}{a-dx_0x_1y_0y_1}\right) = \left(\frac{-ax_1}{a}, \frac{-ay_1}{a}\right) = (-x_1, -y_1)$$

which, again by Theorem 1.24, is indeed equal to the sum $2T + Q$.
Lastly, if $P = -T$, then Theorem 1.24 gives us that P is equal to $(-\alpha, 0)$. hence, we have

$$\left(\frac{a(x_0y_1+x_1y_0)}{a+dx_0x_1y_0y_1}, \frac{ay_0y_1-x_0x_1}{a-dx_0x_1y_0y_1}\right) = \left(\frac{a(-\alpha y_1)}{a}, \frac{\alpha x_1}{a}\right) = \left(-\alpha y_1, \frac{x_1}{\alpha}\right)$$

which is equal to the sum $-T + Q$ by Theorem 1.24. □

We have given here a formula for the group law that works in most situations. However we have excluded some cases. For instance this formula does not give the coordinates of the point $P+Q$ when P or Q is one of the points in $\{\infty_{x,+}, \infty_{x,-}, \infty_{y,+}, \infty_{y,-}\}$ and excludes the points $P=(x_0,y_0)$ and $Q=(x_1,y_1)$ for which $a+dx_0x_1y_0y_1=0$ or $a-dx_0x_1y_0y_1=0$. The aim for the rest of the section is to give a complete formula for the group law of E. This will be stated as Theorem 1.42.

Lemma 1.30. *Let θ be an be an automorphism of E fixing the point O which is not the identity. Suppose that $\theta^n=1$ for some n in $\mathbb{Z}_{>0}$ and that $\theta(S)=S$ for some point S on E. Then there is an integer $d|n$, $d\neq 1$, such that $S\in E[\Phi_d(1)]$ where Φ_d denotes the d-th cyclotomic polynomial.*

Proof. By assumption, we have $\theta^n-1=0$, i.e $\prod_{d|n}\Phi_d(\theta)=0$. By [6, Chapter III, Proposition 4.2(c)] the endomorphism ring $\mathrm{End}(E)$ has no zero divisors, so the previous equation implies that $\Phi_d(\theta)=0$ for some $d|n$, with $d>1$ since $\theta\neq 1$ by assumption. Now, evaluating the latter equation on S yields $\Phi_d(1)S=0$ because $\theta(S)=S$. Hence S is in $E[\Phi_d(1)]$. □

Lemma 1.31. *Let θ be an be an automorphism of E such that $\theta(O)=O$ and $\theta(T)=T$. Then θ is the identity morphism.*

Proof. The curve E is defined on a field k with $\mathrm{char}(k)\neq 2$ so by [6, Chapter III, Theorem 10.1.], we have either $\theta=1$, $\theta^2=1$, $\theta^3=1$, $\theta^4=1$ or $\theta^6=1$. Assume $\theta\neq 1$. If $\theta^2=1$, then by the previous lemma, T must be in $E[\Phi_2(1)]=E[2]$ but this is not possible for $2T=(0,-1)\neq O_E$. Similarly, if $\theta^3=1$, or $\theta^4=1$, or $\theta^6=1$, then the previous lemma yields either $T\in E[3]$, or $T\in E[2]$ or $T=O_E$. But T does not satisfy any of those conditions, so we must have $\theta=1$. □

Theorem 1.32. *The map $\tau_{\infty_{x,+}}\colon E\to E$ sending a point P to $P+\infty_{x,+}$ is given on the coordinates by*

$$(x,y)\mapsto\left(\frac{a}{\delta x},\frac{1}{\delta y}\right).$$

Proof. Define $\chi\colon E\to E$ to be the map $(x,y)\mapsto\left(\frac{a}{\delta x},\frac{1}{\delta y}\right)$. The map is well defined since

$$\left(\frac{a}{\delta x}\right)^2+a\left(\frac{1}{\delta y}\right)^2=\frac{a(x^2+ay^2)}{dx^2y^2}=\frac{a(a+dx^2y^2)}{dx^2y^2}=a+\frac{a^2}{dx^2y^2}$$

and

$$a+d\left(\frac{a}{\delta x}\right)^2\left(\frac{1}{\delta y}\right)^2=a+\frac{a^2}{dx^2y^2}.$$

Consider now the map $\theta=\tau_{-\infty_{x,+}}\circ\chi$ where $\tau_{-\infty_{x,+}}$ denotes translation by $-\infty_{x,+}$. Since $\chi(O)=\infty_{x,+}$, we have $\theta(O)=O$ so θ is an isogeny. Moreover, we have $\chi^2=\mathrm{id}$ and $\tau_{-\infty_{x,+}}\circ\tau_{\infty_{x,+}}=\mathrm{id}$ so θ is a bijection with inverse $\chi\circ\tau_{\infty_{x,+}}$. Hence θ is an element of $\mathrm{Aut}(E)$. Now, we have $\chi(T)=\infty_{y,+}=\infty_{x,+}+T$ and so we get

$$\theta(T)=\tau_{-\infty_{x,+}}(\chi(T))=\tau_{-\infty_{x,+}}(\infty_{x,+}+T)=T.$$

Hence by Lemma 1.31, θ must be the identity. Hence $\chi=\tau_{\infty_{x,+}}$. □

Corollary 1.33. *The map $\tau_{\infty_{y,+}}\colon E\to E, P\mapsto P+\infty_{y,+}$ is given by*

$$(x,y)\mapsto\left(\frac{\alpha}{\delta y},-\frac{\alpha}{\delta x}\right).$$

The map $\tau_{\infty_{x,-}} : E \to E, P \mapsto P + \infty_{x,-}$ *is given by*

$$(x, y) \mapsto \left(-\frac{a}{\delta x}, -\frac{1}{\delta y}\right).$$

The map $\tau_{\infty_{y,-}} : E \to E, P \mapsto P + \infty_{y,+}$ *is given by*

$$(x, y) \mapsto \left(-\frac{\alpha}{\delta y}, \frac{\alpha}{\delta x}\right).$$

Proof. By Corollary 1.25, we have $\infty_{y,+} = \infty_{x,+} + T$. Hence we have $\tau_{\infty_{y,+}} = \tau_T \circ \tau_{\infty_{x,+}}$ and so, for a point $P = (x, y)$ on E, we get by Theorem 1.24 and Theorem 1.32 that

$$\tau_{\infty_{y,+}}(x, y) = \tau_T \left(\frac{a}{\delta x}, \frac{1}{\delta y}\right) = \left(\frac{\alpha}{\delta y}, -\frac{\alpha}{\delta x}\right).$$

Similarly, using the fact that $\infty_{x,-} = \infty_{x,+} + 2T$ and $\infty_{y,-} = \infty_{x,+} + 3T = \infty_{x,+} - T$, we find

$$\tau_{\infty_{x,-}}(x, y) = \left(-\frac{a}{\delta x}, -\frac{1}{\delta y}\right)$$

and

$$\tau_{\infty_{y,-}}(x, y) = \left(-\frac{\alpha}{\delta y}, \frac{\alpha}{\delta x}\right).$$

□

Corollary 1.34. *The map* $\sigma_{\infty_{x,+}}$ *sending a point* P *on* E *to* $\infty_{x,+} - P$ *is given by*

$$(x, y) \mapsto \left(-\frac{a}{\delta x}, \frac{1}{\delta y}\right).$$

Proof. The map $\sigma_{\infty_{x,+}}$ is given by the composition $\tau_{\infty_{x,+}} \circ \iota$ and so for a point $P = (x, y)$ on E we have by Theorem 1.24 and Theorem 1.32 that

$$\sigma_{\infty_{x,+}}(x, y) = \tau_{\infty_{x,+}}(-x, y) = \left(-\frac{a}{\delta x}, \frac{1}{\delta y}\right).$$

□

Corollary 1.35. *The map* $\sigma_{\infty_{x,-}} : E \to E, P \mapsto \infty_{x,-} - P$ *is given by*

$$(x, y) \mapsto \left(\frac{a}{\delta x}, -\frac{1}{\delta y}\right).$$

The map $\sigma_{\infty_{y,+}} : E \to E, P \mapsto \infty_{y,+} - P$ *is given by*

$$(x, y) \mapsto \left(\frac{\alpha}{\delta y}, \frac{\alpha}{\delta x}\right).$$

The map $\sigma_{\infty_{y,-}} : E \to E, P \mapsto \infty_{y,-} - P$ *is given by*

$$(x, y) \mapsto \left(-\frac{\alpha}{\delta y}, -\frac{\alpha}{\delta x}\right).$$

Proof. Combine Corollary 1.25 and Corollary 1.34. □

In particular, we now have a formula for the sum $P + Q$ when at least one of the points P and Q is a point which is not on E^0. We are now left to find a formula for the sum $P + Q$ when $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ are points on the curve such that $a + dx_0x_0y_0y_1 = 0$ or $a - dx_0x_1y_0y_1 = 0$.

Theorem 1.36. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be two points on E^0 such that their sum $P + Q$ is on E^0. Let $P + Q$ be given by (x_2, y_2). If $x_0x_1 + ay_0y_1 \neq 0$, then*

$$x_2 = \frac{a(x_0y_0 + x_1y_1)}{x_0x_1 + ay_0y_1}.$$

Proof. We introduce the following notation:

$$\begin{aligned} f_0 &= x_0^2 + ay_0^2 - a - dx_0^2y_0^2 \\ f_1 &= x_1^2 + ay_1^2 - a - dx_1^2y_1^2 \\ g &= x_0y_1 + x_1y_0 \\ j &= x_0y_0 + x_1y_1 \\ h &= a + dx_0x_1y_0y_1 \\ k &= x_0x_1 + ay_0y_1. \end{aligned}$$

Notice that we have

$$kg - jh = x_1y_1f_0 + x_0y_0f_1.$$

For $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ on E, we have $f_0 = 0$ and $f_1 = 0$, hence we get

$$kg - jh = 0.$$

In particular, when $h = a + dx_0x_1y_0y_1 \neq 0$ and $k = x_0x_1 + ay_0y_1 \neq 0$, this implies

$$\frac{ag}{h} = \frac{aj}{k}.$$

Notice that

$$\frac{ag}{h} = \frac{a(x_0y_1 + x_1y_0)}{a + dx_0x_1y_0y_1}$$

which is equal to the first coordinate of the sum $P + Q$ by Theorem 1.29 and so we have

$$x_2 = \frac{ag}{h} = \frac{aj}{k}.$$

Hence, for a fixed point $P = (x_0, y_0)$, we get that for almost all $Q = (x_1, y_1)$ with $k = x_0x_1 + ay_0y_1 \neq 0$, the coordinate x_2 is given by

$$\frac{a(x_0y_0 + x_1y_1)}{x_0x_1 + ay_0y_1}.$$

Since the translation by P is uniquely extensible to all Q, we have that for points P and Q on E for which the expression $\frac{aj}{k}$ is well defined, i.e., for which we have $k = x_0x_1 + ay_0y_1 \neq 0$, the coordinate x_2 is indeed given by

$$x_2 = \frac{a(x_0y_0 + x_1y_1)}{x_0x_1 + ay_0y_1}.$$

□

We now have a formula to compute the first coordinate of the sum of two points $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ when either $a + dx_0x_1y_0y_1 \neq 0$ or $x_0x_1 + ay_0y_1 \neq 0$. We also have the following.

Lemma 1.37. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points on E^0 such that $a + dx_0x_1y_0y_1 = 0$. Then $P + Q \in \{\infty_{x,+}, \infty_{x,-}\}$ or $P - Q \in \{\infty_{y,+}, \infty_{y,-}\}$.*

Proof. Let h be the function given by $h(x, y) = a + dx_0y_0xy$. It is clear that h has four poles given by $\infty_{x,+}, \infty_{x,-}, \infty_{y,+}$ and $\infty_{y,-}$. Since $\deg(\mathrm{div}(h)) = 0$, the function h must therefore have four zeroes, counted with multiplicities. We see that the points

$$\infty_{x,+} - P = \left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right)$$

and

$$\infty_{x,-} - P = \left(\frac{a}{\delta x_0}, -\frac{1}{\delta y_0}\right)$$

are zeroes of h since

$$a - dx_0y_0\frac{a}{\delta x_0}\frac{1}{\delta y_0} = a - a = 0.$$

Moreover the points

$$P - \infty_{y,+} = \left(-\frac{\alpha}{\delta y_0}, \frac{\alpha}{\delta x_0}\right)$$

and

$$P - \infty_{y,-} = \left(\frac{\alpha}{\delta y_0}, -\frac{\alpha}{\delta x_0}\right)$$

are also zeroes of h, for

$$a - dx_0y_0\frac{\alpha}{\delta y_0}\frac{\alpha}{\delta x_0} = a - a = 0.$$

If those four points are distinct, then they are the only four zeroes of h since h has four poles and so we have that $a + dx_0x_1y_0y_1 = 0$ if and only if $Q = \infty_{x,+} - P$ or $Q = \infty_{x,-} - P$ or $Q = P - \infty_{y,+}$ or $Q = P - \infty_{y,-}$, i.e., if $P + Q = \infty_{x,+}$, or $P + Q = \infty_{x,-}$ or $P - Q = \infty_{y,+}$ or $P - Q = \infty_{y,-}$.
The points $\infty_{x,+} - P$ and $\infty_{x,-} - P$ can not be equal since $\infty_{x,+} \neq \infty_{x,-}$, for $d \neq 1$. Similarly the points $P - \infty_{y,+}$ and $P - \infty_{y,-}$ can also never be equal. Suppose that $\infty_{x,+} - P = P - \infty_{y,+}$. Then we have $2P = T$. In other words, P is invariant under the map $P \mapsto T - P$ which is equal to the composite $\tau_T \circ \iota$ and thus given by $(x, y) \mapsto (\alpha y, \frac{x}{\alpha})$. Hence we get the equation

$$(x_0, y_0) = \left(\alpha y_0, \frac{x_0}{\alpha}\right)$$

and so we have in this case

$$x_0 = \alpha y_0.$$

Moreover we then also automatically have

$$\infty_{x,-} - P = \infty_{x,+} + 2T - P = (\infty_{x,+} + T) + (T - P) = \infty_{y,+} + P = P - \infty_{y,-}.$$

Hence the function has two zeroes given here by $\left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right)$ and $\left(-\frac{a}{\delta x_0}, -\frac{1}{\delta y_0}\right)$. We want to show that each of those points occur with multiplicity 2.
Take $Q = (x_1, y_1) = \infty_{x,+} - P = \left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right)$. Let $\mathfrak{m}$ be the maximal ideal in the local ring

corresponding to the point Q, i.e., $\mathfrak{m} = (x - x_1, y - y_1)$. We want to know the value of h modulo $\mathfrak{m}^2$. For (x, y) on E, we have the following equations:

$$x^2 + ay^2 = a + dx^2y^2,$$
$$x_1^2 + ay_1^2 = a + dx_1^2y_1^2.$$

Subtracting the second from the first now yields the equation

$$\begin{aligned} x^2 - x_1^2 + a(y^2 - y_1^2) &= d(x^2y^2 - x_1^2y_1^2) \\ &= d(y^2(x^2 - x_1^2) + x_1^2(y^2 - y_1^2)) \end{aligned}$$

which we can rewrite as

$$(x^2 - x_1^2)(1 - dy^2) = (dx_1^2 - a)(y^2 - y_1^2)$$

and so we have

$$x = x_1 + (dx_1^2 - a)(y^2 - y_1^2)\frac{1}{1 - dy^2}\frac{1}{x + x_1}.$$

Now, $\frac{1}{1-dy^2} \equiv \frac{1}{1-dy_1^2}$ modulo $\mathfrak{m}$ and $\frac{1}{x+x_1} \equiv \frac{1}{2x_1}$ modulo $\mathfrak{m}$. Since $y - y_1$ is in $\mathfrak{m}$, this means that modulo $\mathfrak{m}^2$, we get

$$\begin{aligned} x &\equiv x_1 + (dx_1^2 - a)(y + y_1)(y - y_1)\frac{1}{1 - dy_1^2}\frac{1}{2x_1} \\ &\equiv x_1 + (dx_1^2 - a)2y_1(y - y_1)\frac{1}{1 - dy_1^2}\frac{1}{2x_1}. \end{aligned}$$

Hence, the function h modulo $\mathfrak{m}^2$ is given by

$$\begin{aligned} h &= a + dx_0y_0xy \\ &= a + dx_0y_0x(y - y_1 + y_1) \\ &= a + dx_0y_0y_1x + dx_0y_0(y - y_1)x_1 \\ &\equiv a + dx_0y_0y_1\left(x_1 + (dx_1^2 - a)2y_1(y - y_1)\frac{1}{1 - dy_1^2}\frac{1}{2x_1}\right) + dx_0y_0(y - y_1)x_1 \\ &\equiv a + dx_0y_0y_1x_1 + (y - y_1)\left[dx_0y_0y_1(dx_1^2 - a)y_1\frac{1}{1 - dy_1^2}\frac{1}{x_1} + dx_0y_0x_1\right]. \end{aligned}$$

We now use that $(x_1, y_1) = \left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right)$. Modulo $\mathfrak{m}^2$, we get

$$\begin{aligned} h &\equiv a - a + (y - y_1)\left[dx_0y_0\frac{1}{\delta y_0}\left(\frac{a^2}{x_0^2} - a\right)\frac{1}{\delta y_0}\frac{y_0^2}{y_0^2 - 1}\frac{\delta x_0}{-a} + dx_0y_0\frac{-a}{\delta x_0}\right] \\ &\equiv (y - y_1)\left((x_0^2 - a)\frac{y_0}{y_0^2 - 1}\delta - a\delta y_0\right). \end{aligned}$$

Finally we use $x_0 = \alpha y_0$. This gives us the following expression for h modulo $\mathfrak{m}^2$.

$$h \equiv (y - y_1)\left(a(y_0^2 - 1)\frac{y_0}{y_0^2 - 1}\delta - a\delta y_0\right) = 0.$$

So, we have $h \equiv 0 \mod \mathfrak{m}^2$. This implies that h has a zero of order at least 2 at the point $Q = \infty_{x,+} - P$. Similarly, we have that the point $\infty_{x,-} - P$ has order at least 2. Because h has four poles, they must both have order exactly 2. Hence we have then that those zeroes are the only zeroes of h, and they are counted with multiplicity 2. The same holds when $\infty_{x,+} - P = P - \infty_{y,-}$. In that case, we have $2P = -T$ and we also automatically have that $\infty_{x,-} - P = P - \infty_{y,+}$ and the proof goes analogously. □

Lemma 1.38. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points on E^0 such that $x_0x_1 + ay_0y_1 = 0$. Then $P + Q \in \{\infty_{x,+}, \infty_{x,-}\}$ or $P - Q \in \{T, -T\}$.*

Proof. Let g be the function given by $x_0x + ay_0y$. It is clear that g has four poles given by $\infty_{x,+}$, $\infty_{x,-}$, $\infty_{y,+}$ and $\infty_{y,-}$. Since $\deg(\mathrm{div}(g)) = 0$, this means that the function g must also have 4 zeroes, counted with multiplicities. The points $\infty_{x,+} - P = \left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right)$ and $\infty_{x,-} - P = \left(\frac{a}{\delta x_0}, -\frac{1}{\delta y_0}\right)$ are zeroes of g since

$$-x_0\frac{a}{\delta x_0} + ay_0\frac{1}{\delta y_0} = -\frac{a}{\delta} + \frac{a}{\delta} = 0.$$

Moreover the points $P - T = (-\alpha y_0, \frac{x_0}{\alpha})$ and $P + T = (\alpha y_0, -\frac{x_0}{\alpha})$ are also zeroes of g, for

$$-x_0\alpha y_0 + ay_0\frac{x_0}{\alpha} = -\alpha x_0y_0 + \alpha x_0y_0 = 0.$$

We are left to show that those are the only zeroes of g. If those four points are distinct, it is surely the case since g has four poles and so we have that $x_0x_1 + ay_0y_1 = 0$ if and only if $Q = \infty_{x,+} - P$ or $Q = \infty_{x,-} - P$ or $Q = P - T$ or $Q = P + T$, i.e., if $P + Q = \infty_{x,+}$, or $P + Q = \infty_{x,-}$ or $P - Q = T$ or $P - Q = -T$.
The points $\infty_{x,+} - P$ and $\infty_{x,-} - P$ can not be equal since $\infty_{x,+} \neq \infty_{x,-}$ and the points $P - T$ and $P + T$ can also never be equal since $T = -T$, for $a \neq 0$. So, two of those four points can only be equal when $\infty_{x,+} - P = P - T$ or $\infty_{x,+} - P = P + T$, i.e., when $2P = \infty_{y,+}$ or $2P = \infty_{y,-}$ If $\infty_{x,+} - P = P - T$, then automatically we have also $\infty_{x,-} - P = P + T$ and if $\infty_{x,+} - P = P + T$, then we must also have $\infty_{x,-} - P = P - T$. Suppose that $2P = \infty_{y,+}$. Then P is invariant under the map $\sigma_{\infty_{y,+}} : P \mapsto \infty_{y,+} - P$. By Corollary 1.35, this means that we have

$$x_0y_0 = \frac{\alpha}{\delta}.$$

Set $Q = (x_1, y_1) = \infty_{x,+} - P = P - T$, and let $\mathfrak{m}$ be the maximal ideal of the local ring corresponding to this point, i.e., $\mathfrak{m} = (x - x_1, y - y_1)$. Again for (x, y) on E we have the equations

$$x^2 + y^2 = a + dx^2y^2$$

and

$$x_1^2 + y_1^2 = a + dx_1^2y_1^2.$$

and so modulo $\mathfrak{m}^2$, we get again

$$x \equiv x_1 + (dx_1^2 - a)y_1(y - y_1)\frac{1}{1 - dy_1^2}\frac{1}{x_1}.$$

And so the function g modulo $\mathfrak{m}^2$ is given by

$$\begin{aligned} x_0x + ay_0y &\equiv x_0\left(x_1 + (dx_1^2 - a)y_1(y - y_1)\frac{1}{1 - dy_1^2}\frac{1}{x_1}\right) + ay_0(y - y_1 + y_1) \\ &\equiv x_0x_1 + ay_0y_1 + (y - y_1)\left(x_0y_1(dx_1^2 - a)\frac{1}{1 - dy_1^2}\frac{1}{x_1} + ay_0\right). \end{aligned}$$

We use now $(x_1, y_1) = \left(\frac{-a}{\delta x_0}, \frac{1}{\delta y_0}\right)$. This yields

$$\begin{aligned} g &\equiv (y - y_1)\left(-\frac{x_0^2}{ay_0}a\frac{a - x_0^2}{x_0^2}\frac{y_0^2}{y_0^2 - 1} + ay_0\right) \\ &\equiv (y - y_1)\left(-\frac{(a - x_0^2y_0)}{y_0^2 - 1} + ay_0\right). \end{aligned}$$

Finally, we use the equation $x_0y_0 = \frac{\alpha}{\delta}$, we get

$$\begin{aligned} g &\equiv (y - y_1)\left(-a\frac{dy_0^2 - 1}{y_0^2 - 1}\frac{1}{dy_0} + ay_0\right) \\ &\equiv (y - y_1)\left(-a^2\frac{dy_0^2 - 1}{a(y_0^2 - 1)}\frac{1}{dy_0} + ay_0\right). \end{aligned}$$

Notice that since P is on E^0, we have $x_0^2 = \frac{a(y_0^2-1)}{dy_0^2-1}$. We therefore get

$$\begin{aligned} g &\equiv (y - y_1)\left(-a^2\frac{1}{x_0^2}\frac{1}{dy_0} + ay_0\right) \\ &\equiv (y - y_1)\left(-\frac{a^2}{dy_0}\frac{dy_0^2}{a} + ay_0\right) \\ &\equiv (y - y_1)(-ay_0 + ay_0) = 0. \end{aligned}$$

Hence the point $Q = \infty_{x,+} - P$ has order at least 2. Similarly, the point $\infty_{x,-} - P$ has order at least 2. Because the degree of the divisor of g is zero and g has four poles, those are then the only zeroes of g.
The proof goes analogously for when $\infty_{x,+} - P = P + T$ and $\infty_{x,-} - P = P - T$. □

We can also give another formula for the second coordinate of the sum of two points on the curve E^0.

Theorem 1.39. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be two points on E^0 such that their sum $P + Q$ is on E^0. Let $P + Q$ be given by (x_2, y_2). If $x_0y_1 - x_1y_0 \neq 0$, then*

$$y_2 = \frac{x_0y_0 - x_1y_1}{x_0y_1 - x_1y_0}.$$

Proof. Consider the map $E \to E$ given by $P \mapsto T - P$. It is equal to the composite $\tau_T \circ \iota$ and so by Theorem 1.24 is given on coordinates by $(x, y) \mapsto \left(\alpha y, \frac{x}{\alpha}\right)$. In particular, we have

$$\alpha y_2 = x(T - (P + Q)) = x((T - P) + (-Q))$$

where $x(T - (P + Q))$ denotes the first coordinate of the point $T - (P + Q)$. The coordinates of $T - P$ are given by $(x', y') = \left(\alpha y_0, \frac{x_0}{\alpha}\right)$ and those of $-Q$ by $(\tilde{x}, \tilde{y}) = (-x_1, y_1)$. Moreover, we have

$$x'\tilde{x} + ay'\tilde{y} = -\alpha y_0x_1 + a\frac{x_0}{\alpha}y_1 = \alpha(x_0y_1 - x_1y_0)$$

which is non-zero by assumption, and so by Theorem 1.36, the coordinate $x((T - P) + (-Q))$ is given by

$$\frac{a(x'y' + \tilde{x}\tilde{y})}{x'\tilde{x} + ay'\tilde{y}} = \frac{a(x_0y_0 - x_1y_1)}{\alpha(x_0y_1 - x_1y_0)} = \frac{\alpha(x_0y_0 - x_1y_1)}{x_0y_1 - x_1y_0}.$$

Hence we have indeed

$$y_2 = \frac{x_0y_0 - x_1y_1}{x_0y_1 - x_1y_0}.$$

□

Lemma 1.40. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points on E^0 such that $a - dx_0x_1y_0y_1 = 0$. Then $P + Q \in \{\infty_{y,+}, \infty_{y,-}\}$ or $P - Q \in \{\infty_{x,+}, \infty_{x,-}\}$.*

Proof. The proof is similar to the one of Lemma 1.37. Take this time $h = a - dx_0y_0xy$. Then the poles of h are given by $\infty_{x,+}$,$\infty_{x,-}$,$\infty_{y,+}$ and $\infty_{y,-}$ and the zeroes are given by the points

$$\begin{aligned}\left(\frac{\alpha}{\delta y_0}, \frac{\alpha}{\delta x_0}\right) &= \infty_{y,+} - P,\\ \left(-\frac{\alpha}{\delta y_0}, -\frac{\alpha}{\delta x_0}\right) &= \infty_{y,-} - P,\\ \left(-\frac{a}{\delta x_0}, \frac{1}{\delta y_0}\right) &= P - \infty_{x,+}\end{aligned}$$

and

$$\left(-\frac{a}{\delta x_0}, -\frac{1}{\delta y_0}\right) = P - \infty_{x,-}.$$

When two of those zeroes are equal, then either $2P = T$ or $2P = -T$ and one can show, analogously as in the proof of Lemma 1.37 that those zeroes then also have multiplicity 2. □

Lemma 1.41. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points on E^0 such that $x_0y_1 - x_1y_0 = 0$. Then $P + Q \in \{\infty_{y,+}, \infty_{y,-}\}$ or $P - Q \in \{O, 2T\}$.*

Proof. The proof is similar to the one of Lemma 1.38. Take this time $g = x_0y - y_0x$. Then the poles of g are given by $\infty_{x,+}$,$\infty_{x,-}$,$\infty_{y,+}$ and $\infty_{y,-}$ and the zeroes are given by the points

$$\begin{aligned}\left(\frac{\alpha}{\delta y_0}, \frac{\alpha}{\delta x_0}\right) &= \infty_{y,+} - P,\\ \left(-\frac{\alpha}{\delta y_0}, -\frac{\alpha}{\delta x_0}\right) &= \infty_{y,-} - P,\\ (x_0, y_0) &= P\end{aligned}$$

and

$$(-x_0, y_0) = P - 2T.$$

When two of those zeroes are equal, then either $2P = \infty_{y,+}$ or $2P = \infty_{y,-}$ and one can show, analogously as in the proof of lemma 1.38 that those zeroes also have with multiplicity 2. □

To summarize, we get the following formulae for the group law.

Theorem 1.42. *Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be two points on E^0. If $P + Q$ in on E^0, then we write (x_2, y_2) for the coordinate of the point $P + Q$. We then have the following.*

- *If $a + dx_0x_1y_0y_1 \neq 0$, then*
$$x_2 = \frac{a(x_0y_1 + x_1y_0)}{a + dx_0x_1y_0y_1}.$$
- *If $x_0x_1 + ay_0y_1 \neq 0$, then*
$$x_2 = \frac{a(x_0y_0 + x_1y_1)}{x_0x_1 + ay_0y_1}.$$
- *If $a - dx_0x_1y_0y_1 \neq 0$, then*
$$y_2 = \frac{ay_0y_1 - x_0x_1}{a - dx_0x_1y_0y_1}.$$
- *If $x_0y_1 - x_1y_0 \neq 0$, then*
$$y_2 = \frac{x_0y_0 - x_1y_1}{x_0y_1 - x_1y_0}.$$

Moreover if $a + dx_0x_1y_0y_1 = 0$ *and* $x_0x_1 + ay_0y_1 = 0$*, then* $dy_0^2y_1^2 = 1$ *and*

- $P + Q = \infty_{x,+}$ *if* $y_0y_1 = \frac{1}{\delta}$,
- $P + Q = \infty_{x,-}$ *if* $y_0y_1 = -\frac{1}{\delta}$,

and when $a - dx_0x_1y_0y_1 = 0$ *and* $x_0y_1 - x_1y_0 = 0$*, we have* $dx_0^2y_1^2 = a$ *and*

- $P + Q = \infty_{y,+}$ *if* $x_0y_1 = \frac{\alpha}{\delta}$,
- $P + Q = \infty_{y,-}$ *if* $x_0y_1 = -\frac{\alpha}{\delta}$.

Proof. This follows directly from Theorem 1.29, Corollary 1.34, Corollary 1.35, Theorem 1.36, Theorem 1.39, Lemma 1.37, Lemma 1.38, Lemma 1.40 and Lemma 1.41. □

Remark. Some of these results can also be found in [3].

Remark. Whenever d and ad are not squares then the points $\infty_{x,+}$, $\infty_{x,-}$, $\infty_{y,+}$ and $\infty_{y,-}$ are not rational and so the cases where we have $P + Q \in \{\infty_{x,+}, \infty_{x,-}, \infty_{y,+}, \infty_{y,-}\}$ or $P - Q \in \{\infty_{x,+}, \infty_{x,-}, \infty_{y,+}, \infty_{y,-}$ for $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ rational points on the curve can not occur. Therefore, we always have in this case that $a + dx_0x_1y_0y_1 \neq 0$ and $a - dx_0x_1y_0y_1 \neq 0$ and so Theorem 1.29 is sufficient and we have only one simple formula for the group law. This is the reason why Edwards curves are widely used in cryptography.

2 Identifying Edwards curves.

Let E be an elliptic curve over a perfect field k with $\mathrm{char}(k) \neq 2$. Let O be the neutral element of the group law of the curve. Assume that E admits a point $T \in E(\bar{k})$ of order 4 such that for $C = \langle T \rangle$ and for all $\sigma \in G = \mathrm{Gal}(\bar{k}/k)$, we have $\sigma(C) = C$. Because $C = \langle T \rangle = \{O, T, 2T, -T\}$ where $\mathrm{ord}(O) = 1$, $\mathrm{ord}(2T) = 2$ and $\mathrm{ord}(T) = \mathrm{ord}(-T) = 4$, this means that for all $\sigma \in G$ we have $\sigma(O) = O$, $\sigma(2T) = 2T$ and $\sigma(T) = \pm T$. Hence O and $2T$ are in $E(k)$ and T is either in $E(k)$ or in $E(l)$ where l is a quadratic extension of k.
We can then state the following theorem.

Theorem 2.1. *The elliptic curve* E *is isomorphic to a twisted Edwards curve.*

The goal of this section is to prove the above theorem.

Theorem 2.2. *There exist points* R *and* R' *such that the* 2*-torsion subgroup* $E(\bar{k})[2]$ *of* E *is given by*

$$E(\bar{k})[2] = \{0, 2T, R, R'\}.$$

Proof. We have that E is an elliptic curve over k where $\mathrm{char}(k) \neq 2$ so we know that the 2-torsion subgroup $E(\bar{k})[2]$ of E is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ so $\#(E(\bar{k})[2]) = 4$. Since $2T$ has order 2 and O has order 0, they are both necessarily contained in that subgroup. Hence, the 2-torsion group must be given by

$$E(\bar{k})[2] = \{O, 2T, R, R'\}$$

where R and R' are two distinct points of order 2 on the curve that are neither O nor $2T$. □

We can now state the following theorem.

Theorem 2.3. *The divisor* $(O) + (2T) - (R) - (R')$ *of* $E_{\bar{k}}$ *is a principal divisor of* E.

Proof. Let σ be an element in $G = \mathrm{Gal}(\bar{k}/k)$. We know already that $\sigma(O) = O$ and $\sigma(2T) = 2T$. Because R and R' are the points of order 2 of E that are neither O or $2T$, we thus have that σ either leaves R and R' invariant or σ exchanges them. In any of those cases, the divisor $(R)+(R')$ remains therefore invariant under G so we have that $(R) + (R')$ is defined over k. Now, the sum $R + R'$ in $E(\bar{k})$ must still have order 2 and therefore also be one of the points inside $E(\bar{k})[2]$. We see that the only possibility here is that $R + R' = 2T$ since every other configuration would imply either that $R = O$ or $R' = O$ or $R = R'$ which is impossible for they must all be distinct points. Hence $R + R' = 2T$ so by Lemma 1.23 the divisor given by $(2T) + (O) - (R) - (R')$ is indeed principal. □

Corollary 2.4. *There exists a function in $\kappa(E)$ whose divisor is equal to $(O)+(2T)-(R)-(R')$.*

Proof. This follows immediately from Theorem 2.3. □

Throughout this section, we let x be such a function. So, up to scalar multiplication, the function x is the unique function satisfying $\mathrm{div}(x) = (O) + (2T) - (R) - (R')$.

Now, from Theorem 2.2, we also get the coset

$$T + E(\bar{k})[2] = \{T, -T, R + T, R' + T\}.$$

We claim the following.

Theorem 2.5. *The divisor $(T) + (-T) - (R + T) - (R' + T)$ of $E_{\bar{k}}$ is a principal divisor of E.*

Proof. Let σ be an element of $G = \mathrm{Gal}(\bar{k}/k)$. Then we have that $\sigma(R + T) = \sigma(R) + \sigma(T)$ so $\sigma(R+T)$ is either $R+T$ or $R-T$ or $R'+T$ or $R'-T$. However, we also know that $R+R' = 2T$, so we get that $R' - T = 2T - R - T = R + T$ and $R - T = 2T - R' - T = R' + T$ since R and R' have order 2. Hence $\sigma(R + T)$ is either equal to $R + T$ or to $R' + T$ and by a similar argument, the same holds for $\sigma(R' + T)$. Now, if $\sigma(R + T) = R + T$, then $\sigma(R' + T) = R' + T$ and if $\sigma(R + T) = R' + T$, then $\sigma(R' + T) = R + T$, so in any case we get on the divisor that $\sigma((R+T)+(R'+T)) = (R+T)+(R'+T)$. Hence the divisor $(R+T)+(R'+T)$ is defined over k itself. Similarly as for $E(\bar{k})[2]$, we see here that on $E(\bar{k})$ we have that $T-T-(R+T)-(R'+T) = -R-T-R'-T = -4T = O$ so the divisor defined by $(T) + (-T) - (R+T) - (R'-T)$ is again principal by Lemma 1.23. □

Corollary 2.6. *There exists a function in $\kappa(E)$ whose divisor is equal to $(T) + (-T) - (R + T) - (R' + T)$.*

Proof. This follows immediately from Theorem 2.5. □

Throughout this section, we let y be such a function. Hence y is, up to scalar multiplication, the unique function satisfying the condition $\mathrm{div}(y) = (T) + (-T) - (R + T) - (R' + T)$.

The aim of this section is to find a relationship between x and y which would yield the equation of an Edwards curve. We will do so by using the Riemann-Roch theorem, which we stated in the previous section.
First, it gives us the following result, where we denote respectively by D_x and D_y the divisors $(R) + (R')$ and $(R + T) + (R' + T)$ corresponding to the poles of x and y.

Theorem 2.7. *The Riemann-Roch spaces $L(D_x)$ and $L(D_y)$ are respectively equal to $\langle 1, x\rangle$ and $\langle 1, y\rangle$.*

Proof. Since E is an elliptic curve we get directly by Lemma 1.17, that both $L(D_x)$ and $L(D_y)$ must have dimension 2. Moreover, we know that both 1 and x are inside $L(D_x)$ and that those two functions must be linearly independent since $\mathrm{div}(x) \neq 0$. Similarly, we have that the

functions 1 and y are linearly independent and both contained in $L(D_y)$. Hence $L(D_x) = \langle 1, x\rangle$ and $L(D_y) = \langle 1, y\rangle$. □

Theorem 2.8. *The Riemann-Roch spaces $L(D_x + D_y)$ is equal to $\langle 1, x, y, xy\rangle$.*

Note that this theorem is consistent with Corollary 1.20 in section 1, and again its proof will follow from the following result.

Lemma 2.9. *The functions 1, x, y and xy are linearly independent.*

Proof of the lemma. Let a, b, c, d be constants such that $axy + bx + cy + d = 0$.
Assume that $a \neq 0$. By scaling the equation if necessary, we can assume without loss of generality that $a = 1$. This yields the following equation:

$$xy + bx + cy + d = 0 \Rightarrow (x + c)(y + b) = bc - d$$

meaning that the expression $(x + c)(y + b)$ must be equal to a constant $e = bc - d$.
If $e = 0$ then either $x + c = 0$ or $y + b = 0$, which would mean that either 1 and x, or 1 and y are linearly dependent. This is not the case, so necessarily $e \neq 0$. Hence $x + c = \frac{e}{y+b}$ with $e \neq 0$.
In terms of divisors, this implies that we have the following equation:

$$\operatorname{div}(x + c) = -\operatorname{div}(y + b)$$

However we know that $\operatorname{div}(x + c) = (S) + (S') - (R) - (R')$ where S and S' are points such that $x(S) = -c = x(S')$. Besides, since $\operatorname{div}(x + c) = (S) + (S') - (R) - (R')$, we must have on the curve that $S + S' = R + R' = 2T$.
Now, we also know that $\operatorname{div}(y + b) = (Q) + (Q') - (R + T) - (R' + T)$ where Q and Q' are points such that $y(Q) = -b = y(Q')$, so with the previous equation $\operatorname{div}(x + c) = -\operatorname{div}(y + b)$, this implies that $\{S, S'\} = \{R + T, R' + T\}$. However since $S + S' = 2T$ and $R + T + R' + T = O$, this would mean that $2T = O$, which is impossible, since T has order 4.
Hence $a = 0$ and we now have the equation $bx + cy + d = 0$.
Assume now that $b \neq 0$. With the same argument we can take $b = 1$ and get:

$$x + cy + d = 0 \Rightarrow x = -cy - d$$

This gives us:

$$\operatorname{div}(x) = \operatorname{div}(cy + d)$$

which is again impossible because x and $cy + d$ do not have the same poles.
Therefore $b = 0$ and we are left with the equation $cy + d = 0$. Now, since 1 and y are linearly independent, this immediately implies that $c = 0$ and $d = 0$.
Hence $a = b = c = d = 0$ and the functions 1, x, y and xy are linearly independent. □

Proof of Theorem 2.8. By Lemma 1.17, the space $L(D_x + D_y)$ has dimension 4. Moreover we know that the functions 1, x, y and xy are all contained in $L(D_x + D_y)$ since $\operatorname{div}(xy) = \operatorname{div}(x) + \operatorname{div}(y) = (O) + (2T) + (T) + (-T) - D_x - D_y$. So the space $\langle 1, x, y, xy\rangle$ is contained in the Riemann-Roch space $L(D_x + D_y)$ of dimension 4. Now, by Lemma 2.9, we know that the space $\langle 1, x, y, xy\rangle$ also has dimension 4, since the functions 1, x, y, xy are linearly independent. Hence the spaces $L(D_x + D_y)$ and $\langle 1, x, y, xy\rangle$ must be equal. □

Consider now the following theorem which states that on a smooth projective curve, a divisor of large enough degree is very ample.

Theorem 2.10. *Let C be a smooth projective curve of genus g. Let D be a divisor on C such that $\deg(D) \geq 2g + 1$ and let $(s_0, \dots s_n)$ be a basis for $L(D)$. Then the map $\varphi\colon C \to \mathbb{P}^n$ given by $P \mapsto (s_0(P) : \cdots : s_n(P))$ is an embedding.*

Proof. See for instance [2, Chapter IV, Corollary 3.2]. □

This theorem can be used to get the following result.

Theorem 2.11. *The map*

$$\phi\colon E \to \mathbb{P}^1 \times \mathbb{P}^1$$

$$P \mapsto ((x(P) : 1), (y(P) : 1))$$

is an embedding.

Proof. Since $\deg(D) = 4 \geq 2 \cdot 1 + 1$ by lemma 1.17, we can apply Theorem 2.10 to the divisor $D = D_x + D_y$. This yields us an embedding $\varphi\colon E \to \mathbb{P}^3$ given by

$$P \mapsto (1 : x(P) : y(P) : (xy)(P))$$

since $L(D) = \langle 1, x, y, xy\rangle$ by Theorem 2.8. In particular, we have an isomorphism $E \to \mathrm{im}(\varphi)$. It is also quite clear that if a point $P = (z_0 : z_1 : z_2 : z_3)$ in $\mathbb{P}^3$ is contained in $\mathrm{im}(\varphi)$, then P satisfies the equation $z_0z_3 = z_1z_2$ since P is then of the form $(1 : x : y : xy)$ for some x and y. Hence $\mathrm{im}(\varphi) \subseteq Q$ where Q is the quadric in $\mathbb{P}^3(z_0 : z_1 : z_2 : z_3)$ defined by the equation $z_0z_3 = z_1z_2$. Now, we also have an isomorphism between Q and $\mathbb{P}^1 \times \mathbb{P}^1$ which is induced by the Segre embedding defined by

$$\psi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$$

$$((x_0 : x_1), (y_0 : y_1)) \mapsto (x_1y_1 : x_0y_1 : x_1y_0 : x_0y_0)$$

whose inverse $\chi : Q \to \mathbb{P}^1 \times \mathbb{P}^1$ is given by

$$(z_0 : z_1 : z_2, z_3) \mapsto ((z_1 : z_0), (z_2 : z_0)).$$

Now the composition $\chi \circ \varphi$ eventually yields an embedding

$$\phi : E \to \mathbb{P}^1 \times \mathbb{P}^1$$

$$P \mapsto ((x(P) : 1), (y(P) : 1))$$

which completes the proof. □

We can use this embedding to prove interesting results about some maps on the function field $\kappa(E)$. Consider for example the involutions defined by

$$\sigma\colon E \to E,\ P \mapsto -P$$

and

$$\tau\colon E \to E,\ P \mapsto 2T - P.$$

Those maps induce maps $\sigma^*\colon \kappa(E) \to \kappa(E)$ given by $f \mapsto f \circ \sigma$ and $\tau^*\colon \kappa(E) \to \kappa(E)$ given by $f \mapsto f \circ \tau$ on the function field, as well as maps

$$\sigma^*\colon \mathrm{Div}(E) \to \mathrm{Div}(E),\ (P) \mapsto \sum_{Q \in \sigma^{-1}(P)} e_\sigma(Q) \cdot (Q)$$

$$\tau^*\colon \mathrm{Div}(E) \to \mathrm{Div}(E),\ (P) \mapsto \sum_{Q \in \tau^{-1}(P)} e_\tau(Q) \cdot (Q)$$

on the divisors groups. Here e_σ and e_τ denote the ramification index of σ and τ, respectively. Now since σ and τ are automorphisms on E we know that their ramification indexes are simply equal to 1. Hence for every divisor D of the form $\sum n_p(P)$, we get

$$\sigma^*(D) = \sigma^*\left(\sum n_P(P)\right) = \sum n_p(\sigma^{-1}(P)) = \sum n_P(-P)$$

and

$$\tau^*(D) = \tau^*\left(\sum n_P(P)\right) = \sum n_p(\tau^{-1}(P)) = \sum n_P(2T - P).$$

Corollary 2.12. *Let $\sigma^*\colon \kappa(E) \to \kappa(E)$ and $\tau^*\colon \kappa(E) \to \kappa(E)$ be the maps defined above. Then*

$$\sigma^*(x) = -x,\ \sigma^*(y) = y$$

and

$$\tau^*(x) = x,\ \tau(y) = -y.$$

Proof. We will start by looking at the map σ^*. To know how σ^* acts on y, let S be a point on E which is neither $R+T$ nor $R'+T$, set $y_0 = y(S)$ and consider the function $y - y_0$. We know that

$$\operatorname{div}(y - y_0) = (S) + (S') - (R+T) - (R'+T)$$

where S and S' are the (not necessarily distinct) points on the curve such that $y(S) = y(S') = y_0$. On the curve, this means that $S+S' = R+R'+2T = 4T = O$. Hence we see that $S' = -S = \sigma(S)$ and therefore $y(S) = y(\sigma(S)) = y_0$. Since this holds for almost all S, we conclude that $\sigma^*(y) = y$. Now, to know how it acts on x we can start by computing the divisor of $\sigma^*(x)$. We get

$$\operatorname{div}(\sigma^*(x)) = \sigma^*(\operatorname{div}(x)) = \sigma^*((O) + (2T) - (R) - (R')) = (-O) + (-2T) - (-R) - (-R')$$

$$= (O) + (2T) - (R) - (R') = \operatorname{div}(x).$$

This means in particular that

$$\operatorname{div}\left(\frac{\sigma^*(x)}{x}\right) = 0.$$

Therefore, there exists a constant λ such that $\sigma^*(x) = \lambda x$. Moreover, since $(\sigma^*)^2 = \mathrm{id}$, we know that this constant λ must be either 1 or -1.
We will now use the embedding $\phi\colon E \to \mathbb{P}^1 \times \mathbb{P}^1$ that we defined in Theorem 2.11. Because it is an embedding, we know in particular that $\phi(P) = ((x(P) : 1, (y(P) : 1))$ can not be equal to $\phi(-P) = ((x(-P) : 1), (y(-P) : 1))$ whenever $\operatorname{ord}(P) > 2$, as is for instance the case for $P = T$. But since we have seen that $y(-P) = y(P)$ this implies that we must have $x(P) \neq x(-P)$ on those points. Hence, $\sigma^*(x) \neq x$, so the only possibility is $\sigma^*(x) = -x$.
For τ^*, we can use a similar reasoning. To know how τ^* acts on x, let Q be a point on E which is neither R nor R', set $x_0 = x(Q)$ and consider the function $x - x_0$. We know that

$$\operatorname{div}(x - x_0) = (Q) + (Q') - (R) - (R')$$

where Q and Q' are the (not necessarily distinct) points on the curve with $x(Q) = x(Q') = x_0$. On the curve, this means that $Q + Q' = R + R' = 2T$ so $Q' = \tau(Q)$. Therefore $x(Q) = x(\tau(Q))$ for almost all Q, so $\tau^*(x) = x$.
In order to see what $\tau^*(y)$ is, we can start by computing the divisor of $\tau^*(y)$. We get

$$\operatorname{div}(\tau^*(y)) = \tau^*(\operatorname{div}(y)) = \tau^*((T) + (-T) - (R+T) - (R'+T))$$

$= (2T-T)+(2T+T)-(2T-R-T)-(2T-R'-T) = (T)+(-T)-(R+T)-(R'+T) = \mathrm{div}(y)$,

since R and R' have order 2 and T has order 4. So again, in particular we have that

$$\mathrm{div}\left(\frac{\tau^*(y)}{y}\right) = 0$$

meaning that there exists a constant μ such that $\tau^*(y) = \mu y$ which must be either 1 or -1, since $(\tau^*)^2 = \mathrm{id}$. Using the embedding ψ, we see this time that $\psi(P) = ((x(P):1),(y(P):1))$ can not be equal to $\psi(2T-P) = ((x(2T-P):1),(y(2T-P):1))$ whenever $P \notin \{T, -T, R+T, R'+T\}$. Now, since $x(P) = x(2T-P)$, this means that $y(P) \neq y(2T-P)$ for such point. Therefore $\mu = -1$ and $\tau^*(y) = -y$. □

Now that we know how σ^* and τ^* act on x and y, we can see how they act on some Riemann-Roch spaces and use that to show that E is isomorphic to a twisted Edwards curve. To do so, we will use the following theorem from linear algebra.

Theorem 2.13. *Let V be a finite-dimensional vector space and let $f_1, \ldots, f_k : V \to V$ be diagonalizable endomorphisms that commute in pairs. Then $f_1, \ldots, f_k : V \to V$ are simultaneously diagonalizable, i.e., there exists a basis for V consisting of vectors that are eigenvectors for all the f_i at the same time.*

Proof. See [7, Theorem 5.14]. □

Theorem 2.14. *There exists a linear relation between 1, x^2, y^2 and x^2y^2.*

Proof. Since $\langle 1, x\rangle$ and $\langle 1, y\rangle$ are bases of the spaces $L(D_x)$ and $L(D_y)$ respectively, and since we have $\sigma^*(x) = -x$ and $\sigma^*(y) = y$ as well as $\tau^*(x) = x$ and $\tau^*(y) = -y$, the spaces $L(D_x)$ and $L(D_y)$ are invariant under both σ^* and τ^*. The restriction of σ^* to $L(D_y)$ is the identity on $L(D_y)$, while its restriction to $L(D_x)$ has eigenvalues 1 and -1. By switching $L(D_x)$ and $L(D_y)$, we get the analogous statement for τ^*. Moreover, for P on E, we notice

$$\sigma(\tau(P)) = \sigma(2T - P) = -2T + P = 2T + P$$

and

$$\tau(\sigma(P)) = \tau(-P) = 2T + P$$

so τ and σ commute, which implies that σ^* and τ^* commute as well.
We can therefore use Theorem 2.13 on σ^* and τ^* restricted to various subspaces of $\kappa(E)$ and list for each element $x^t y^r$ with $t, r \in \{0, 1, 2\}$ in the Riemann-Roch spaces $L(D_x)$, $L(D_y)$, $L(D_x+D_y)$ and $L(2D_x + 2D_y)$ in which intersection of eigenspaces of σ^* and τ^* they lie in. This yields the following table.

$L(D)$ \ eigenvalue of σ^* and τ^*	$+1,+1$	$-1,+1$	$+1,-1$	$-1,-1$
$L(D_x)$	1	x	0	0
$L(D_y)$	1	0	y	0
$L(D_x + D_y)$	1	x	y	xy
$L(2D_x + 2D_y)$	$1, x^2, y^2, x^2y^2$	x, xy^2	y, x^2y	xy

Using this table, we see in the last column that the subspace corresponding to the intersection of the eigenspaces $E_{-1}(\sigma^*)$ and $E_{-1}(\tau^*)$ with σ^* and τ^* acting on $L(2D_x + 2D_y)$ has dimension at least 1. Moreover, since 1 and x^2 are linearly independent, the elements y and yx^2 in the third column are also linearly independent. Hence the subspace in the third column corresponding to

the intersection of the eigenspaces $E_1(\sigma^*)$ and $E_{-1}(\tau^*)$ with σ^* and τ^* acting on $L(2D_x + 2D_y)$ must have dimension at least 2. Using the fact that 1 and y^2 are also linearly independent we can prove similarly that the subspace in the second column corresponding to the intersection of the eigenspaces $E_{-1}(\sigma^*)$ and $E_1(\tau^*)$ with σ^* and τ^* acting on $L(2D_x + 2D_y)$ must also have dimension at least 2. Now, by Lemma 1.17, we have

$$\dim(L(2D_x + 2D_y)) = \deg(2D_x + 2D_y) = 8$$

so the subspace in the first column corresponding to the intersection of the eigenspaces $E_1(\sigma^*)$ and $E_1(\tau^*)$ with σ^* and τ^* acting on $L(2D_x+2D_y)$ cannot have dimension bigger than $8-2-2-1 = 3$. But we see in the table that it contains at least 4 elements so there must exist a linear relation between those elements. □

The linear relation that we get in Theorem 2.14 will now give us the equation of an Edwards curve for E.

Corollary 2.15. *Assume that the point T on E is rational. Then $x(T) \neq 0$ and $y(O) \neq 0$ and the functions $x' = \lambda x$ with $\lambda = x(T)^{-1}$ and $y' = \mu y$ with $\mu = y(O)^{-1}$ induce an isomorphism $P \mapsto ((x'(P) : 1), (y'(P) : 1))$ from E to an Edwards curve sending the point $T \in E(k)$ to $(1, 0)$ and the point $O \in E(k)$ to $(0, 1)$.*

Proof. Since $\operatorname{div}(x) = (O) + (2T) - (R) - (R')$, we know that $x(T) \neq 0$ and since T is rational, we have that $\lambda = x(T)^{-1}$ is a constant in k. So we can define the function $x' = \lambda x$ in $\kappa(E)$ which is a function satisfying $x'(T) = 1$. For the same reason, we can set $\mu = y(O)^{-1}$ and define the function $y' = \mu y$ with the property $y'(O) = 1$. We now also know by Theorem 2.14 that there is a linear relation between 1, x'^2, y'^2 and $x'^2y'^2$, so there are constants $\alpha, \beta, \gamma, \delta \in k$ such that

$$\alpha + \beta x'^2 + \gamma y'^2 + \delta x'^2 y'^2 = 0.$$

On the points T and O, we thus get the following equations

$$\begin{cases} \alpha + \beta = 0 \\ \alpha + \gamma = 0. \end{cases}$$

This means in particular that none of those constants can be zero because otherwise all of $\alpha, \beta, \gamma, \delta$ would be zero and the functions would be linearly independent, which is impossible because of Theorem 2.14. We can therefore scale all of those constants and for instance set $\alpha = 1$, which yields $\gamma = \beta = -1$. So the equation becomes

$$1 - x'^2 - y'^2 + \delta x'^2 y'^2 = 0$$

which yields

$$x'^2 + y'^2 = 1 + \delta x'^2 y'^2$$

which is exactly the equation of an Edwards curve as seen in section 1. □

Corollary 2.16. *We have $y(O) \neq 0$ and the function $y' = \mu y$ with $\mu = y(O)^{-1}$ induces an isomorphism $P \mapsto ((x(P) : 1), (y'(P) : 1))$ from E to a twisted Edwards curve.*

Proof. The proof is very similar to the previous one, however this time for T non-rational, we can not take a λ such that $x'(T) = 1$ for $x' = \lambda x$. But since O is always rational, we can still set $\mu = y(O)^{-1}$ and define the function $y' = \mu y$ with the property $y'(O) = 1$. Now again by Theorem 2.14 there exist constants $\alpha, \beta, \gamma, \delta \in k$ such that

$$\alpha + \beta x^2 + \gamma y'^2 + \delta x^2 y'^2 = 0$$

so, on O we still get the equation

$$\alpha + \gamma = 0.$$

Now, of the terms 1, x^2, y'^2 and $x^2y'^2$, only x^2 and $x^2y'^2$ have poles at the points R and R'. So, in a linear relation, either both those terms occur, or neither. If neither occur, then 1 and y^2 would be linearly dependent, which is not possible. So both x^2 and x^2y^2 occur in the linear relation, meaning that both β and δ are nonzero. After scaling, we may assume $\beta = 1$ and so we have

$$\alpha + x^2 - \alpha y'^2 + \delta x^2 y'^2 = 0$$

which yields

$$x^2 - \alpha y'^2 = -\alpha - \delta x^2 y'^2.$$

Setting $a = -\alpha$ and $d = -\delta$, we therefore get

$$x^2 + a y'^2 = a + d x^2 y'^2$$

which is indeed the equation of a twisted Edwards curve. □

3 A 2-descent on Edwards curves.

In this section we will apply descent by 2-isogeny on Edwards curves. We will start by recalling the method of descent by 2-isogeny for general elliptic curves C defined over $\mathbb{Q}$ in short Weierstraß form. Let C be such an elliptic curve with a 2-torsion point. Possibly after a suitable change of variables, we can assume its 2-torsion point to be the point $(0, 0)$ and its equation to be of the form

$$v^2 = u(u^2 + cu + e)$$

with $c, e \in \mathbb{Z}$ and we have $e \neq 0$ and $c^2 - 4e \neq 0$ for C is non-singular.

Theorem 3.1. *There is a second elliptic curve C' over $\mathbb{Q}$ and an isogeny $\phi\colon C \to C'$ having kernel $\{O_C, (0, 0)\}$. Specifically, C' can be given by*

$$v'^2 = u'(u'^2 + c'u' + e')$$

with $c' = -2c$ and $e' = c^2 - 4e$; and ϕ can be given by

$$\phi(u, v) = \begin{cases} (u + c + e/u, v - ev/u^2) & \text{if } u \neq 0, \\ O_{C'} & \text{if } (u, v) = (0, 0). \end{cases}$$

Proof. See [6, Chapter III, Example 4.5]. □

Theorem 3.2. *Under the conditions of Theorem 3.1, there is a second isogeny $\hat{\phi}\colon C' \to C$ defined by*

$$\hat{\phi}(u', v') = \begin{cases} \left(\frac{1}{4}\left(u' + c' + e'/u'\right), \frac{1}{8}\left(v' - e'v'/(u')^2\right)\right) & \text{if } u' \neq 0, \\ O_C & \text{if } (u', v') = (0, 0) \end{cases}$$

such that $\phi \circ \hat{\phi} = [2]_{C'}$ and $\hat{\phi} \circ \phi = [2]_C$ where $[2]_{C'}$ and $[2]_C$ denote multiplication by 2 on C' and C, respectively.

Proof. See [6, Chapter III, Example 4.5]. □

We seek to understand the image of $C(\mathbb{Q})$ inside $C'(\mathbb{Q})$ where C' is the curve defined in the previous theorem. For this, we introduce a map from $C'(\mathbb{Q})$ to the quotient group $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ as follows.

Lemma 3.3. *Let $q\colon C'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ be the function defined by*

$$\begin{aligned} q((u',v')) &= [u'] \text{ if } u' \neq 0, \\ q((0,0)) &= [e'], \\ q(O) &= [1]. \end{aligned}$$

Then q is a group homomorphism and the sequence

$$C(\mathbb{Q}) \xrightarrow{\phi} C'(\mathbb{Q}) \xrightarrow{q} \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is exact.

Proof. See [1, Lemma 6]. □

In particular, the previous lemma implies that $\operatorname{coker}(\phi) = C'(\mathbb{Q})/\phi(C(\mathbb{Q}))$ is equal to $\operatorname{im}(q)$. We are therefore interested in finding the elements of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ that lie in the image of q. To do so, we have the following useful proposition.

Proposition 3.4. *Let $C'\colon v'^2 = u'(u'^2 + c'u' + e')$ with c' and e' in $\mathbb{Z}$ be an elliptic curve over $\mathbb{Q}$ and q the corresponding homomorphism from Lemma 3.3. Let b be a square-free integer. Then the class $[b]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ lies in the image of q if and only if the equation*

$$b^2l^4 + c'bl^2m^2 + e'm^4 = bn^2$$

admits a non-zero solution (l,m,n) with $l,m,n \in \mathbb{Z}$. Furthermore, this can only happen if b divides e'.

Proof. First of all, since $q(O) = [1]$ and $q((0,0)) = [e']$, the class $[b]$ lies in the image of q whenever $b = 1$ or $b = e'$ and we see that in those cases, the equation

$$b^2l^4 + c'bl^2m^2 + e'm^4 = bn^2$$

admits $(1,0,1)$ or $(0,1,1)$ respectively as a solution. Suppose now that b is a square-free integer such that $[b] \neq 1$ and $[b] \neq e'$ and that there exists a (u',v') on C' such that $q((u',v')) = [b]$. Since $[b] \neq e'$, we have $u' \neq 0$ and $[u'] = [b]$. Because the equation of C' is given by $v'^2 = u'(u'^2 + c'u' + e')$, we have in particular that $u'(u'^2 + c'u' + k')$ is a square, so we also have $[u'^2 + c'u' + e'] = [u'] = [b]$. In other words, there exist s,t in $\mathbb{Q}$ such that $u' = bt^2$ and $u'^2 + c'u' + e' = bs^2$. Together with the first equation, we get

$$(bt^2)^2 + c'bt^2 + e' = bs^2$$

Now, t in in $\mathbb{Q}$, so we can write t as $t = \frac{l}{m}$ with l,m coprime integers. This yields the equation

$$b^2l^4 + c'bl^2m^2 + e'm^4 = bs^2m^4$$

Write now $n = sm^2$. Then the previous equation becomes $b^2l^4 + c'bl^2m^4 + e'm^4 = bn^2$. Moreover $n = sm^2$ must be an integer: indeed, the left-hand side of the equation is clearly an integer so the right-hand side of the equation must be one as well. But the right-hand side is equal to bn^2 with b being square-free, so this can only happen if n is itself also an integer. Hence, if b is in the image of q, the equation

$$b^2l^4 + c'bl^2m^2 + e'm^4 = bn^2 \tag{1}$$

must have a solution with $l, m, n \in \mathbb{Z}$ and l, m coprime. Conversely if the equation (1) has a non-zero solution (l, m, n) with $l, m, n \in \mathbb{Z}$, then setting $u' = b(\frac{l}{m})^2$ gives us a point (u', v') on C' such that $q((u', v')) = [b]$. We are left to prove that the class $[b]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ can only lie in the image of q if b divides e'. Suppose that we have a solution (l, m, n) in $\mathbb{Z}^3$ such that there is a prime p dividing b but not e'. Then from the equation (1) we see that p must divide $e'm^4$ and so it must divide m. Hence every term in the left-hand side of the equation (1) is divisible by p^2, and so bn^2 is divisible by p^2. This implies that p divides n, for b is square-free. In particular, we see now that the terms $c'bl^2m^4$, $e'm^4$ and bn^2 are all divisible by p^3, so b^2l^4 must also be divisible by p^3. Using again the fact that b is square-free, we thus have that p divides l. But l and m are coprime so this leads to a contradiction. Hence b must divide e'. □

While this proposition gives necessary and sufficient conditions for a class $[b]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ to lie in the image of the map q defined in Lemma 3.3, we will show that for Edwards curves, there exist some necessary conditions that are easier to verify, thus often making it quicker to narrow down the image of q and hence the cokernel of ϕ. To show this we will want to apply some the theorems and isogenies mentioned above, so we first introduce the following isomorphism between a general twisted Edwards curve and a Weierstraß curve.

Theorem 3.5. *Let $E\colon x^2 + ay^2 = a + dx^2y^2$ be a twisted Edwards curve and let E^W then be the Weierstraß curve given by the equation $\eta^2 = \xi(\xi^2 + 2a(d+1)\xi + a^2(d-1)^2)$. Then we have an isomorphism $\chi\colon E \to E^W$ sending the 2-torsion point $2T$ of E to the 2-torsion point $(0,0)$ of E^W given by*

$$(x, y) \mapsto \left(a(d-1)\frac{y+1}{y-1}, 2a^2(d-1)\frac{y+1}{x(y-1)}\right).$$

Proof. We are looking for an equation of the form

$$E^W : \eta^2 = \xi(\xi^2 + p\xi + q)$$

with p and q constants and we know that on a Edwards curve E, the point $2T = (0, -1)$ is a rational 2-torsion point of E. Hence, we want the function ξ in the equation of E^W to satisfy the condition

$$\operatorname{div}(\xi) = 2(2T) - 2(O).$$

Consider the function $\frac{y+1}{y-1}$. Since $\operatorname{div}(y+1) = 2(2T) - (R+T) - (R-T)$ and $\operatorname{div}(y-1) = 2(O) - (R+T) - (R-T)$ by section 1, we get that

$$\operatorname{div}\left(\frac{y+1}{y-1}\right) = 2(2T) - 2(O)$$

as desired. We therefore set $\xi = c\frac{y+1}{y-1}$ where c is a constant to be determined.
We have that $E[2] = \{O, 2T, R, R'\}$ so we need η to be a function such that:

$$\operatorname{div}(\eta) = (2T) + (R) + (R') - 3(O)$$

Firstly, note that with this we get:

$$\operatorname{div}\left(\frac{\eta}{\xi}\right) = (R) + (R') - (O) - (2T) = \operatorname{div}\left(\frac{1}{x}\right)$$

Hence, we have $\eta = c'\frac{\xi}{x} = \bar{c}\frac{y+1}{(y-1)x}$ with c' and $\bar{c} = c' \cdot c$ constants.
Assume for now that these constant are all equal 1. Then we get

$$x = \frac{\xi}{\eta}, \quad y = \frac{\xi + 1}{\xi - 1},$$

and so the equation of the curve

$$x^2 + ay^2 = a + dx^2y^2$$

yields

$$\frac{\xi^2}{\eta^2} + a\left(\frac{\xi+1}{\xi-1}\right)^2 = a + d\left(\frac{\xi^2(\xi+1)^2}{\eta^2(\xi-1)^2}\right)$$

which in turn gives us the equation

$$\xi^2(\xi-1)^2 + a(\xi+1)^2\eta^2 = a\eta^2(\xi-1)^2 + d\xi^2(\xi+1)^2$$

which implies

$$4a\xi\eta^2 = \xi^2\left[(d-1)\xi^2 + 2(d+1)\xi + d - 1\right].$$

Now, multiplying both sides of the equation by $\frac{a^3(d-1)^2}{\xi}$ yields

$$(2a^2(d-1)\eta)^2 = a^3(d-1)^2\xi\left[(d-1)\xi^2 + 2(d+1)\xi + d - 1\right]$$

and this gives us the equation

$$(2a^2(d-1)\eta)^2 = a(d-1)\xi\left[(a(d-1)\xi)^2 + 2a(d+1)(a(d-1)\xi) + a^2(d-1)^2\right].$$

Setting $c = a(d-1)$ and $c' = 2a^2(d-1)$, i.e. setting $\eta = 2a^2(d-1)\frac{y+1}{x(y-1)}$ and $\xi = a(d-1)\frac{y+1}{y-1}$ we get

$$\eta^2 = \xi(\xi^2 + 2a(d+1)\xi + a^2(d-1)^2)$$

which is the desired Weierstraß form with constants $p = 2a(d+1)$ and $q = a^2(d-1)^2$. □

For the rest of this section we fix a twisted Edwards curve $E : x^2 + ay^2 = a + dx^2y^2$ and we denote by $E^W : \eta^2 = \xi(\xi^2 + 2a(d+1)\xi + a^2(d-1)^2)$ the isomorphic Weierstraß curve from Theorem 3.5. We see that the map $\chi\colon E \to E^W$ given by $(x, y) \mapsto (a(d-1)\frac{y+1}{y-1}, 2a^2(d-1)\frac{y+1}{x(y-1)})$ from Theorem 3.5 is an isogeny as it sends the neutral element O_E of E to the point at infinity. By Lemma 3.3 we have a homomorphism $\varphi\colon E^W(\mathbb{Q}) \to \mathbb{Q}/(\mathbb{Q}^*)^2$ defined as

$$\begin{aligned} P = (\xi, \eta) &\mapsto [\xi] \text{ if } P \neq (0,0), \\ (0,0) &\mapsto [a^2(d-1)^2], \\ O_{E^W} &\mapsto [1]. \end{aligned}$$

Now through the identification $\chi : E \to E^W$, we get a map $\psi : E(\mathbb{Q}) \to \mathbb{Q}/(\mathbb{Q}^*)^2$ and for a point $P = (x, y)$ on E which is not in $E[2]$, we have

$$\psi(P) = \left[a(d-1)\frac{y+1}{y-1}\right] = [a(d-1)(y^2-1)] = [(d-1)(dy^2-1)]. \tag{2}$$

Since $\chi(2T) = (0, 0)$, we have $\psi(2T) = [1]$. When the points $\infty_{x,+}$ and $\infty_{x,-}$ are rational then we have $\psi(\infty_{x,\pm}) = [-a(1 \pm \delta)^2] = [-a]$. When $\infty_{y,+}$ and $\infty_{y,-}$ are rational, then we have $\psi(\infty_{y,\pm}) = [a(d-1)]$. We want to identify the elements of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ which lie in the image of ψ. To do so, we introduce the following notion which will later yield a necessary condition for an element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ to be in the image in ψ.

Definition 3.6. Let k be a number field and let ν be a place of k. Let a and b be two elements of k_ν^*. The *Hilbert symbol* $(a,b)_\nu$ of a and b at ν is defined as

$$(a,b)_\nu = \begin{cases} 1 & \text{if the conic } ax^2+by^2=z^2 \text{ has a } k_\nu\text{-rational point,} \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol has many useful properties.

Proposition 3.7. *Let k be a number field, let ν be a place of k and let a,b,c be in k_ν^*. Then*

(i) $(a,b)_\nu = (b,a)_\nu$ *and* $(a,c^2)_\nu = 1$*;*

(ii) $(a,-a)_\nu = 1$*;*

(iii) If $a \neq 1$ *then* $(a,1-a)_\nu = 1$*;*

(iv) If $(a,b)_\nu = 1$ *then* $(ac,b)_\nu = (c,b)_\nu$*.*

Proof of properties (i)-(iii). Symmetry of Hilbert symbol follows from symmetry of the equation of the conic in the definition. If $b = c^2$ for some $c \in k_\nu^*$, then $(x,y,z) = (0,1,c)$ is a k_ν-rational point on the conic. This proves property (i). Now if $b = -a$, the conic admits $(x,y,z) = (1,1,0)$ as a rational point, and the same can be said for the point $(1,1,1)$ whenever $a \neq 1$ and $b = 1-a$. This proves (ii) and (iii). □

Property (iv) can be proven using the following proposition.

Proposition 3.8. *Let k be a number field and let ν be a place of k. Let a,b be in k_ν^*. Then $(a,b)_\nu = 1$ if and only if a is a norm from $k_\nu(\sqrt{b})$.*

Proof. Is b is a square, then by property (i) of the previous proposition $(a,b)_\nu = 1$ and we have $k_\nu(\sqrt{b}) = k_\nu$ so $a \in k_\nu^*$ is clearly a norm from $k_\nu(\sqrt{b})$. So let now b to be a element which is not a square in k_ν^* and let β be a square-root of b. Then all elements of $k_\nu(\sqrt{b})$ can be written as $u+\beta v$ with $u,v \in k_\nu$. Assume that a is the norm of such an element $u+\beta v$. Then we have $a = u^2 - bv^2$ and hence the conic $ax^2+by^2=z^2$ admits $(x,y,z) = (1,v,u)$ as rational point, so $(a,b)_\nu = 1$. Now assume that $(a,b)_\nu = 1$, i.e., that there are $x,y,z \in k_\nu$ not all zero such that $ax^2+by^2=z^2$. If x is zero, then y must be non-zero so b would be equal to $(z/y)^2$ which is a square and we are back to the first case. Now, if x is non-zero, we have that $a = (z/x)^2 - b(y/x)^2$, so a is the norm of the element $(z/x)+\beta(y/x)^2$ in $k_\nu(\sqrt{b})$. □

Proof of property (iv). If $(a,b)_\nu = 1$, then by the previous proposition a is a norm from $k_\nu(\sqrt{b})$. So, for $c \in k_\nu^*$, we have that ac is a norm if and only if c is a norm since the norm map is multiplicative. □

For k a completion of $\mathbb{Q}$, there are explicit formulae to compute the Hilbert symbol.

Proposition 3.9. *(i) Let a,b be in $\mathbf{R}^*$. Then:*

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a>0 \text{ or } b>0, \\ -1 & \text{if } a<0 \text{ and } b<0. \end{cases}$$

(ii) Let p an odd prime and $a,b \in \mathbf{Q}_p^*$. Write $a = p^\alpha u$ and $b = p^\beta v$ with u and v in $\mathbf{Z}_p^*$ and define $\epsilon(p) = (p-1)/2$. Then

$$(a,b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$$

where $(\frac{u}{p})$ *denotes the Legendre symbol.*

(iii) Let $p = 2$ *and* $a, b \in \mathbf{Q}_2^*$. *Write* $a = 2^\alpha u$ *and* $b = 2^\beta v$ *with* u *and* v *in* $\mathbf{Z}_2^*$. *For* $x \in \mathbf{Z}_2^*$, *define* $\epsilon(x) = (x-1)/2 \ (mod\, 2)$ *and* $\omega(x) = (x^2-1)/8 \ (mod\, 2)$. *Then*

$$(a, b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}.$$

Proof. See [4, Chapitre III, Théorème 1.]. □

For odd primes in particular, we may notice the following property.

Proposition 3.10. *Let* p *is an odd prime and* a, b *be elements in* $\mathbb{Z}_p^*$. *Then* $(a, b)_p = 1$.

Proof. This follows directly from (ii) of Proposition 3.9 since we have then the decomposition $a = p^0 a$ and $b = p^0 b$. □

We can now state the following theorem.

Theorem 3.11. *Let* b *be a square-free integer. If the class* $[b]$ *in* $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ *lies in the image of* ψ, *then* $(b, a)_\infty = (b, d)_\infty = 1$ *and* $(b, a)_p = (b, d)_p = 1$ *for all primes* p.

Proof. If $b = 1$, then $[b]$ lies in the image of ψ since $\psi(O) = [1]$ and we have $(a, 1)_\infty = (d, 1)_\infty = 1$ and $(a, 1)_p = (d, 1)_p = 1$ for all primes p by property (i) of Proposition 3.7 since $1 = 1^2$. Let now $b \neq 1$ be a square-free integer. For b to be in the image of ψ, there has to be a rational point $(x, y) \in E(\mathbb{Q})$ such that

$$[a(d-1)(y^2-1)] = [(d-1)(dy^2-1)] = [b].$$

Here (x, y) is not in $\{O, 2T\}$ since $\psi(O) = \psi(2T) = [1]$. In other words, we must have

$$a(d-1)(y^2-1) = bz^2$$

for some $z \in \mathbb{Q}^*$.
Consider now the curve C_b defined by the previous equation and the equation for E, i.e., the curve C_b defined by the equations

$$C_b := \begin{cases} a(y^2-1) = x^2(dy^2-1), \\ a(d-1)(y^2-1) = bz^2. \end{cases}$$

We have that if (x, y) is a rational point on E with $\psi(x, y) = [b]$, i.e., with $a(d-1)(y^2-1) = bz^2$ for some $z \in \mathbb{Q}^*$, then the point (x, y, z) is a rational point on C_b.
Write $X = \frac{abz}{x}$, $Y = a(d-1)y$, $Z = bz$ and $W = a(d-1)$. Then, multiplying the second equation by $ba(d-1)$ yields the equation

$$bY^2 = bW^2 + a(d-1)Z^2. \tag{$C_{b,1}$}$$

Subtracting $(d-1)$ times the first equation from the second then and multiplying both sides by $a^2b(d-1)$ also gives us the following equation

$$bdY^2 = bW^2 + (d-1)X^2. \tag{$C_{b,2}$}$$

Now, removing the variable Y by computing $dC_{b,4} - C_{b,2}$ and then dividing by $(d-1)$, we get

$$X^2 = bW^2 + adZ^2 \tag{$C_{b,3}$}$$

and removing W by computing $C_{b,2} - C_{b,4}$ and then dividing by $(d-1)$, we get

$$X^2 = bY^2 + aZ^2. \tag{$C_{b,4}$}$$

Every equation $(C_{b,i})$ with $i \in \{1,2,3,4\}$ defines a conic $C_{b,i}$ and so we get four conic $C_{b,1}$, $C_{b,2}$, $C_{b,3}$ and $C_{b,4}$ as well as projections $C_b \to C_{b,i}$ for $i \in \{1,2,3,4\}$. Hence, if one of those conic admits no rational points, then necessarily, C_b admits no rational points and therefore b can not lie in the image of ψ. Now, for $C_{b,4}$ to have rational points, we must have $(b,a)_\nu = 1$ for $\nu = \infty$ and $\nu = p$ for all p prime. Similarly, $C_{b,3}$ can only have rational points if $(b,ad)_\nu = 1$. Using property (iv) pf Proposition 3.7, this implies that we must have $(b,a)_\nu = 1$ and $(b,d)_\nu = 1$ for $\nu = \infty$ and $\nu = p$ for all prime numbers p. □

Remark. The conics $C_{b,1}$ and $C_{b,2}$ do not give any extra conditions. Indeed the point $(Y,Z,W) = (1,1,0)$ always lies on $C_{b,1}$ so $C_{b,1}$ surely admits rational points. As for $C_{b,2}$ we notice that multiplying $(C_{b,2})$ by b yields the equation

$$(bW)^2 = d(bY)^2 + b(1-d)X^2$$

which defines a conic that admits rational points over k_ν if and only if $(d, b(1-d))_\nu = 1$. By properties (iii) and (iv) of Proposition 3.7, that is if and only if $(d,b)_\nu = 1$ which is a condition we already have.

In particular if $(a,b)_\nu = -1$ with $\nu = \infty$ or $\nu = p$ for some prime number p, then b does not lie in the image of ψ. Hence, thanks to a simple computation of the Hilbert symbol, we may discard some values of b a bit quicker than with the usual method as in Proposition 3.4. We shall illustrate this with an example.

Theorem 3.12. *Let E be the twisted Edwards curve over $\mathbb{Q}$ given by*

$$x^2 + 5y^2 = 5 + 2x^2y^2.$$

Then $E(\mathbb{Q})$ is an abelian group of rank 1.

Proof. We work with the twisted Edwards curves $E : x^2+5y^2 = 5+2x^2y^2$ meaning we have $a = 5$ and $d = 2$. We want to compute the group $E(\mathbb{Q})/2E(\mathbb{Q})$. By Theorem 3.5, the corresponding Weierstraß equation is given by

$$C : \eta^2 = \xi(\xi^2 + 30\xi + 25).$$

and Theorem 3.1 and 3.2 give us a second elliptic curve C' over $\mathbb{Q}$ given by

$$C' : v^2 = u(u^2 - 60u + 800)$$

together with isogenies $\phi : C \to C'$ and $\hat{\phi} : C' \to C$. Moreover by Lemma 3.3 we have a homomorphism $\varphi : C(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ given by

$$\begin{aligned} P = (\xi,\eta) &\mapsto [\xi] \text{ if } P \neq (0,0), \\ (0,0) &\mapsto [25], \\ O_{E^W} &\mapsto [1] \end{aligned}$$

and through the identification $\chi : E \to C$, we have a map $\psi : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ such that for a point P on E which is not in $E[2]$, we have

$$\psi(P) = [5(y^2-1)] = [2y^2 - 1]$$

as seen in equation (2).
We will first compute $C(\mathbb{Q})/\hat{\phi}(C'(\mathbb{Q}))$. By Lemma 3.3, it is isomorphic to $\mathrm{im}(\psi)$. The square-free integers b for which the class $[b] \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ may lie in the image of ψ are the square-free integers which divide $a(d-1)$, so which divide 5 in this case, hence we only have to look at the integers ± 1 and ± 5. Now, the necessary conditions we have found in Theorem 3.11 on the Hilbert symbols for b to be in the image of ψ are here given by $(5,b)_\nu = 1 = (2,b)_\nu$ for all places ν of $\mathbb{Q}$, i.e., for $\nu = \infty$ and for $\nu = p$ with p any prime. Since both 2 and 5 are positive integers, those conditions are satisfied for every b when $\nu = \infty$ by Proposition 3.9.
Take now $b = -5$ and $p = 2$. We have $2 = 2^1 \cdot 1$ and $-5 = 2^0 \cdot (-5)$, so we get:

$$(2,-5)_2 = (-1)^{\epsilon(1)\epsilon(-5)+\omega(-5)} = (-1)^{\omega(-5)} = -1$$

because $\epsilon(1) = \frac{1-1}{2} \pmod 2 = 0$ and $\omega(-5) = \frac{25-1}{8} \pmod 2 = 3 \pmod 2 = 1$. Therefore, for $b = -5$, we know directly with this simple computation that $[-5]$ is not contained in the image of ψ by Theorem 3.11.
For $b = 5$, we find that $(5,2)_2 = (-1)^{\omega(5)} = -1$ so by Theorem 3.11 we can also discard 5 right away.
For $b = -1$, we see that for the point $(-5, -2/3)$ on the curve E, we have

$$\psi((-5,-2/3)) = [5 \cdot 1 \cdot (4/9 - 1)] = [5 \cdot (-5/9)] = [-1]$$

so $[-1]$ is in the image of ψ. Therefore $\mathrm{im}(\psi)$ is the group $\{\pm 1\}$.
We now want to find the order of $C'(\mathbb{Q})/\phi(C(\mathbb{Q}))$. Let q be the map given in Lemma 3.3. By proposition 3.4 we need to look at the square-free integers b dividing 800, i.e., at $b \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$. All negative b can not give a non-zero solutions to the equation

$$bl^4 - 60l^2m^2 + \frac{800}{b}m^4 = n^2$$

for the left-hand side will always be negative and the right-hand side positive. Moreover, we have $[800] = [2 \cdot 10^2] = [2]$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, so $[2] = q((0,0))$. Hence $[2]$ is in $\mathrm{im}(q)$, meaning that $\mathrm{im}(q)$ is either the group $\{1,2\}$ or $\{1,2,5,10\}$. Now for $b = 5$, we see that for the point $(20,0)$ on C' we have

$$q((20,0)) = [20] = [5]$$

So $[5]$ is in the image of q and so $\mathrm{im}(q) = \{1,2,5,10\}$. Hence $C'(\mathbb{Q})/\phi(C(\mathbb{Q}))$ has order 4.
Write now r for the rank of $E(\mathbb{Q})$. By [5, Section 3.6], we have

$$2^r = \frac{\#(C(\mathbb{Q})/\hat{\phi}(C'(\mathbb{Q})))\#(C'(\mathbb{Q})/\phi(C(\mathbb{Q})))}{4} = \frac{2 \cdot 4}{4} = 2.$$

Hence, we have indeed $r = 1$. □

Remark. We could have found the same result using the method described in Proposition 3.4, but it would have required some work. For instance, when computing $C(\mathbb{Q})/\hat{\phi}(C'(\mathbb{Q}))$, we have discarded the value $b = -5$ quickly by noticing that $(2,-5)_2 = -1$, and so that the conic $C_{b,3}$ for $b = -5$ has no $\mathbb{Q}_2$-adic points. But then C_b has no $\mathbb{Q}_2$-adic points either, which can be verified using Proposition 3.4. However, this is a bit more tedious, even if already know that $p = 2$ is a useful prime to consider. Indeed, to see that C_b for $b = -5$ has no $\mathbb{Q}_2$-adic points, we then need to look at the equation

$$bl^4 + 2a(d+1)l^2m^2 + \frac{a^2(d-1)^2}{b}m^4 = n^2$$

so in this example at the equation

$$-5(l^4 - 6l^2m^2 + m^4) = n^2.$$

We want to show here that this equation admits no solutions in $\mathbb{Q}_2$. Modulo 2 and 4, this equation admits $(l, m, n) = (1, 1, 0)$ as solution, so we must at least look at the equation modulo 8. Take $l = 1$ and $m = 1$ modulo 8, then

$$-5(l^4 - 6l^2m^2 + m^4) = -5(1 - 6 + 1) = 20 = 4 \pmod 8 = 2^2 \pmod 8$$

so $(1, 1, 2)$ is a solution here. Modulo 16, when taking $l = m = 1$, we have again that

$$-5(l^4 - 6l^2m^2 + m^4) = -5(1 - 6 + 1) = 20 = 4 \pmod{16} = 2^2 \pmod{16}$$

so $(1, 1, 2)$ is again a solution. Consider now the equation modulo 32. Suppose first that l is even and m is odd. Then, modulo 8, we have that l^2 must be either 0 or 4 so in any case $6l^2$ must be congruent to 0 modulo 8. Moreover, we have then also that l^4 is congruent to 0 modulo 8, so modulo 8 we get the equation $-5m^4 \equiv n^2$ which has no solutions since -5 is not a square modulo 8 and $m^4 \equiv 1$ modulo 8. Hence the equation $-5(l^4 - 6l^2m^2 + m^4) = n^2$ can not have solutions modulo 32 for l even and m odd. By symmetry of the equation, the same happens for l odd and m even. Assume now that both l and m are odd. For x and odd integer, we have that x^2 is congruent to either 1, -7, 9 or 17 modulo 32. So the possible values of l^2 modulo 32 are 1, -7, 9 or 17 and the same holds for m^2 modulo 32. In every case, we get that the value of $l^4 - 6l^2m^2 + m^4$ is congruent to -4 modulo 32. Hence, for any possible value of l and m, we have that $-5(l^4 - 6l^2m^2 + m^4)$ is congruent to 20 modulo 32 so the equation $-5(l^4 - 6l^2m^2 + m^4) = n^2$ becomes $20 = n^2$ modulo 32 and this equation has no solution modulo 32 since 20 is not a square modulo 32. Hence the equation

$$-5(l^4 - 6l^2m^2 + m^4) = n^2$$

has no rational solution, therefore the class $[-5]$ does not lie in the image of ψ by Proposition 3.4. We get the same result but we here had to look at the equation $-5(l^4 - 6l^2m^2 + m^4) = n^2$ modulo 32 for this.
In a similar way, one can show that to discard the value $b = 5$ with the method in Proposition 3.4, we would have had to look at the equation $5(l^4 + 6l^2m^2 + m^4) = n^2$ modulo 16 to find that it has no solution in $\mathbb{Q}_2$.

4 Constructing a 4-isogeny.

Throughout this section, E will denote a twisted Edwards curve $E : x^2 + ay^2 = a + dx^2y^2$ over a perfect field k with $\mathrm{char}(k) \neq 2$. Let α be a root of the polynomial $X^2 - a$ and δ a root of $X^2 - d$. Denote by T the 4-torsion point $T = (\alpha, 0)$ and by G the group of order 4 generated by T.

Theorem 4.1. *There is a second twisted Edwards curve $\tilde{E}$ over k and an isogeny $\psi\colon E \to \tilde{E}$ whose kernel is equal to G. Specifically, $\tilde{E}$ can be given by the equation*

$$\tilde{E}\colon \tilde{x}^2 + \tilde{a}\tilde{y}^2 = \tilde{a} + \tilde{d}\tilde{x}^2\tilde{y}^2$$

with $\tilde{a} = -\frac{1}{a}$ and $\tilde{d} = 1 - d$; and ψ can be given by

$$(x, y) \mapsto \left(\frac{2xy}{x^2 - ay^2}, \frac{x^2 + ay^2}{2a - x^2 - ay^2}\right).$$

Proof. First of all, we need to verify that for $(x, y) \in E$, the image $\psi(x, y)$ is indeed a point on the given curve $\tilde{E}$, so we need to prove that

$$\left(\frac{2xy}{x^2 - ay^2}\right)^2 - \frac{1}{a}\left(\frac{x^2 + ay^2}{2a - x^2 - ay^2}\right)^2 + \frac{1}{a} - (1 - d)\left(\frac{2xy}{x^2 - ay^2}\right)^2\left(\frac{x^2 + ay^2}{2a - x^2 - ay^2}\right)^2 = 0.$$

Using the identity $2a - x^2 - ay^2 = a - dx^2y^2$ and multiplying the previous expression by $a(a - dx^2y^2)^2(x^2 - ay^2)^2$, this is equivalent to proving that the expression

$$A = 4ax^2y^2(a - dx^2y^2)^2 - (x^4 - a^2y^4)^2 + (x^2 - ay^2)^2(a - dx^2y^2)^2 + 4a(d - 1)x^2y^2(x^2 + ay^2)^2$$

is equal to zero. We have

$$\begin{aligned}
A &= 2a^3x^2y^2 + 2ad^2x^6y^6 - x^8 + 2a^2x^4y^4 - a^4y^8 + a^2x^4 - 2a^3x^2y^2 + a^4y^4 - 2adx^6y^2 \\
&\quad + 4a^2dx^4y^4 - 2a^3dx^2y^6 + d^2x^8y^4 + a^2d^2x^4y^8 + 4adx^6y^2 - 4ax^6y^2 - 8a^2x^4y^4 \\
&\quad + 4a^3dx^2y^6 - 4a^3x^2y^6 \\
&= -2a^3x^2y^2 + 3adx^6y^4 + 3a^2dx^4y^6 - 2a^2dx^4y^4 - x^8 + 2a^2x^4y^4 - a^4y^8 + a^2x^4 - 3a^4y^4 \\
&\quad - 2ax^6 + 6a^2x^4y^2 + 2a^2x^4 + 6a^3x^2y^4 + 2a^4y^6 + 2a^4y^4 + dx^8y^2 - adx^6y^2 + a^3dx^2y^8 \\
&\quad - a^3dx^2y^6 + 4ax^6 - 4a^2x^4 - 4ax^6y^2 - 8a^2x^4y^4 - 4a^3x^2y^6 \\
&= -2a^3x^2y^2 + 3ax^6y^2 + 3a^2x^4y^4 - 3a^2x^4y^2 + 3a^2x^4y^4 + 3a^3x^2y^6 - 3a^3x^2y^4 - 2a^2x^4y^2 \\
&\quad - 2a^3x^2y^4 + 2a^3x^2y^2 - x^8 + 2a^2x^4y^4 - a^4y^8 + a^2x^4 - 3a^4y^4 - 2ax^6 + 6a^2x^4y^2 + 2a^2x^4 \\
&\quad + 6a^3x^2y^4 + 2a^4y^6 + 2a^4y^4 + x^8 + ax^6y^2 - 2ax^6 - a^2x^4y^2 + a^2x^4 + a^3x^2y^6 + a^4y^8 \\
&\quad - a^4y^6 + a^4y^4 + 4ax^6 - 4a^2x^4 - 4ax^6y^2 - 8a^2x^4y^4 - 4a^3x^2y^6 \\
&= 0
\end{aligned}$$

using the equality $dx^2y^2 = x^2 + ay^2 - a$ when needed. Hence the map ψ is well-defined on the affine points (x, y) where $x^2 - ay^2$ and $a - dx^2y^2$ do not vanish. Because rational map from a smooth curve to a projective curve extend uniquely to a morphism, the map ψ is a well-defined morphism $E \to \tilde{E}$.
We are left to prove that its kernel is equal to $G = \langle T \rangle$. The curve $\tilde{E}$ is a twisted Edwards curve with identity element given by $O_{\tilde{E}} = (0, 1)$. For a point $((x_0 : x_1), (y_0 : y_1))$ on E, we have

$$\psi((x_0 : x_1), (y_0 : y_1)) = ((2x_0y_0x_1y_1 : x_0^2y_1^2 - ay_0^2x_1^2), (x_0^2y_1^2 + ay_0^2x_1^2 : 2ax_1^2y_1^2 - x_0^2y_1^2 - ay_0^2x_1^2))$$

and so we see that the points at infinity $\infty_{x,+}$, $\infty_{x,-}$, $\infty_{y,+}$ and $\infty_{y,-}$ on E are all sent to the point $(0, -1)$ on $\tilde{E}$ under ψ. Hence they are not in the kernel of ψ. For a point $P = (x, y)$ to lie in the kernel, we need to have

$$\left(\frac{2xy}{x^2 - ay^2}, \frac{x^2 + ay^2}{2a - x^2 - ay^2}\right) = (0, 1).$$

If $x^2 - ay^2 = 0$, then from $x^2 + ay^2 = a + dx^2y^2$, we get $2ay^2 = a + dx^2y^2 = a + ady^4 = a(1 + dy^4)$, so $dy^4 = 2y^2 - 1$. Hence we then have $y \neq 0$ and $x \neq 0$, so $2xy \neq 0$ and therefore (x, y) is sent to a point at infinity and is therefore not in the kernel of ψ.
If $2a - x^2 - ay^2 = 0$ then from $x^2 + ay^2 = a + dx^2y^2$, we have $a - dx^2y^2 = 0$ and so $x^2y^2 \neq 0$. Hence $x^2 + ay^2 = a + dx^2y^2 \neq 0$ and so (x, y) is sent to a point at infinity and is therefore not in the kernel of ψ.
If $x^2 - ay^2 \neq 0$ and $2a - x^22 - ay^2 \neq 0$, then for (x, y) to be in the kernel, we need to have

$$2xy = 0.$$

This can only happen when $x = 0$ or $y = 0$, i.e., when P is equal to either O_E, T, $2T$ or $-T$. Hence $\ker(\psi) \subseteq G$. It is not difficult to see that we also have $G \subseteq \ker(\psi)$ since for all $P \in G$, we have

$$\psi(P) = \left(0, \frac{a}{a}\right) = (0, 1) = O_{\tilde{E}}.$$

Hence $\ker(\psi) = G$. In particular we have $\psi(O_E) = O_{\tilde{E}}$ so ψ is indeed an isogeny. □

Remark. In the proof above, we have simply verified that the given map satisfies the required conditions but it may be interesting to get a idea on how we might have found this map ψ and the curve $\tilde{E}$ to begin with. One way to do it is to state that if there was an isogeny ψ from E to an elliptic curve $\tilde{E}$, then the image under ψ of the point $R = ((1 : 0), (1 : \delta))$, which is a two-torsion point on E would still be a 2-torsion point on $\tilde{E}$ as R is not contained in G and so the image of a point S on E satisfying $2S = R$ would be a 4-torsion point on $\tilde{E}$. Now, we notice that $E[\bar{k}][4]$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$ and is invariant under $\mathrm{Gal}(\bar{k}/k)$. Hence the image $\psi(E[\bar{k}][4])$ is also fixed under $\mathrm{Gal}(\bar{k}/k)$ and this image is isomorphic to $E[\bar{k}][4]/G \cong (\mathbb{Z}/4\mathbb{Z})^2/G \cong \mathbb{Z}/4\mathbb{Z}$. By section 2, this means that $\tilde{E}$ is a twisted Edwards curve and can therefore be defined by an equation of the form $\tilde{x}^2 + \tilde{a}\tilde{y}^2 = \tilde{a} + \tilde{d}\tilde{x}^2\tilde{y}^2$. We are now left to find the functions $\tilde{x}, \tilde{y}$ and the constants $\tilde{a}$ and $\tilde{d}$. The group $\tilde{E}[2]$ consists of the points $O_{\tilde{E}}$, $\psi(R)$, $\psi(Q)$ and $\psi(Q) + \psi(R)$ where Q is a point on E satisfying $2Q = T$ and by section 2, we therefore know that

$$\mathrm{div}_{\tilde{E}}(\tilde{x}) = (O_{\tilde{E}}) + (\psi(R)) - (\psi(Q)) - (\psi(Q) + \psi(R))$$

and

$$\mathrm{div}_{\tilde{E}}(\tilde{y}) = (\psi(S)) + (\psi(R)) + \psi(S)) - (\psi(Q) + \psi(S)) - (\psi(Q) + \psi(R) + \psi(S)).$$

Hence we have

$$\begin{aligned}\mathrm{div}_E(\psi^*(\tilde{x})) = {} & (O_E) + (T) + (2T) + (-T) + (R) + (R+T) + (R+2T) + (R-T) \\ & - (Q) - (Q+T) - (Q+2T) - (Q-T) - (Q+R) - (Q+R+T) \\ & - (Q+R+2T) - (Q+R-T)\end{aligned}$$

and

$$\begin{aligned}\mathrm{div}_E(\psi^*(\tilde{y})) = {} & (S) + (S+T) + (S+2T) + (S-T) + (R+S) + (R+S+T) + (R+S+2T) \\ & + (R+S-T) - (Q+S) - (Q+S+T) - (Q+S+2T) - (Q+S-T) \\ & - (Q+S+R) - (Q+S+R+T) - (Q+S+R+2T) - (Q+S+R-T)\end{aligned}$$

We are left to find the points Q and S. The coordinates of Q can be found by looking at the points which are invariant under the map $E \to E, P \mapsto T - P$ which is given on the coordinates by $(x, y) \mapsto \left(\alpha y, \frac{x}{\alpha}\right)$. The coordinates of S can also be found by looking at the points invariant under the map $E \to E, P \mapsto R - P$ which is given on the coordinates by $(x, y) \mapsto \left(-\frac{a}{\delta x}, \frac{1}{\delta y}\right)$. Using this, we get $\psi^*(\tilde{x}) = \lambda f$ and $\psi^*(\tilde{y}) = \lambda' g$ with $f(x, y) = \frac{xy}{x^2 - ay^2}$ and $g(x, y) = \frac{x^2 + ay^2}{2a - x^2 - ay^2}$ and λ, λ' constants. Now, $\tilde{a}$ corresponds to the square of the first coordinates of $\psi(S)$ so we can find its value by evaluating $f(S)^2$. Similarly we can find the value of $\tilde{d}$ by evaluating $g(Q)^2$. Setting $\lambda = 2$ and $\lambda' = 1$, we find $\tilde{a} = -\frac{1}{a}$ and $\tilde{d} = 1 - d$.

Consider now the elliptic curve $E' \subset \mathbb{P}^3(p, q, r, s)$ defined by the affine equations in the affine patch with $s = 1$

$$\begin{cases} q^2 = pr \\ p + ar = a + dq^2 \end{cases}$$

with base point $O_{E'} = (0, 0, 1)$ and consider the isogeny $\phi\colon E \to E'$ given by

$$\phi\colon ((x : 1), (y : 1)) \mapsto (x^2 : xy : y^2 : 1).$$

Lemma 4.2. *The curve $E' \subset \mathbb{P}^3(p,q,r,s)$ is smooth.*

Proof. The curve E' is given in $\mathbb{P}^3(p,q,r,s)$ by

$$\begin{cases} q^2 = pr \\ ps + ars = as^2 + dq^2. \end{cases}$$

Let $F(p,q,r,s)$ be the function given by $q^2 - pr$ and $G(p,q,r,s)$ the function given by $ps + ars - as^2 - dq^2$. We have

$$\frac{\partial F}{\partial p} = -r; \quad \frac{\partial F}{\partial r} = -p; \quad \frac{\partial F}{\partial q} = 2q; \quad \frac{\partial F}{\partial s} = 0$$

and

$$\frac{\partial G}{\partial p} = s; \quad \frac{\partial G}{\partial r} = as; \quad \frac{\partial G}{\partial q} = -2dq; \quad \frac{\partial G}{\partial s} = p + ar - 2as.$$

So, if E' is singular at a point $(p:q:r:s)$ then the matrix

$$A = \begin{pmatrix} -r & -p & 2q & 0 \\ s & as & -2dq & p + ar - 2as \end{pmatrix}$$

has rank smaller than 2.
If $q = 0$, then we have $pr = q^2 = 0$ and so either $p = 0$ or $r = 0$. Since the matrix

$$B = \begin{pmatrix} -r & -p \\ s & as \end{pmatrix}$$

has rank smaller than 2, we have

$$0 = \det(B) = -asr - ps$$

and so we get

$$s(p + ar) = 0.$$

Hence, we then have either $s = 0$ or $p = ar$. So either we have $q = p = r = 0$ or $q = r = s = 0$ or $q = p = s = 0$.
In the first case, the identity

$$ps + ars = as^2 + dq^2$$

implies $p = q = r = s = 0$.
In the last two cases we also have $p = q = r = s = 0$ since A has rank smaller than two.
Now if $q \neq 0$, then we have that the second row is $-d$ times the first row. Hence we get $s = dr$, $as = dp$ and $p + ar - 2as = 0$. The first two yield $p = ar$, since $d \neq 0$. Together with $p + ar - 2as = 0$, we then get $r = s$, for $a \neq 0$. Hence we have $s = r$ and $s = dr$, so $r = dr$. Since $d \neq 1$, this implies that we have $r = 0$. Because $q^2 = pr$, this then implies $q = 0$ which contradicts $q \neq 0$.
Hence the curve E' is smooth. □

Lemma 4.3. *Let $C' \subset \mathbb{P}^2$ be the elliptic curve defined by the Weierstraß equation*

$$v^2 = u(u-a)(u-ad).$$

Then we have an isomorphism $\chi' : E' \to C'$ given by $(p,q,r) \mapsto \left(\frac{a^2}{p}, \frac{a^2(p-a)}{pq}\right)$ with inverse $(u,v) \mapsto \left(\frac{a^2}{u}, \frac{a(a-u)}{v}, \frac{a-u}{u-ad}\right)$.

Proof. The map χ' is well-defined for

$$\begin{aligned}\frac{a^2}{p}\left(\frac{a^2}{p}-a\right)\left(\frac{a^2}{p}-ad\right) &= \frac{a^2}{p}\left(\frac{a(a-p)}{p}\right)\left(\frac{a(a-dp)}{p}\right)\\ &= \frac{a^4(a-p)(a-dp)}{p^3}\\ &= \frac{a^4(a-p)(ar-dq^2)}{p^3r}\\ &= \frac{a^4(a-p)^2}{p^2q^2}.\end{aligned}$$

It is an isogeny since it sends the base point $O_{E'} = (0,0,1)$ to the infinity point and it is clearly of degree 1, with inverse $(u,v) \mapsto \left(\frac{a^2}{u}, \frac{a(a-u)}{v}, \frac{a-u}{u-ad}\right)$. □

Let $C \subset \mathbb{P}^2$ be the curve given by

$$\eta^2 = \xi(\xi + 2a(d+1)\xi + a^2(d-1)^2).$$

By Theorem 3.5, C represents the Weierstraß form of the twisted Edwards curve E and we have an isomorphism $\chi\colon E \to C$ given by $(x,y) \mapsto \left(a(d-1)\frac{y+1}{y-1}, 2a^2(d-1)\frac{y+1}{x(y-1)}\right)$.

Lemma 4.4. *The map $\hat{\phi}\colon C' \to C$ given by $(u,v) \mapsto \left(u - a(d+1) + \frac{a^2d}{u}, v - \frac{a^2dv}{u^2}\right)$ is a well defined isogeny of degree 2.*

Proof. The map is well-defined, for

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

Now, on $\mathbb{P}^2(U,V,W)$, the curve C' is given by the equation

$$V^2W = U(U - aW)(U - adW)$$

and we have

$$\begin{aligned}\hat{\phi}([U:V:W]) &= \left[\frac{U}{W} - a(d+1) + \frac{a^2dW}{U} : \frac{V}{W} - \frac{a^2dVW}{U^2} : W\right]\\ &= [UV^3 - a(d+1)V^3W + \frac{a^2dV^3W^2}{U} : V^4 - \frac{a^2dV^4W^2}{U^2} : V^3W^2].\end{aligned}$$

Now, using the equation of the curve, we can rewrite the first coordinate as

$$UV^3 - a(d+1)V^3W + a^2dVW(U - aW)(U - adW)$$

and the second one as

$$V^4 - a^2d(U - aW)^2(U - adW)^2$$

so $\hat{\phi}$ sends a point $[U:V:W]$ to the point

$$[UV^3 - a(d+1)V^3W + a^2dVW(U - aW)(U - adW) : V^4 - a^2d(U - aW)^2(U - adW)^2 : V^3W^2].$$

In particular, we see that $\hat{\phi}([0:1:0]) = [0:1:0]$ and so it is indeed an isogeny. Finally, if (u,v) is in $C'(\bar{k})$ and $u \neq 0$, then $\hat{\phi}((u,v))$ is a well defined point on the affine part of C and so (u,v) is not in the kernel of $\hat{\phi}$. We thus have

$$\ker(\hat{\phi}) = \{O_{C'}, (0,0)\}.$$

Hence $\hat{\phi}$ has indeed degree 2. □

Lemma 4.5. *The morphism $E \to E$ given by the composition $\chi^{-1} \circ \hat{\phi} \circ \chi' \circ \phi$ is equal to multiplication by -2 in the group law of E.*

Proof. Let $\bar{C}$ be the elliptic curve given by the equation $\bar{v}^2 = \bar{u}(\bar{u}^2 - 4a(d+1)\bar{u} + 16a^2 d)$ and consider the map $\varphi\colon C \to \bar{C}$ given by

$$\begin{cases} (\xi,\eta) \mapsto \left(\left(\frac{\eta}{\xi}\right)^2, \eta - \frac{a^2(d-1)^2\eta}{\xi^2}\right), & \xi \neq 0 \\ O_{\bar{C}}, & \xi = 0. \end{cases}$$

This map is well-defined by Theorem 3.1.

Set $\hat{\varphi} = \hat{\phi}$ and consider the diagram

$$\begin{array}{ccc} C & \xrightarrow{\quad\varphi\quad} & \bar{C} \\ & {\scriptstyle\hat{\varphi}}\nwarrow \quad \swarrow{\scriptstyle\epsilon} & \\ & C' & \end{array}$$

where $\epsilon : \bar{C} \to C'$ is the isomorphism given by $(\bar{u},\bar{v}) \mapsto \left(\frac{\bar{u}}{4}, -\frac{\bar{v}}{8}\right)$. Then, for $(\bar{u},\bar{v}) \in \bar{C}$, we have

$$\begin{aligned} \hat{\varphi}(\epsilon(\bar{u},\bar{v})) &= \left(\frac{1}{4}\bar{u} - a(d+1) + \frac{4a^2 d}{\bar{u}}, -\frac{1}{8}\bar{v} + \frac{2a^2 d\bar{v}}{\bar{u}^2}\right) \\ &= \left(\frac{1}{4}\left(\bar{u} - 4a(d+1) + \frac{16a^2 d}{\bar{u}}\right), -\frac{1}{8}\left(\bar{v} + \frac{16a^2 d\bar{v}}{\bar{u}^2}\right)\right). \end{aligned}$$

Therefore, by Theorem 3.2, the composite $\hat{\varphi} \circ \epsilon \circ \varphi$ is equal to multiplication by -2. Hence, we are now only left to show that the diagram

$$\begin{array}{ccc} E & \xrightarrow{\quad\phi\quad} & E' \\ \downarrow{\scriptstyle\chi} & & \downarrow{\scriptstyle\chi'} \\ C & \xrightarrow[\epsilon\circ\varphi]{} & C' \end{array}$$

commutes. Indeed, if it commutes, then we have

$$\chi^{-1} \circ \hat{\phi} \circ \chi' \circ \phi = \chi^{-1} \circ \hat{\phi} \circ \epsilon \circ \varphi \circ \chi = \chi^{-1} \circ \hat{\varphi} \circ \epsilon \circ \varphi \circ \chi = \chi^{-1} \circ [-2] \circ \chi = [-2].$$

So let (x,y) be on E. Then

$$\chi'(\phi(x,y)) = \chi'(x^2, xy, y^2) = \left(\frac{a^2}{x^2}, \frac{a^2(x^2-a)}{x^3 y}\right)$$

and

$$\begin{aligned}
\epsilon(\varphi(\chi(x,y))) &= \epsilon\left(\varphi\left(a(d-1)\frac{y+1}{y-1}, 2a^2(d-1)\frac{y+1}{x(y-1)}\right)\right)\\
&= \epsilon\left(\frac{4a^4(d-1)^2(y+1)^2(y-1)^2}{a^2(d-1)^2x^2(y+1)^2(y-1)^2}, 2a^2(d-1)\frac{y+1}{x(y-1)}\left(1-\frac{(y-1)^2}{(y+1)^2}\right)\right)\\
&= \epsilon\left(4\frac{a^2}{x^2}, 8a^2\frac{(d-1)y}{x(y^2-1)}\right)\\
&= \epsilon\left(4\frac{a^2}{x^2}, 8a^2\frac{(d-1)x^2y^2}{x^3y(y^2-1)}\right)\\
&= \epsilon\left(4\frac{a^2}{x^2}, 8a^2\frac{(x^2+ay^2-a-x^2y^2)}{x^3y(y^2-1)}\right)\\
&= \epsilon\left(4\frac{a^2}{x^2}, 8a^2\frac{(a-x^2)}{x^3y}\right)\\
&= \left(\frac{a^2}{x^2}, \frac{a^2(x^2-a)}{x^3y}\right)\\
&= \chi'(\phi(x,y)).
\end{aligned}$$

Hence, the diagram above commutes, which concludes the proof. □

Now, "symmetrically", we can define similar maps for the Edwards curve $\tilde{E}$. Denote by $\tilde{C} \subset \mathbb{P}^2$ the curve given by the Weierstraß equation

$$\tilde{\eta}^2 = \tilde{\xi}(\tilde{\xi}^2 + 2\tilde{a}(\tilde{d}+1)\tilde{\xi} + \tilde{a}^2(\tilde{d}-1)^2)$$

and by $\tilde{\chi}$ the isomorphism $\tilde{E} \to \tilde{C}$ given by

$$(\tilde{x}, \tilde{y}) \mapsto \left(\tilde{a}(\tilde{d}-1)\frac{\tilde{y}+1}{\tilde{y}-1}, 2\tilde{a}^2(\tilde{d}-1)\frac{\tilde{y}+1}{\tilde{x}(\tilde{y}-1)}\right).$$

Let $\tilde{E}' \subset \mathbb{P}^3(\tilde{p}, \tilde{q}, \tilde{r}, \tilde{s})$ be the elliptic curve defined by the equation

$$\begin{cases} \tilde{q}^2 = \tilde{p}\tilde{r} \\ \tilde{p} + \tilde{a}\tilde{r} = \tilde{a} + \tilde{d}\tilde{q}^2 \end{cases}$$

together with the base point $O_{\tilde{E}'} = (0,0,1)$ and $\tilde{\phi}$ be the morphism $\tilde{E} \to \tilde{E}'$ given by

$$((\tilde{x}:1),(\tilde{y}:1)) \mapsto (\tilde{x}^2 : \tilde{x}\tilde{y} : \tilde{y}^2 : 1).$$

Finally consider the curve $\tilde{C}' \subset \mathbb{P}^2$ given by the equation

$$\tilde{v}^2 = \tilde{u}(\tilde{u}-\tilde{a})(\tilde{u}-\tilde{d}\tilde{a})$$

and the morphisms $\tilde{\chi}' \colon \tilde{E}' \to \tilde{C}'$ given by

$$(\tilde{p}, \tilde{q}, \tilde{r}) \mapsto \left(\frac{\tilde{a}^2}{\tilde{p}}, \frac{\tilde{a}^2(\tilde{p}-\tilde{a})}{\tilde{p}\tilde{q}}\right)$$

and $\hat{\tilde{\phi}} \colon \tilde{C}' \to \tilde{C}$ given by

$$(\tilde{u}, \tilde{v}) \mapsto \left(\tilde{u} - \tilde{a}(\tilde{d}+1) + \frac{\tilde{a}^2\tilde{d}}{\tilde{u}}, \tilde{v} - \frac{\tilde{a}^2\tilde{d}\tilde{v}}{\tilde{u}^2}\right).$$

By the previous part, it is clear that all those maps are well-defined isogenies.

Lemma 4.6. *Let n be in $\mathbb{Z}$ and E_1 and E_2 be elliptic curves. Let $p\colon E_1 \to E_2$ and $q\colon E_2 \to E_1$ be isogenies. If $p \circ q = [n]_{E_2}$, then $q \circ p = [n]_{E_1}$.*

Proof. We have

$$(q \circ p) \circ q = q \circ (p \circ q) = q \circ [n]_{E_2} = [n]_{E_1} \circ q.$$

Because q is surjective, we get $q \circ p = [n]_{E_1}$. □

Lemma 4.7. *The morphism $\tilde{C}' \to \tilde{C}'$ given by the composite $\tilde{\chi}' \circ \tilde{\phi} \circ \tilde{\chi}^{-1} \circ \hat{\tilde{\phi}}$ is equal to multiplication by -2 in the group law of $\tilde{C}'$.*

Proof. Appply Lemma 4.5 to the twisted Edwards curve $\tilde{E}$, then use Lemma 4.6 with $p = \tilde{\chi}' \circ \tilde{\phi}$ and $q = \tilde{\chi}^{-1} \circ \hat{\tilde{\phi}}$. □

Lemma 4.8. *The isogeny $\sigma\colon C' \to \tilde{C}'$ given by $(u, v) \mapsto \left(\frac{u}{a^2} - \frac{1}{a}, -\frac{v}{a^3}\right)$ defines an isomorphism between C' and $\tilde{C}'$. Its inverse is given by the morphism $\tau : \tilde{C}' \to C', (\tilde{u}, \tilde{v}) \mapsto \left(\frac{\tilde{u}}{\tilde{a}^2} - \frac{1}{\tilde{a}}, \frac{\tilde{v}}{\tilde{a}^3}\right)$.*

Proof. We have

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

since $\tilde{a} = -\frac{1}{a}$ and $\tilde{d} = 1 - d$. Hence, we have

$$\begin{aligned}\left(\frac{u}{a^2} - \frac{1}{a}\right)\left(\frac{u}{a^2} - \frac{1}{a} - \tilde{a}\right)\left(\frac{u}{a^2} - \frac{1}{a} - \tilde{d}\tilde{a}\right) &= \frac{u(u-a)(u-da)}{a^6} \\ &= \frac{v^2}{a^6} \\ &= \left(-\frac{v}{a^3}\right)^2\end{aligned}$$

and so the map σ is well defined.
The curve C' in $\mathbb{P}^2(U, V, W)$ is given by the equation

$$V^2W = U^3 - a(d+1)U^2W + a^2dUW^2$$

and the map σ by

$$[U : V : W] \mapsto [-aU + a^2W : V : -a^3W].$$

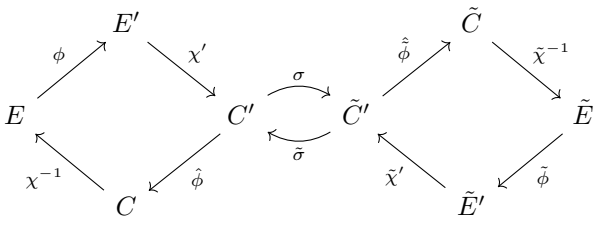
We see that $\sigma(O_{C'}) = \sigma([0:1:0]) = [0:1:0] = O_{\tilde{C}'}$ so σ is indeed an isogeny.

Let now $(\tilde{u}, \tilde{v})$ be a point on $\tilde{C}'$. Then

$$\sigma(\tau(\tilde{u}, \tilde{v}))) = \sigma\left(\frac{\tilde{u}}{\tilde{a}^2} - \frac{1}{\tilde{a}}, \frac{\tilde{v}}{\tilde{a}^3}\right) = \left(\tilde{a}^2\left(\frac{\tilde{u}}{\tilde{a}^2} - \frac{1}{\tilde{a}}\right) + \tilde{a}, -\tilde{a}^3\frac{-\tilde{v}}{\tilde{a}^3}\right) = (\tilde{u} - \tilde{a} + \tilde{a}, \tilde{v}) = (\tilde{u}, \tilde{v}).$$

so σ defines indeed an bijection $C' \to \tilde{C}'$ with inverse τ. □

Consider now the map $\tilde{\sigma}\colon \tilde{C}' \to C'$ defined by $(\tilde{u}, \tilde{v}) \mapsto \left(\frac{\tilde{u}}{\tilde{a}^2} - \frac{1}{\tilde{a}}, -\frac{\tilde{v}}{\tilde{a}^3}\right)$. We have $\tilde{\sigma} = -\tau$, so $\sigma \circ \tilde{\sigma} = \tilde{\sigma} \circ \sigma = [-1]$. To summarize, we get the following diagram



where going around the left square yields the map $[-2]\colon E \to E, P \mapsto -2P$, going around the right square yields the map $[-2]\colon \tilde{E} \to \tilde{E}, P \mapsto 2P$ and $\sigma \circ \tilde{\sigma} = [-1]$.

Lemma 4.9. *The morphism $\psi\colon E \to \tilde{E}$ is equal to the composition $\tilde{\chi}^{-1} \circ \hat{\tilde{\phi}} \circ \sigma \circ \chi' \circ \phi$.*

Proof. For (x, y) on E, we have

$$(\sigma \circ \chi' \circ \phi)(x, y) = \sigma(\chi'(x^2, xy, y^2)) = \sigma\left(\frac{a^2}{x^2}, \frac{a^2(x^2 - a)}{x^3 y}\right) = \left(\frac{a - x^2}{ax^2}, -\frac{x^2 - a}{ax^3 y}\right).$$

Now the map $\hat{\tilde{\phi}}\colon \tilde{C}' \to \tilde{C}$ is given by $(\tilde{u}, \tilde{v}) \mapsto \left(\tilde{u} - \tilde{a}(\tilde{d} + 1) + \frac{\tilde{a}^2\tilde{d}}{\tilde{u}}, \tilde{v} - \frac{\tilde{a}^2\tilde{d}\tilde{v}}{\tilde{u}^2}\right)$, i.e. by

$$(\tilde{u}, \tilde{v}) \mapsto \left(\tilde{u} + \frac{(2 - d)}{a} + \frac{1 - d}{a^2\tilde{u}}, \tilde{v} - \frac{(1 - d)\tilde{v}}{a^2\tilde{u}^2}\right).$$

Hence for (x, y) on E, we get

$$\begin{aligned}
\hat{\tilde{\phi}}(\sigma(\chi'(\phi(x, y)))) &= \hat{\tilde{\phi}}\left(\frac{a - x^2}{ax^2}, -\frac{x^2 - a}{ax^3 y}\right) \\
&= \left(\frac{(a - x^2)^2 + (2 - d)x^2(a - x^2) + (1 - d)x^4}{ax^2(a - x^2)}, \frac{(x^2 - a)^2 - (1 - d)x^4}{ayx^3(a - x^2)}\right) \\
&= \left(\frac{a^2 - adx^2}{ax^2(a - x^2)}, -\frac{2ax^2 - dx^4 - a^2}{ayx^3(a - x^2)}\right) \\
&= \left(\frac{a^2 - a(\frac{x^2 + ay^2 - a}{y^2})}{ax^2(a - x^2)}, -\frac{2ax^2 - x^2\frac{x^2 + ay^2 - a}{y^2} - a^2}{ayx^3(a - x^2)}\right) \\
&= \left(\frac{1}{x^2y^2}, -\frac{(a - x^2)(x^2 - ay^2)}{ay^3x^3(a - x^2)}\right) \\
&= \left(\frac{1}{x^2y^2}, -\frac{(x^2 - ay^2)}{ay^3x^3}\right)
\end{aligned}$$

and the map $\tilde{\chi}^{-1}$ is given by $(\tilde{\xi}, \tilde{\eta}) \mapsto \left(2\tilde{a}\frac{\tilde{\xi}}{\tilde{\eta}}, \frac{\tilde{\xi} + \tilde{a}(\tilde{d} - 1)}{\tilde{\xi} - \tilde{a}(\tilde{d} - 1)}\right)$, i.e. by $(\tilde{\xi}, \tilde{\eta}) \mapsto \left(-\frac{2\tilde{\xi}}{a\tilde{\eta}}, \frac{a\tilde{\xi} + d}{a\tilde{\xi} - d}\right)$. So we get

$$\begin{aligned}
\tilde{\chi}^{-1}(\hat{\tilde{\phi}}(\sigma(\chi'(\phi(x, y))))) &= \tilde{\chi}^{-1}\left(\frac{1}{x^2y^2}, -\frac{(x^2 - ay^2)}{ay^3x^3}\right) \\
&= \left(\frac{2 \cdot ay^3x^3}{ax^2y^2(x^2 - ay^2)}, \frac{a + dx^2y^2}{a - dx^2y^2}\right) \\
&= \left(\frac{2xy}{x^2 - ay^2}, \frac{x^2 + ay^2}{2a - x^2 - ay^2}\right).
\end{aligned}$$

Hence we have that $\tilde{\chi}^{-1} \circ \hat{\tilde{\phi}} \circ \sigma \circ \chi' \circ \phi = \psi$. □

Define now $\tilde{\psi}\colon \tilde{E} \to E$ be the morphism

$$(\tilde{x}, \tilde{y}) \mapsto \left(\frac{2\tilde{x}\tilde{y}}{\tilde{x}^2 - \tilde{a}\tilde{y}^2}, \frac{\tilde{x}^2 + \tilde{a}\tilde{y}^2}{2\tilde{a} - \tilde{x}^2 - \tilde{a}\tilde{y}^2}\right).$$

This is well defined by Theorem 4.1.

Theorem 4.10. *The morphism $E \to E$ given by the composite $\tilde{\psi} \circ \psi$ is equal to multiplication by -4 in the group law of E.*

Proof. By Lemma 4.9, we also have similarly that $\tilde{\psi} \colon \tilde{E} \to E$ given by $(\tilde{x}, \tilde{y}) \mapsto \left(\frac{2\tilde{x}\tilde{y}}{\tilde{x}^2 - \tilde{a}\tilde{y}^2}, \frac{\tilde{x}^2 + \tilde{a}\tilde{y}^2}{2\tilde{a} - \tilde{x}^2 - \tilde{a}\tilde{y}^2} \right)$ is equal to $\chi^{-1} \circ \hat{\phi} \circ \tilde{\sigma} \circ \tilde{\chi}' \circ \tilde{\phi}$. Hence from Lemma 4.5 and Lemma 4.7, we get

$$\begin{aligned}
\tilde{\psi} \circ \psi &= \chi^{-1} \circ \hat{\phi} \circ \tilde{\sigma} \circ \tilde{\chi}' \circ \tilde{\phi} \circ \tilde{\chi}^{-1} \circ \hat{\tilde{\phi}} \circ \sigma \circ \chi' \circ \phi \\
&= \chi^{-1} \circ \hat{\phi} \circ \tilde{\sigma} \circ [-2] \circ \sigma \circ \chi' \circ \phi \\
&= [-2] \circ \chi^{-1} \circ \hat{\phi} \circ [-1] \circ \chi' \circ \phi \\
&= [2] \circ \chi^{-1} \circ \hat{\phi} \circ \chi' \circ \phi \\
&= [2] \circ [-2] \\
&= [-4]
\end{aligned}$$

which completes the proof. □

This implies that the map $E \to E$ given by the composite $\iota \circ \hat{\psi} \circ \psi$, where $\iota \colon E \to E$ is the map $(x, y) \mapsto (-x, y)$, is equal to multiplication by 4 in the group law of E.
It could be interesting to use the 4-isogeny ψ constructed in this section to do a descent by 4-isogeny on Edwards curve. Unfortunately, this is beyond the scope of this thesis since the computations appeared to be more cumbersome than expected.

References

[1] Martin Bright. *Descent by 2-isogeny*. URL: `http://www.boojum.org.uk/maths/descent.pdf`.

[2] Robin Hartshorne. *Algebraic geometry*. eng. Graduate texts in mathematics ; 52. New York: Springer Science+Business Media, Inc, 2010. ISBN: 9781475738490.

[3] David Kohel. "Addition law structure of elliptic curves". eng. In: *Journal of number theory* 131.5 (2011), pp. 894–919. ISSN: 0022-314X.

[4] J.P. Serre. *Cours d'arithmétique*. Collection SUP.: Mathématicien. Presses universitaires de France, 1977.

[5] Joe Silverman and John Tate. *Rational Points on Elliptic Curves*. eng. 2nd ed. 2015. Undergraduate Texts in Mathematics. Cham : Cham: Springer International Publishing ; Imprint: Springer, 2015. ISBN: 9783319185880.

[6] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. eng. 2nd ed. Graduate texts in mathematics. Springer New York, NY, 2009.

[7] Michael Stoll. *Linear Algebra II*. 2007.