Efficient arithmetic of elliptic curves in characteristic 2

David Kohel
Institut de Mathématiques de Luminy

Indocrypt 2012, Kolkatta, 12 December 2012

Edwards model and symmetries

In 2007, Edwards introduced a new model for elliptic curves defined by the affine model $x^2 + y^2 = a^2(1 + z^2)$ with identity $O = (0, a)$, where $z = xy$. This model is valid over k of $\mathrm{char(k)} \neq 2$.

The complete linear system associated to this degree 4 model has basis $\{1, x, y, z\}$ such that the image $(1 : x : y : z)$ lies on the surface $X_0X_3 = X_1X_2$ in $\mathbb{P}^3$, defined by

$$X_1^2 + X_2^2 = a^2(X_0^2 + X_3^2),\ \mathrm{O} = (a : 0 : 1 : 0).$$

The remarkable properties of the Edwards model are its remarkably simple addition law, and large symmetry group given by simple scaled coordinate permutations.

Evolution of the Edwards model

Bernstein and Lange introduced a coordinate rescaling to descend to to $k(d) = k(a^4)$, and coined the term Edwards curve.

With Joye, Birkner, and Peters, they introduced quadratic twists by c, we obtain the twisted Edwards model

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

The model in this form appears in Hisil et al as extended Edwards coordinates, on which they develop the fastest known algorithms for ellitpic curve arithmetic.

We next recall the principal properties of the Edwards normal form (reverting to the untwisted $c = 1$ to maximize the symmetries), with a view to their generalization to our models in $\mathrm{char(k)} = 2$.

Edwards normal form properties

Let $E/k \subset \mathbb{P}^3$ be in Edwards normal form

$$\boxed{X_0^2 + dX_3^2 = X_1^2 + X_2^2,\ X_0X_3 = X_1X_2,\ \mathrm{O} = (1:0:1:0).}$$

Properties:

1. The point $T = (1:1:0:0)$ is 4-torsion.
2. The translation–by–T morphism is given by:
$$\tau_T(X_0 : X_1 : X_2 : X_3) = (-X_0 : -X_2 : X_1 : X_3).$$
3. The inverse morphism is defined by:
$$[-1](X_0 : X_1 : X_2 : X_3) = (-X_0 : X_1 : -X_2 : X_3).$$
4. E admits a factorization through $\mathbb{P}^1 \times \mathbb{P}^1$, where
$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2) = (X_1 : X_3),$$
$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_2 : X_3).$$

Remark: $X_3 = 0$ cuts out $\langle T \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Axioms for normal forms

The group generated by $[-1]$ and τ_T generate a dihedral group D_4 acting by signed coordinate permutations. Unfortunately, the signed action is degenerate in characteristic 2.

Instead we ask what elliptic curve models are stabilized by the natural D_4-action on the coordinate functions $\{X_0, X_1, X_2, X_3\}$. Up to isomorphism, there are exactly two such permutation representations. We may suppose that T is a 4-torsion point which acts by cyclic coordinate permutation

$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2).$$

The two representations of $D_4 = \langle [-1], \tau_T \rangle$ are then distinguished by the image of the action of the inversion morphism:

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

$\mathbb{Z}/4\mathbb{Z}$-normal form

An elliptic curve $E_c = E/k \subset \mathbb{P}^3$ in $\mathbb{Z}/4\mathbb{Z}$-normal form is defined (in $\mathrm{char(k)} = 2$) by

$$X_0^2 + X_1^2 + X_2^2 + X_3^2 = cX_0X_2 = cX_1X_3,\ \mathrm{O} = (1:0:0:1).$$

Properties:

1. The point $T = (1:1:0:0)$ is 4-torsion.
2. The translation–by–T morphism is given by:
$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2).$$
3. The inverse morphism is defined by:
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_3 : X_2 : X_1 : X_0).$$
4. E admits a factorization through $\mathbb{P}^1 \times \mathbb{P}^1$, where
$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_3 : X_2),$$
$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_3) = (X_1 : X_2),$$

Remark: $X_0 + X_1 + X_2 + X_3 = 0$ cuts out $\langle T \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Split $\boldsymbol{\mu}_4$-normal form

An elliptic curve $C_c = C/k \subset \mathbb{P}^3$ in split $\boldsymbol{\mu}_4$-normal form is defined (in $\mathrm{char}(\mathrm{k}) = 2$) by

$$\boxed{X_0^2 + X_2^2 = c^2\, X_1X_3,\ X_1^2 + X_3^2 = c^2\, X_0X_2,\ \mathrm{O} = (c : 1 : 0 : 1).}$$

Properties:

1. The point $T = (1 : c : 1 : 0)$ is 4-torsion.
2. The translation–by–T morphism is given by:
$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2).$$
3. The inverse morphism is defined by:
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : X_3 : X_2 : X_1).$$
4. E does not admit a factorization through $\mathbb{P}^1 \times \mathbb{P}^1$.

Remark: The hyperplane $X_2 = 0$ cuts out $4(\mathrm{O})[\sim \boldsymbol{\mu}_4/k]$.

Classification of elliptic curves

Theorem

Let E/k be an elliptic curve over a field of characteristic 2 with identity O, rational 4-torsion point T, and j-invariant $j = c^8$.

1. *There exists a unique embedding $\iota : E \to E_{c^2} \subset \mathbb{P}^3$ as a curve in split $\mathbb{Z}/4\mathbb{Z}$-normal form such that*
$$\iota(\mathrm{O}) = (1 : 0 : 0 : 1) \text{ and } \iota(T) = (1 : 1 : 0 : 0).$$
2. *There exists a unique embedding $\iota : E \to C_c \subset \mathbb{P}^3$ as a curve in split $\boldsymbol{\mu}_4$-normal form such that*
$$\iota(\mathrm{O}) = (c : 1 : 0 : 1) \text{ and } \iota(T) = (1 : c : 1 : 0).$$
3. *There exists no linear isomorphism $E_{c^2} \cong C_c$.*
4. *Any symmetric quartic embedding of E in $\mathbb{P}^3$ is linearly isomorphic to either E_{c^2} or C_c.*

We first recall known results for the Edwards curve standard.

Theorem

Let E/k be an elliptic curve in Edwards normal form:

$$X_0^2 + dX_3^2 = X_1^2 + X_2^2,\ X_0X_3 = X_1X_2.$$

A basis for the bilinear addition law projections for $\pi_1 \circ \mu$ is

$$\left\{ \begin{array}{c} (X_0Y_0 + dX_3Y_3, X_1Y_2 + X_2Y_1), \\ (X_1Y_1 + X_2Y_2, X_0Y_3 + X_3Y_0) \end{array} \right\},$$

and for $\mu \circ \pi_2$, we have

$$\left\{ \begin{array}{c} (X_1Y_2 - X_2Y_1, -X_0Y_3 + X_3Y_0), \\ (X_0Y_0 - dX_3Y_3, -X_1Y_1 + X_2Y_2) \end{array} \right\}.$$

Addition laws of bidegree $(2, 2)$ are recovered by composition with the Segre embedding:

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

Corollary (Hisil, et al.)

Addition of generic points on an elliptic curve in Edwards normal form can be computed with $8\mathbf{M}$.

The $\mathbb{Z}/4\mathbb{Z}$-normal form admits analogous addition law structure.

Theorem

Let E/k be an elliptic curve in $\mathbb{Z}/4\mathbb{Z}$-normal form:

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

A basis for the bilinear addition law projections for $\pi_1 \circ \mu$ is

$$\left\{ \begin{array}{l} (X_0Y_3 + X_2Y_1, X_1Y_0 + X_3Y_2), \\ (X_1Y_2 + X_3Y_0, X_0Y_1 + X_2Y_3) \end{array} \right\},$$

and for $\pi_2 \circ \mu$ is:

$$\left\{ \begin{array}{l} (X_0Y_0 + X_2Y_2, X_1Y_1 + X_3Y_3), \\ (X_1Y_3 + X_3Y_1, X_0Y_2 + X_2Y_0) \end{array} \right\}.$$

Addition laws of bidegree $(2,2)$ are recovered by composition with the skew-Segre embedding:

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

Corollary

Addition of generic points on an elliptic curve in $\mathbb{Z}/4\mathbb{Z}$-normal form can be computed with $12\mathbf{M}$.

But the $\boldsymbol{\mu}_4$-normal form yields a more efficient addition algorithm.

Theorem

Let E/k be an elliptic curve in $\boldsymbol{\mu}_4$-normal form:

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

A basis for bidegree $(2,2)$-addition laws is

$$\left\{\begin{array}{l}
(\,X_3^2Y_1^2 + X_1^2Y_3^2,\ c\,(X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3),\ X_2^2Y_0^2 + X_0^2Y_2^2,\ c\,(X_2X_3Y_0Y_1 + X_0X_1Y_2Y_3)\,),\\
(\,X_0^2Y_0^2 + X_2^2Y_2^2,\ c\,(X_0X_1Y_0Y_1 + X_2X_3Y_2Y_3),\ X_1^2Y_1^2 + X_3^2Y_3^2,\ c\,(X_1X_2Y_1Y_2 + X_0X_3Y_0Y_3)\,),\\
(\,X_2X_3Y_1Y_2 + X_0X_1Y_0Y_3,\ c\,(X_0X_2Y_2^2 + X_1^2Y_1Y_3),\ X_1X_2Y_0Y_1 + X_0X_3Y_2Y_3,\ c\,(X_2^2Y_0Y_2 + X_1X_3Y_3^2)\,),\\
(\,X_0X_3Y_0Y_1 + X_1X_2Y_2Y_3,\ c\,(X_1X_3Y_1^2 + X_2^2Y_0Y_2),\ X_0X_1Y_1Y_2 + X_2X_3Y_0Y_3,\ c\,(X_0X_2Y_2^2 + X_3^2Y_1Y_3)\,)
\end{array}\right\}$$

Corollary

Addition of generic points on an elliptic curve in $\boldsymbol{\mu}_4$-normal form can be computed with $7\mathbf{M} + 2\mathbf{S} + 2m_c$.

Montgomery differential addition

Montgomery endomorphism. An efficient differential addition is a consequence of the existence of simple forms for arithmetic of the *Montgomery endomorphism*

$$(P+Q,Q) \longmapsto (2(P+Q), P+2Q),$$

on the Kummer curve $\mathbb{P}^1 = E/\{\pm 1\}$. Its restriction to the image of $\Delta_P = \{(P+Q,Q)\}$ in $\mathbb{P}^1 \times \mathbb{P}^1$, is isomorphic to E, allows one to carry out scalar multiplication with point recovery. This gives the follow asymptotic complexity.

Theorem

Montgomery endomorphism achieves scalar multiplication of a fixed point $P = (t_0 : t_1 : t_2 : t_3)$ in $4\mathbf{M} + 4\mathbf{S} + \mathbf{m}_t + \mathbf{m}_c$ per bit.

The duplication morphism

In *Binary Edwards curves*, Bernstein et al. report: *"All of the doubling formulas for binary elliptic curves presented in the literature have exceptional cases, such as doubling a point of order 2."* This state of affairs was corrected by the authors, and is correctable for any elliptic curve over any field:

Theorem

Given an embedding of E in $\mathbb{P}^{d-1}$ by a complete linear system, there exists a unique d-tuple of polynomials of degree 4 defining the duplication morphism on E.

For a Weierstrass model ($d = 3$), duplication does not decompose as Frobenius $\varphi(X : Y : Z) = (X^2 : Y^2 : Z^2)$ composed with quadratic polynomials (even though $[2] = \hat{\varphi}\varphi$ with $\deg(\hat{\varphi}) = 2$).

Efficient duplication

In the case of quartic models in in $\mathbb{P}^3$, the quartic polynomials for duplication do factor through Frobenius, but the resulting four squarings and quadratic evaluations does not necessarily yeild the most efficient algorithm.

Corollary

The duplication morphism on an elliptic curve C in split $\boldsymbol{\mu}_4$-normal form is given by $[2](X_0 : X_1 : X_2 : X_3) =$
$(X_0^4 + X_2^4 : c(X_0^2X_1^2 + X_2^2X_3^2) : X_1^4 + X_3^4 : c(X_0^2X_3^2 + X_1^2X_2^2))$.

A naïve application gives a complexity $3\mathbf{M} + 6\mathbf{S} + 2\mathbf{m}_c$. A more carefully constructed algorithm, detailed hereafter, saves $1\mathbf{M} + 1\mathbf{S}$.

Proof of complexity

We describe the evaluation of the forms of the preceeding corollary using the equivalent expressions. Setting

$$(U, V, W) = ((X_0 + X_2)^2, (X_1 + X_3)^2, (X_0 + cX_1)^2),$$

the duplication formula can be expressed as:

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

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

Corollary

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

Proof of complexity

We need to evaluate $(c^5U^2 : c^4F^2 : c^5V^2 : c^4G^2)$, where

$$F^2 = U^2 + c^{-4}V^2 + (U + c^2V + W)W + c^2UV,$$
$$G^2 = U^2 + c^{-4}V^2 + (U + c^2V + W)W = F^2 + c^2UV.$$

The evaluation follows the steps

- $(U, V, W) = ((X_0 + X_2)^2, (X_1 + X_3)^2, (X_0 + cX_1)^2)$ — $3\mathbf{S} + 1\mathbf{m}_c$
- c^2V, c^2UV, $(U + c^2V + W)W$, U^2, V^2 — $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_c$

then we determine

- c^5U^2, c^5V^2 — $2\mathbf{m}_c$
- $c^4G^2 = c^4U^2 + V^2 + c^4(U + c^2V + W)\,W$ — $2\mathbf{m}_c$
- $c^4F^2 = c^4G^2 + c^4\,c^2UV$ — $1\mathbf{m}_c$

This gives the asserted complexity. □

Comparison with known results

The multiplication by constants can be reduced for addition and doubling by a coordinate scaling to the semi-split $\boldsymbol{\mu}_4$-normal form:

$$X_0^2 + X_2^2 = X_1 X_3,\ X_1^2 + X_3^2 = c^4\, X_0 X_2,\ \mathrm{O} = (1:1:0:1).$$

We conclude with a tabulation of the best known complexity results for doubling and addition algorithms on projective curves, and incorporate the best complexity for this semi-split $\boldsymbol{\mu}_4$-normal form.

We report the best possible complexity result for binary Edwards curves, which holds for for $d_1 = d_2$, admitting a rational 4-torsion point. We report the complexity for the López-Dahab model with $a_2 = 0$, having a rational 4-torsion point, although the fastest arithmetic is achieved on the quadratic twists with $a_2 = 1$. The Hessian model, with a rational 3-torsion structure, and the only degree 3 model reported here, is given for comparison.

Tabular comparison with known results

Curve model	Doubling	Addition
$\mathbb{Z}/4\mathbb{Z}$-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	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$

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.

Conclusions

Main results:

- A $4\mathbf{M} + 4\mathbf{S} + \mathbf{m}_t + \mathbf{m}_c$ differential addition algorithm on binary curves with $|E(k)| \equiv 0 \bmod 4$, with point recovery.
  - Immediate application to other models — $\boldsymbol{\mu}_4$-normal form, $\mathbb{Z}/4\mathbb{Z}$-normal form, short Weierstrass with $a_2 = 0$.
  - Best complexity for differential addition on curves with 4-torsion point (cf. Gaudry and Lubicz).
- Improving addition algorithm from $13\mathbf{M} + 3\mathbf{S}$ to $7\mathbf{M} + 2\mathbf{S}$
  - Windowing length $n = 3$ beats previous $n = 5$, and gives better results than differential addition for a generic point.
  - Windowing length $n = 4$ beats previous $n = 7$, and gives better results than differential addition for a small point.

Open or ongoing problem:

- extension to quadratic twists ($|E(k)| \equiv 2 \bmod 4$).

Thanks for your attention!

Conclusions

Main results:

- A $4\mathbf{M} + 4\mathbf{S} + \mathbf{m}_t + \mathbf{m}_c$ differential addition algorithm on binary curves with $|E(k)| \equiv 0 \bmod 4$, with point recovery.
  - Immediate application to other models — $\boldsymbol{\mu}_4$-normal form, $\mathbb{Z}/4\mathbb{Z}$-normal form, short Weierstrass with $a_2 = 0$.
  - Best complexity for differential addition on curves with 4-torsion point (cf. Gaudry and Lubicz).
- Improving addition algorithm from $13\mathbf{M} + 3\mathbf{S}$ to $7\mathbf{M} + 2\mathbf{S}$
  - Windowing length $n = 3$ beats previous $n = 5$, and gives better results than differential addition for a generic point.
  - Windowing length $n = 4$ beats previous $n = 7$, and gives better results than differential addition for a small point.

Open or ongoing problem:

- extension to quadratic twists ($|E(k)| \equiv 2 \bmod 4$).

Thanks for your attention!