A normal form for elliptic curves *in characteristic 2*

David R. Kohel
Institut de Mathématiques de Luminy

Arithmetic, Geometry, Cryptography et Coding Theory 2011
CIRM, Luminy, 15 March 2011

Edwards model for elliptic curves

In 2007, Edwards introduced a new model for elliptic curves, 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 the degree 4 model determines a nonsingular model in $\mathbb{P}^3$ with identity $\mathrm{O} = (a : 0 : 1 : 0)$:

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

as a family of curves over $k(a) = k(X(4))$. Lange and Bernstein introduced a rescaling to descend to $k(d) = k(a^4) = k(X_1(4))$, and subsequently (with Joye, Birkner, and Peters) a quadratic twist by c, to define the twisted Edwards model with $\mathrm{O} = (1 : 0 : 1 : 0)$:

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

Edwards model for elliptic curves

Properties:

1. The divisor at infinity is equivalent to $3(O) + (T)$ where
$$T = (1 : 0 : -1 : 0).$$
2. The model admits a factorization $S \circ (\pi_1 \times \pi_2)$ through $\mathbb{P}^1 \times \mathbb{P}^1$, where
$$\begin{aligned}\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_2 : X_3),\\ \pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2) = (X_1 : X_3),\end{aligned}$$
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 inverse morphism is
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : -X_1 : X_2 : -X_3),$$
hence the embedding and the factorization are *symmetric*.

Edwards model for elliptic curves

The remarkable property of the Edwards model is that the symmetry of the embedding and factorization implies that the composition of the addition morphism

$$\mu : E \times E \longrightarrow E$$

with each of the projectons $\pi_i : E \to \mathbb{P}$ admits a basis of *bilinear* defining polynomials. For $\pi_1 \circ \mu$, we have

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

and for $\pi_2 \circ \mu$, 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 given by polynomial maps of bidegree $(2, 2)$ are recovered by composing with the Segre embedding.

A few lemmas (symmetric condition)

Lemma

$\mathcal{L}(D)$ is symmetric if and only if $\mathcal{L}(D) \cong \mathcal{L}((d-1)(O) + (T))$ for some T in $E[2]$.

As opposed to prior models (Weierstrass, Hessian, Jacobi), the Edwards model is symmetric but not defined by $D \sim d(O)$ — perhaps this is why it escaped description until the 21st century.

Lemma

Let $E \subset \mathbb{P}^r$ be an embedding with respect to the complete linear system of a divisor D. Then $\mathcal{L}(D)$ is symmetric if and only if $[-1]$ is projectively linear.

The property that D is symmetric is stronger — it implies that the automorphism inducing $[-1]$ fixes a line $X_0 = 0$ (cutting out D).

A few lemmas (linear translations)

Lemma

Let $E \subset \mathbb{P}^r$ be embedded with respect to the complete linear system of a divisor D, let T be in $E(\bar{k})$, and let τ_T be the translation-by-T morphism. The following are equivalent:

- $\tau_T^*(D) \sim D$.
- $[\deg(D)]T = \mathrm{O}$.
- τ_T *is induced by a projective linear automorphism of* $\mathbb{P}^r$.

These lemmas 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 representation of

$$D_4 \cong \langle [-1] \rangle \ltimes \langle \tau_T \rangle,$$

induced by the action on the global sections $\Gamma(E, \mathcal{L}(D)) \cong k^4$.

CONSTRUCTION OF A NORMAL FORM IN $\mathrm{char}(k) = 2$

Suppose that E/k is an elliptic curve with $\mathrm{char}(k) = 2$. In view of the previous lemmas and the properties of Edwards' normal form, we consider reasonable hypotheses for a characteristic 2 analog.

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 $\mathbb{P}^1 \times \mathbb{P}^1$.

Construction of the normal form...

In order for the representation of τ_T to stabilize the image of $\mathbb{P}^1 \times \mathbb{P}^1$, we have

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

where S is defined by $X_0X_2 = X_1X_3$ and

$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_3 : X_2),$$

$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_3) = (X_1 : X_2).$$

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 $[-1]$:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Construction of the normal form...

In order for the representation of τ_T to stabilize the image of $\mathbb{P}^1 \times \mathbb{P}^1$, we have

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

where S is defined by $X_0X_2 = X_1X_3$ and

$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_3 : X_2),$$

$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_3) = (X_1 : X_2).$$

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 $[-1]$:

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

or

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

Construction of a normal form. . .

Considering the form of the projection morphisms from $X_0X_2 = X_1X_3$:

$$\pi_1(X_0 : X_1 : X_2 : X_3) = (X_0 : X_1) = (X_3 : X_2),$$
$$\pi_2(X_0 : X_1 : X_2 : X_3) = (X_0 : X_3) = (X_1 : X_2),$$

we see that only the first of the possible actions of $[-1]$:

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

stabilizes π_1 and π_2 (the second exchanges them).
It remains to consider the forms of degree 2 which are D_4-invariant modulo the relation $X_0X_2 = X_1X_3$, which is spanned by

$$\left\{ \, (X_0 + X_1 + X_2 + X_3)^2, \; (X_0 + X_2)(X_1 + X_3), \; X_0X_2 \, \right\}.$$

Construction of a normal form. . .

It follows that an elliptic curve satisfying the hypotheses must be the intersection of $X_0X_2 = X_1X_3$ with a form

$$a\,(X_0 + X_1 + X_2 + X_3)^2 + b\,(X_0 + X_2)(X_1 + X_3) + c\,X_0X_2 = 0.$$

Moreover, in order to be invariant under $[-1]$, the identity lies on the line $X_0 = X_3, X_1 = X_2$, hence

$$b\,(X_0 + X_1)^2 + c\,X_0X_1 = 0.$$

If $c = 0$, we obtain $\mathrm{O} = (1 : 1 : 1 : 1)$, which is fixed by τ_T, a contradiction. If $b = 0$, we may take

$$\mathrm{O} = (1 : 0 : 0 : 1),\ S = (0 : 1 : 1 : 0) = 2T.$$

For any other nonzero b and c we can transform the model to such a *normal form* with $b = 0$.

A normal form in characteristic 2

This construction determines a normal form in $\mathbb{P}^3$ for elliptic curves E/k with rational 4-torsion point T:

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

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

An alternative normal form

What happens if we drop the symmetry of the factorization?

The alternative permutation representation for $[-1]$ is given by

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

and on $X_0X_2 = X_1X_3$ an elliptic curve must still be the intersection with an invariant form:

$$a\,(X_0 + X_1 + X_2 + X_3)^2 + b\,(X_0 + X_2)(X_1 + X_3) + c\,X_0X_2 = 0.$$

The new condition for O to be fixed by $[-1]$ is that it lies on $X_1 = X_3$, hence

$$a\,(X_0 + X_2)^2 + c\,X_0X_2 = 0.$$

Analogously, we find $a = 0$, with $\mathrm{O} = (1 : 0 : 0 : 0)$, giving the normal form

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

An alternative normal form

This above form lacks the symmetric projections π_1 and π_2; and the divisor class defining the embedding is equivalent to $4(\mathrm{O})$. A transformation of the ambient space:

$$\iota(X_0, X_1, X_2, X_3) = \begin{array}{l}(\, c\,X_0 + X_1 + X_3, X_0 + c\,X_1 + X_2, \\ \;\; X_1 + c\,X_2 + X_3, X_0 + X_2 + c\,X_3 \;\;)\end{array}$$

yields a new normal form with identity $\mathrm{O} = (c : 1 : 0 : 1)$:

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

Remark: The hyperplane $X_2 = 0$ cuts out $4(\mathrm{O})$.

We refer to this as the (split) $\boldsymbol{\mu}_4$-normal form for an elliptic curve, and the prior model as $\mathbb{Z}/4\mathbb{Z}$-normal form.

Construction of the $\boldsymbol{\mu}_4$-normal form

The simplest addition on elliptic curves are obtained as eigenvectors for the action of a torsion subgroup on elliptic curve models (Edwards excluded) for which a cyclic torsion subgroup acts as a coordinate scaling by $\boldsymbol{\mu}_n$. In the case of the Edwards model, we twist the constant subgroup scheme $\mathbb{Z}/4\mathbb{Z}$ by -1 in order to have a $\boldsymbol{\mu}_4$, and diagonalize the torsion action. This gives an isomorphism $E \to C$, where E is the twisted Edwards curve

$$X_0^2 + X_1^2 = X_2^2 - 16rX_3^2,\ X_0X_3 = X_1X_2,$$

and C is the $\boldsymbol{\mu}_4$-normal form:

$$C : X_0^2 - rX_2^2 = X_1X_3,\ X_1^2 - X_3^2 = X_0X_2.$$

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : X_1 + X_2 : X_3 : -X_1 + X_2).$$

THE HIERARCHY OF $\boldsymbol{\mu}_4$-NORMAL FORMS

Noting that $k(r) = k(X_1(4))$, we consider normal forms for this family under the base extensions

$$k(r) = k(X_0(4)) \to k(s) = k(X(\Gamma(2) \cap \Gamma_0(4))) \to k(t) = k(X(4))$$

Let C_0 be the elliptic curve in $\boldsymbol{\mu}_4$-normal form described above:

$$\boxed{X_0^2 - rX_2^2 = X_1X_3,\ X_1^2 - X_3^2 = X_0X_2,}$$

If $s = 1/r^2$, then renormalization of X_2 gives the curve C_1:

$$\boxed{X_0^2 - X_2^2 = X_1X_3,\ X_1^2 - X_3^2 = sX_0X_2.}$$

Finally if $s = t^4$, a rescaling of X_0 and X_2 gives the elliptic curve C_2 with identity $(t : 1 : 0 : 1)$ and full level 4 structure:

$$\boxed{X_0^2 - X_2^2 = t^2X_1X_3,\ X_1^2 - X_3^2 = t^2X_0X_2.}$$

The split $\boldsymbol{\mu}_4$-normal form

Let k be a field, and consider the elliptic curve C_2 in split $\boldsymbol{\mu}_4$-normal form

$$\boxed{X_0^2 - X_2^2 = t^2 X_1 X_3,\ X_1^2 - X_3^2 = t^2 X_0 X_2,}$$

with identity $O = (t : 1 : 0 : 1)$. The inverse morphism is given by

$$(X_0, X_1, X_2, X_3) \mapsto (X_0, X_3, -X_2, X_1),$$

the with

$$C_2[2](k) = \{O,\ (-e : 1 : 0 : 1),\ (0 : 1 : e : -1),\ (0 : -1 : e : 1)\}.$$

The divisor $X_2 = 0$ defines a subgroup $\boldsymbol{\mu}_4 \subset E[4]$, with rational points in $k[i] = k[x]/(x^2+1)$:

$$\boldsymbol{\mu}_4(k) = \{O,\ (it : 1 : 0 : 1),\ (-t : 1 : 0 : 1),\ (-it : 1 : 0 : 1)\},$$

and a constant subgroup $\mathbb{Z}/4\mathbb{Z} \subset E[4]$ is given by

$$\mathbb{Z}/4\mathbb{Z}(k) = \{O,\ (1 : -t : 1 : 0),\ (0 : 1 : t : -1),\ (-1 : 0 : 1 : t)\}.$$

Construction of the $\mathbb{Z}/4\mathbb{Z}$-normal form

On the Edwards model, the automorphism τ_T acts by

$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2 : -X_1 : -X_3),$$

as a result, τ_T induces a cyclic permutation of the forms

$$\begin{aligned} U_0 &= X_0 + X_1 + X_2 + X_3, \\ U_1 &= X_0 + X_1 - X_2 - X_3, \\ U_2 &= X_0 - X_1 - X_2 + X_3, \\ U_3 &= X_0 - X_1 + X_2 - X_3. \end{aligned}$$

which transforms the Edwards curve (with identity $(1 : 0 : 1 : 0)$)

$$X_0^2 + (16u + 1)X_3^2 = X_1^2 - X_2^2,\ X_0X_3 = X_1X_2$$

to the elliptic curve (with identity $(1 : 0 : 0 : 1)$)

$$(U_0 - U_1 + U_2 - U_3)^2 = 1/u\, U_0U_2 = 1/u\, U_1U_3.$$

Addition law structure for $\boldsymbol{\mu}_4$-normal form

The interest in alternative models of elliptic curves has been driven by the simple form of *addition laws* — the polynomial maps which define the addition morphism $\mu : E \times E \to E$ as rational maps.

Theorem

Let E/k, $\mathrm{char}(k) = 2$, be an elliptic curve in $\boldsymbol{\mu}_4$-normal form:

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

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

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

Addition law structure for $\mathbb{Z}/4\mathbb{Z}$-normal form

Theorem

Let E/k, $\mathrm{char}(k)=2$, 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:

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

The addition laws are independent of the curve parameters!