A complete set of addition laws for incomplete Edwards curves

Daniel J. Bernstein[a], Tanja Lange[b]

[a] *Department of Computer Science (MC 152)*
University of Illinois at Chicago
Chicago, IL 60607–7053
USA
[b] *Department of Mathematics and Computer Science*
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven
Netherlands

Abstract

Edwards curves were the first curves shown to have a complete addition law. However, the completeness of the addition law depends on the curve parameters and even a complete Edwards curve becomes incomplete over a quadratic field extension. This paper covers arbitrary Edwards curves and gives a set of two addition laws that for any pair of input points P_1, P_2 produce the sum $P_1 + P_2$.

Key words: Elliptic curves, Edwards curves, complete addition law, points at infinity.

1. Introduction

This paper presents a complete set of two addition laws for arbitrary Edwards curves, and more generally twisted Edwards curves, embedded into $\mathbf{P}^1 \times \mathbf{P}^1$. Specifically, what this paper shows is that

$$((X_1 : Z_1), (Y_1 : T_1)) + ((X_2 : Z_2), (Y_2 : T_2)) =$$
$$\begin{cases} \big((X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 : Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2), \\ \quad (Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 : Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2)\big) & \text{if defined,} \\ \big((X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1 : aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2), \\ \quad (X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1 : X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2)\big) & \text{if defined} \end{cases}$$

is a complete set of addition laws for the curve

$$\overline{\mathrm{E}}_{\mathrm{E},a,d} = \left\{((X : Z), (Y : T)) \in \mathbf{P}^1 \times \mathbf{P}^1 : aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2\right\}$$

whenever a, d are distinct nonzero elements of a field k with $\mathrm{char}(k) \neq 2$. These two addition laws cover all possible pairs of curve points; the outputs coincide if they are both defined; each defined output is on the curve; and this addition turns the set of curve points into a group.

For Weierstrass curves embedded in $\mathbf{P}^2$, Bosma and Lenstra proved in [6] that the minimal cardinality of a complete set of addition laws is 2, and they provided a complete set of 2 addition laws, improving upon the set of 3 addition laws given in [12] (and earlier in [11, Section 3] for the case of short Weierstrass

*Permanent ID of this document: `a5f451aa5d649b88126facfc4303065d`. Date of this document: 2010.10.06. This work has been supported in part by the European Commission through the ICT Programme under Contract ICT–2007–216676 ECRYPT-II, in part by the National Science Foundation under grant ITR–0716498, and in part by the beautiful atmosphere of Costa Adeje, Tenerife, Spain.

Email addresses: `djb@cr.yp.to` (Daniel J. Bernstein), `tanja@hyperelliptic.org` (Tanja Lange)
URL: `cr.yp.to/djb.html` (Daniel J. Bernstein), `hyperelliptic.org/tanja` (Tanja Lange)

$$
\begin{aligned}
&(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = \\
&\quad\begin{cases}
\big(a_4X_1^2Z_2^2 - 2X_1Y_1Y_2Z_2 - X_1Z_1Y_2^2 + 3a_6X_1Z_1Z_2^2 \\
\qquad + Y_1^2X_2Z_2 + 2Y_1Z_1X_2Y_2 - a_4Z_1^2X_2^2 - 3a_6Z_1^2X_2Z_2 : \\
\quad 3X_1^2X_2Y_2 - 3X_1Y_1X_2^2 - a_4X_1Y_1Z_2^2 + 2a_4X_1Z_1Y_2Z_2 + Y_1^2Y_2Z_2 \\
\qquad - 2a_4Y_1Z_1X_2Z_2 - Y_1Z_1Y_2^2 - 3a_6Y_1Z_1Z_2^2 + a_4Z_1^2X_2Y_2 + 3a_6Z_1^2Y_2Z_2 : \\
\quad - 3X_1^2X_2Z_2 + 3X_1Z_1X_2^2 - a_4X_1Z_1Z_2^2 + Y_1^2Z_2^2 + a_4Z_1^2X_2Z_2 - Z_1^2Y_2^2\big) & \text{if defined,} \\
\big(a_4X_1^2X_2Z_2 + X_1^2Y_2^2 + 3a_6X_1^2Z_2^2 - a_4X_1Z_1X_2^2 \\
\qquad - a_4^2X_1Z_1Z_2^2 - Y_1^2X_2^2 - 3a_6Z_1^2X_2^2 + a_4^2Z_1^2X_2Z_2 : \\
\quad a_4X_1^2Y_2Z_2 - 2a_4X_1Y_1X_2Z_2 + X_1Y_1Y_2^2 - 3a_6X_1Y_1Z_2^2 \\
\qquad + 2a_4X_1Z_1X_2Y_2 + 6a_6X_1Z_1Y_2Z_2 - Y_1^2X_2Y_2 - a_4Y_1Z_1X_2^2 \\
\qquad - 6a_6Y_1Z_1X_2Z_2 + a_4^2Y_1Z_1Z_2^2 + 3a_6Z_1^2X_2Y_2 - a_4^2Z_1^2Y_2Z_2 : \\
\quad - a_4X_1^2Z_2^2 - 2X_1Y_1Y_2Z_2 + X_1Z_1Y_2^2 - 3a_6X_1Z_1Z_2^2 \\
\qquad - Y_1^2X_2Z_2 + 2Y_1Z_1X_2Y_2 + a_4Z_1^2X_2^2 + 3a_6Z_1^2X_2Z_2\big) & \text{if defined,} \\
\big(-2a_4X_1^2Y_2Z_2 - 4a_4X_1Y_1X_2Z_2 + 2X_1Y_1Y_2^2 - 6a_6X_1Y_1Z_2^2 \\
\qquad - 4a_4X_1Z_1X_2Y_2 - 12a_6X_1Z_1Y_2Z_2 + 2Y_1^2X_2Y_2 - 2a_4Y_1Z_1X_2^2 \\
\qquad - 12a_6Y_1Z_1X_2Z_2 + 2a_4^2Y_1Z_1Z_2^2 - 6a_6Z_1^2X_2Y_2 + 2a_4^2Z_1^2Y_2Z_2 : \\
\quad 6a_4X_1^2X_2^2 + 18a_6X_1^2X_2Z_2 - 2a_4^2X_1^2Z_2^2 + 18a_6X_1Z_1X_2^2 \\
\qquad - 8a_4^2X_1Z_1X_2Z_2 - 6a_4a_6X_1Z_1Z_2^2 + 2Y_1^2Y_2^2 - 2a_4^2Z_1^2X_2^2 \\
\qquad - 6a_4a_6Z_1^2X_2Z_2 + (-2a_4^3 - 18a_6^2)Z_1^2Z_2^2 : \\
\quad 6X_1^2X_2Y_2 + 6X_1Y_1X_2^2 + 2a_4X_1Y_1Z_2^2 + 4a_4X_1Z_1Y_2Z_2 + 2Y_1^2Y_2Z_2 \\
\qquad + 4a_4Y_1Z_1X_2Z_2 + 2Y_1Z_1Y_2^2 + 6a_6Y_1Z_1Z_2^2 + 2a_4Z_1^2X_2Y_2 + 6a_6Z_1^2Y_2Z_2\big) & \text{if defined.}
\end{cases}
\end{aligned}
$$

Figure 1.1: The H. Lange–Ruppert complete set of three addition laws for a short Weierstrass curve $\{(X : Y : Z) \in \mathbf{P}^2 : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3\}$. We obtained this from [12, Proposition 2.1] by substituting $a_1 = a_2 = a_3 = 0$; replacing "$(x_0 : x_1 : x_2)$" with $(Z_1 : X_1 : Y_1)$, "$(y_0 : y_1 : y_2)$" with $(Z_2 : X_2 : Y_2)$, etc.; and sorting terms. For more general Weierstrass curves except in characteristic 2, see [12, Proposition 2.1] with the correction stated by Bosma and Lenstra in [6, page 240], namely changing "$a_1b_6 + a_3b_4$" to "$a_1b_6 + a_3a_4$". For characteristic 2, see [12, Theorem 2.2], and note the change of scale from "$Z^{(3)}$" to "$Z^{(4)}$".

curves). For elliptic curves in other shapes no similar result was known until now. H. Lange and Ruppert had shown in [11] that any abelian variety has a complete system of low-degree addition laws, but had also commented that "The proof is nonconstructive ... To determine explicitly a complete system of addition laws requires tedious computations already in the easiest case of an elliptic curve in Weierstrass normal form." See Figure 1.1 for the H. Lange–Ruppert laws (in the short-Weierstrass case), and Figure 1.2 for the Bosma–Lenstra laws.

The addition laws in this paper are much simpler, much easier to prove, and much more efficient than the addition laws in [11], [12], and [6]. Applications of elliptic-curve groups in cryptography and computer algebra can use the $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ group for any curve expressible in twisted Edwards form, often gaining speed without creating any troublesome failure cases. Note that every elliptic curve outside characteristic 2 can be expressed in Edwards form at the expense of a small field extension; see [2, Theorem 3.3]. Note also that our addition laws are open (i.e., each law computes $P + Q$ for a nonempty open set of pairs (P, Q), as in [11], [12], and [6]) and therefore usable for elliptic-curve addition over any finite ring containing $1/2$, by an adaptation of the procedures discussed in [13, Section 3] and [6, page 231].

For affine inputs $((x : 1), (y : 1))$, our first addition law is exactly the Edwards addition law. We showed in [4, Theorem 3.3] that the Edwards addition law for the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ has no exceptional cases defined over k if the curve parameter d is not a square in k. More generally, the Edwards

$$
\begin{aligned}
&(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = \\
&\quad \begin{cases}
\big(a_4 X_1^2 Z_2^2 - 2X_1 Y_1 Y_2 Z_2 - X_1 Z_1 Y_2^2 + 3a_6 X_1 Z_1 Z_2^2 \\
\qquad + Y_1^2 X_2 Z_2 + 2Y_1 Z_1 X_2 Y_2 - a_4 Z_1^2 X_2^2 - 3a_6 Z_1^2 X_2 Z_2 : \\
\quad 3X_1^2 X_2 Y_2 - 3X_1 Y_1 X_2^2 - a_4 X_1 Y_1 Z_2^2 + 2a_4 X_1 Z_1 Y_2 Z_2 + Y_1^2 Y_2 Z_2 \\
\qquad - 2a_4 Y_1 Z_1 X_2 Z_2 - Y_1 Z_1 Y_2^2 - 3a_6 Y_1 Z_1 Z_2^2 + a_4 Z_1^2 X_2 Y_2 + 3a_6 Z_1^2 Y_2 Z_2 : \\
\quad - 3X_1^2 X_2 Z_2 + 3X_1 Z_1 X_2^2 - a_4 X_1 Z_1 Z_2^2 + Y_1^2 Z_2^2 + a_4 Z_1^2 X_2 Z_2 - Z_1^2 Y_2^2\big) & \text{if defined,} \\
\big(a_4 X_1^2 Y_2 Z_2 + 2a_4 X_1 Y_1 X_2 Z_2 - X_1 Y_1 Y_2^2 + 3a_6 X_1 Y_1 Z_2^2 \\
\qquad + 2a_4 X_1 Z_1 X_2 Y_2 + 6a_6 X_1 Z_1 Y_2 Z_2 - Y_1^2 X_2 Y_2 + a_4 Y_1 Z_1 X_2^2 \\
\qquad + 6a_6 Y_1 Z_1 X_2 Z_2 - a_4^2 Y_1 Z_1 Z_2^2 + 3a_6 Z_1^2 X_2 Y_2 - a_4^2 Z_1^2 Y_2 Z_2 : \\
\quad - 3a_4 X_1^2 X_2^2 - 9a_6 X_1^2 X_2 Z_2 + a_4^2 X_1^2 Z_2^2 - 9a_6 X_1 Z_1 X_2^2 \\
\qquad + 4a_4^2 X_1 Z_1 X_2 Z_2 + 3a_4 a_6 X_1 Z_1 Z_2^2 - Y_1^2 Y_2^2 + a_4^2 Z_1^2 X_2^2 \\
\qquad + 3a_4 a_6 Z_1^2 X_2 Z_2 + (a_4^3 + 9a_6^2) Z_1^2 Z_2^2 : \\
\quad - 3X_1^2 X_2 Y_2 - 3X_1 Y_1 X_2^2 - a_4 X_1 Y_1 Z_2^2 - 2a_4 X_1 Z_1 Y_2 Z_2 - Y_1^2 Y_2 Z_2 \\
\qquad - 2a_4 Y_1 Z_1 X_2 Z_2 - Y_1 Z_1 Y_2^2 - 3a_6 Y_1 Z_1 Z_2^2 - a_4 Z_1^2 X_2 Y_2 - 3a_6 Z_1^2 Y_2 Z_2\big) & \text{if defined.}
\end{cases}
\end{aligned}
$$

Figure 1.2: The Bosma–Lenstra complete set of two addition laws for a short Weierstrass curve $\{(X : Y : Z) \in \mathbf{P}^2 : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3\}$. We obtained this from [6, pages 236–238] by negating all terms (for consistency with the first definition of "$Z_3^{(1)}$" in [6, page 236]); correcting "$(3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1)$" to "$(3a_2a_6 - a_4^2)(-2X_1Z_2 - X_2Z_1)X_2Z_1$" in the second Y output; substituting $a_1 = a_2 = a_3 = 0$; and sorting terms. For more general Weierstrass curves one can take the formulas from [6], make the same correction in the second Y output, and make an additional correction of "$a_3a_4(X_1Z_2 - 2X_2Z_1)X_2Z_1$" to "$a_3a_4(-2X_1Z_2 - X_2Z_1)X_2Z_1$" in the second X output. The corrections stated here were pointed out several years ago by Nicole L. Pitcher. The similarities between Figure 1.1 and Figure 1.2 follow from [6, page 240, first full paragraph].

addition law for the twisted Edwards curve $ax^2 + y^2 = 1 + dx^2y^2$ has no exceptional cases if d and a/d are not squares in k. However, over $k(\sqrt{d})$ or $k(\sqrt{a/d})$ there are points at infinity, and no study of how to handle these points has appeared in the literature.

Hisil et al. in [9] introduced a different addition law on affine twisted Edwards curves, and showed for generic pairs of input points that the addition law produces the same results as the Edwards addition law. Our second addition law is, for affine inputs, exactly the addition law from Hisil et al. It turns out that, on the closure of the curve in $\mathbf{P}^1 \times \mathbf{P}^1$, this second law handles all of the inputs and outputs at infinity that are not handled by the first law. We refer to the second addition law as the "dual addition law" for reasons discussed in Section 8, and we refer to the first addition law as the "original addition law".

Note that for a doubling (i.e., an addition where both inputs are the same) one can simplify the formulas with the help of the curve equation. Readers interested in the exact speed of explicit formulas for the original addition law, the dual addition law, doublings, triplings, etc. should consult, e.g., [4], [2], [9], and [3]. See the Explicit-Formulas Database [5] for a broader view covering many more curve shapes.

2. Review of Edwards curves

Edwards in [7] introduced a new normal form of elliptic curves. He showed that every elliptic curve over $\mathbf{Q}$ can be written in this normal form over an extension of $\mathbf{Q}$. More generally, every elliptic curve over a field k with $2 \neq 0$ can be written in this normal form over an extension of k. To reduce the need for extensions we use the slightly generalized form of Edwards curves introduced in [4].

An Edwards curve, at the level of generality of [4], is given by an equation of the form $x^2 + y^2 = 1 + dx^2y^2$, for some $d \notin \{0, 1\}$. The Edwards addition law is given by

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

The addition law is strongly unified; i.e., the same formulas can also be used for doubling. The point $(0,1)$ is the neutral element of the addition law. The negative of a point (x,y) is $(-x,y)$.

If d is not a square then, by [4, Theorem 3.3], the Edwards addition law is complete: the denominators $1+dx_1x_2y_1y_2$ and $1-dx_1x_2y_1y_2$ are always nonzero, and the points (x,y) on the curve form a group. However, if d is a square then the addition law is not necessarily a group law: there can be pairs (x_1,y_1) and (x_2,y_2) where $1+dx_1x_2y_1y_2=0$ or $1-dx_1x_2y_1y_2=0$.

3. Review of twisted Edwards curves

For some additional generality we use the *twisted Edwards curve* $\mathrm{E}_{\mathrm{E},a,d}$ given by

$$\mathrm{E}_{\mathrm{E},a,d} : ax^2+y^2 = 1+dx^2y^2,$$

where a,d are distinct nonzero elements of k. We introduced this generalization together with Birkner, Joye, and Peters in [2].

If $a\bar{d}=\bar{a}d$ then the two curves $\mathrm{E}_{\mathrm{E},a,d}$ and $\mathrm{E}_{\mathrm{E},\bar{a},\bar{d}}$ are isomorphic over $k(\sqrt{a/\bar{a}})$ and therefore quadratic twists over k. An isomorphism is given by $(x,y)\mapsto(\bar{x},\bar{y})=(x\sqrt{a/\bar{a}},y)$.

The Edwards addition law generalizes immediately to the addition law

$$(x_1,y_1),(x_2,y_2)\mapsto\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2}\right)$$

on a twisted Edwards curve. The neutral element and negation are unchanged.

The twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d}$ is birationally equivalent to the Montgomery curve $\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3+Au^2+u$, where $A=2(a+d)/(a-d)$ and $B=4/(a-d)$. The map $(x,y)\mapsto(u,v)=((1+y)/(1-y),(1+y)/((1-y)x))$ is a birational equivalence from $\mathrm{E}_{\mathrm{E},a,d}$ to $\mathrm{E}_{\mathrm{M},A,B}$, with inverse $(u,v)\mapsto(x,y)=(u/v,(u-1)/(u+1))$.

As pointed out in [2] the map from $\mathrm{E}_{\mathrm{E},a,d}$ is undefined at $(0,\pm1)$. The map from $\mathrm{E}_{\mathrm{M},A,B}$ is undefined at $(0,0)$, at $(-1,\pm\sqrt{(A-2)/B})=(-1,\pm\sqrt{d})$, and at $((-A\pm\sqrt{A^2-4})/2,0)=((1\mp\sqrt{a/d})/(1\pm\sqrt{a/d}),0)$; furthermore, the point at infinity on $\mathrm{E}_{\mathrm{M},A,B}$ is not covered by the map between affine curves. To study the corresponding points on $\mathrm{E}_{\mathrm{E},a,d}$ we consider two different embeddings of the affine curve, first into $\mathbf{P}^2$ (Section 4) and then into $\mathbf{P}^1\times\mathbf{P}^1$ (Section 5).

4. Embedding of $\mathrm{E}_{\mathrm{E},a,d}$ into $\mathbf{P}^2$

The projective closure of $\mathrm{E}_{\mathrm{E},a,d}$ in $\mathbf{P}^2$ is

$$\left\{(X:Y:Z)\in\mathbf{P}^2 : aX^2Z^2+Y^2Z^2=Z^4+dX^2Y^2\right\}.$$

This curve consists of the points (x,y) on the affine curve $\mathrm{E}_{\mathrm{E},a,d}$, embedded as usual into $\mathbf{P}^2$ by $(x,y)\mapsto(x:y:1)$, and extra points at infinity, i.e., points where $Z=0$. There are exactly two such points, namely $\Omega_1=(1:0:0)$ and $\Omega_2=(0:1:0)$. These points are singular.

A blowup of $\mathrm{E}_{\mathrm{E},a,d}$ around Ω_1 is $a+\bar{y}^2z^2=z^2+d\bar{y}^2$, where we put $y=\bar{y}z$. Above Ω_1 there are two distinct points $(\bar{y},z)=(\pm\sqrt{a/d},0)$. These points are minimally defined over $k(\sqrt{a/d})$.

A blowup of $\mathrm{E}_{\mathrm{E},a,d}$ around Ω_2 is $a\bar{x}^2z^2+1=z^2+d\bar{x}^2$, where we put $x=\bar{x}z$. Above Ω_2 there are two distinct points $(\bar{x},z)=(\pm1/\sqrt{d},0)$. These points are minimally defined over $k(\sqrt{d})$.

This projective closure is useful for computations in two ways. First, expressing the addition law on coordinates $(X:Y:Z)$ avoids inversions and leads to extremely fast arithmetic, as discussed in [4]. Second, the points Ω_1 and Ω_2 are important in formulating a geometric interpretation of the addition law, as used in computing pairings; see [1].

If d and a/d are not squares then the k-rational points of the projective closure are the k-rational points of the affine curve and form a group. However, one cannot distinguish the points over Ω_1 if a/d is a square, or over Ω_2 if d is a square; either way, the points of the projective closure do not form a group.

5. Embedding of $\mathbf{E}_{\mathbf{E},a,d}$ into $\mathbf{P}^1 \times \mathbf{P}^1$

The projective closure of $\mathrm{E}_{\mathrm{E},a,d}$ in $\mathbf{P}^1 \times \mathbf{P}^1$ is

$$\overline{\mathrm{E}}_{\mathrm{E},a,d} = \left\{((X:Z),(Y:T)) \in \mathbf{P}^1 \times \mathbf{P}^1 : aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2\right\}.$$

This curve consists of the points (x, y) on the affine curve $\mathrm{E}_{\mathrm{E},a,d}$, embedded as usual into $\mathbf{P}^1 \times \mathbf{P}^1$ by $(x, y) \mapsto ((x : 1), (y : 1))$, and extra points at infinity, i.e., points where $(X : Z) = (1 : 0)$ or $(Y : T) = (1 : 0)$.

At $(X : Z) = (1 : 0)$ the curve equation is $aT^2 = dY^2$. There are two points here, namely $((X : Z), (Y : T)) = ((1 : 0), (\pm\sqrt{a/d} : 1))$. These points are minimally defined over $k(\sqrt{a/d})$.

At $(Y : T) = (1 : 0)$ the curve equation is $Z^2 = dX^2$. There are also two points here, namely $((X : Z), (Y : T)) = ((1 : \pm\sqrt{d}), (1 : 0))$. These points are minimally defined over $k(\sqrt{d})$.

The rational map $((X : Z), (Y : T)) \mapsto (XT : YZ : TZ)$ from $\mathbf{P}^1 \times \mathbf{P}^1$ to $\mathbf{P}^2$ is defined on all points of $\overline{\mathrm{E}}_{\mathrm{E},a,d}$. It maps $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ onto the projective closure of $\mathrm{E}_{\mathrm{E},a,d}$ in $\mathbf{P}^2$. It is bijective on the affine points, maps both points $((1 : 0), (\pm\sqrt{a/d} : 1))$ to Ω_1, and maps both points $((1 : \pm\sqrt{d}), (1 : 0))$ to Ω_2.

6. Group law on $\overline{\mathbf{E}}_{\mathbf{E},a,d}$

The original Edwards addition law readily generalizes to an addition law for $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$, but it has exceptional cases if d or a/d is a square in k. The dual addition law from Hisil et al. also generalizes to an addition law for $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$, also having exceptional cases.

We show in this section that these two addition laws together form a complete set of addition laws for $\overline{\mathrm{E}}_{\mathrm{E},a,d}$. Specifically, for each pair of points $P_1, P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}$, at least one of the addition laws produces output in $\mathbf{P}^1 \times \mathbf{P}^1$; furthermore, if both addition laws produce output in $\mathbf{P}^1 \times \mathbf{P}^1$, then the outputs are the same; finally, each output in $\mathbf{P}^1 \times \mathbf{P}^1$ is in $\overline{\mathrm{E}}_{\mathrm{E},a,d}$. We denote the resulting element of $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ as $P_1 + P_2$.

We show later in the paper that addition on $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ matches, in all cases, standard chord-and-tangent addition on the Montgomery curve $\mathrm{E}_{\mathrm{M},A,B}$ where $A = 2(a + d)/(a - d)$ and $B = 4/(a - d)$. Consequently $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ is a group. The fact that $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ is a group can also be proven directly.

Our proof that outputs from the original addition law are in $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ generalizes [4, Theorem 3.1] from affine points on Edwards curves to arbitrary points on twisted Edwards curves. Our proof that outputs from the dual addition law are in $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ is new.

Theorem 6.1. *Fix a field k with $\mathrm{char}(k) \neq 2$. Fix distinct nonzero elements $a, d \in k$. Fix $P_1, P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$. Write P_1 as $((X_1 : Z_1), (Y_1 : T_1))$ and write P_2 as $((X_2 : Z_2), (Y_2 : T_2))$. Define*

$$\begin{aligned}
X_3 &= X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,\\
Z_3 &= Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,\\
Y_3 &= Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2,\\
T_3 &= Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2;
\end{aligned}$$

and

$$\begin{aligned}
X_3' &= X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,\\
Z_3' &= aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,\\
Y_3' &= X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,\\
T_3' &= X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.
\end{aligned}$$

Then $X_3Z_3' = X_3'Z_3$ and $Y_3T_3' = Y_3'T_3$. Furthermore, at least one of the following cases occurs:

- *$(X_3, Z_3) \neq (0, 0)$ and $(Y_3, T_3) \neq (0, 0)$.*
- *$(X_3', Z_3') \neq (0, 0)$ and $(Y_3', T_3') \neq (0, 0)$.*

Proof. **Part 1.** Observe that

$$\begin{aligned}
X_3Z_3' &= (X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2)(aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2) \\
&= (aX_2^2T_2^2 + Y_2^2Z_2^2)X_1Y_1Z_1T_1 + (aX_1^2T_1^2 + Y_1^2Z_1^2)X_2Y_2Z_2T_2 \\
&= (Z_2^2T_2^2 + dX_2^2Y_2^2)X_1Y_1Z_1T_1 + (Z_1^2T_1^2 + dX_1^2Y_1^2)X_2Y_2Z_2T_2 \\
&= (X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1)(Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2) = X_3'Z_3.
\end{aligned}$$

Similarly

$$\begin{aligned}
Y_3T_3' &= (Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2)(X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2) \\
&= (Y_2^2Z_2^2 + aX_2^2T_2^2)X_1Y_1Z_1T_1 - (Y_1^2Z_1^2 + aX_1^2T_1^2)X_2Y_2Z_2T_2 \\
&= (Z_2^2T_2^2 + dX_2^2Y_2^2)X_1Y_1Z_1T_1 - (Z_1^2T_1^2 + dX_1^2Y_1^2)X_2Y_2Z_2T_2 \\
&= (X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1)(Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2) = Y_3'T_3.
\end{aligned}$$

Part 2. Assume that $(X_3, Z_3) = (0,0)$; i.e., $X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 = 0$ and $Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2 = 0$. The following calculations show that $(X_3', Z_3') \neq (0,0)$ and $(Y_3', T_3') \neq (0,0)$.

Consider first the possibility that $T_1 = 0$. Then $Y_1 \neq 0$ (since $(Y_1 : T_1) \in \mathbf{P}^1$), and the curve equation for P_1 implies $Z_1^2 = dX_1^2$ and $X_1, Z_1 \neq 0$. The equations $X_3 = 0$ and $Z_3 = 0$ simplify to $X_2T_2 = 0$ and $X_2Y_2 = 0$, so $X_2 = 0$, so $Z_2 \neq 0$. Now the curve equation for P_2 implies $Y_2^2 = T_2^2$ and $Y_2, T_2 \neq 0$. Hence $X_3' = X_1Y_1Z_2T_2 \neq 0$ and $Y_3' = X_1Y_1Z_2T_2 \neq 0$.

Consider next the possibility that $Z_2 = 0$. Then $X_2 \neq 0$, and the curve equation for P_2 implies $aT_2^2 = dY_2^2$ and $Y_2, T_2 \neq 0$. The equations $X_3 = 0$ and $Z_3 = 0$ simplify to $Y_1Z_1 = 0$ and $X_1Y_1 = 0$, so $Y_1 = 0$, so $T_1 \neq 0$. Now the curve equation for P_1 implies $aX_1^2 = Z_1^2$ and $X_1, Z_1 \neq 0$. Hence $X_3' = X_2Y_2Z_1T_1 \neq 0$ and $Y_3' = -X_2Y_2Z_1T_1 \neq 0$.

The same arguments, exchanging indices 1 and 2, also apply if $T_2 = 0$ or if $Z_1 = 0$. Assume from now on that $T_1 \neq 0$, $T_2 \neq 0$, $Z_1 \neq 0$, and $Z_2 \neq 0$.

Multiply the equation $X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 = 0$ by dX_1Y_2, multiply the equation $Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2 = 0$ by Z_1T_2, subtract, and divide by Z_2T_1, to see that $dX_1^2Y_2^2 = Z_1^2T_2^2$. Define $r = X_1Y_2/(Z_1T_2)$; then $r^2 = 1/d$ and $-rZ_2T_1 = -X_1Y_2Z_2T_1/(Z_1T_2) = X_2Y_1Z_1T_2/(Z_1T_2) = X_2Y_1$.

Note that $X_1, Y_2 \neq 0$ since $dX_1^2Y_2^2 = Z_1^2T_2^2 \neq 0$. Hence $T_3' \neq 0$: otherwise $X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2 = 0$ so $2X_1Y_2Z_2T_1 = 0$.

Now $dX_1Y_1X_3' = dX_1^2Y_1^2Z_2T_2 + dX_1X_2Y_1Y_2Z_1T_1 = dX_1^2Y_1^2Z_2T_2 + d(rZ_1T_2)(-rZ_2T_1)Z_1T_1 = (dX_1^2Y_1^2 - Z_1^2T_1^2)Z_2T_2$ and also $X_1Y_1Z_3' = aX_1^2X_2Y_1T_1T_2 + X_1Y_1^2Y_2Z_1Z_2 = -arX_1^2Z_2T_1^2T_2 + rY_1^2Z_1^2Z_2T_2 = (Y_1^2Z_1^2 - aX_1^2T_1^2)rZ_2T_2$.

Suppose that $X_3' = 0$ and $Z_3' = 0$. Then $dX_1^2Y_1^2 = Z_1^2T_1^2$ and $Y_1^2Z_1^2 = aX_1^2T_1^2$. The curve equation for P_1 states that $aX_1^2T_1^2 + Y_1^2Z_1^2 = Z_1^2T_1^2 + dX_1^2Y_1^2$ so $2Y_1^2Z_1^2 = 2Z_1^2T_1^2$; i.e., $Y_1^2 = T_1^2$. Hence $dX_1^2T_1^2 = Z_1^2T_1^2 = Z_1^2Y_1^2 = aX_1^2T_1^2$. Hence $d = a$, contradicting the hypothesis that $a \neq d$.

Part 3. Assume that $(Y_3, T_3) = (0,0)$; i.e., $Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 = 0$ and $Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2 = 0$. The following calculations show that $(X_3', Z_3') \neq (0,0)$ and $(Y_3', T_3') \neq (0,0)$.

Consider first $T_1 = 0$. Then $Z_1^2 = dX_1^2$ and $X_1, Z_1, Y_1 \neq 0$. The equations $Y_3 = 0$ and $T_3 = 0$ simplify to $Y_2Z_2 = 0$ and $X_2Y_2 = 0$, so $Y_2 = 0$. Now $aX_2^2 = Z_2^2$ and $X_2, Z_2, T_2 \neq 0$. Hence $X_3' = X_1Y_1Z_2T_2 \neq 0$ and $Y_3' = X_1Y_1Z_2T_2 \neq 0$.

Consider next $Z_1 = 0$. Then $aT_1^2 = dY_1^2$ and $X_1, Y_1, T_1 \neq 0$. The equations $Y_3 = 0$ and $T_3 = 0$ simplify to $X_2T_2 = 0$ and $X_2Y_2 = 0$, so $X_2 = 0$. Now $Y_2^2 = T_2^2$ and $Z_2, Y_2, T_2 \neq 0$. Hence $X_3' = X_1Y_1Z_2T_2 \neq 0$ and $Y_3' = X_1Y_1Z_2T_2 \neq 0$.

The same arguments apply if $T_2 = 0$ or $Z_2 = 0$. Assume from now on that $T_1 \neq 0$, $T_2 \neq 0$, $Z_1 \neq 0$, and $Z_2 \neq 0$.

Multiply the equation $Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 = 0$ by dY_1Y_2, multiply the equation $Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2 = 0$ by aT_1T_2, subtract, and divide by Z_1Z_2, to see that $dY_1^2Y_2^2 = aT_1^2T_2^2$. Define $s = Y_1Y_2/(T_1T_2)$; then $s^2 = a/d$ and $sZ_1Z_2 = Y_1Y_2Z_1Z_2/(T_1T_2) = aX_1X_2T_1T_2/(T_1T_2) = aX_1X_2$.

Note that $Y_1, Y_2 \neq 0$ since $dY_1^2Y_2^2 = aT_1^2T_2^2 \neq 0$. Hence $Z_3' \neq 0$: otherwise $aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2 = 0$ so $2Y_1Y_2Z_1Z_2 = 0$.

We have $adX_1Y_1Y_3' = adX_1^2Y_1^2Z_2T_2 - adX_1X_2Y_1Y_2Z_1T_1 = adX_1^2Y_1^2Z_2T_2 - ds^2Z_1^2Z_2T_1^2T_2 = (dX_1^2Y_1^2 - Z_1^2T_1^2)aZ_2T_2$ and also $aX_1Y_1T_3' = aX_1^2Y_1Y_2Z_2T_1 - aX_1X_2Y_1^2Z_1T_2 = asX_1^2Z_2T_1^2T_2 - sZ_2Y_1^2Z_1^2T_2 = (aX_1^2T_1^2 - Y_1^2Z_1^2)sZ_2T_2$.

Suppose that $Y_3' = 0$ and $T_3' = 0$. Then $dX_1^2Y_1^2 = Z_1^2T_1^2$ and $aX_1^2T_1^2 = Y_1^2Z_1^2$. As before $Y_1^2 = T_1^2$, leading to the same contradiction. □

Theorem 6.2. *Fix a field k with $\mathrm{char}(k) \neq 2$. Fix distinct nonzero elements $a, d \in k$. Fix $P_1, P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$. Write P_1 as $((X_1 : Z_1), (Y_1 : T_1))$ and write P_2 as $((X_2 : Z_2), (Y_2 : T_2))$. Define $X_3, Y_3, Z_3, T_3, X_3', Y_3', Z_3', T_3'$ as in Theorem 6.1. Define P_3 as follows:*

- $P_3 = ((X_3 : Z_3), (Y_3 : T_3))$ *if* $(X_3, Z_3) \neq (0, 0)$ *and* $(Y_3, T_3) \neq (0, 0)$.
- $P_3 = ((X_3' : Z_3'), (Y_3' : T_3'))$ *if* $(X_3', Z_3') \neq (0, 0)$ *and* $(Y_3', T_3') \neq (0, 0)$.

Then $P_3 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$.

Proof. Note that by Theorem 6.1 at least one definition of P_3 applies, and both definitions are the same when both cases are applicable.

One can mechanically verify that the polynomial $aX_3^2T_3^2 + Y_3^2Z_3^2 - dX_3^2Y_3^2$ in $k[X_1, Z_1, Y_1, T_1, X_2, Z_2, Y_2, T_2]$ factors as Q_1Q_2 where

$$\begin{aligned} Q_1 &= (aX_1^2T_1^2 + Y_1^2Z_1^2)Z_2^2T_2^2 - (aX_2^2T_2^2 + Y_2^2Z_2^2)dX_1^2Y_1^2, \\ Q_2 &= (aX_2^2T_2^2 + Y_2^2Z_2^2)Z_1^2T_1^2 - (aX_1^2T_1^2 + Y_1^2Z_1^2)dX_2^2Y_2^2. \end{aligned}$$

The curve equations for P_1 and P_2 now imply

$$\begin{aligned} Q_1 &= (Z_1^2T_1^2 + dX_1^2Y_1^2)Z_2^2T_2^2 - (Z_2^2T_2^2 + dX_2^2Y_2^2)dX_1^2Y_1^2 \\ &= Z_1^2Z_2^2T_1^2T_2^2 - d^2X_1^2X_2^2Y_1^2Y_2^2 \\ &= (Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2)(Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2) = Z_3T_3. \end{aligned}$$

Reverse the roles of P_1 and P_2 to see that $Q_2 = Z_3T_3$. Hence $aX_3^2T_3^2 + Y_3^2Z_3^2 - dX_3^2Y_3^2 = Z_3^2T_3^2$; i.e., $((X_3 : Z_3), (Y_3 : T_3)) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ in the first case.

The second case is similar. The polynomial $aX_3'^2T_3'^2 + Y_3'^2Z_3'^2 - Z_3'^2T_3'^2$ factors as $Q_1'Q_2'$ where

$$\begin{aligned} Q_1' &= (aX_1^2T_1^2 + Y_1^2Z_1^2)Z_2^2T_2^2 - (aX_2^2T_2^2 + Y_2^2Z_2^2)Z_1^2T_1^2, \\ Q_2' &= X_1^2Y_1^2(aX_2^2T_2^2 + Y_2^2Z_2^2) - X_2^2Y_2^2(aX_1^2T_1^2 + Y_1^2Z_1^2). \end{aligned}$$

The curve equations now imply

$$\begin{aligned} Q_1' &= (Z_1^2T_1^2 + dX_1^2Y_1^2)Z_2^2T_2^2 - (Z_2^2T_2^2 + dX_2^2Y_2^2)Z_1^2T_1^2 \\ &= d(X_1^2Y_1^2Z_2^2T_2^2 - X_2^2Y_2^2Z_1^2T_1^2) \\ &= d(X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1)(X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1) = dX_3'Y_3' \end{aligned}$$

and

$$\begin{aligned} Q_2' &= X_1^2Y_1^2(Z_2^2T_2^2 + dX_2^2Y_2^2) - X_2^2Y_2^2(Z_1^2T_1^2 + dX_1^2Y_1^2) \\ &= X_1^2Y_1^2Z_2^2T_2^2 - X_2^2Y_2^2Z_1^2T_1^2 = X_3'Y_3'. \end{aligned}$$

Hence $aX_3'^2T_3'^2 + Y_3'^2Z_3'^2 - Z_3'^2T_3'^2 = dX_3'^2Y_3'^2$; i.e., $((X_3' : Z_3'), (Y_3' : T_3')) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ in the second case. □

7. Isomorphism between $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ and $\overline{\mathrm{E}}_{\mathrm{M},A,B}$

The projective closure of the Montgomery curve $\mathrm{E}_{\mathrm{M},A,B}$ in $\mathbf{P}^2$ is

$$\overline{\mathrm{E}}_{\mathrm{M},A,B} = \left\{(U : V : W) \in \mathbf{P}^2 : BV^2W = U^3 + AU^2W + UW^2\right\}.$$

In this section the reader is assumed to be familiar with the standard chord-and-tangent group law on $\overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$.

Theorem 7.1 defines a bijection between $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ and $\overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$, and Theorem 7.3 shows that this bijection is a group isomorphism. For the special case of affine inputs and outputs on an Edwards curve, Theorem 7.3 is equivalent to [4, Theorem 3.2].

Theorem 7.1. *Fix a field k with $\mathrm{char}(k) \neq 2$. Fix distinct nonzero elements $a, d \in k$. Define $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. Then*

$$((X : Z), (Y : T)) \mapsto \begin{cases} (0:0:1) \text{ if } ((X:Z),(Y:T)) = ((0:1),(-1:1)), \\ ((T+Y)X : (T+Y)Z : (T-Y)X) \text{ otherwise} \end{cases}$$

is a bijection from $\overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ to $\overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$, and

$$(U : V : W) \mapsto \begin{cases} ((0:1),(1:1)) \text{ if } (U:V:W) = (0:1:0), \\ ((0:1),(-1:1)) \text{ if } (U:V:W) = (0:0:1), \\ ((U:V),(U-W:U+W)) \text{ otherwise} \end{cases}$$

is the inverse bijection.

Proof. Write f for the first map, and g for the second.

Fix $P \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$. We will show that $f(P) \in \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$ and $g(f(P)) = P$.

Case 1: $P = ((0:1),(1:1))$. Then $f(P) = (0:2:0) = (0:1:0) \in \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$ and $g(f(P)) = ((0:1),(1:1)) = P$.

Case 2: $P = ((0:1),(-1:1))$. Then $f(P) = (0:0:1) \in \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$ and $g(f(P)) = ((0:1),(-1:1)) = P$.

Case 3: $P \neq ((0:1),(1:1))$ and $P \neq ((0:1),(-1:1))$. Write P as $((X:Z),(Y:T))$, and define $U = (T+Y)X$, $V = (T+Y)Z$, $W = (T-Y)X$. Then $X \neq 0$. Furthermore $T+Y \neq 0$: otherwise $aX^2 = dX^2$ from the curve equation so $a = d$, contradiction. Thus $U \neq 0$, and $f(P) = (U:V:W) \in \mathbf{P}^2(k)$. Now

$$\begin{aligned} &BV^2W - (U^3 + AU^2W + UW^2) \\ &= \frac{4}{a-d}(T+Y)^2Z^2(T-Y)X \\ &\quad - \left((T+Y)^3X^3 + 2\frac{a+d}{a-d}(T+Y)^2X^2(T-Y)X + (T+Y)X(T-Y)^2X^2\right) \\ &= \frac{X(T+Y)}{a-d}\left(4(T^2-Y^2)Z^2 - 2(a+d)(T^2-Y^2)X^2 - (a-d)X^2\left((T+Y)^2 + (T-Y)^2\right)\right) \\ &= \frac{X(T+Y)}{a-d}(4Z^2T^2 + 4dX^2Y^2 - 4aX^2T^2 - 4Y^2Z^2) = 0 \end{aligned}$$

so $f(P) \in \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$. Furthermore $g(f(P)) = ((U:V),(U-W:U+W)) = (((T+Y)X : (T+Y)Z), ((T+Y)X - (T-Y)X : (T+Y)X + (T-Y)X)) = ((X:Z),(Y:T))$.

Conversely, fix $Q \in \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$. We will show that $g(Q) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ and $f(g(Q)) = Q$.

Case 1: $Q = (0:1:0)$. Then $g(Q) = ((0:1),(1:1)) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ and $f(g(Q)) = (0:1:0) = Q$.

Case 2: $Q = (0:0:1)$. Then $g(Q) = ((0:1),(-1:1)) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$ and $f(g(Q)) = (0:0:1) = Q$.

Case 3: $Q \neq (0:1:0)$ and $Q \neq (0:0:1)$. Write Q as $(U:V:W)$, and define $(X,Z,Y,T) = (U,V,U-W,U+W)$. Then $U \neq 0$ so $X \neq 0$ and $T+Y \neq 0$ so $g(Q) = ((X:Z),(Y:T)) \in \mathbf{P}^2(k)$. Now

$$\begin{aligned}
&aX^2T^2 - dX^2Y^2 + Y^2Z^2 - Z^2T^2 \\
&\quad = aU^2(U+W)^2 - dU^2(U-W)^2 + (U-W)^2V^2 - V^2(U+W)^2 \\
&\quad = (a-d)U^2(U^2+W^2) + 2aU^3W + 2dU^3W - 4UV^2W \\
&\quad = (a-d)U\left(U^3 + 2\frac{a+d}{a-d}U^2W + UW^2 - \frac{4}{a-d}V^2W\right) = 0,
\end{aligned}$$

so $g(Q) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$, and $f(g(Q)) = ((T+Y)X : (T+Y)Z : (T-Y)X) = (2U^2 : 2UV : 2WU) = (U:V:W) = Q$. □

Hilfslemma 7.2. *Fix a field k with $\mathrm{char}(k) \neq 2$. Fix distinct nonzero elements $a, d \in k$. Fix $P_1, P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$. Write P_1 as $((X_1:Z_1),(Y_1:T_1))$ and write P_2 as $((X_2:Z_2),(Y_2:T_2))$. Then $P_1+P_2 = ((0:1),(-1:1))$ if and only if $(X_2:Z_2) = (X_1:Z_1)$ and $(Y_2:T_2) = (-Y_1:T_1)$.*

Proof. Define $X_3, Z_3, Y_3, T_3, X_3', Z_3', Y_3', T_3'$ as in Theorem 6.1. If $(X_2:Z_2) = (X_1:Z_1)$ and $(Y_2:T_2) = (-Y_1:T_1)$ then $X_3' = 0$, $Y_3' = -T_3'$, $X_3 = 0$, and (from the curve equation) $Y_3 = -T_3$, so $P_1+P_2 = ((0:1),(-1:1))$.

Conversely, assume that $P_1 + P_2 = ((0:1),(-1:1))$. Then either $((X_3:Z_3),(Y_3:T_3)) = ((0:1),(-1:1))$ or $((X_3':Z_3'),(Y_3':T_3')) = ((0:1),(-1:1))$ or both. Either way $X_3 = 0$ and $Y_3 + T_3 = 0$; in the case $((X_3':Z_3'),(Y_3':T_3')) = ((0:1),(-1:1))$ this follows from $X_3Z_3' = X_3'Z_3$ and $Y_3T_3' = Y_3'T_3$. Note for future reference that, since $(Y_3:T_3) = (-1:1)$ or $(Y_3':T_3') = (-1:1)$, it is not possible to have simultaneously $Y_3 = T_3$ and $Y_3' = T_3'$.

First consider the case $T_1 = 0$. Then $X_1, Y_1, Z_1 \neq 0$. Now $X_3 = 0$ implies $X_2T_2 = 0$ so $Y_2 \neq 0$; and $Y_3 + T_3 = 0$ implies $Y_1Y_2Z_1Z_2 - dX_1X_2Y_1Y_2 = 0$, i.e., $Y_1Y_2(Z_1Z_2 - dX_1X_2) = 0$, so $Z_1Z_2 = dX_1X_2$. If $X_2 = 0$ then $Z_2 = 0$, contradiction; hence $X_2 \neq 0$ and $T_2 = 0$. Now both P_1 and P_2 have the form $((1:\pm\sqrt{d}),(1:0))$, and the equation $Z_1Z_2 = dX_1X_2$ implies that the square-root signs are the same. Hence $(X_2:Z_2) = (X_1:Z_1)$ and $(Y_2:T_2) = (1:0) = (-Y_1:T_1)$.

Similar comments apply if $T_2 = 0$. Assume from now on that $T_1 \neq 0$ and $T_2 \neq 0$.

Next consider the case $X_2 = 0$. Then $Z_2, Y_2, T_2 \neq 0$. Now $X_3 = 0$ implies $X_1 = 0$ so $Z_1 \neq 0$. Now both P_1 and P_2 have the form $((0:1),(\pm 1:1))$. The equation $Y_3 + T_3 = 0$ implies $Z_1Z_2(Y_1Y_2 + T_1T_2) = 0$ so $Y_1Y_2 = -T_1T_2$; i.e., P_1 and P_2 have opposite signs in the ± 1. Hence $(X_2:Z_2) = (X_1:Z_1)$ and $(Y_2:T_2) = (-Y_1:T_1)$.

Similar comments apply if $X_1 = 0$. Assume from now on that $X_1 \neq 0$ and $X_2 \neq 0$.

Next consider the case $Z_1 = 0$. Now $X_3 = 0$ implies $Y_2Z_2 = 0$, and $Y_3 + T_3 = 0$ implies $-aX_1X_2T_1T_2 - dX_1X_2Y_1Y_2 = 0$, i.e., $X_1X_2(aT_1T_2 + dY_1Y_2) = 0$, so $aT_1T_2 + dY_1Y_2 = 0$. In particular $Y_2 \neq 0$ (since $aT_1T_2 \neq 0$) so $Z_2 = 0$. Now both P_1 and P_2 have the form $((1:0),(\pm\sqrt{a/d}:1))$, and the equation $aT_1T_2 + dY_1Y_2 = 0$ implies that P_1 and P_2 have opposite signs in the $\pm\sqrt{a/d}$. Hence $(X_2:Z_2) = (X_1:Z_1)$ and $(Y_2:T_2) = (-Y_1:T_1)$.

Similar comments apply if $Z_2 = 0$. Assume from now on that $Z_1 \neq 0$ and $Z_2 \neq 0$.

The equation $X_3 = 0$ is $X_2Y_1Z_1T_2 = -X_1Y_2Z_2T_1$, and the equation $Y_3 + T_3 = 0$ is $Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 + Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2 = 0$. Multiply the second equation by $X_2Z_1T_2$, eliminate $X_2Y_1Z_1T_2$ using the first equation, and use $T_1 \neq 0$, to obtain

$$-X_1Z_1(Y_2^2Z_2^2 + aX_2^2T_2^2) + X_2Z_2(Z_1^2T_2^2 + dX_1^2Y_2^2) = 0.$$

Now use the P_2 curve equation to see that

$$-X_1Z_1(Z_2^2T_2^2 + dX_2^2Y_2^2) + X_2Z_2(Z_1^2T_2^2 + dX_1^2Y_2^2) = 0,$$

i.e., $(X_2Z_1 - X_1Z_2)(Z_1Z_2T_2^2 - dX_1X_2Y_2^2) = 0$.

Suppose $X_2Z_1 \neq X_1Z_2$. Then $Z_1Z_2T_2^2 = dX_1X_2Y_2^2$. Multiply this equation by $X_1X_2^2Z_1^2T_1^2$, use the P_2 curve equation, and rearrange to obtain

$$(X_2Z_1 + X_1Z_2)X_1X_2Z_1^2Z_2T_1^2T_2^2 = X_1^2X_2Z_1^2T_1^2(aX_2^2T_2^2 + Y_2^2Z_2^2).$$

Multiply the P_1 curve equation by $X_2^3Z_1^2T_2^2$, replace $X_2^2Y_1^2Z_1^2T_2^2$ with $X_1^2Y_2^2Z_2^2T_1^2$ (twice), and replace $dX_1X_2Y_2^2 = Z_1Z_2T_2^2$ to obtain

$$X_1^2X_2Z_1^2T_1^2(aX_2^2T_2^2 + Y_2^2Z_2^2) = Z_1T_1^2T_2^2(X_2^3Z_1^3 + X_1^3Z_2^3).$$

Hence

$$(X_2Z_1 + X_1Z_2)X_1X_2Z_1^2Z_2T_1^2T_2^2 = Z_1T_1^2T_2^2(X_2^3Z_1^3 + X_1^3Z_2^3);$$

i.e., $(X_2Z_1-X_1Z_2)^2(X_2Z_1+X_1Z_2)Z_1T_1^2T_2^2 = 0$. Hence $X_2Z_1+X_1Z_2 = 0$. The equation $X_3 = 0$ then implies $X_2Z_1(Y_1T_2-Y_2T_1) = 0$ so $Y_1T_2 = Y_2T_1$. Hence $Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1 = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2 = T_3'$ and

$$\begin{aligned} Y_3Z_1T_1 &= Y_1Y_2Z_1^2Z_2T_1 - aX_1X_2Z_1T_1^2T_2 \\ &= (Y_1^2Z_1^2 + aX_1^2T_1^2)Z_2T_2 \\ &= (Z_1^2T_1^2 + dX_1^2Y_1^2)Z_2T_2 \\ &= Z_1^2Z_2T_1^2T_2 - dX_1X_2Y_1Y_2Z_1T_1 = T_3Z_1T_1 \end{aligned}$$

so $Y_3 = T_3$. Contradiction.

Hence $X_2Z_1 = X_1Z_2$. Then $X_3 = 0$ implies $X_2Y_1Z_1T_2 = -X_1Y_2Z_2T_1 = -X_2Y_2Z_1T_1$, i.e., $X_2Z_1(Y_1T_2 + Y_2T_1) = 0$. Both X_2 and Z_1 are nonzero so $Y_1T_2 + Y_2T_1 = 0$ so $(X_2 : Z_2) = (X_1 : Z_1)$ and $(Y_2 : T_2) = (-Y_1 : T_1)$. □

Theorem 7.3. *Fix a field k with $\operatorname{char}(k) \neq 2$. Fix distinct nonzero elements $a, d \in k$. Define $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. Define $f : \overline{\mathrm{E}}_{\mathrm{E},a,d}(k) \to \overline{\mathrm{E}}_{\mathrm{M},A,B}(k)$ as the bijection in Theorem 7.1. Then $f(P_1 + P_2) = f(P_1) + f(P_2)$ for all $P_1, P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$.*

Proof. Write P_1 as $((X_1 : Z_1), (Y_1 : T_1))$ and write P_2 as $((X_2 : Z_2), (Y_2 : T_2))$. Define X_3, Z_3, Y_3, T_3, X_3', Z_3', Y_3', T_3' as in Theorem 6.1.

There are several cases in the definition of addition on $\overline{\mathrm{E}}_{\mathrm{M},A,B}$, and we split the proof into several cases accordingly.

Case 1: $P_1 = ((0 : 1), (1 : 1))$. Then $f(P_1) = (0 : 1 : 0)$ so on $\overline{\mathrm{E}}_{\mathrm{M},A,B}$ we have $f(P_1) + f(P_2) = f(P_2)$.

Now $(X_3 : Z_3) = (X_2T_2 : Z_2T_2)$ and $(Y_3 : T_3) = (Y_2Z_2 : Z_2T_2)$ so if $(X_3, Z_3) \neq (0, 0)$ and $(Y_3, T_3) \neq (0, 0)$ then $P_1 + P_2 = ((X_3 : Z_3), (Y_3 : T_3)) = ((X_2 : Z_2), (Y_2 : T_2)) = P_2$.

Similarly $(X_3' : Z_3') = (X_2Y_2 : Y_2Z_2)$ and $(Y_3' : Z_3') = (X_2Y_2 : X_2T_2)$ so if $(X_3', Z_3') \neq (0, 0)$ and $(Y_3', T_3') \neq (0, 0)$ then $P_1 + P_2 = ((X_3' : Z_3'), (Y_3' : T_3')) = ((X_2 : Z_2), (Y_2 : T_2)) = P_2$.

Case 2: $P_2 = ((0 : 1), (1 : 1))$. Exchange indices 1 and 2 above to see that $P_1 + P_2 = P_1$ so $f(P_1 + P_2) = f(P_1) = f(P_1) + f(P_2)$.

Case 3: $P_2 = ((-X_1 : Z_1), (Y_1 : T_1))$ and $P_1 \neq ((0 : 1), (1 : 1))$.

If $P_1 = ((0 : 1), (-1 : 1))$ then $P_2 = P_1$ so $f(P_2) = f(P_1) = (0 : 0 : 1)$. Furthermore $P_1 + P_2 = ((0 : 1), (1 : 1))$ so $f(P_1 + P_2) = (0 : 1 : 0) = (0 : 0 : 1) + (0 : 0 : 1) = f(P_1) + f(P_2)$.

If $P_1 = ((1 : 0), (\pm\sqrt{a/d} : 1))$ then $P_2 = P_1$ so $f(P_2) = f(P_1) = (1 \pm \sqrt{a/d} : 0 : 1 \mp \sqrt{a/d})$. Furthermore $(X_3 : Z_3) = (0 : 1)$ and $(Y_3 : T_3) = (-a : -d\sqrt{a/d}^2) = (1 : 1)$ so $P_1 + P_2 = ((0 : 1), (1 : 1))$ so $f(P_1 + P_2) = (0 : 1 : 0) = (1 \pm \sqrt{a/d} : 0 : 1 \mp \sqrt{a/d}) + (1 \pm \sqrt{a/d} : 0 : 1 \mp \sqrt{a/d}) = f(P_1) + f(P_2)$.

Otherwise $X_1, Z_1 \neq 0$ and $P_2 \neq P_1$. Now $X_3' = 0$ and $Y_3' = T_3'$ and $X_3 = 0$ and (by the P_1 curve equation) $Y_3 = T_3$, so $P_1 + P_2 = ((0 : 1), (1 : 1))$. Put $(U_1 : V_1 : W_1) = f(P_1)$; then $f(P_2) = (-U_1 : V_1 : -W_1) = (U_1 : -V_1 : W_1) = -f(P_1)$ so $f(P_1) + f(P_2) = (0 : 1 : 0) = f(P_1 + P_2)$.

Case 4: $P_2 = P_1$ and $P_2 \neq ((-X_1 : Z_1), (Y_1 : T_1))$.

Note that $X_1, Z_1 \neq 0$ since otherwise $(-X_1 : Z_1) = (X_1 : Z_1)$. Furthermore $T_1 + Y_1 \neq 0$ since otherwise $aX_1^2 + Z_1^2 = Z_1^2 + dX_1^2$, forcing $a = d$. Note also that $(Y_3', T_3') = (0, 0)$ and thus $P_1 + P_2 = ((X_3 : Z_3), (Y_3 : T_3))$.

Again put $(U_1 : V_1 : W_1) = f(P_1)$. Then $V_1 \neq 0$ since $(T_1 + Y_1)Z_1 \neq 0$.

If $Y_1 = 0$ then $aX_1^2 = Z_1^2$ and $(U_1 : V_1 : W_1) = (1 : \pm\sqrt{a} : 1)$. The tangent line at $(U_1 : V_1 : W_1)$ on $\overline{\mathrm{E}}_{\mathrm{M},A,B}$ has slope $(3U_1^2 + 2AU_1W_1 + W_1^2)/(2BV_1W_1) = (a - d + a + d)/(\pm 2\sqrt{a}) = \pm\sqrt{a} = V_1/U_1$ and therefore passes through $(0 : 0 : 1)$.

If $T_1 = 0$ then $Z_1^2 = dX_1^2$ and $(U_1 : V_1 : W_1) = (-1 : \pm\sqrt{d} : 1)$. The tangent line at $(U_1 : V_1 : W_1)$ on $\overline{\mathrm{E}}_{\mathrm{M},A,B}$ has slope $(3U_1^2 + 2AU_1W_1 + W_1^2)/(2BV_1W_1) = (a - d - a - d)/(\pm 2\sqrt{d}) = \mp\sqrt{d} = V_1/U_1$ and therefore passes through $(0 : 0 : 1)$.

Either way $P_1 + P_2 = ((0 : 1), (-1 : 1))$ and $f(P_1 + P_2) = (0 : 0 : 1) = f(P_1) + f(P_2)$.

Otherwise $X_1, Y_1, Z_1, T_1 \neq 0$ so $X_3 = 2X_1Y_1Z_1T_1 \neq 0$, $Z_3 = Z_1^2T_1^2 + dX_1^2Y_1^2 = aX_1^2T_1^2 + Y_1^2Z_1^2$, $Y_3 = Y_1^2Z_1^2 - aX_1^2T_1^2$, and $T_3 = Z_1^2T_1^2 - dX_1^2Y_1^2$. Thus $f(P_1+P_2) = ((T_3+Y_3)X_3 : (T_3+Y_3)Z_3 : (T_3-Y_3)X_3)$.

The tangent line through $f(P_1) = ((T_1 + Y_1)X_1 : (T_1 + Y_1)Z_1 : (T_1 - Y_1)X_1)$ on $\overline{\mathrm{E}}_{\mathrm{M},A,B}$ has slope $(3U_1^2 + 2AU_1W_1 + W_1^2)/(2BV_1W_1)$. The following script in the Sage computer-algebra system [15] verifies that this line passes through $-f(P_1 + P_2)$:

```
R.<a,d,X1,Z1,Y1,T1>=QQ[]
A=2*(a+d)/(a-d)
B=4/(a-d)
S=R.quotient([
  a*X1^2*T1^2+Z1^2*Y1^2-Z1^2*T1^2-d*X1^2*Y1^2
])
X3=X1*Y1*Z1*T1+X1*Y1*Z1*T1
Z3=Z1*Z1*T1*T1+d*X1*X1*Y1*Y1
Y3=Y1*Y1*Z1*Z1-a*X1*X1*T1*T1
T3=Z1*Z1*T1*T1-d*X1*X1*Y1*Y1
U1=(T1+Y1)*X1
V1=(T1+Y1)*Z1
W1=(T1-Y1)*X1
U3=(T3+Y3)*X3
V3=(T3+Y3)*Z3
W3=(T3-Y3)*X3
slope11 = (3*U1^2+2*A*U1*W1+W1^2)/(2*B*V1*W1)
slope13 = (V1*W3+V3*W1)/(U1*W3-U3*W1)
print 0 == S(numerator(slope11-slope13))
```

Hence $f(P_1 + P_2) = f(P_1) + f(P_1) = f(P_1) + f(P_2)$.

Case 5: $P_2 \neq P_1$ and $P_2 \neq ((-X_1 : Z_1), (Y_1 : T_1))$ and $P_1 \neq ((0 : 1), (1 : 1))$ and $P_2 \neq ((0 : 1), (1 : 1))$.

If $P_1 = ((0 : 1), (-1 : 1))$ then $P_2 \neq ((0 : 1), (-1 : 1))$ so $f(P_1) = (0 : 0 : 1)$ and $f(P_2) = ((T_2 + Y_2)X_2 : (T_2 + Y_2)Z_2 : (T_2 - Y_2)X_2)$. Note that $(T_2 + Y_2)X_2, (T_2 - Y_2)X_2 \neq 0$. Thus $f(P_1) + f(P_2) = (0 : 0 : 1)+((T_2+Y_2)X_2 : (T_2+Y_2)Z_2 : (T_2-Y_2)X_2) = ((T_2-Y_2)X_2 : -(T_2-Y_2)Z_2 : (T_2+Y_2)X_2)$. If $(X_3, Z_3) \neq (0, 0)$ and $(Y_3, T_3) \neq (0, 0)$ then $(X_3 : Z_3) = (-X_2T_2 : Z_2T_2) = (-X_2 : Z_2)$ and $(Y_3 : T_3) = (-Y_2Z_2 : Z_2T_2) = (-Y_2 : Z_2)$; if $(X_3', Z_3') \neq (0, 0)$ and $(Y_3', T_3') \neq (0, 0)$ then $(X_3' : Z_3') = (X_2Y_2 : -Y_2Z_2) = (-X_2 : Z_2)$ and $(Y_3' : T_3') = (-X_2Y_2 : X_2T_2) = (-Y_2 : T_2)$; either way $f(P_1 + P_2) = ((T_2 - Y_2)(-X_2) : (T_2 - Y_2)Z_2 : (T_2 + Y_2)(-X_2)) = ((T_2 - Y_2)X_2 : -(T_2 - Y_2)Z_2 : (T_2 + Y_2)X_2) = f(P_1) + f(P_2)$.

Similar comments apply if $P_2 = ((0 : 1), (-1 : 1))$. Assume from now on that $P_1 \neq ((0 : 1), (-1 : 1))$ and $P_2 \neq ((0 : 1), (-1 : 1))$. Then $f(P_1) = ((T_1+Y_1)X_1 : (T_1+Y_1)Z_1 : (T_1-Y_1)X_1)$ and $f(P_2) = ((T_2+Y_2)X_2 : (T_2 + Y_2)Z_2 : (T_2 - Y_2)X_2)$.

If $P_1 + P_2 = ((0 : 1), (-1 : 1))$ then $(X_2 : Z_2) = (X_1 : Z_1)$ and $(Y_2 : T_2) = (-Y_1 : T_1)$ by Hilfslemma 7.2 so $f(P_1) = ((T_1+Y_1)X_1 : (T_1+Y_1)Z_1 : (T_1-Y_1)X_1)$ and $f(P_2) = ((T_1-Y_1)X_1 : (T_1-Y_1)Z_1 : (T_1+Y_1)X_1)$. Hence $f(P_1) + f(P_2) = (0 : 0 : 1) = f(P_1 + P_2)$.

Assume from now on that $P_1 + P_2 \neq ((0 : 1), (-1 : 1))$. If $(X_3, Z_3) \neq (0, 0)$ and $(Y_3, T_3) \neq (0, 0)$ then $P_1 + P_2 = ((X_3 : Z_3), (Y_3 : T_3))$ so $f(P_1 + P_2) = ((T_3 + Y_3)X_3 : (T_3 + Y_3)Z_3 : (T_3 - Y_3)X_3)$. The following Sage script verifies that $((T_3 + Y_3)X_3 : -(T_3 + Y_3)Z_3 : (T_3 - Y_3)X_3)$ is on the line from $((T_1 + Y_1)X_1 : (T_1 + Y_1)Z_1 : (T_1 - Y_1)X_1)$ to $((T_2 + Y_2)X_2 : (T_2 + Y_2)Z_2 : (T_2 - Y_2)X_2)$:

```
R.<a,d,X1,Z1,Y1,T1,X2,Z2,Y2,T2>=QQ[]
S=R.quotient([
  a*X1^2*T1^2+Z1^2*Y1^2-Z1^2*T1^2-d*X1^2*Y1^2,
  a*X2^2*T2^2+Z2^2*Y2^2-Z2^2*T2^2-d*X2^2*Y2^2
])
X3=X1*Y2*Z2*T1+X2*Y1*Z1*T2
Z3=Z1*Z2*T1*T2+d*X1*X2*Y1*Y2
Y3=Y1*Y2*Z1*Z2-a*X1*X2*T1*T2
T3=Z1*Z2*T1*T2-d*X1*X2*Y1*Y2
U1=(T1+Y1)*X1
V1=(T1+Y1)*Z1
W1=(T1-Y1)*X1
U2=(T2+Y2)*X2
V2=(T2+Y2)*Z2
W2=(T2-Y2)*X2
U3=(T3+Y3)*X3
V3=(T3+Y3)*Z3
W3=(T3-Y3)*X3
slope13 = (V1*W3+V3*W1)/(U1*W3-U3*W1)
slope12 = (V1*W2-V2*W1)/(U1*W2-U2*W1)
print 0 == S(numerator(slope13-slope12))
```

Hence $f(P_1) + f(P_2) = f(P_1 + P_2)$.

If $(X_3', Z_3') \neq (0,0)$ and $(Y_3', T_3') \neq (0,0)$ then $P_1 + P_2 = ((X_3' : Z_3'), (Y_3' : T_3'))$ so $f(P_1 + P_2) = ((T_3'+Y_3')X_3' : (T_3'+Y_3')Z_3' : (T_3'-Y_3')X_3')$. The following Sage script verifies that $((T_3'+Y_3')X_3' : -(T_3'+Y_3')Z_3' : (T_3' - Y_3')X_3')$ is on the line from $((T_1 + Y_1)X_1 : (T_1 + Y_1)Z_1 : (T_1 - Y_1)X_1)$ to $((T_2 + Y_2)X_2 : (T_2 + Y_2)Z_2 : (T_2 - Y_2)X_2)$:

```
R.<a,d,X1,Z1,Y1,T1,X2,Z2,Y2,T2>=QQ[]
S=R.quotient([
  a*X1^2*T1^2+Z1^2*Y1^2-Z1^2*T1^2-d*X1^2*Y1^2,
  a*X2^2*T2^2+Z2^2*Y2^2-Z2^2*T2^2-d*X2^2*Y2^2
])
X3=X1*Y1*Z2*T2 + X2*Y2*Z1*T1
Z3=a*X1*X2*T1*T2 + Y1*Y2*Z1*Z2
Y3=X1*Y1*Z2*T2 - X2*Y2*Z1*T1
T3=X1*Y2*Z2*T1 - X2*Y1*Z1*T2
U1=(T1+Y1)*X1
V1=(T1+Y1)*Z1
W1=(T1-Y1)*X1
U2=(T2+Y2)*X2
V2=(T2+Y2)*Z2
W2=(T2-Y2)*X2
U3=(T3+Y3)*X3
V3=(T3+Y3)*Z3
W3=(T3-Y3)*X3
slope13 = (V1*W3+V3*W1)/(U1*W3-U3*W1)
slope12 = (V1*W2-V2*W1)/(U1*W2-U2*W1)
print 0 == S(numerator(slope13-slope12))
```

Hence $f(P_1) + f(P_2) = f(P_1 + P_2)$. □

8. Special cases

The neutral element of $\overline{\mathrm{E}}_{\mathrm{E},a,d}$ is $((0:1),(1:1))$.

The negative of $((X_1:Z_1),(Y_1:T_1)) \in \overline{\mathrm{E}}_{\mathrm{E},a,d}$ is $((-X_1:Z_1),(Y_1:T_1))$. This implies in particular that points of order 2 have $(X_1:Z_1) \in \{(0:1),(1:0)\}$.

Theorem 8.1 below gives linear characterizations of the pairs $(P_1,P_2) \in \overline{\mathrm{E}}_{\mathrm{E},a,d} \times \overline{\mathrm{E}}_{\mathrm{E},a,d}$ that can be added by each of our addition laws. For example, the dual addition law fails for all doublings, so the original addition law works for all doublings. One can also express the exceptional divisors as functions of $P_2 - P_1$, as one would guess by analogy to [6, Theorem 2]: the original addition law fails for exactly the pairs (P_1,P_2) such that $P_2 - P_1$ is $((1:\pm\sqrt{d}),(1:0))$ or $((1:0),(\pm\sqrt{a/d}:1))$, and the dual addition law fails for exactly the pairs (P_1,P_2) such that $P_2 - P_1$ is $((1:\pm\sqrt{a}),(0:1))$ or $((0:1),(\pm 1:1))$. These characterizations rely on, e.g., the "$\sqrt{d}$ formula"

$$((X_1:Z_1),(Y_1:T_1)) + ((1:\sqrt{d}),(1:0)) = ((T_1:\sqrt{d}Y_1),(Z_1:-\sqrt{d}X_1)).$$

This formula follows immediately from the original addition law when $X_1Y_1 \neq 0$, as pointed out by Edwards in [7, page 404, last sentence]; and it follows immediately from the dual addition law when $T_1Z_1 \neq 0$.

The same $\sqrt{d}$ formula can also be used as a way to "rotate" addition laws, and in particular to obtain the dual addition law from the original addition law. Specifically, add $((1:\sqrt{d}),(1:0))$ to $((X_1:Z_1),(Y_1:T_1))$, using the $\sqrt{d}$ formula; further add $((X_2:Z_2),(Y_2:T_2))$, using the original addition law; and then subtract $((1:\sqrt{d}),(1:0))$, using the $\sqrt{d}$ formula. The final result is exactly the dual addition law for $((X_1:Z_1),(Y_1:T_1))$ and $((X_2:Z_2),(Y_2:T_2))$. Applying the same rotation to the dual addition law recovers the original addition law; this justifies our "dual" terminology. Rotating the exceptional cases for the original addition law produces the exceptional cases for the dual addition law.

Theorem 8.1. *Fix a field k with $\mathrm{char}(k) \neq 2$. Fix distinct nonzero elements $a,d \in k$. Fix $P_1,P_2 \in \overline{\mathrm{E}}_{\mathrm{E},a,d}(k)$. Write P_1 as $((X_1:Z_1),(Y_1:T_1))$ and write P_2 as $((X_2:Z_2),(Y_2:T_2))$. Define $X_3,Y_3,Z_3,T_3,X_3',Y_3',Z_3',T_3'$ as in Theorem 6.1. Then*

- $(X_3,Z_3) = (0,0)$ *if and only if* $P_2 = ((T_1:\pm\sqrt{d}Y_1),(Z_1:\mp\sqrt{d}X_1))$.
- $(Y_3,T_3) = (0,0)$ *if and only if* $P_2 = ((\pm\sqrt{a/d}Z_1:aX_1),(\pm\sqrt{a/d}T_1:Y_1))$.
- $(X_3',Z_3') = (0,0)$ *if and only if* $P_2 = ((Y_1:\pm\sqrt{a}T_1),(\mp\sqrt{a}X_1:Z_1))$.
- $(Y_3',T_3') = (0,0)$ *if and only if* $P_2 = ((\pm X_1:Z_1),(\pm Y_1:T_1))$.

Proof. **Part 1.** Assume without loss of generality that $(X_2,Z_2,Y_2,T_2) = (T_1,\pm\sqrt{d}Y_1,Z_1,\mp\sqrt{d}X_1)$. Then $X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 = X_1Z_1(\pm\sqrt{d}Y_1)T_1 + T_1Y_1Z_1(\mp\sqrt{d}X_1) = 0$ and $Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2 = Z_1(\pm\sqrt{d}Y_1)T_1(\mp\sqrt{d}X_1) + dX_1T_1Y_1Z_1 = 0$.

Conversely, assume that $(X_3,Z_3) = (0,0)$.

If $T_1 = 0$ then $Z_1^2 = dX_1^2$ and $X_2 = 0$ and $Y_2^2 = T_2^2$, as shown before in Part 2 of the proof of Theorem 6.1. Write $s = -Z_1T_2/(X_1Y_2)$; then $s^2 = d$ and $((T_1:sY_1),(Z_1:-sX_1)) = ((0:1),(Y_2:T_2)) = ((X_2:Z_2),(Y_2:T_2))$.

If $Z_2 = 0$ then $aT_2^2 = dY_2^2$ and $Y_1 = 0$ and $aX_1^2 = Z_1^2$, as shown before. Again write $s = -Z_1T_2/(X_1Y_2)$; then $s^2 = d$ and $((T_1:sY_1),(Z_1:-sX_1)) = ((1:0),(Y_2:T_2)) = ((X_2:Z_2),(Y_2:T_2))$.

Similar comments apply if $T_2 = 0$ or $Z_1 = 0$. The only remaining case is that $Z_1,Z_2,T_1,T_2 \neq 0$. Then $X_1Y_2 = rZ_1T_2$ and $X_2Y_1 = -rZ_2T_1$ for some r satisfying $r^2 = 1/d$, as shown before. Write $s = -1/r$; then $s^2 = d$ and $((T_1:sY_1),(Z_1:-sX_1)) = ((X_2:Z_2),(Y_2:T_2))$.

Part 2. Assume without loss of generality that $(X_2,Z_2,Y_2,T_2) = (\pm\sqrt{a/d}Z_1,aX_1,\pm\sqrt{a/d}T_1,Y_1)$. Then $Y_3 = Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 = Y_1(\pm\sqrt{a/d}T_1)Z_1aX_1 - aX_1(\pm\sqrt{a/d}Z_1)T_1Y_1 = 0$ and $T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2 = Z_1aX_1T_1Y_1 - dX_1(\pm\sqrt{a/d}Z_1)Y_1(\pm\sqrt{a/d}T_1) = 0$.

Conversely, assume that $(Y_3,T_3) = (0,0)$.

If $T_1 = 0$ then $Z_1^2 = dX_1^2$ and $Y_2 = 0$ and $aX_2^2 = Z_2^2$, as shown before in Part 3 of the proof of Theorem 6.1. Write $s = aX_1X_2/(Z_1Z_2)$; then $s^2 = a/d$ and $((sZ_1 : aX_1), (sT_1 : Y_1)) = ((X_2 : Z_2), (0 : 1)) = ((X_2 : Z_2), (Y_2 : T_2))$.

If $Z_1 = 0$ then $aT_1^2 = dY_1^2$ and $X_2 = 0$ and $Y_2^2 = T_2^2$, as shown before. Write $s = Y_1Y_2/(T_1T_2)$; then $s^2 = a/d$ and $((sZ_1 : aX_1), (sT_1 : Y_1)) = ((0 : 1), (Y_2 : T_2)) = ((X_2 : Z_2), (Y_2 : T_2))$.

Similar comments apply if $T_2 = 0$ or $Z_2 = 0$. The only remaining case is that $Z_1, Z_2, T_1, T_2 \neq 0$. Then $Y_1Y_2 = sT_1T_2$ and $aX_1X_2 = sZ_1Z_2$ for some s satisfying $s^2 = a/d$, as shown before, so $((sZ_1 : aX_1), (sT_1 : Y_1)) = ((X_2 : Z_2), (Y_2 : T_2))$.

Part 3. Assume without loss of generality that $(X_2, Z_2, Y_2, T_2) = (Y_1, \pm\sqrt{a}T_1, \mp\sqrt{a}X_1, Z_1)$. Then $X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1 = X_1Y_1(\pm\sqrt{a}T_1)Z_1 + Y_1(\mp\sqrt{a}X_1)Z_1T_1 = 0$ and $Z_3' = aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2 = aX_1Y_1T_1Z_1 + Y_1(\mp\sqrt{a}X_1)Z_1(\pm\sqrt{a}T_1) = 0$.

Conversely, assume that $(X_3', Z_3') = (0, 0)$.

If $X_1 = 0$ then $X_2Y_2 = 0$ and $Y_2Z_2 = 0$ so $Y_2 = 0$. Furthermore $Y_1^2 = T_1^2$ and $aX_2^2 = Z_2^2$. Write $r = Y_1Z_2/(X_2T_1)$; then $r^2 = a$ and $((Y_1 : rT_1), (-rX_1 : Z_1)) = ((X_2 : Z_2), (0 : 1)) = ((X_2 : Z_2), (Y_2 : T_2))$.

If $T_1 = 0$ then $Z_2T_2 = 0$ and $Y_2Z_2 = 0$ so $Z_2 = 0$. Furthermore $Z_1^2 = dX_1^2$ and $aT_2^2 = dY_2^2$. Write $r = -Y_2Z_1/(X_1T_2)$; then $r^2 = a$ and $((Y_1 : rT_1), (-rX_1 : Z_1)) = ((1 : 0), (Y_2 : T_2)) = ((X_2 : Z_2), (Y_2 : T_2))$.

Similar comments apply if $X_2 = 0$ or $T_2 = 0$, so assume that $X_1, X_2, T_1, T_2 \neq 0$. Then $aX_1^2X_2T_1T_2^2 = -X_1Y_1Y_2Z_1Z_2T_2 = X_2Y_2^2Z_1^2T_1$ so $X_2T_1(aX_1^2T_2^2 - Y_2^2Z_1^2) = 0$ so $aX_1^2T_2^2 = Y_2^2Z_1^2$. Write $r = -Y_2Z_1/(X_1T_2)$. Then $r^2 = a$ and $rX_2T_1 = -X_2Y_2Z_1T_1/(X_1T_2) = X_1Y_1Z_2T_2/(X_1T_2) = Y_1Z_2$ so $((Y_1 : rT_1), (-rX_1 : Z_1)) = ((X_2 : Z_2), (Y_2 : T_2))$.

Part 4. Assume now that $(X_2, Z_2, Y_2, T_2) = (\pm X_1, Z_1, \pm Y_1, T_1)$. Then $Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1 = X_1Y_1Z_1T_1 - (\pm X_1)(\pm Y_1)Z_1T_1 = 0$ and $T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2 = X_1(\pm Y_1)Z_1T_1 - (\pm X_1)Y_1Z_1T_1 = 0$.

Conversely, assume that $(Y_3', T_3') = (0, 0)$.

If $X_1 = 0$ then $X_2Y_2 = 0$ and $X_2T_2 = 0$ so $X_2 = 0$. If $Z_1 = 0$ then $Z_2T_2 = 0$ and $Y_2Z_2 = 0$ so $Z_2 = 0$. If $Y_1 = 0$ then $X_2Y_2 = 0$ and $Y_2Z_2 = 0$ so $Y_2 = 0$. If $T_1 = 0$ then $Z_2T_2 = 0$ and $X_2T_2 = 0$ so $T_2 = 0$. In all four cases one sees easily that $((rX_1 : Z_1), (rY_1 : T_1)) = ((X_2 : Z_2), (Y_2 : T_2))$ for some $r \in \{-1, 1\}$. Similar comments apply if $X_2 = 0$ or $Z_2 = 0$ or $Y_2 = 0$ or $T_2 = 0$.

In the remaining case $X_1^2Y_1Z_2^2T_2 = X_1X_2Y_2Z_2Z_1T_1 = X_2^2Y_1Z_1^2T_2$ so $X_1^2Z_2^2 = X_2^2Z_1^2$. Write $r = X_2Z_1/(X_1Z_2)$. Then $r \in \{-1, 1\}$ and $rY_1T_2 = X_2Y_1Z_1T_2/(X_1Z_2) = X_1Y_2Z_2T_1/(X_1Z_2) = Y_2T_1$ so $((rX_1 : Z_1), (rY_1 : T_1)) = ((X_2 : Z_2), (Y_2 : T_2))$. □

References

[1] Christophe Arène, Tanja Lange, Michael Naehrig, Christophe Ritzenthaler, *Faster computation of the Tate pairing*, to appear, Journal of Number Theory (2010). URL: http://eprint.iacr.org/2009/155.

[2] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, *Twisted Edwards curves*, in Africacrypt 2008 [16] (2008), 389–405. URL: http://eprint.iacr.org/2008/013.

[3] Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *ECM using Edwards curves* (2010). URL: http://eprint.iacr.org/2008/016.

[4] Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in Asiacrypt 2007 [10] (2007), 29–50. URL: http://eprint.iacr.org/2007/286.

[5] Daniel J. Bernstein, Tanja Lange, *Explicit-formulas database* (2010). URL: http://hyperelliptic.org/EFD.

[6] Wieb Bosma, Hendrik W. Lenstra, Jr., *Complete systems of two addition laws for elliptic curves*, Journal of Number Theory **53** (1995), 229–240. ISSN 0022–314X. MR 96f:11079.

[7] Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html.

[8] Andrew M. Gleason (editor), *Proceedings of the International Congress of Mathematicians, volume 1*, American Mathematical Society, Providence, 1987. ISBN 0–8218–0110–4. MR 89c:00042. See [13].

[9] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, *Twisted Edwards curves revisited*, in Asiacrypt 2008 [14] (2008). URL: http://eprint.iacr.org/2008/522.

[10] Kaoru Kurosawa (editor), *Advances in cryptology — ASIACRYPT 2007, 13th international conference on the theory and application of cryptology and information security, Kuching, Malaysia, December 2–6, 2007, proceedings*, Lecture Notes in Computer Science, 4833, Springer, 2007. ISBN 978-3-540-76899-9. See [4].

[11] Herbert Lange, Wolfgang M. Ruppert, *Complete systems of addition laws on abelian varieties*, Inventiones Mathematicae **79** (1985), 603–610.

[12] Herbert Lange, Wolfgang M. Ruppert, *Addition laws on elliptic curves in arbitrary characteristics*, Journal of Algebra **107** (1987), 106–116.

[13] Hendrik W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms*, in [8] (1987), 99–120. MR 89d:11114. URL: https://openaccess.leidenuniv.nl/dspace/bitstream/1887/3822/1/346_080.pdf.

[14] Josef Pieprzyk (editor), *Advances in cryptology — ASIACRYPT 2008, 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, December 7–11, 2008*, Lecture Notes in Computer Science, 5350, 2008. ISBN 978-3-540-89254-0. See [9].

[15] William Stein (editor), *Sage Mathematics Software (Version 2.8.12)*, The Sage Group, 2008. URL: http://www.sagemath.org.

[16] Serge Vaudenay (editor), *Progress in cryptology — AFRICACRYPT 2008, first international conference on cryptology in Africa, Casablanca, Morocco, June 11–14, 2008, proceedings*, Lecture Notes in Computer Science, 5023, Springer, 2008. ISBN 978-3-540-68159-5. See [2].