Elliptic curves *in characteristic 2*

David R. Kohel
Institut de Mathématiques de Luminy

ECC Rump Session
Nancy, 19 September 2011

Edwards normal form

An elliptic curve $E/k \subset \mathbb{P}^3$ (in $\mathrm{char}(\mathrm{k}) \neq 2$) in (twisted) Edwards normal form is defined by

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

Properties:

1. The identity is $\mathrm{O} = (1:0:0:1)$ and $T = (1:1:0:0)$ is a point of 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 $\mathbb{Z}/4\mathbb{Z} \cong \langle T \rangle$.

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

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

$$\boxed{(X_0 + X_1 + X_2 + X_3)^2 = cX_0X_2 = cX_1X_3.}$$

Properties:

1. The identity is $\mathrm{O} = (1:0:0:1)$ and $T = (1:1:0:0)$ is a point of 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 $\mathbb{Z}/4\mathbb{Z} \cong \langle T \rangle$.

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

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

$$\boxed{\begin{array}{l}(X_0 + X_2)^2 = c^2\, X_1 X_3,\\ (X_1 + X_3)^2 = c^2\, X_0 X_2.\end{array}}$$

Properties:

1. The identity is $\mathrm{O} = (c:1:0:1)$ and $T = (1:0:1:c)$ is a point of 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 $4(\mathrm{O})[\sim \boldsymbol{\mu}_4/k]$.

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*
$$\iota(\mathrm{O}) = (c : 1 : 0 : 1) \text{ and } \iota(T) = (1 : 0 : 1 : c).$$
3. *There exists no linear isomorphism $E_{c^2} \cong C_c$.*
4. *Any symmetric embedding of E in $\mathbb{P}^3$ is linearly isomorphic to either E_{c^2} or C_c.*

Independently Diao introduced an affine plane quartic model whose embedding by the associated complete linear system can be identified with E_c, and Diao and Lubicz have studied the model C_c for efficient pairings.

Theorem

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

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

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

$$\left\{ \begin{array}{l} (X_0Y_0 + dX_3Y_3,\ X_1Y_2 + X_2Y_1), \\ (cX_1Y_1 + X_2Y_2,\ X_0Y_3 + X_3Y_0) \end{array} \right\},$$

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

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

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 $8\mathbf{M}$.

Theorem

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

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

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 $12\mathbf{M}$.

Theorem

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

$$\begin{aligned}(X_0 + X_2)^2 + c^2\, X_1 X_3,\\ (X_1 + X_3)^2 + c^2\, X_0 X_2.\end{aligned}$$

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

$$\left\{\begin{array}{l}
\big(\, X_3^2 Y_1^2 + X_1^2 Y_3^2,\ c\,(X_0 X_3 Y_1 Y_2 + X_1 X_2 Y_0 Y_3),\ X_2^2 Y_0^2 + X_0^2 Y_2^2,\ c\,(X_2 X_3 Y_0 Y_1 + X_0 X_1 Y_2 Y_3)\,\big),\\
\big(\, X_0^2 Y_0^2 + X_2^2 Y_2^2,\ c\,(X_0 X_1 Y_0 Y_1 + X_2 X_3 Y_2 Y_3),\ X_1^2 Y_1^2 + X_3^2 Y_3^2,\ c\,(X_1 X_2 Y_1 Y_2 + X_0 X_3 Y_0 Y_3)\,\big),\\
\big(\, X_2 X_3 Y_1 Y_2 + X_0 X_1 Y_0 Y_3,\ c\,(X_0 X_2 Y_2^2 + X_1^2 Y_1 Y_3),\ X_1 X_2 Y_0 Y_1 + X_0 X_3 Y_2 Y_3,\ c\,(X_2^2 Y_0 Y_2 + X_1 X_3 Y_3^2)\,\big),\\
\big(\, X_0 X_3 Y_0 Y_1 + X_1 X_2 Y_2 Y_3,\ c\,(X_1 X_3 Y_1^2 + X_2^2 Y_0 Y_2),\ X_0 X_1 Y_1 Y_2 + X_2 X_3 Y_0 Y_3,\ c\,(X_0 X_2 Y_2^2 + X_3^2 Y_1 Y_3)\,\big)
\end{array}\right\}$$

Corollary

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

Theorem

Scalar multiplication of a point $P = (t_0 : t_1 : t_2 : t_3)$ on an elliptic curve in $\mathbb{Z}/4\mathbb{Z}$-normal form can be computed using $4\mathbf{M} + 4\mathbf{S} + m_t + m_c$ per bit.

Montgomery endomorphism. The above theorem 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 $\mathbb{P}^1 = E/\{\pm 1\}$ (or rather for its restriction to the diagonal image of $\Delta_P = \{(P + Q, Q)\} \cong E$ in $\mathbb{P}^1 \times \mathbb{P}^1$).

Quadratic twists. We cover all ordinary elliptic curves over a finite field of characteristic 2 and odd degree by considering twists by $k[\omega]/k$ where $\omega^2 + \omega + 1 = 0$ (e.g. this covers all recommended curves in the NIST standards for characteristic 2).

1. For an elliptic curve E in $\mathbb{Z}/4\mathbb{Z}$-normal form, the twisted group $E'(k)$ embeds in $E(k[\omega])$ as:

$$(U_0 + \omega U_1 : U_2 + \omega U_3 : U_2 + \overline{\omega} U_3 : U_0 + \overline{\omega} U_1).$$

2. For an elliptic curve C in $\boldsymbol{\mu}_4$-normal form, the twisted group $C'(k)$ embeds in $C(k[\omega])$ as:

$$(U_0 : U_1 + \omega U_3 : U_2 : U_1 + \overline{\omega} U_3).$$