Isogenies between (twisted) Edwards and Montgomery curves

Craig Costello and Michael Naehrig

Microsoft Research

Let $p > 3$ be a prime and let $\mathbb{F}_p$ be the finite field with $p$ elements. For elements $a, d \in \mathbb{F}_p \setminus \{0\}$ with $a \neq d$, let $E_{a,d}$ be the twisted Edwards curve over $\mathbb{F}_p$ defined by

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$  

For elements $A \in \mathbb{F}_p \setminus \{-2, 2\}$ and $B \in \mathbb{F}_p \setminus \{0\}$, let $E_{M,A,B}$ be the Montgomery curve over $\mathbb{F}_p$ defined by

$$E_{M,A,B} : Bv^2 = u^3 + Au^2 + u.$$  

**Proposition 1.** Let $p \equiv 1 \pmod{4}$. Fix a square root of $-1$, i.e. let $s \in \mathbb{F}_p$ such that $s^2 + 1 = 0$. Let $A = 4d + 2$. Then, the map

$$\phi : E_{−1,d} \rightarrow E_{M,A,1}, \ (x, y) \mapsto (u, v) = \left(-\frac{y^2}{x^2}, -\frac{ys(x^2 - y^2 + 2)}{x^3}\right)$$

is a 4-isogeny defined over $\mathbb{F}_p$ with dual isogeny

$$\hat{\phi} : E_{M,A,1} \rightarrow E_{−1,d}, \ (u, v) \mapsto (x, y) = \left(\frac{4sv(u - 1)(u + 1)}{u^2 - 2u^2 + 4v^2 + 1}, -\frac{u^4 + 2u^2 + 4v^2 + 2Au + 4u^2 + 1}{u^4 - 2u^2 + 4v^2 + 1}\right).$$

**Proof.** A direct calculation using the curve equation of $E_{−1,d}$ shows that $(u, v) = \phi(x, y)$ satisfies the curve equation $v^2 = u^3 + Au^2 + u$. Similarly, using the curve equation of $E_{M,A,1}$ shows that $(x, y) = \hat{\phi}(u, v)$ satisfies the equation $−x^2 + y^2 = 1 + dx^2y^2$. Thus, both $\phi$ and $\hat{\phi}$ are rational maps between the curves [1, Def. 5.5.1]

To show that these rational maps are both morphisms, it remains to show that $\phi$ (resp. $\hat{\phi}$) is regular at all points in $E_{−1,d}(\mathbb{F}_p)$ (resp. $E_{M,A,1}(\mathbb{F}_p)$) [1, Def. 5.5.12]. Following [1, Def. 5.5.1], rewrite $\phi$ as

$$E_{−1,d} \rightarrow \mathbb{P}^2, \ (x, y) \mapsto (U : V : W) = (-xy^2 : −sy(x^2 − y^2 + 2) : x^3),$$

from which it is easy to verify that there are no points in $E_{−1,d}(\mathbb{F}_p)$ that map to $(0 : 0 : 0)$ under $\phi$, so $\phi$ is a morphism. Similarly, we rewrite $\hat{\phi}$ as

$$E_{M,A,1} \rightarrow \mathbb{P}^2, \ (u, v) \mapsto (X : Y : Z),$$

$$X = (4sv(u - 1)(u + 1)(-u^4 + 2uv^2 + 2Au + 4u^2 + 1),$$

$$Y = (u^4 + 2uv - 1)(u^4 - 2u^2 + 4v^2 + 1),$$

$$Z = (u^4 - 2u^2 + 4v^2 + 1)(-u^4 + 2uv^2 + 2Au + 4u^2 + 1),$$

from which one can verify that there are no points in $E_{M,A,1}$ that map to $(0 : 0 : 0)$ under $\hat{\phi}$, so $\hat{\phi}$ is a morphism as well.

12 March 2015
Following [1, Def. 9.6.1], $\phi$ maps the neutral element $O_{E, -1, d} = (0, 1)$ to the point at infinity $O_{E, M, A, 1} = (0 : 1 : 0)$, so $\phi$ is an isogeny. For $\hat{\phi}$, we homogenize $E_{M, A, 1}$ under $u = U/W^2$ and $v = V/W^3$, so that $O_{E, M, A, 1} = (\lambda^2 : \lambda^3 : 0)$ for $\lambda \in \mathbb{F}_p \setminus \{0\}$ and $\hat{\phi} : (U : V : W) \mapsto (X : Y : Z)$, where

\[
X = (4sVW(-W^4 + U^2)(2AUW^6 + W^8 + 4U^2W^4 - U^4 + 2UV^2)),
\]

\[
Y = (-W^4 + U^2 + 2VW)(-W^4 + U^2 - 2VW)(W^8 - 2U^2W^4 + U^4 + 4V^2W^2),
\]

\[
Z = (W^8 - 2U^2W^4 + U^4 + 4V^2W^2)(2AUW^6 + W^8 + 4U^2W^4 - U^4 + 2UV^2)),
\]

takes $(\lambda^2 : \lambda^3 : 0)$ to $(0 : 1 : 1)$. Thus, $\hat{\phi}(O_{E, M, A, 1}) = O_{E, -1, d}$, so $\hat{\phi}$ is an isogeny.

It remains to show that $\phi$ is a 4-isogeny and that $\hat{\phi}$ is its dual. To describe the full kernel of $\phi$, we follow [1, p. 173] and use the non-singular projective variety $V_{-1, d} : \{-X^2 + Y^2 - Z^2 - dT^2, ZT - XY\}$, as well as the corresponding homogenized version of $\phi$, which is given as

$$(T : X : Y : Z) \mapsto (-XY^2 : -sY(X^2 - Y^2 + 2Z^2) : X^3).$$

The full kernel of $\phi$ is the set of points $\{(0 : 0 : 1 : 1), (0 : 0 : -1 : 1), (1 : 0 : \sqrt{d} : 0), (1 : 0 : -\sqrt{d} : 0)\}$, all points of order dividing 4, which shows that $\phi$ is a 4-isogeny. It is a simple exercise to verify that $\phi \circ \hat{\phi} = [4]$ on $E_{-1, d}$, so $\hat{\phi}$ is indeed the dual isogeny [1, Thm. 9.6.21 and Def. 9.6.23].

**Proposition 2.** Let $p \equiv 3 \pmod{4}$. Let $A = -(4d - 2)$. Then, the map

$$\phi : E_{E, 1, d} \rightarrow E_{M, A, 1}, \quad (x, y) \mapsto (u, v) = \left(\frac{y^2}{x^2}, -\frac{y(x^2 + y^2 - 2)}{x^3}\right)$$

is a 4-isogeny defined over $\mathbb{F}_p$ with dual isogeny

$$\hat{\phi} : E_{M, A, 1} \rightarrow E_{E, 1, d}, \quad (u, v) \mapsto (x, y) = \left(\frac{-4(1 - u^2)v}{u^4 - 2u^2 + 4v^2 + 1}, \frac{(u^2 + 2v - 1)(u^2 - 2v - 1)}{2Au^3 + u^4 + 2Au + 6u^2 + 1}\right).$$

**Proof.** The proof proceeds in a similar way as the proof of Proposition 1. Again, it can be verified by direct calculations that $(u, v) = \phi(x, y)$ satisfies the curve equation $v^2 = u^3 + Au^2 + u$ and that $(x, y) = \hat{\phi}(u, v)$ satisfies $x^2 + y^2 = 1 + dx^2y^2$, using the respective curve equations of $E_{E, 1, d}$ and $E_{M, A, 1}$. This shows that $\phi$ and $\hat{\phi}$ are rational maps [1, Def. 5.5.1].

To show that $\phi$ is regular everywhere, we rewrite it as

$$E_{E, 1, d} \rightarrow \mathbb{P}^2, \quad (x, y) \mapsto (U : V : W) = (xy^2 : -y(x^2 + y^2 - 2) : x^3),$$

from which it is straightforward to deduce that there are no points in $E_{E, 1, d}(\mathbb{F}_p)$ that map to $(0 : 0 : 0)$ under $\phi$. Similarly, to show that $\hat{\phi}$ is regular everywhere we rewrite it as

$$E_{M, A, 1} \rightarrow \mathbb{P}^2, \quad (u, v) \mapsto (X : Y : Z),$$

\[
X = -(4(-u^2 + 1)v(2Au^3 + u^4 + 2Au + 6u^2 + 1),
\]

\[
Y = (u^2 + 2v - 1)(u^2 - 2v - 1)(u^4 - 2u^2 + 4v^2 + 1),
\]

\[
Z = (2Au^3 + u^4 + 2Au + 6u^2 + 1)(u^4 - 2u^2 + 4v^2 + 1),
\]

from which it is again straightforward to deduce that no points in $E_{M, A, 1}(\mathbb{F}_p)$ map to $(0 : 0 : 0)$ under $\hat{\phi}$. Thus, $\phi$ and $\hat{\phi}$ are both regular everywhere, so they are both morphisms [1, Def. 5.5.12].
Following [1, Def. 9.6.1], \( \phi \) maps the neutral element \( \mathcal{O}_{E_1,d} = (0, 1) \) to the point at infinity \( \mathcal{O}_{E_{M,1}} = (0 : 1 : 0) \), so \( \phi \) is an isogeny. For \( \hat{\phi} \), we again homogenize \( E_{M,1} \) under \( u = U/W^2 \) and \( v = V/W^3 \), so that \( \mathcal{O}_{E_{M,1}} = (\lambda^2 : \lambda^3 : 0) \) for \( \lambda \in \mathbb{F}_p \setminus \{0\} \) and \( \hat{\phi} : (U : V : W) \mapsto (X : Y : Z) \), where

\[
X = 4W(-W^2 + U)(W^2 + U)V(2AUW^6 + W^8 + 2AU^3W^2 + 6U^2W^4 + U^4),
Y = (-W^4 + U^2 + 2VW)(-W^4 + U^2 - 2VW)(W^8 - 2U^2W^4 + U^4 + 4V^2W^2),
Z = (2AUW^6 + W^8 + 2AU^3W^2 + 6U^2W^4 + U^4)(W^8 - 2U^2W^4 + U^4 + 4V^2W^2),
\]

takes \( (\lambda^2 : \lambda^3 : 0) \) to \( (0 : 1 : 1) \). Thus, \( \hat{\phi}(\mathcal{O}_{E_{M,1}}) = \mathcal{O}_{E_{1,d}} \), so \( \hat{\phi} \) is an isogeny.

It remains to show that \( \phi \) is a 4-isogeny and that \( \hat{\phi} \) is its dual. As in the proof of Proposition 1, we again follow [1, p. 173] and use the non-singular projective variety \( V_{1,d} : \{X^2 + Y^2 - Z^2 - dT^2, ZT - XY\} \), as well as the corresponding homogenized version of \( \phi \), which is given as

\[
(T : X : Y : Z) \mapsto (XY^2 : -Y(X^2 + Y^2 - 2Z^2) : X^3).
\]

The kernel of \( \phi \) is \( \{(0 : 0 : 1 : 1), (0 : 0 : -1 : 1), (1 : 0 : \sqrt{d} : 0), (1 : 0 : -\sqrt{d} : 0)\} \), all points of order dividing 4, which shows that \( \phi \) is a 4-isogeny. Again, one can verify that \( \hat{\phi} \circ \phi = [4] \) on \( E_{1,d} \), so \( \hat{\phi} \) is indeed the dual isogeny [1, Thm. 9.6.21 and Def. 9.6.23].

\[\square\]

References