Efficient arithmetic on elliptic curves in characteristic 2

David Kohel

Efficient arithmetic on elliptic curves in characteristic 2

David Kohel

Institut de Mathématiques de Luminy
Université d'Aix-Marseille
163, avenue de Luminy, Case 907
13288 Marseille Cedex 9
France

Abstract. We present normal forms for elliptic curves over a field of characteristic 2 analogous to Edwards normal form, and determine bases of addition laws, which provide strikingly simple expressions for the group law. We deduce efficient algorithms for point addition and scalar multiplication on these forms. The resulting algorithms apply to any elliptic curve over a field of characteristic 2 with a 4-torsion point, via an isomorphism with one of the normal forms. We deduce algorithms for duplication in time $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}_c$ and for addition of points in time $7\mathbf{M} + 2\mathbf{S}$, where $\mathbf{M}$ is the cost of multiplication, $\mathbf{S}$ the cost of squaring, and $\mathbf{m}_c$ the cost of multiplication by a constant. By a study of the Kummer curves $\mathscr{K} = E/\{[\pm 1]\}$, we develop an algorithm for scalar multiplication with point recovery which computes the multiple of a point P with $4\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}_c + \mathbf{m}_t$ per bit where $\mathbf{m}_t$ is multiplication by a constant that depends on P.

1 Introduction

The last five years have seen significant improvements in the efficiency of known algorithms for arithmetic on elliptic curves, spurred by the introduction of the Edwards model [11] and its analysis [1, 2, 13]. Previously, it had been recognized that alternative models of elliptic curves could admit efficient arithmetic [8], but the fastest algorithms could be represented in terms of functions on elliptic curves embedded in $\mathbb{P}^2$ as Weierstrass models.

Among the best alternative models one finds a common property of symmetry. They admit a large number of (projective) linear automorphisms, often given by signed or scaled coordinate permutations. An elliptic curve with j-invariant $j \neq 0, 12^3$ admits only $\{[\pm 1]\}$ as automorphism group *fixing the identity element.* However, as a genus 1 curve, it also admits translations by rational points, and a translation morphism $\tau_Q(P) = P + Q$ on E is projectively linear, i.e. induced by a linear transformation of the ambient projective space, if and only if E is a degree n model determined by a complete linear system in $\mathbb{P}^{n-1}$ and Q is in the n-torsion subgroup. As a consequence the principal models of cryptographic interest are elliptic curves in $\mathbb{P}^2$ with rational 3-torsion points (e.g. the Hessian

models) and in $\mathbb{P}^3$ with 2-torsion or 4-torsion points (e.g. the Jacobi quadratic intersections and Edwards model), and unfortunately, the latter models do not have good reduction to characteristic 2. The present work aims to fill this gap.

A rough combinatorial explanation for the role of symmetry in efficiency is the following. Suppose that the sum of $x = (x_0 : \cdots : x_r)$ and $y = (y_0 : \cdots : y_r)$ is expressed by polynomials $(p_0(x, y) : \cdots : p_r(x, y))$ of low bidegree, say $(2, 2)$, in x_i and y_j. Such polynomials form a finite dimensional space. A translation morphism τ given by scaled coordinate transformation on E determines a new tuple $(p_0(\tau(x), \tau^{-1}(y)) : \ldots, p_r(\tau(x), \tau^{-1}(y)))$. If $(p_0(x, y) : \cdots : p_r(x, y))$ is an eigenvector for this transformation then it tends to have few monomials. In the case of Hessian, Jacobi, Edwards, and similar models, there exist bases of eigenvector polynomial addition laws such that the p_j achieve the minimal value of two terms.

Section 2 recalls several results, observations, and conclusions of Kohel [17] on symmetries of elliptic curves in their embeddings. As illustration, Section 3 recalls the main properties of the Edwards model as introduced by Edwards [11], reformulated by Bernstein and Lange [1] with twists by Bernstein et al. [2], and properties of its arithmetic described in Hisil et al. [13] and Bernstein and Lange [3].

This background motivates the introduction and classification of new models for elliptic curves in Section 4, based on imitation of the desired properties of Edwards curves, and in Section 5 we present new elliptic curve models, the $\mathbf{Z}/4\mathbf{Z}$-normal form and the split $\boldsymbol{\mu}_4$-normal form, which satisfy these properties. In Section 6 we classify all symmetric quartic elliptic curves in $\mathbb{P}^3$ with a rational 4-torsion point, up to projective linear isomorphism.[1] In particular we prove that any such curve is linearly isomorphic to one of these two models. In Section 7 we determine the polynomial addition laws and resulting complexity for arithmetic on these forms. Finally Section 8 develops models for the Kummer curve $\mathscr{K} = E/\{[\pm 1]\}$ and exploits an embedding of E in $\mathscr{K}^2$ in order to develop a Montgomery ladder for scalar multiplication with point recovery. Section 9 summarizes the new complexity results for these models in comparison with previously known models and algorithms. An appendix gives the addition laws for a descended $\boldsymbol{\mu}_4$-normal form that allows us to save on multiplications by constants involved in the curve equation.

Notation.

In what follows we use $\mathbf{M}$ and $\mathbf{S}$ for the complexity of multiplication and squaring, respectively, in the field k, and $\mathbf{m}_c$ for a multiplication by a fixed (possibly small) constant c (or constants c_i).[2] For the purposes of complexity analysis we ignore field additions.

[1] Note that any quartic plane model has a canonical extension to a nonsingular quartic model in $\mathbb{P}^3$ by extending to a complete linear system.

[2] When the small constant is a bounded power of a fixed constant we omit the squarings or products entailed in its construction and continue to consider $c^{O(1)}$ a fixed constant.

When describing a morphism $\varphi : X \to Y$ given by polynomial maps, we write

$$\varphi(x) = \begin{cases} \big(p_{1,0}(x) : \cdots : p_{1,n}(x)\big), \\ \qquad\qquad \vdots \\ \big(p_{m,0}(x) : \cdots : p_{m,n}(x)\big), \end{cases}$$

to indicate that each of the tuples of polynomials $(p_{i,0}(x), \ldots, p_{i,n}(x))$ defines the morphism on an open neighborhood $U_i \subset X$, namely on the complement of the common zeros $p_{i,0}(x) = \cdots p_{i,m}(x) = 0$, that any two agree on the intersections $U_i \cap U_j$, and that the union of the U_i is all of X.

For the projective coordinate functions on $\mathbb{P}^r$, with $r > 3$, we use X_i and so $x = (X_0 : \cdots : X_r)$ represents a generic point. We also use X_i for their restriction to a curve E, in which case the X_i are defined modulo the defining ideal of E. In the product $\mathbb{P}^r \times \mathbb{P}^r$, we continue to write x for the first coordinate and use (x, y) for a generic point in $\mathbb{P}^r \times \mathbb{P}^r$, where $y = (Y_0 : \cdots : Y_r)$.

2 Elliptic curves with symmetries

We consider conditions for an elliptic curve embedding in $\mathbb{P}^r$ to admit many projective linear transformations, or symmetries. In what follows, we recall standard definitions and conclusions drawn from Kohel [17] (reformulated here without the language of invertible sheaves). The examples of Hessian curves and Edwards curves[3] play a pivotal role in motivating [17] and further examples (see Bernstein and Lange [3], Joye and Rezaeian Farashahi [14], Kohel [17, Section 8]) suggest that such symmetries go hand-in-hand with efficient forms for their arithmetic.[4]

The automorphism group of an elliptic curve E is a finite group, and if $j(E) \neq 0, 12^3$, this group is $\{\, [\pm 1] \,\}$. Inspection of standard projective models for elliptic curves shows that the symmetry group can be much greater. The disparity is explained by the existence of subgroups of rational torsion. The automorphism group of an elliptic curve is defined to be the automorphisms of the curve which fix the identity point, which does not include translations. For any rational torsion point T, the translation-by-T map τ_T is an automorphism of the curve, which may give rise to the additional symmetries.

We restrict to models of elliptic curves given by complete linear systems of a given degree d. Basically, such a curve is defined by $E \subset \mathbb{P}^r$ such that $r = d - 1$, E is not contained in any hyperplane, and any hyperplane H intersects E in exactly d points, counted with multiplicities. For embedding degree 3, such a

[3] In particular my discussions of symmetries with Bernstein and Lange motivated a study of symmetries in the unpublished work [5] (see the EFD [6]) on twisted Hessian curves, picked up by Joye and Rezaeian Farashahi [14] after posting to the EFD). This further led the author to develop a general framework for symmetries and to classify the linear action of torsion in [17].

[4] By efficient forms, we mean sparse polynomials expressions with small coefficients. These may or may not yield the most efficient *algorithms*, as seen in comparing the evaluation of similarly sparse addition laws for the Edwards and $\mathbf{Z}/4\mathbf{Z}$-normal forms.

curve is given by a single homogeneous form $F(X, Y, Z)$ of degree 3, and for degree 4 we have an intersection of two quadrics in $\mathbb{P}^3$. Quartic plane models formally lie outside of this scope — they are neither nonsingular nor given by a complete linear system — but determine a unique degree 4 elliptic curve in $\mathbb{P}^3$ after completing the basis of functions. As in the case of the Edwards curve, we always pass to this model to apply the theory.

Definition 1. *Let $E \subset \mathbb{P}^r$ be an elliptic curve embedded with respect to a complete linear system. We say that E is a symmetric model if $[-1]$ is induced by a projective linear transformation of $\mathbb{P}^r$.*

We next recall a classification of symmetric embeddings of elliptic curves (cf. Kohel [17, Lemma 2] for the statement in terms of invertible sheaves).

Lemma 2. *Let $E \subset \mathbb{P}^r$ be an elliptic curve over k embedded with respect to a complete linear system. There exists a point S in $E(k)$ such that for any hyperplane H in $\mathbb{P}^r$ not containing E, the set of points in the intersection $E \cap H = \{P_0, \ldots, P_r\}$, in $E(\bar{k})$, counted with multiplicity, sum to S. The model is symmetric if and only if S is in the subgroup $E[2]$ of 2-torsion points.*

Definition 3. *Let E be a degree d embedding in $\mathbb{P}^r$ with respect to a complete linear system, and let S be the point as in the previous lemma. We define the embedding divisor class of E to be $(d-1)(\mathrm{O}) + (S)$.*

We describe here the classification of elliptic curves with projective embedding, up to *linear* isomorphism, rather than isomorphism.[5] The notion of isomorphisms given by linear transformations plays an important role in the addition laws, since such a change of variables gives an isomorphism between the respective spaces of addition laws of fixed bidegree (m, n), as described in Kohel [17, Section 7]. For a point T, we denote the translation-by-T morphism by τ_T, given by $\tau_T(P) = P + T$. We now recall the classification of symmetries which arise from the group law [17, Lemma 5].

Lemma 4. *Let $E \subset \mathbb{P}^r$ be embedded with respect to the complete linear system of degree d and let T be in $E(\bar{k})$. The translation-by-T morphism is induced by a projective linear automorphism of $\mathbb{P}^r$ if and only if $dT = \mathrm{O}$.*

Similarly, we recall the classification of projective linear isomorphisms between curves in $\mathbb{P}^r$ (see Kohel [17, Lemma 3] for a slightly stronger formulation).

Lemma 5. *Let E_1 and E_2 be isomorphic elliptic curves embedded in $\mathbb{P}^r$ with respect to complete linear systems of the same degree d. An isomorphism $\varphi : E_1 \to E_2$ is induced by a projective linear transformation if and only if $\varphi(S_1) = S_2$, where $S_i \in E_i(k)$ determine the embedding divisor classes $(d-1)(\mathrm{O}) + (S_i)$ of the embeddings.*

[5] In recent cryptographic literature, there has been a trend to refer to existence of a *birational equivalence*. In the context of elliptic curves, by definition nonsingular projective curves, this concept coincides with isomorphism, and we want to identity the subclass of isomorphisms which are linear with respect to the coordinate functions of the given embedding.

Remark. By definition, an isomorphism $\varphi : E_1 \to E_2$ of elliptic curves takes the identity of E_1 to the identity of E_2. It may be possible to define a projective linear transformation from E_1 to E_2 which does not respect the group identities (hence is not a group isomorphism).

3 Properties of the Edwards normal form

In this section we suppose that k is a field of characteristic different from 2. To illustrate the symmetry properties of the previous section and motivate the analogous construction in characteristic 2, we recall the principal properties of the Edwards normal form, summarizing work of Edwards [11], Hisil et al. [13], and Bernstein and Lange [3]. We follow the definitions and notation of Kohel [17], defining the twisted Edwards normal form E/k in $\mathbb{P}^3$:

$$cX_1^2 + X_2^2 = X_0^2 + dX_3^2,\ X_0X_3 = X_1X_2,\ \mathrm{O} = (1:0:1:0).$$

Edwards model for elliptic curves

In 2007, Edwards introduced a new model for elliptic curves [11], defined by the affine model

$$x^2 + y^2 = a^2(1 + z^2),\ z = xy,$$

over any field k of characteristic different from 2. The complete linear system associated to this degree 4 model has basis $\{1, x, y, z\}$ such that the image $(1 : x : y : z)$ is a nonsingular projective model in $\mathbb{P}^3$:

$$X_1^2 + X_2^2 = a^2(X_0^2 + X_3^2),\ X_0X_3 = X_1X_2,$$

with identity $\mathrm{O} = (a : 0 : 1 : 0)$, as a family of curves over $k(a)$ We hereafter refer to this model as the split Edwards model. Bernstein and Lange [1] introduced a rescaling to descend to $k(d) = k(a^4)$, and subsequently (with Joye, Birkner, and Peters [2]) a quadratic twist by c, to define the twisted Edwards model with $\mathrm{O} = (1 : 0 : 1 : 0)$:

$$cX_1^2 + X_2^2 = X_0^2 + dX_3^2,\ X_0X_3 = X_1X_2.$$

The twisted Edwards model in this form appears in Hisil et al. [13] (as extended Edwards coordinates), which provides the most efficient arithmetic. We next recall the principal properties of the Edwards normal form (with $c = 1$).

Symmetry properties

1. The embedding divisor class is $3(\mathrm{O}) + (S)$ where $S = 2T$.
2. The point $T = (1 : -1 : 0 : 0)$ is a rational 4-torsion point.

3. The translation–by–T and inverse morphisms are given by:

$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_0 : -X_2 : X_1 : -X_3),$$
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : -X_1 : X_2 : -X_3).$$

4. The model admits a factorization $s \circ (\pi_1 \times \pi_2)$ through $\mathbb{P}^1 \times \mathbb{P}^1$, where

$$\pi_1(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_1), \\ (X_2 : X_3) \end{cases}, \ \pi_2(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_2), \\ (X_1 : X_3). \end{cases}$$

and s is the Segre embedding

$$s((U_0 : U_1), (V_0 : V_1)) = (U_0V_0 : U_1V_0 : U_0V_1 : U_1V_1).$$

Remark. The linear expression for $[-1]$ implies that the embedding is symmetric. This linearity is a consequence of the form of the embedding divisor $3(\mathrm{O}) + (S)$, in view of Lemma 2. In addition the two projections are symmetric, in the sense that they are stable under $[-1]$. This is due to the fact that the divisors $2(O) = \pi_1^*(\infty)$ and $(O) + (T) = \pi_2^*(\infty)$ are symmetric.

A remarkable factorization

Hisil et al. [13] discovered amazingly simple bilinear rational expressions for the affine addition laws, which can be described as a factorization of the addition laws through the isomorphic curve in $\mathbb{P}^1 \times \mathbb{P}^1$ (see Bernstein and Lange [3] for further properties). As a consequence of the symmetry of the embedding and its projections, the composition of the addition morphism $\mu : E \times E \longrightarrow E$ with each of the projections $\pi_i : E \to \mathbb{P}^1$ admits a basis of *bilinear* defining polynomials. For $\pi_1 \circ \mu$ $\pi_1 \circ \mu$, respectively, we have

$$\left\{ \begin{matrix} (X_0Y_0 + dX_3Y_3,\ X_1Y_2 + X_2Y_1), \\ (cX_1Y_1 + X_2Y_2,\ X_0Y_3 + X_3Y_0) \end{matrix} \right\} \text{ and } \left\{ \begin{matrix} (X_1Y_2 - X_2Y_1,\ -X_0Y_3 + X_3Y_0), \\ (X_0Y_0 - dX_3Y_3,\ -cX_1Y_1 + X_2Y_2) \end{matrix} \right\}.$$

Addition laws given by polynomial maps of bidegree $(2, 2)$ are recovered by composing with the Segre embedding. This factorization led the author to prove dimension formulas for these addition law projections and classify the exceptional divisors [17]. In particular, this permits one to prove *a priori* the form of the exceptional divisors described in Bernstein and Lange [3, Section 8], show that these addition laws span all possible addition laws of the given bidegree, and conclude their completeness.

4 Axioms for a D_4-linear model

The previous sections motivate the study of symmetric quartic models of elliptic curves with a rational 4-torsion point T. For such a model, we obtain a 4-dimensional linear representation of $D_4 \cong \langle [-1] \rangle \ltimes \langle \tau_T \rangle$, induced by the action on the linear automorphisms of $\mathbb{P}^3$. Here we give characterizations of elliptic curve models for which this representation is given by coordinate permutation.

Suppose that E/k is an elliptic curve with $\mathrm{char}(k) = 2$ and T a rational 4-torsion point. In view of the previous lemmas and the properties of Edwards' normal form, we consider reasonable hypotheses for a characteristic 2 analog. We note that in the Edwards model, τ_T acts by signed coordinate permutation, which we replace with a permutation action in characteristic 2.

1. The embedding of $E \to \mathbb{P}^3$ is a quadratic intersection.
2. E has a rational 4-torsion point T.
3. The group $\langle [-1] \rangle \ltimes \langle \tau_T \rangle \cong D_4$ acts by coordinate permutation, and in particular $\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2)$.
4. There exists a symmetric factorization of E through $\mathbb{P}^1 \times \mathbb{P}^1$.

Combining conditions 3 and 4, we assume that E lies in the skew-Segre image $X_0X_2 = X_1X_3$ of $\mathbb{P}^1 \times \mathbb{P}^1$. In order for the representation of τ_T to stabilize the image of $\mathbb{P}^1 \times \mathbb{P}^1$, we have

$$\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3,$$

whose image is $X_0X_2 = X_1X_3$, in isomorphism with $\mathbb{P}^1 \times \mathbb{P}^1$ by the projections

$$\pi_1(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_1), \\ (X_3 : X_2), \end{cases}, \ \pi_2(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_3), \\ (X_1 : X_2). \end{cases}$$

Secondly, up to isomorphism, there are *two* permutation representations of D_4, both having the same image. The two representations are distinguished by the image of $[-1]$, up to coordinate permutation, being one of the two

$$[-1](X_0 : X_1 : X_2 : X_3) = (X_3 : X_2 : X_1 : X_0) \text{ or } (X_0 : X_3 : X_2 : X_1).$$

Considering the form of the projection morphisms π_1 and π_2, we see that only the first of the possible actions of $[-1]$ stabilizes π_1 and π_2, while the second exchanges them. In the next section we are able to write down a normal form with D_4-permutation action associated to each of the possible actions of $[-1]$.

5 Normal forms

The objective of this section is to introduce elliptic curve models which satisfy the desired axioms of the previous section. After their definition we list their main properties, whose proof is essentially immediate from the symmetry properties of the model. We first present the objects of study over a general field k before passing to k of characteristic 2. Additional details of their construction can be found in the talk notes [18] where they were first introduced.

Definition 6. *An elliptic curve E/k in $\mathbb{P}^3$ is said to be in $\mathbf{Z}/4\mathbf{Z}$-normal form if it is given by the equations*

$$X_0^2 - X_1^2 + X_2^2 - X_3^2 = eX_0X_2 = eX_1X_3,$$

with identity $\mathrm{O} = (1 : 0 : 0 : 1)$.

The $\mathbf{Z}/4\mathbf{Z}$-normal form is the unique model, up to linear isomorphism (see Theorem 12), satisfying the complete set of axioms of the previous section. If we drop the condition for the factorization through $\mathbb{P}^1 \times \mathbb{P}^1$ (condition 4), we obtain the following normal form, which admits the alternative action of $[-1]$.

Definition 7. *An elliptic curve C/k in $\mathbb{P}^3$ is said to be in split $\boldsymbol{\mu}_4$-normal form if it is given by the equations*

$$X_0^2 - X_2^2 = c^2\, X_1 X_3,\ X_1^2 - X_3^2 = c^2\, X_0 X_2,$$

with identity $\mathrm{O} = (c : 1 : 0 : 1)$.

These normal forms both have good reduction in characteristic 2. The $\mathbf{Z}/4\mathbf{Z}$-normal form admits a rational 4-torsion point $T = (1 : 1 : 0 : 0)$, and the isomorphism

$$\langle T \rangle = \{(1:0:0:1), (1:1:0:0), (0:1:1:0), (0:0:1:1)\} \cong \mathbf{Z}/4\mathbf{Z}$$

gives the name to curves in this form.

On the split $\boldsymbol{\mu}_4$-normal form, the point $T = (1 : c : 1 : 0)$ is a rational 4-torsion point, and if $\mathrm{char}(k) \neq 2$ and there exists a primitive 4-th root of unity i in k, then $R = (c : i : 0, -i)$ is a rational 4-torsion point (dual to T under the Weil pairing) such that $\langle T, R \rangle = C[4]$. The subgroup

$$\langle R \rangle = \{(c:1:0:1), (c:i:0:-i), (c:-1:0:-1), (c:-i:0:i)\} \cong \boldsymbol{\mu}_4$$

is a group (scheme) isomorphic to the group (scheme) $\boldsymbol{\mu}_4$ of 4-th roots of unity, which gives the name to this normal form. The nonsplit variant (see Remark following Corollary 21) descends to any subfield containing c^4, does not necessarily have a rational 4-torsion point, but in the application to elliptic curves over finite fields of characteristic 2, every such model can be put in the split form. The action of the respective points T by translation gives the coordinate permutation action which we desire, the dual subgroup $\langle R \rangle$ degenerates in characteristic 2 to the identity group $\{\mathrm{O}\} = \{(c : 1 : 0 : 1)\}$, and the embedding divisor $3(\mathrm{O}) + (S)$, where $S = 2R$, degenerates to $4(\mathrm{O})$. Hereafter we consider these models only over a field of characteristic 2.

We now formally state and prove the main symmetry properties of the new models over a field of characteristic 2 with analogy to the Edwards model.

Theorem 8. *Let E/k be a curve in $\mathbf{Z}/4\mathbf{Z}$-normal form over a field of characteristic 2.*

1. *The embedding divisor class is $3(\mathrm{O}) + (S)$ where $S = (0 : 1 : 1 : 0) = 2T$.*
2. *The point $T = (1 : 1 : 0 : 0)$ is a rational 4-torsion point.*
3. *The translation–by–T and inverse morphisms are given by:*

$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2),$$
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_3 : X_2 : X_1 : X_0).$$

4. E admits a factorization through $\mathbb{P}^1 \times \mathbb{P}^1$, where

$$\pi_1(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_1), \\ (X_3 : X_2), \end{cases}, \ \pi_2(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0 : X_3), \\ (X_1 : X_2). \end{cases}$$

More precisely, if (U_0, U_1) and (V_0, V_1) are the coordinate functions on $\mathbb{P}^1 \times \mathbb{P}^1$, the product morphism $\pi_1 \times \pi_2$ determines an isomorphism $E \to E_1$, where E_1 is the curve $(U_0+U_1)^2(V_0+V_1)^2 = cU_0U_1V_0V_1$, whose inverse is the restriction of the skew-Segre embedding $((U_0 : U_1), (V_0 : V_1)) \longrightarrow (U_0V_0 : U_1V_0 : U_1V_1 : U_0V_1)$.

Proof. The correctness of the forms for $[-1]$ and τ_T follow from the fact that they are automorphisms, that the asserted map for $[-1]$ fixes O and that for τ_T has no fixed point, and that $\tau_T(\mathrm{O}) = T$. Since $\tau_T^4 = 1$, it follows that T is 4-torsion. The hypersurface $X_0 + X_1 + X_2 + X_3 = 0$ cuts out the subgroup $\langle T \rangle \cong \mathbf{Z}/4\mathbf{Z}$, which determines the embedding divisor class as $3(\mathrm{O})+(S)$ where $S = \mathrm{O}+T+2T+3T = 2T \in E[2]$. The factorization is determined by the automorphism group, and the image curve can be verified by elementary substitution. □

Lemma 9. *The $\mathbf{Z}/4\mathbf{Z}$-normal form is isomorphic to a curve in Weierstrass form $Y(Y+X)Z = X(X+c^{-1}Z)^2$. The linear map $(X : Y : Z) = (X_1 + X_2 : X_2 : c(X_0 + X_3))$ defines the isomorphism except at* O.

Proof. The existence of a linear map is implied by Kohel [17, Lemma 3], and the exact form of this map can be easily verified. The exceptional divisor of the given rational map follows since $X_1 = X_2 = 0$ only meets the curve at O. □

Theorem 10. *Let C/k be a curve in $\boldsymbol{\mu}_4$-normal form over a field of characteristic* 2*.*

1. *The embedding divisor class of C is* $4(\mathrm{O})$*.*
2. *The point $T = (1 : c : 1 : 0)$ is a rational* 4*-torsion point.*
3. *The translation–by–T and inverse morphisms are given by:*

$$\begin{aligned} \tau_T(X_0 : X_1 : X_2 : X_3) &= (X_3 : X_0 : X_1 : X_2), \\ [-1](X_0 : X_1 : X_2 : X_3) &= (X_0 : X_3 : X_2 : X_1). \end{aligned}$$

Proof. As in Theorem 8, the correctness of automorphisms is implied by action on the points O and T, and the relation $\tau_T^4 = 1$ shows that T is 4-torsion. Since the hyperplanes $X_i = 0$ cut out the divisors $4(T_{i+2})$ where $T_k = kT$, and T is 4-torsion, this gives the form of the embedding divisor class. □

Lemma 11. *An elliptic curve in split $\boldsymbol{\mu}_4$-normal form is isomorphic to the curve $Y(Y+X)Z = X(X+c^{-2}Z)^2$ in Weierstrass form. The linear map $(X : Y : Z) = (c(X_1 + X_3) : X_0 + cX_1 + X_2 : c^4X_2)$ defines the isomorphism except at* O*.*

Proof. As above, the existence of a linear map is implied by Kohel [17, Lemma 3], and the exact form of this map can be easily verified. The exceptional divisor of the given rational map follows since $X_2 = 0$ only meets the curve at O. □

Remark. The rational maps of Lemma 9 and 11 extend to isomorphisms, but there is no base-point free linear representative for these isomorphisms.

6 Isomorphisms with normal forms

Let E_{c^2} denote an elliptic curve in $\mathbf{Z}/4\mathbf{Z}$-normal form and C_c a curve in $\boldsymbol{\mu}_4$-normal form. By Lemmas 9 and 11, the curves E_{c^2} and C_c are isomorphic, but by classification of their embedding divisor classes in Theorems 8 and 10, it follows from Lemma 4 that there is no linear isomorphism between them. In this section we obtain a classification of curves over with rational 4-torsion point and make the isomorphism explicit for E_{c^2} and C_c.

Theorem 12. *Let X/k be an elliptic curve over a field k of characteristic 2, with identity O and k-rational point T of order 4, and suppose that c is an element of k such that $j(X) = c^8$.*

1. *There exists a unique isomorphism of X over k to a curve E_{c^2} in $\mathbf{Z}/4\mathbf{Z}$-normal form sending O to $(1:0:0:1)$ and T to $(1:1:0:0)$.*
2. *There exists a unique isomorphism of X over k to a curve C_c in split $\boldsymbol{\mu}_4$-normal form sending O to $(c:1:0:1)$ and T to $(1:c:1:0)$.*

If X is embedded as a symmetric quartic model in $\mathbb{P}^3$, then either the isomorphism of X with E_{c^2} or the isomorphism with C_c is induced by a linear automophism of $\mathbb{P}^3$.

Proof. The j-invariants of E_{c^2} and C_c are each c^8 ($\neq 0$ since X is not supersingular by existence of a 2-torsion point), which implies the existence of the isomorphisms over the algebraic closure. The rational 4-torsion point T fixes the quadratic twist, hence the isomorphism is defined over k. Since there is a unique 2-torsion point $S = 2T$, the embedding divisor of X in $\mathbb{P}^3$ is either $3(\mathrm{O}) + (S)$ or $4(\mathrm{O})$ by Lemma 2. In the former case, the isomorphism to E_{c^2} is linear, and in the latter case the isomorphism to C_c is linear by Lemma 5. □

The following theorem classifies the isomorphisms between E_{c^2} and C_c.

Theorem 13. *Let C_c be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form and E_{c^2} an elliptic curve in $\mathbf{Z}/4\mathbf{Z}$-normal form. Then there exists an isomorphism $\iota : C_c \to E_{c^2}$ determined by the projections*

$$\pi_1 \circ \iota((X_0 : X_1 : X_2 : X_3)) = \begin{cases} (cX_0 : X_1 + X_3), \\ (X_1 + X_3 : cX_2), \end{cases}$$
$$\pi_2 \circ \iota((X_0 : X_1 : X_2 : X_3)) = \begin{cases} (X_0 + X_2 : cX_1), \\ (cX_3 : X_0 + X_2). \end{cases}$$

The morphism to E_{c^2} is recovered by composing $\pi_1 \times \pi_2$ with the skew-Segre embedding. The inverse morphism is given by

$$\iota^{-1}(X_0 : X_1 : X_2 : X_3) = \begin{cases} (X_0X_1 + X_2X_3 : cX_2^2 : X_0X_1 + c^2X_1X_2 + X_2X_3 : cX_1^2), \\ (X_0X_3 : (X_2 + X_3)^2 : X_1X_2 : (X_0 + X_1)^2), \\ ((X_0 + X_3)^2 : cX_2X_3 : (X_1 + X_2)^2 : cX_0X_1), \\ (cX_3^2 : X_0X_3 + X_1X_2 + c^2X_2X_3 : cX_2^2 : X_1X_2 + X_0X_3). \end{cases}$$

Neither ι nor its inverse can be represented by a projective linear transformation.

Proof. This correctness of this isomorphism can be verified explicitly (e.g. as implemented in Echidna [19]). The nonexistence of a linear isomorphism is a consequence of Lemma 4 and the classification of the embedding divisor classes in Theorems 8 and 10. □

7 Addition law structure and efficient arithmetic

The interest in alternative models of elliptic curves has been driven by the simple form of their *addition laws* — the polynomial maps which define the addition morphism $\mu : E \times E \to E$ as rational maps. In this section we determine bases of simple forms for the addition laws of the $\mathbf{Z}/4\mathbf{Z}$-normal form and of the $\boldsymbol{\mu}_4$-normal form.

The verification that a system of putative addition laws determines a well-defined morphism can be verified symbolically. In particular we refer to the implementations of these models and their addition laws in Echidna [19] (in the Magma [21] language) for a verification that the systems are consistent and define rational maps. The dimensions of the spaces of given bidegree are known *a priori* by Kohel [17], as well as their completeness as morphisms. By the Rigidity Theorem [22, Theorem 2.1], a morphism μ of abelian varieties is the composition of a homomorphism and translation. In order to verify that $\mu : E \times E \to E$ is the addition morphism, it suffices to check that the restrictions of μ to $E \times \{\mathrm{O}\}$ and $\{\mathrm{O}\} \times E$ agree with the restrictions of π_1 and π_2, respectively. Similarly, for a particular addition law of bidegree $(2, 2)$, the exceptional divisors, on which the polynomials of the addition law simultaneously vanish, are known by Lange and Ruppert [20] and the generalizations in Kohel [17] to have components of the form $\Delta_P = \{(P + Q, Q) \mid Q \in E\}$. Consequently, as pointed out in Kohel [17] (Corollary 11 and the Remark following Corollary 12), the exceptional divisors can be computed (usually by hand) by intersecting with $E \times \{\mathrm{O}\}$.

Addition law structure for the Z/4Z-normal form

Theorem 14. *Let E/k, $\mathrm{char}(k) = 2$, be an elliptic curve in $\mathbf{Z}/4\mathbf{Z}$-normal form:*

$$(X_0 + X_1 + X_2 + X_3)^2 = cX_0X_2 = cX_1X_3.$$

Bases for the bilinear addition law projections $\pi_1 \circ \mu$ and $\pi_2 \circ \mu$ are, respectively:

$$\left\{ \begin{matrix} (X_0Y_3 + X_2Y_1,\ X_1Y_0 + X_3Y_2), \\ (X_1Y_2 + X_3Y_0,\ X_0Y_1 + X_2Y_3) \end{matrix} \right\} \text{ and } \left\{ \begin{matrix} (X_0Y_0 + X_2Y_2,\ X_1Y_1 + X_3Y_3), \\ (X_1Y_3 + X_3Y_1,\ X_0Y_2 + X_2Y_0) \end{matrix} \right\}.$$

Addition laws of bidegree $(2, 2)$ are recovered by composition with the skew-Segre embedding $s((U_0 : U_1), (V_0 : V_1)) = (U_0V_0 : U_1V_0 : U_1V_1 : U_0V_1)$. Each of these basis elements has an exceptional divisor of of the form $2\Delta_{nT}$ for some $0 \leq n \leq 3$.

Proof. That the addition laws determine a well-defined morphism is verified symbolically.[6] The morphism is the addition morphism since the substitution

[6] In Echidna [19], the constructor is `EllipticCurve_C4_NormalForm` after which `AdditionMorphism` returns this morphism as a composition.

$(Y_0, Y_1, Y_2, Y_3) = (1, 0, 0, 1)$, gives the projection onto the first factor. By symmetry of the spaces in X_i and Y_i, the same holds for the second factor.

The form of the exceptional divisor is verified by a similar substitution. For example, for the exceptional divisor $X_1Y_2 + X_3Y_0 = X_0Y_1 + X_2Y_3 = 0$, we intersect with $(Y_0, Y_1, Y_2, Y_3) = (1, 0, 0, 1)$ to find $X_3 = X_2 = 0$, which defines the unique point $T = (1, 1, 0, 0)$ with a multiplicity of 2, hence the exceptional divisor is $2\Delta_T$. The other exceptional divisors are determined similarly. □

Remark. We observe that the entire space of addition laws of bidgree $(2, 2)$ is independent of the curve parameters. This is not a feature of the Edwards addition laws.

Corollary 15. *Addition of generic points on E can be carried out in* $12\mathbf{M}$.

Proof. Since each of the pairs is equivalent under a permutation of the input variables it suffices to consider the first, which each require $4\mathbf{M}$. Composition with the skew-Segre embedding requires an additional $4\mathbf{M}$, which yields the bound of $12\mathbf{M}$. □

Evaluation of the addition forms along the diagonal yields the duplication formulas.

Corollary 16. *Let $E = E_c$ be an elliptic curve in $\mathbf{Z}/4\mathbf{Z}$-normal form. The duplication morphism on E is given by*

$$\pi_1 \circ [2](X_0 : X_1 : X_2 : X_3) = (X_0X_3 + X_1X_2 : X_0X_1 + X_2X_3),$$
$$\pi_2 \circ [2](X_0 : X_1 : X_2 : X_3) = ((X_0 + X_2)^2 : (X_1 + X_3)^2),$$

composed with the skew-Segre embedding.

This immediately gives the following complexity for duplication.

Corollary 17. *Duplication on E can be carried out in* $7\mathbf{M} + 2\mathbf{S}$.

Proof. The pair $(X_0X_3 + X_1X_2, X_0X_1 + X_2X_3)$ can be computed with $3\mathbf{M}$ by exploiting the usual Karatsuba trick using the factorization of their sum:

$$(X_0X_3 + X_1X_2) + (X_0X_1 + X_2X_3) = (X_0 + X_2)(X_1 + X_3).$$

After the two squarings, the remaining $4\mathbf{M}$ come from the Segre morphism. □

Addition law structure for the split $\boldsymbol{\mu_4}$-normal form

Theorem 18. *Let C be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form:*

$$(X_0 + X_2)^2 = c^2\, X_1X_3,\ (X_1 + X_3)^2 = c^2\, X_0X_2.$$

A basis for the space of addition laws of bidegree $(2, 2)$ is given by:

$$\left\{\begin{array}{l}((X_0Y_0+X_2Y_2)^2,\, c(X_0X_1Y_0Y_1+X_2X_3Y_2Y_3),\, (X_1Y_1+X_3Y_3)^2,\, c(X_0X_3Y_0Y_3+X_1X_2Y_1Y_2)),\\ (c(X_0X_1Y_0Y_3+X_2X_3Y_1Y_2),\, (X_1Y_0+X_3Y_2)^2,\, c(X_0X_3Y_2Y_3+X_1X_2Y_0Y_1),\, (X_0Y_3+X_2Y_1)^2),\\ ((X_3Y_1+X_1Y_3)^2,\, c(X_0X_3Y_1Y_2+X_1X_2Y_0Y_3),\, (X_0Y_2+X_2Y_0)^2,\, c(X_0X_1Y_2Y_3+X_2X_3Y_0Y_1)),\\ (c(X_0X_3Y_0Y_1+X_1X_2Y_2Y_3),\, (X_0Y_1+X_2Y_3)^2,\, c(X_0X_1Y_1Y_2+X_2X_3Y_0Y_3),\, (X_1Y_2+X_3Y_0)^2).\end{array}\right\}$$

The exceptional divisor of each addition law is of the form $4\Delta_{nT}$.

Proof. As for the $\mathbf{Z}/4\mathbf{Z}$-normal form the consistency of the addition laws is verified symbolically[7] and the space is known to have dimension four by Kohel [17]. Evaluation of the first addition law at $(Y_0, Y_1, Y_2, Y_3) = (c, 1, 0, 1)$ gives

$$(c^2X_0^2,\, c^2X_0X_1,\, (X_1+X_3)^2,\, c^2X_0X_3).$$

Using $(X_1+X_3)^2 = c^2X_0X_2$, after removing the common factor c^2X_0, this agrees with projection to the first factor, and identifies the exceptional divisor $4\Delta_S$ where S is the 2-torsion point $(0:1:c:1)$ with $X_0 = 0$. □

Corollary 19. *Addition of generic points on* C *can be carried out in* $7\mathbf{M}+2\mathbf{S}+2\mathbf{m}_c$.

Proof.
- Evaluate $(Z_0, Z_1, Z_2, Z_3) = (X_0Y_0, X_1Y_1, X_2Y_2, X_3Y_3)$ with $4\mathbf{M}$.
- Evaluate $(X_0Y_0+X_2Y_2)^2 = (Z_0+Z_2)^2$ with $1\mathbf{S}$.
- Evaluate $(X_1Y_1+X_3Y_3)^2 = (Z_1+Z_3)^2$ with $1\mathbf{S}$.
- Evaluate $(X_0Y_0+X_2Y_2)(X_1Y_1+X_3Y_3) = (Z_0+Z_2)(Z_1+Z_3)$ followed by

$$\begin{aligned}X_0X_1Y_0Y_1+X_2X_3Y_2Y_3 &= Z_0Z_1+Z_2Z_3\\ X_0X_3Y_0Y_3+X_1X_2Y_1Y_2 &= Z_0Z_3+Z_1Z_2\end{aligned}$$

  using $3\mathbf{M}$, exploiting the linear relation (following Karatsuba):

$$(Z_0+Z_2)(Z_1+Z_3) = (Z_0Z_1+Z_2Z_3)+(Z_0Z_3+Z_1Z_2).$$

After two scalar multiplications by c, we obtain $7\mathbf{M}+2\mathbf{S}+2\mathbf{m}_c$ for the computation using the first addition law. □

Specializing this to the diagonal we find defining polynomials for duplication.

Corollary 20. *The duplication morphism on an elliptic curve* C *in split* $\boldsymbol{\mu}_4$*-normal form is given by*

$$\begin{aligned}&[2](X_0:X_1:X_2:X_3) =\\ &\quad((X_0+X_2)^4 : c(X_0X_1+X_2X_3)^2 : (X_1+X_3)^4 : c(X_0X_3+X_1X_2)^2).\end{aligned}$$

This gives an obvious complexity bound of $3\mathbf{M}+6\mathbf{S}+2\mathbf{m}_c$ for duplication, however we note that along the curve we have the following equivalent expressions:

$$\begin{aligned}c^2(X_0X_1+X_2X_3)^2 &= (X_0+X_2)^4+c^{-4}(X_1+X_3)^4+F^2,\\ c^2(X_0X_3+X_1X_2)^2 &= (X_0+X_2)^4+c^{-4}(X_1+X_3)^4+G^2,\end{aligned}$$

[7] The Echidna [19] constructor is `EllipticCurve_Split_Mu4_NormalForm` after which `AdditionMorphism` returns this morphism as a composition.

for $F = (X_0 + cX_3)(cX_1 + X_2)$ and $G = (X_0 + cX_1)(X_2 + cX_3)$, and that

$$F + G = c(X_0 + X_2)(X_1 + X_3).$$

This leads to a savings of $1\mathbf{M} + 1\mathbf{S}$ from the naive analysis, at the cost of extra multiplications by c.

Corollary 21. *Duplication on C can be carried out in $2\mathbf{M} + 5\mathbf{S} + 7\mathbf{m}_c$.*

Proof. We describe the evaluation of the forms of Corollary 20, using the equivalent expressions. Setting $(U, V, W) = ((X_0 + X_2)^2, (X_1 + X_3)^2, (X_0 + cX_1)^2)$,

$$G^2 = (U + c^2V + W)\,WP \text{ and } F^2 = G^2 + c^2UV,$$

from which the duplication formula can be expressed as:

$$(cU^2 : U^2 + c^{-4}V^2 + (U + c^2V + W)W + c^2UV : cV^2 : U^2 + c^{-4}V^2 + (U + c^2V + W)W).$$

We scale by c^4 to have only integral powers of c, which gives the

- Evaluate $(U, V, W) = ((X_0 + X_2)^2, (X_1 + X_3)^2, (X_0 + cX_1)^2)$ with $3\mathbf{S} + 1\mathbf{m}_c$.
- Evaluate $c^5(X_0 + X_2)^4 = c^5U^2$ with $1\mathbf{S} + 1\mathbf{m}_c$, storing U^2.
- Evaluate $c^5(X_1 + X_3)^4 = c^5V^2$ with $1\mathbf{S} + 1\mathbf{m}_c$, storing V^2.
- Evaluate c^2V, c^2UV, $(U + c^2V + W)\,W$ with $2\mathbf{M} + 1\mathbf{m}_c$, then set

$$\begin{aligned} &c^4(X_0 + X_2)^4 + (X_1 + X_3)^4 = c^4U^2 + V^2, \\ &c^4G^2 = c^4(U + c^2V + W)\,W, \\ &c^4F^2 = c^4G^2 + c^6UV, \end{aligned}$$

using $3m_c$, followed by additions. This gives the asserted complexity. □

Remark. The triple (U, V, W), up to scalars, can be identified with the variables (A, B, C) of the EFD [6] in the improvement of Bernstein et al. [4] to the duplication algorithm of Kim and Kim [16] in "extended López-Dahab coordinates" with $a_2 = 0$. In brief, the extended López-Dahab coordinates defines a curve $Y^2 = (X^2 + a_6)XZ$, in a $(1, 2, 1, 2)$-weighted projective space with coordinate functions X, Y, Z, Z^2. We embed this in a standard $\mathbb{P}^3$, with embedding divisor class 4(O), by the map (X^2, Y, XZ, Z^2). By Lemma 5 this is linearly isomorphic to the curve C in split $\boldsymbol{\mu}_4$-normal form. One derives an equivalent complexity for duplication on this $\mathbb{P}^3$ model, and duplication on C differs only by the cost of scalar multiplications involved in the linear transformation to C.

We remark that this can be interpretted as a factorization of the duplication map as follows. Letting D be the image of C given by (U, V, W) in $\mathbb{P}^2$, the Kim and Kim algorithm can be expressed as a composition $C \xrightarrow{\varphi} D \xrightarrow{\psi} C$ where φ and ψ are each of degree 2, with φ purely inseparable and ψ separable. The curve D is a singular quartic curve in $\mathbb{P}^2$, given by a well-chosen incomplete linear system. The nodal singularities of D are oriented such that the resolved points have the same image under ψ. The omission of a fourth basis element of the complete linear system allows one to save $1\mathbf{S}$ in its computation.

In order to best optimize the multiplications by scalars, we can apply a coordinate scaling. The split $\boldsymbol{\mu}_4$-normal descends to a (non-split) $\boldsymbol{\mu}_4$-normal form over any subfield containing the parameter $s = c^{-4}$, by renormalization of coordinates:

$$s(X_1 + X_3)^2 + X_0X_2,\ (X_0 + X_2)^2 = X_1X_3.$$

In this form the duplication polynomials require fewer multiplications by constants:

$$\begin{array}{l}\big((X_0 + X_2)^4 : (X_0 + X_2)^4 + s^2(X_1 + X_3)^4 + (X_0 + X_3)^2(X_1 + X_2)^2 : \\ s(X_1 + X_3)^4 : (X_0 + X_2)^4 + s^2(X_1 + X_3)^4 + (X_0 + X_1)^2(X_2 + X_3)^2 \big),\end{array}$$

yielding $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}_s$.

Addition law projections for the split $\boldsymbol{\mu}_4$-normal form

Let $C = C_c$ be an elliptic curve in $\boldsymbol{\mu}_4$-normal form and $E = E_{c^2}$ be an elliptic curve in $\mathbf{Z}/4\mathbf{Z}$-normal form. In view of Theorem 13, there is an explicit isomorphism $\iota : C \to E$, determined by the application of the skew-Segre embedding to the pair of projections $\pi_i : C \to \mathbb{P}^1$:

$$\begin{aligned}\pi_1((X_0 : X_1 : X_2 : X_3)) &= \begin{cases}(cX_0 : X_1 + X_3), \\ (X_1 + X_3 : cX_2),\end{cases} \\ \pi_2((X_0 : X_1 : X_2 : X_3)) &= \begin{cases}(X_0 + X_2 : cX_1), \\ (cX_3 : X_0 + X_2).\end{cases}\end{aligned}$$

The first projection π_1 determines a map to $C/\langle[-1]\rangle \cong \mathbb{P}^1$, and the second projection π_2 satisfies $\pi_2 \circ [-1] = \sigma \circ \pi_2$, where $\sigma((U_0 : U_1)) = (U_1 : U_0)$. As a consequence of the addition law structure of Theorem 18, the addition law projections $C \times C \to \mathbb{P}^1$ associated to these projections take a particularly simple form.

Corollary 22. *If $\pi_i : C \to \mathbb{P}^1$ are the projections defined above, the addition law projections $\pi_1 \circ \mu$ and $\pi_2 \circ \mu$ are respectively spanned by*

$$\left\{ \begin{array}{l}(X_0Y_0 + X_2Y_2, X_1Y_1 + X_3Y_3), \\ (X_1Y_3 + X_3Y_1, X_2Y_0 + X_0Y_2)\end{array} \right\} \text{ and } \left\{ \begin{array}{l}(X_0Y_3 + X_2Y_1, X_1Y_0 + X_3Y_2), \\ (X_1Y_2 + X_3Y_0, X_0Y_1 + X_2Y_3)\end{array} \right\}.$$

Proof. The addition law projections can be verified in Echidna [19]. □

The skew-Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ in $\mathbb{P}^3$ induces a map to the isomorphic curve E in $\mathbf{Z}/4\mathbf{Z}$-normal form, rather than the $\boldsymbol{\mu}_4$-normal form. These addition law projections play a central role in the study of the Kummer arithmetic in Section 8, defined more naturally in terms of E.

8 Kummer quotients and the Montgomery ladder

For an abelian variety A, the quotient variety $\mathscr{K}(A) = A/\{[\pm 1]\}$ is called the Kummer variety of A. We investigate explicit models for the Kummer curves $\mathscr{K}(E)$ and $\mathscr{K}(C)$ where $E = E_{c^2}$ and $C = C_c$ are isomorphic elliptic curves in $\mathbf{Z}/4\mathbf{Z}$-normal form and $\boldsymbol{\mu}_4$-normal form, respectively. The objective of this study is to obtain a Montgomery ladder [23] for efficient scalar multiplication on these curves. Such a Montgomery ladder was developed for Kummer curves (or *lines* since they are isomorphic to the projective line $\mathbb{P}^1$) in characteristic 2 by Stam [24]. More recently Gaudry and Lubicz [12] developed efficient pseudo-addition natively on a Kummer line $\mathscr{K} = \mathbb{P}^1$ by means of theta identities. Neither the method of Stam nor Gaudry and Lubicz provides recovery of points on the curve. We show that for fixed P, the morphism $E \to \mathscr{K} \times \mathscr{K}$ sending Q to $(\overline{Q}, \overline{Q - P})$, used for initialization of the Montgomery ladder, is in fact an isomorphism with its image. As a consequence we rederive the equations of Gaudry and Lubicz for pseudo-addition, together with an algorithm for point recovery. In addition, knowledge of the curve equation (in $\mathscr{K} \times \mathscr{K}$) permits the trade-off of a squaring for a multiplication by a constant depending on the base point P (see Corollary 26).

Kummer curves

We consider the structure of $\mathscr{K}(E) = E/\{[\pm 1]\}$ and $\mathscr{K}(C) = C/\{[\pm 1]\}$ for elliptic curves $E = E_{c^2}$ in $\mathbf{Z}/4\mathbf{Z}$-normal form and $C = C_c$ in split $\boldsymbol{\mu}_4$-normal form, respectively. The former has a natural identification with $\mathbb{P}^1$ equipped with the covering $\pi_1 : E \to \mathscr{K}(E)$, given by

$$(X_0 : X_1 : X_2 : X_3) \mapsto \begin{cases} (X_0 : X_1), \\ (X_3 : X_2). \end{cases}$$

The latter quotient has a plane model $\mathscr{K}(C) : Y^2 = c^2 XZ$ in $\mathbb{P}^2$ obtained by taking the $[-1]$-invariant basis $\{X_0, X_1 + X_3, X_2\}$. For $E = E_{c^2}$ and $C = C_c$ as above, the isomorphism $\iota : C \to E$ of Theorem 13 induces an isomorphism $\iota : \mathscr{K}(C) \to \mathscr{K}(E) = \mathbb{P}^1$ of Kummer curves given by

$$\iota(X : Y : Z) = \begin{cases} (cX : Y), \\ (Y : cZ), \end{cases}$$

with inverse $(U_0 : U_1) \mapsto (U_0^2 : cU_0U_1 : U_1^2)$. Hereafter we fix this isomorphism, and obtain the covering morphism $C \to \mathscr{K}(E)$:

$$(X_0 : X_1 : X_2 : X_3) \mapsto \begin{cases} (cX_0 : X_1 + X_3), \\ (X_1 + X_3 : cX_2). \end{cases}$$

We denote this common Kummer curve by $\mathscr{K}$, to distinguish the curve with induced structure from the elliptic curve covering (by both E and C) from $\mathbb{P}^1$.

Montgomery endomorphism

The Kummer curve $\mathscr{K}$ (of an arbitrary elliptic curve E) no longer supports an addition morphism, however scalar multiplication $[n]$ is well-defined, since $[-1]$ commutes with $[n]$. We investigate the general construction of the Montgomery ladder for the Kummer quotient. For this purpose we define the *Montgomery endomorphism* $E \times E \to E \times E$:

$$\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} (Q, R) = (2Q, Q + R).$$

In general this endomorphism, denoted φ, is not well-defined on $\mathscr{K} \times \mathscr{K}$. Instead, for fixed $P \in E(k)$ we consider

$$\Delta_P = \{(Q, R) \in E \times E \mid Q - R = P\} \cong E,$$

and let $\mathscr{K}(\Delta_P)$ be the image of Δ_P in $\mathscr{K} \times \mathscr{K}$, which we call a *Kummer-oriented curve*. In what follows we develop algorithmically the following observations (see Theorems 23, 24, and 25):

1. The morphism $\Delta_P \to \mathscr{K}(\Delta_P)$ is an isomorphism for any $P \notin E[2]$.
2. The Montgomery endomorphism is well-defined on $\mathscr{K}(\Delta_P)$.

By means of the elliptic curve structure on Δ_P determined by the isomorphism $E \to \Delta_P$ given by $Q \mapsto (Q, Q - P)$, the Montgomery endomorphism is the duplication morphism (i.e. $\varphi(Q, Q-P) = (2Q, 2Q-P)$). On the other hand, the Montgomery endomorphism allows us to represent scalar multiplication on P symmetrically as a sequence of compositions. Precisely, we let $\varphi_0 = \varphi$, let σ be the involution $\sigma(Q, R) = (-R, -Q)$ of Δ_P, which induces the exchange of factors on $\mathscr{K}(\Delta_P)$, and set $\varphi_1 = \sigma \circ \varphi \circ \sigma$. For an integer n with binary representation $n_r n_{r-1} \dots n_1 n_0$ we may compute nP by the sequence

$$\varphi_{n_0} \circ \varphi_{n_1} \cdots \circ \varphi_{n_{r-1}}(P, \mathrm{O}) = ((n+1)P, nP),$$

returning the second component.

This composition representation for scalar multiplication on $E \times E$ is a double-and-always-add algorithm [9], which provides a symmetry protection against side-channel attacks in cryptography (see Joye and Yen [15, Section 4]), but is inefficient due to insertion of redundant additions. When applied to $\mathscr{K}(\Delta_P)$, on the other hand, this gives a (potentially) efficient algorithm, conjugate duplication, for carrying out scalar multiplication. In view of this, $\mathscr{K}(\Delta_P)$ should be thought of as a model oriented for carrying out efficient scalar multiplication on a fixed point P in $E(k)$.

The Kummer-oriented curves $\mathscr{K}(\Delta_P)$

Let $E = E_{c^2}$ be a curve in $\mathbf{Z}/4\mathbf{Z}$-normal form, let $P = (t_0 : t_1 : t_2 : t_3)$ be a fixed point in $E(k)$, and let $\mathscr{K}(\Delta_P)$ be the Kummer-oriented curve in $\mathscr{K}^2$, with coordinate functions $((U_0, U_1), (V_0, V_1))$.

Theorem 23. *The Kummer-oriented curve $\mathscr{K}(\Delta_P)$ in $\mathscr{K}^2$, for $P = (t_0 : t_1 : t_2 : t_3)$, has defining equation*

$$t_0^2(U_0V_1 + U_1V_0)^2 + t_1^2(U_0V_0 + U_1V_1)^2 = c^2 t_0 t_1 U_0 U_1 V_0 V_1.$$

If P is not a 2-torsion point, the morphism $\kappa : E \to \mathscr{K}(\Delta_P)$, defined by $Q \mapsto (\overline{Q}, \overline{Q - P})$, is an isomorphism, given by

$$\pi_1 \circ \kappa(X_0 : X_1 : X_2 : X_3) = (U_0 : U_1) = \begin{cases} (X_0 : X_1), \\ (X_3 : X_2), \end{cases}$$

$$\pi_2 \circ \kappa(X_0 : X_1 : X_2 : X_3) = (V_0 : V_1) = \begin{cases} (t_0X_0 + t_2X_2 : t_3X_1 + t_1X_3), \\ (t_1X_1 + t_3X_3 : t_2X_0 + t_0X_2), \end{cases}$$

with inverse

$$\pi_1 \circ \kappa^{-1}((U_0 : U_1), (V_0 : V_1)) = (U_0 : U_1)$$

$$\pi_2 \circ \kappa^{-1}((U_0 : U_1), (V_0 : V_1)) = \begin{cases} (t_1U_0V_0 + t_2U_1V_1 : t_0U_0V_1 + t_3U_1V_0), \\ (t_3U_0V_1 + t_0U_1V_0 : t_2U_0V_0 + t_1U_1V_1). \end{cases}$$

Proof. The form of κ follows from the definition of the addition law. The equation for the image curve can be computed by taking resultants, and verified symbolically. The composition of κ with projection onto the first factor is the Kummer quotient of degree 2. However, for all P not in $E[2]$, the inverse morphism induces a nontrivial involution

$$(\overline{Q}, \overline{Q - P}) \longmapsto (\overline{-Q}, \overline{-Q - P}) = (\overline{Q}, \overline{Q + P})$$

on $\mathscr{K}(\Delta_P)$. Consequently the map to $\mathscr{K}(\Delta_P)$ has degree one, and being nonsingular, gives an isomorphism. □

Remark. We observe that $\mathscr{K}(\Delta_P) = \mathscr{K}(\Delta_{-P})$ in $\mathscr{K}^2$, but that a change of base point changes κ by $[-1]$.

The isomorphism of E_{c^2} with C_c lets us derive the analogous result for curves in $\boldsymbol{\mu}_4$-normal form.

Theorem 24. *Let $C = C_c$ be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form with rational point $S = (s_0 : s_1 : s_2 : s_3)$. The Kummer-oriented curve $\mathscr{K}(\Delta_S)$ in $\mathscr{K}^2$ is given by the equation*

$$s_0(U_0V_1 + U_1V_0)^2 + s_2(U_0V_0 + U_1V_1)^2 = c(s_1 + s_3)U_0U_1V_0V_1.$$

If S is not a 2-torsion point, the morphism $\lambda : C \to \mathscr{K}(\Delta_S)$ is an isomorphism, and defined by

$$\pi_1 \circ \lambda(X_0 : X_1 : X_2 : X_3) = \begin{cases} (cX_0 : X_1 + X_3), \\ (X_1 + X_3 : cX_2), \end{cases}$$

$$\pi_2 \circ \lambda(X_0 : X_1 : X_2 : X_3) = \begin{cases} (s_0X_0 + s_2X_2 : s_1X_1 + s_3X_3), \\ (s_3X_1 + s_1X_3 : s_2X_0 + s_0X_2), \end{cases}$$

with inverse $\lambda^{-1}((U_0 : U_1), (V_0 : V_1))$ equal to

$$\begin{cases}((s_1+s_3)U_0^2V_0 : (s_0U_0^2+s_2U_1^2)V_1 + cs_1U_0U_1V_0 : (s_1+s_3)U_1^2V_0 : (s_0U_0^2+s_2U_1^2)V_1 + cs_3U_0U_1V_0),\\ ((s_1+s_3)U_0^2V_1 : (s_2U_0^2+s_0U_1^2)V_0 + cs_3U_0U_1V_1 : (s_1+s_3)U_1^2V_1 : (s_2U_0^2+s_0U_1^2)V_0 + cs_1U_0U_1V_1).\end{cases}$$

Proof. The isomorphism $\iota : E_{c^2} \to C_c$ sending S to $T = (t_0 : t_1 : t_2 : t_3)$ induces the isomorphism $(s_0 : s_1+s_3 : s_2) = (t_0^2 : ct_0t_1 : t_1^2)$, by which we identify $\mathscr{K}(\Delta_P)$ and $\mathscr{K}(\Delta_S)$. The form of the morphism λ follows from the form of projective addition laws of Corollary 22, and its inverse can be verified symbolically. □

We now give explicit maps and complexity analysis for the Montgomery endomorphism $\varphi(Q, R) = (2Q, Q+R)$, on the Kummer quotient $\mathscr{K}(\Delta_P)$ (or $\mathscr{K}(\Delta_S)$ setting $(t_0 : t_1) = (cs_0 : s_1 + s_3) = (s_1 + s_3 : cs_2)$). In view of the application to scalar multiplication on E or C, this gives an asymptotic complexity per bit of n, for computing $[n]P$.

Theorem 25. *The Montgomery endomorphism φ is defined by:*

$$\begin{aligned}\pi_1 \circ \varphi((U_0 : U_1), (V_0 : V_1)) &= (U_0^4 + U_1^4 : cU_0^2U_1^2),\\ \pi_2 \circ \varphi((U_0 : U_1), (V_0 : V_1)) &= (t_1(U_0V_0 + U_1V_1)^2 : t_0(U_0V_1 + U_1V_0)^2).\end{aligned}$$

The sets of defining polynomials are well-defined everywhere and the following maps are projectively equivalent modulo the defining ideal:

$$\begin{aligned}&(t_1(U_0V_0 + U_1V_1)^2 : t_0(U_0V_1 + U_1V_0)^2)\\ &= (t_0(U_0V_0 + U_1V_1)^2 : t_1(U_0V_0 + U_1V_1)^2 + c\,t_0(U_0V_0)(U_1V_1))\\ &= (t_0(U_0V_1 + U_1V_0)^2 + c\,t_1(U_0V_1)(U_1V_0) : t_1(U_0V_1 + U_1V_0)^2).\end{aligned}$$

Assuming the point normalization with $t_0 = 1$ or $t_1 = 1$, this immediately gives the following corollary.

Corollary 26. *The Montgomery endomorphism on $\mathscr{K}(\Delta_P)$ can be computed with $4\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}_t + 1\mathbf{m}_c$ or with $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}_t + 2\mathbf{m}_c$.*

The formulas so obtained agree with those of Gaudry and Lubicz [12]. The first complexity result agrees with theirs and the second obtains a trade-off of one $\mathbf{m}_c$ for one $\mathbf{S}$ using the explicit equation of $\mathscr{K}(\Delta_P)$ in $\mathscr{K}^2$. Finally, the isomorphisms of Theorems 23 and 24 permit point recovery, hence scalar multiplication on the respective elliptic curves.

9 Conclusion

We conclude with a tabulation of the best known complexity results for doubling and addition algorithms on projective curves (taking the best reported algorithm from the EFD [6]). We include the Hessian model, the only cubic curve model, for comparison. It covers only curves with a rational 3-torsion point. Binary Edwards curves [4] cover general ordinary curves, but the best complexity result we give here is for $d_1 = d_2$ which has a rational 4-torsion point. Similarly, the López-Dahab model with $a_2 = 0$ admits a rational 4-torsion point, hence covers the same classes, but the fastest arithmetic is achieved on the quadratic twists with $a_2 = 1$. The results here for addition and duplication on $\boldsymbol{\mu}_4$-normal form report the better result (in terms of constant multiplications $\mathbf{m}$) for the non-split $\boldsymbol{\mu}_4$ model (see the remark after Corollary 21 and Corollary 28 in the appendix).

Curve model	Doubling	Addition
$\mathbf{Z}/4\mathbf{Z}$-normal form	$7\mathbf{M} + 2\mathbf{S}$	$12\mathbf{M}$
Hessian	$6\mathbf{M} + 3\mathbf{S}$	$12\mathbf{M}$
Binary Edwards	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$16\mathbf{M} + 1\mathbf{S} + 4\mathbf{m}$
López-Dahab ($a_2 = 0$)	$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}$	$14\mathbf{M} + 3\mathbf{S}$
López-Dahab ($a_2 = 1$)	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$	$13\mathbf{M} + 3\mathbf{S}$
$\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$

This provides for the best known addition algorithm combined with essentially optimal doubling. We note that binary Edwards curves with $d_1 = d_2$ and the López-Dahab model with $a_2 = 0$ and have canonical projective embeddings in $\mathbb{P}^3$ such that the transformation to $\boldsymbol{\mu}_4$-normal form is linear, so that, conversely, these models can benefit from the efficient addition of the $\boldsymbol{\mu}_4$-normal form.

References

1. D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves. *Advances in cryptology—ASIACRYPT 2007*, *Lecture Notes in Computer Science*, **4833**, 29–50, 2007.
2. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. *Progress in cryptology – AFRICACRYPT 2008*, *Lecture Notes in Computer Science*, **5023**, 389–405, 2008.
3. D. J. Bernstein, T. Lange, A complete set of addition laws for incomplete Edwards curves. *J. Number Theory*, **131**, 858–872, 2011.
4. D. J. Bernstein, T. Lange, R. Rezaeian Farashahi, Binary Edwards curves. *Cryptographic hardware and embedded systems (CHES 2008, Washington, D.C.)*, *Lecture Notes in Computer Science*, **5154**, 244–265, 2008.
5. D. J. Bernstein, D. Kohel, and T. Lange. Twisted Hessian curves, unpublished 2009.
6. D. J. Bernstein, T. Lange, Explicit-formulas database, 2012. URL: `http://www.hyperelliptic.org/EFD/`
7. W. Bosma and H. W. Lenstra, Jr. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, **53** (2), 229–240, 1995.
8. D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, **7**, (4), 385–434, 1986.
9. J.-S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems. *Cryptographic Hardware and Embedded Systems (CHES 1999)*, *Lecture Notes in Computer Science*, **1717**, 292–302, 1999.
10. O. Diao, *Quelques aspects de l'arithmtique des courbes hyperelliptiques de genre 2*, Ph.D. thesis, Université de Rennes, 2011.
11. H. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, **44**, 393–422, 2007.
12. P. Gaudry and D. Lubicz, The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields and Their Applications*, **15**, 2, 246–260, 2009.
13. H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Twisted Edwards curves revisited. *Advances in cryptology – ASIACRYPT 2008*, *Lecture Notes in Computer Science*, **5350**, 326–343, 2008.

14. M. Joye and R. Rezaeian Farashahi, Efficient Arithmetic on Hessian Curves. *Public Key Cryptography (PKC 2010, Paris)*, *Lecture Notes in Computer Science*, **6056**, 243–260, 2010.
15. M. Joye and S.-M. Yen, The Montgomery Powering Ladder. *Cryptographic hardware and embedded systems (CHES 2002)*, *Lecture Notes in Computer Science*, **2523**, 291–302, 2003.
16. K. H. Kim, S. I. Kim, A New method for speeding up arithmetic on elliptic curves over binary fields, 2007. URL: `http://eprint.iacr.org/2007/181`.
17. D. Kohel, Addition law structure of elliptic curves. *Journal of Number Theory* **131**, Issue 5, 894–919, 2011.
18. D. Kohel, A normal form for elliptic curves in characteristic 2. *Arithmetic, Geometry, Cryptography and Coding Theory, (AGCT 2011, Luminy)*, talk notes, 15 March 2011.
19. D. Kohel et al., Echidna algorithms, v.3.0, 2012. URL: `http://echidna.maths.usyd.edu.au/echidna/index.html`
20. H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, **79** (3), 603–610, 1985.
21. *Magma Computational Algebra System*, Computational Algebra Group, University of Sydney, 2012. URL: `http://magma.maths.usyd.edu.au/`.
22. J. S. Milne, *Abelian Varieties*, version 2.00, 2012. URL: `http://www.jmilne.org/math/CourseNotes/av.html`
23. P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Mathematics of Computation*, **48** 243-264, 1987.
24. M. Stam. On Montgomery-like representations for elliptic curves over $GF(2^k)$, *Public Key Cryptography (PKC 2003, Miami)*, *Lecture Notes in Computer Science*, **2567**, 240–253, 2003.

Appendix

By means of a renormalization of variables, the split $\boldsymbol{\mu}_4$-normal form can be put in $\boldsymbol{\mu}_4$-normal form $(X_0 + X_2)^2 = X_1X_3,\ s(X_1 + X_3)^2 = X_0X_2$, where $s = c^{-4}$. This form loses the elementary symmetry given by cyclic permutation of the coordinates, but by the Remark following Corollary 21, we are able to save on multiplications by scalars in duplication. This renormalization gives the following addition laws (as a consequence of Theorem 18), and give an analogous savings for addition.

Theorem 27. *Let C be an elliptic curve in $\boldsymbol{\mu}_4$-normal form: A basis for the space of addition laws of bidegree $(2, 2)$ is given by:*

$$\left\{\begin{array}{l}\big((X_0Y_0 + X_2Y_2)^2,\ X_0X_1Y_0Y_1 + X_2X_3Y_2Y_3,\ s(X_1Y_1 + X_3Y_3)^2,\ X_0X_3Y_0Y_3 + X_1X_2Y_1Y_2\big),\\ \big(X_0X_1Y_0Y_3 + X_2X_3Y_1Y_2,\ (X_1Y_0 + X_3Y_2)^2,\ X_0X_3Y_2Y_3 + X_1X_2Y_0Y_1,\ (X_0Y_3 + X_2Y_1)^2\big),\\ \big(s(X_1Y_3 + X_3Y_1)^2,\ X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3,\ (X_0Y_2 + X_2Y_0)^2,\ X_0X_1Y_2Y_3 + X_2X_3Y_0Y_1\big),\\ \big(X_0X_3Y_0Y_1 + X_1X_2Y_2Y_3,\ (X_0Y_1 + X_2Y_3)^2,\ X_0X_1Y_1Y_2 + X_2X_3Y_0Y_3,\ (X_1Y_2 + X_3Y_0)^2\big).\end{array}\right\}.$$

The absence of the constant s in the 2nd and 4th addition laws permits us to save the $2\mathbf{m}$ in the computation of addition.

Corollary 28. *Addition of generic points on C can be carried out in $7\mathbf{M} + 2\mathbf{S}$.*

Proof. After evaluating $(Z_0, Z_1, Z_2, Z_3) = (X_0Y_1, X_1Y_2, X_2Y_3, X_3Y_0)$ in the last addition law, the algorithm follows that of Corollary 19. □