Pairings on Edwards Curves

Tanja Lange

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

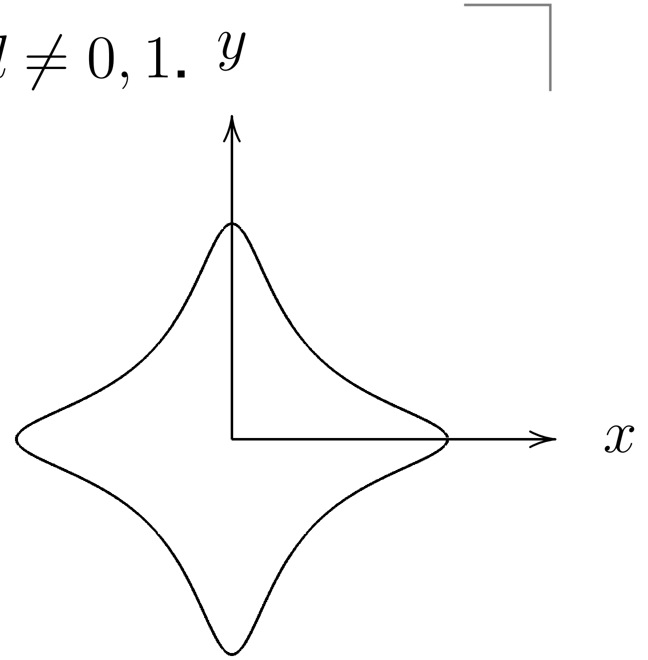
02.04.2009

Joint work with Christophe Arène (IML), Michael Naehrig (TU/e), and Christophe Ritzenthaler (IML)

Edwards curves

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in K \times K | x^2 + y^2 = 1 + dx^2y^2\}$$



Generalization covers more curves over K.

Associative operation on most points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2; $(1, 0)$ and $(-1, 0)$ have order 4.

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.
- Addition on Edwards and Weierstrass corresponds.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\dfrac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \dfrac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\dfrac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \dfrac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- If d is not a square in K the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- If d is not a square in K the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Having addition law work for doubling removes some checks from the code; addition law also works for adding $P + (-P)$ or the neutral element.

Fast addition law

- Very fast point addition 10M + 1S + 1D. Even faster with Inverted Edwards coordinates (9M+1S+1D) and Extended Edwards coordinates (8M+1S+1D).
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstrass curves.
  - Point addition 12M + 4S.
  - Doubling formulas need only 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstrass curves) and many more operations (mixed addition, re-addition, tripling, scaling,. . .) see `www.hyperelliptic.org/EFD`.

Twisted Edwards curves

$$\mathrm{E}_{a,d}: \; ax^2 + y^2 = 1 + dx^2y^2,$$

with $a, d \in K^*, \; a \neq d$.

- Isomorphic to plain Edwards curve $\mathrm{E}_{1,d/a}$ for $a = \square$.
- Set of twisted Edwards curves invariant under quadratic twists.
- Addition formulas very similar to Edwards curves

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

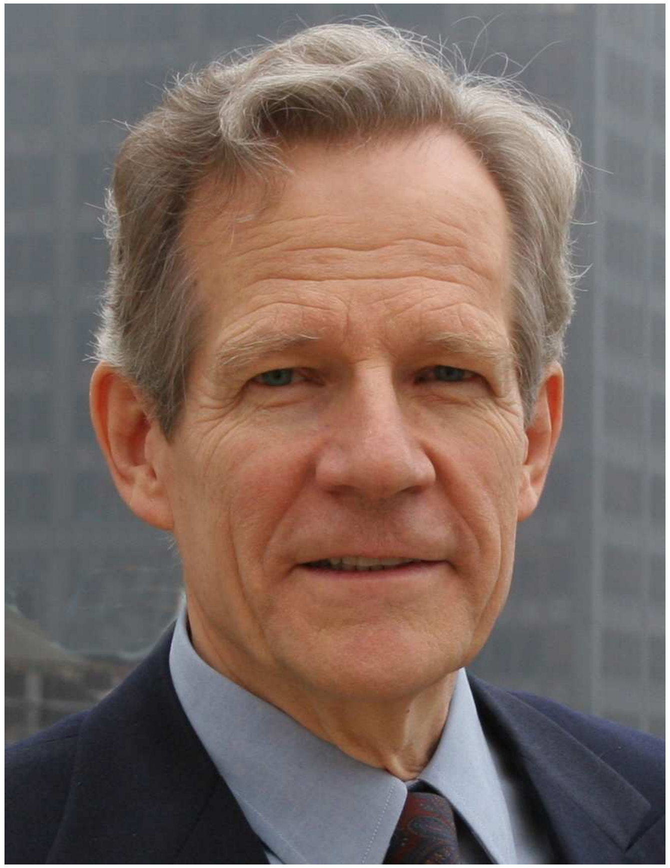
- Arithmetic complete only for $a = \square, d \neq \square$.
- Operation count same as Edwards (except for 1A in DBL and ADD).

Generality of twisted Edwards curves

- Edwards curves require point of order 4; this happens for about $1/3$ of all isomorphism classes if $p \equiv 1 \bmod 4$ and for about $3/8$ if $p \equiv 3 \bmod 4$.
- Twisted Edwards curves have order divisible by 4.
- For $p \equiv 1 \bmod 4$ twisted Edwards curves cover all curves with order divisible by 4, i.e. curves with subgroups isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ or $\mathbb{Z}/4$.
- For $p \equiv 3 \bmod 4$ twisted Edwards curves cover exactly the same as Edwards curves, i.e. they require $\mathbb{Z}/4$.
- Montgomery curves are birationally equivalent to twisted Edwards curves.
- Use 2-isogenies to cover all curves with $4 \mid \#E(\mathbb{F}_p)$.
- (Upcoming preprint: complete addition for all curves.)

Understanding Edwards addition

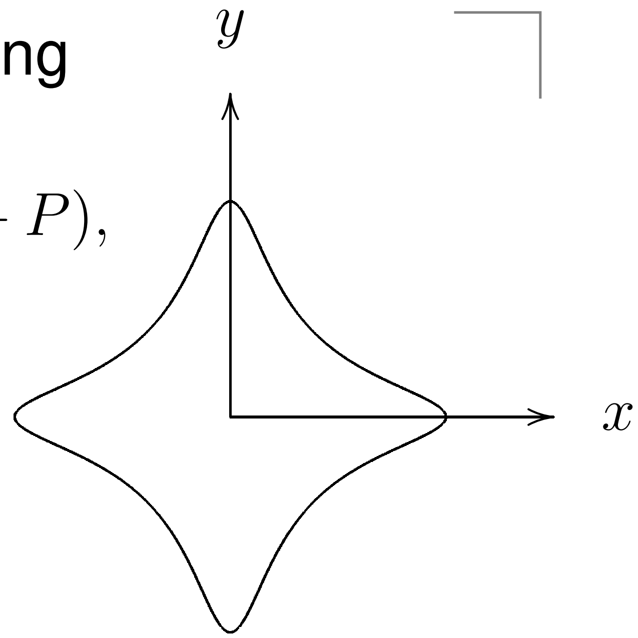
- The Gauss/Euler example is mentioned in some books.
- Edwards generalized this single example to whole class of curves;
- showed how to do arithmetic on this curve;
- gives several proofs of the addition law, e.g. algebraically; via holomorphic differentials; via algebraic variations;
- does not give any geometric interpretation.



- But does have much more! Bulletin of the AMS, **44**, 393–422, 2007

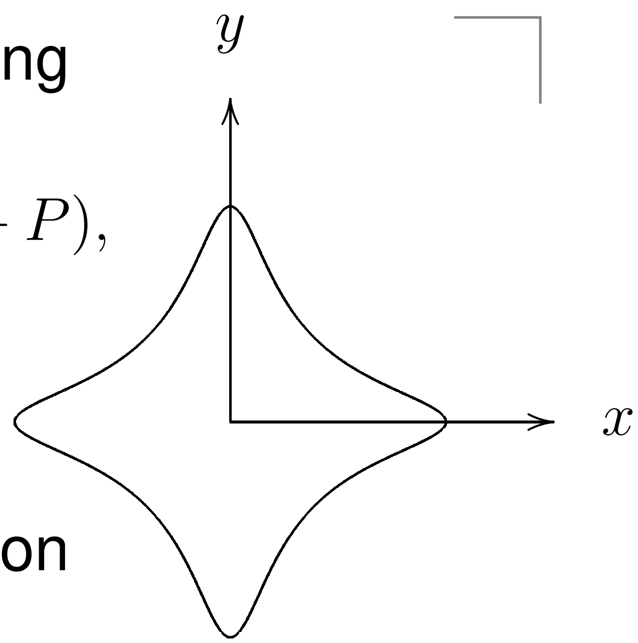
Geometric addition law

- Would like to find function $g_{R,P}$ depending on two input points P, R such that
$$\operatorname{div}(g_{R,P}) = \frac{f_1}{f_2} = R + P - \mathcal{O} - (R + P),$$
where $\mathcal{O} = (0, 1)$ and $R + P$ is the Edwards sum of $R + P$.



Geometric addition law

- Would like to find function $g_{R,P}$ depending on two input points P, R such that
$$\operatorname{div}(g_{R,P}) = \frac{f_1}{f_2} = R + P - \mathcal{O} - (R+P),$$
where $\mathcal{O} = (0,1)$ and $R + P$ is the Edwards sum of $R + P$.



- Equation has degree 4, so expect $4\deg(f)$ intersection points by intersection with function f.
- Functions f_i cannot be linear generically (would have 4 intersection points; need to eliminate 2 out of each).
- Quadratic functions f_i could offer enough freedom of cancellation (8 intersection points).
- Problem: conic is determined by 5 points; not enough control over intersection points.

Conic sections

- Solution: observe that points at infinity $\Omega_1 = (1:0:0)$ and $\Omega_2 = (0:1:0)$ are singular and have multiplicity 2.
- Conic determined by passing through the 5 points $R, P, (0,-1), \Omega_1$, and Ω_2 has only one more intersection point Q with curve; then $Q = -(R+P)$.
- Use f_2 to "replace" $(0,-1)$ by $(0,1)$ and $-(R+P)$ by $R+P = (X_3 : Y_3 : Z_3)$, i.e. put

$$f_2 = l_1 \cdot l_2, \text{ with } l_1 = Z_3Y - Y_3Z \text{ and } l_2 = X.$$

- Conic through $(0,-1), \Omega_1$, and Ω_2 has shape

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ = 0,$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(K)$.

Theorem

(a) If $P_1 \neq P_2$, $P_1 \neq \mathcal{O}'$ and $P_2 \neq \mathcal{O}'$, then

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

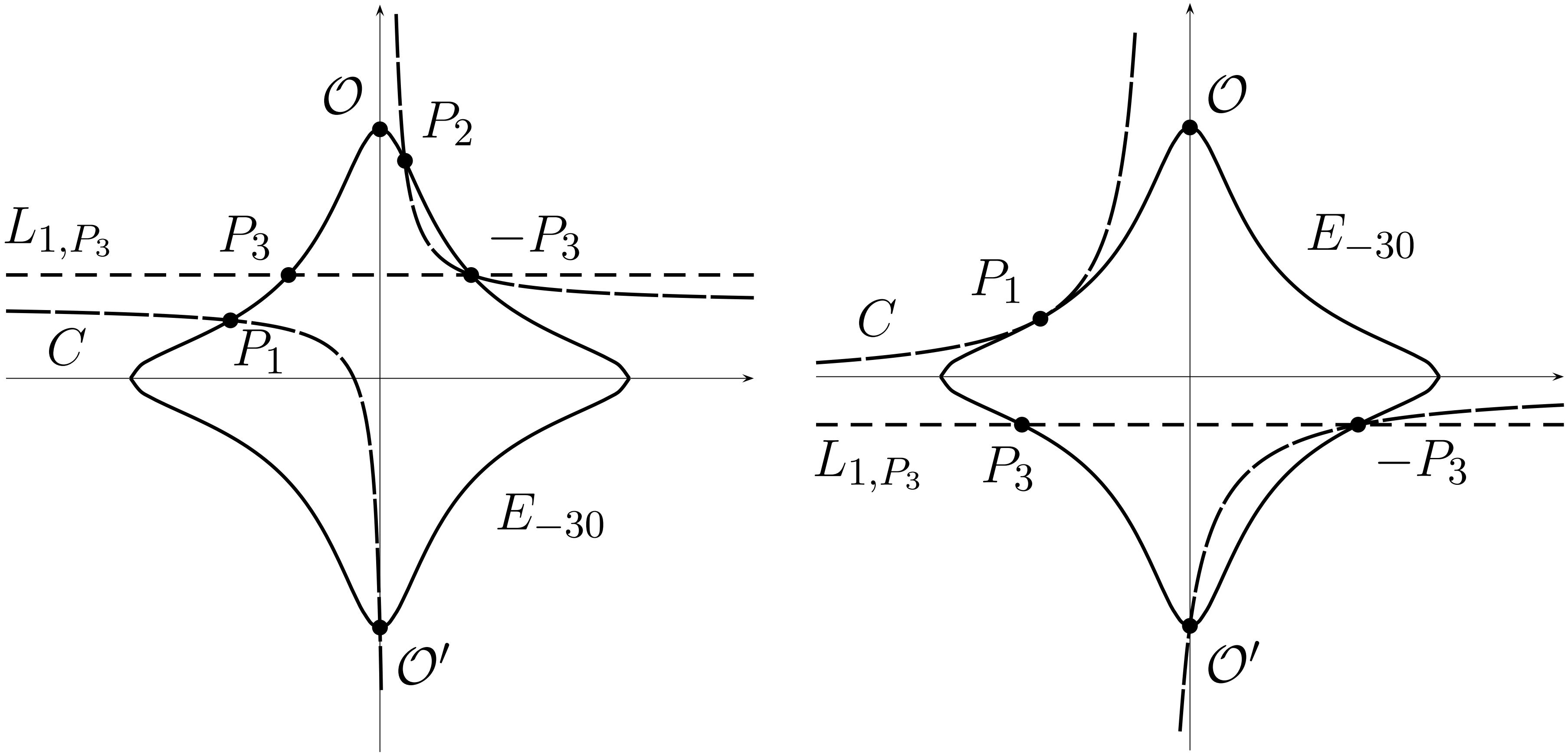
(b) If $P_1 \neq P_2 = \mathcal{O}'$, then

$$c_{Z^2} = -X_1, \; c_{XY} = Z_1, \; c_{XZ} = Z_1.$$

(c) If $P_1 = P_2$, then

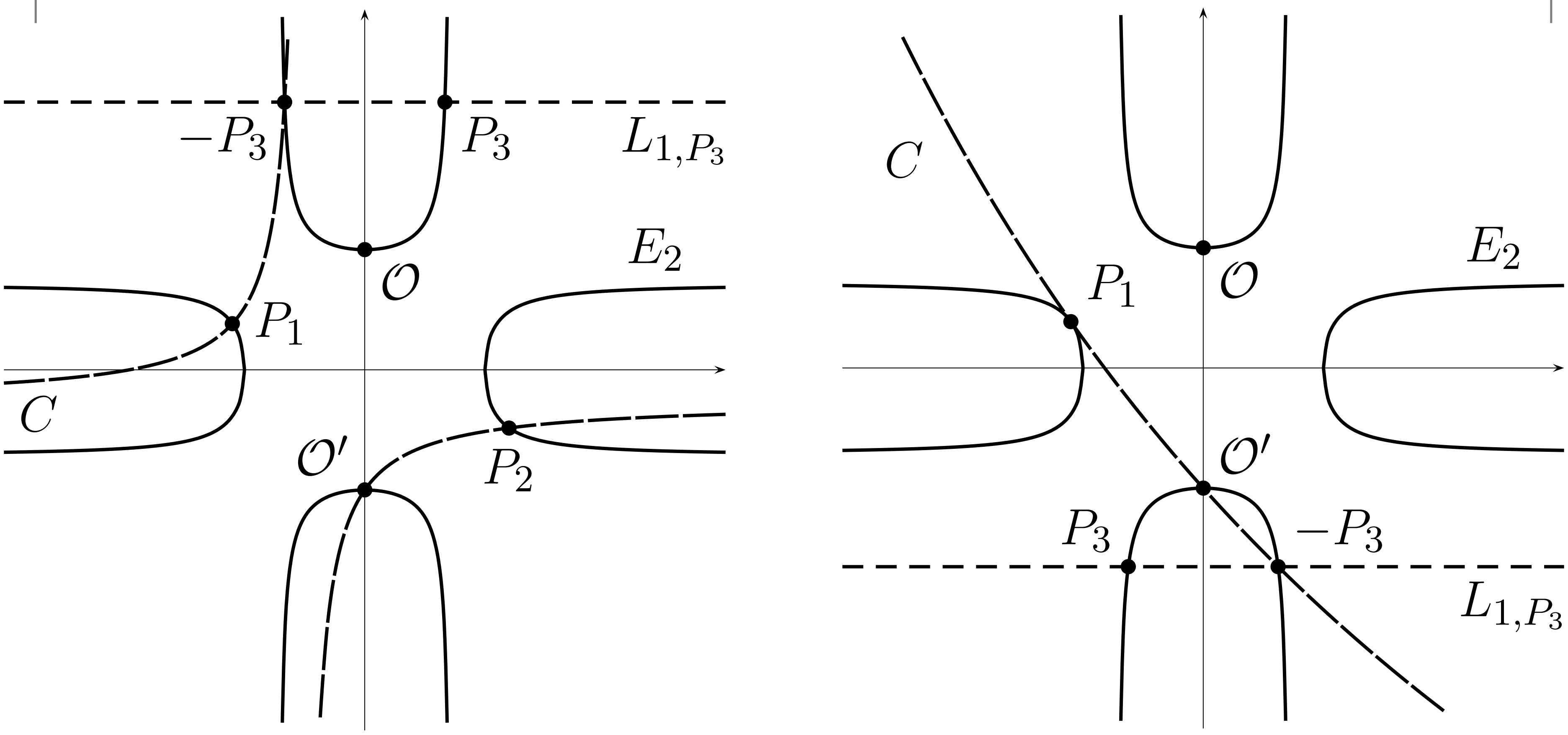
$$\begin{aligned} c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\ c_{XY} &= dX_1^2Y_1 - Z_1^3, \\ c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

Pictures I



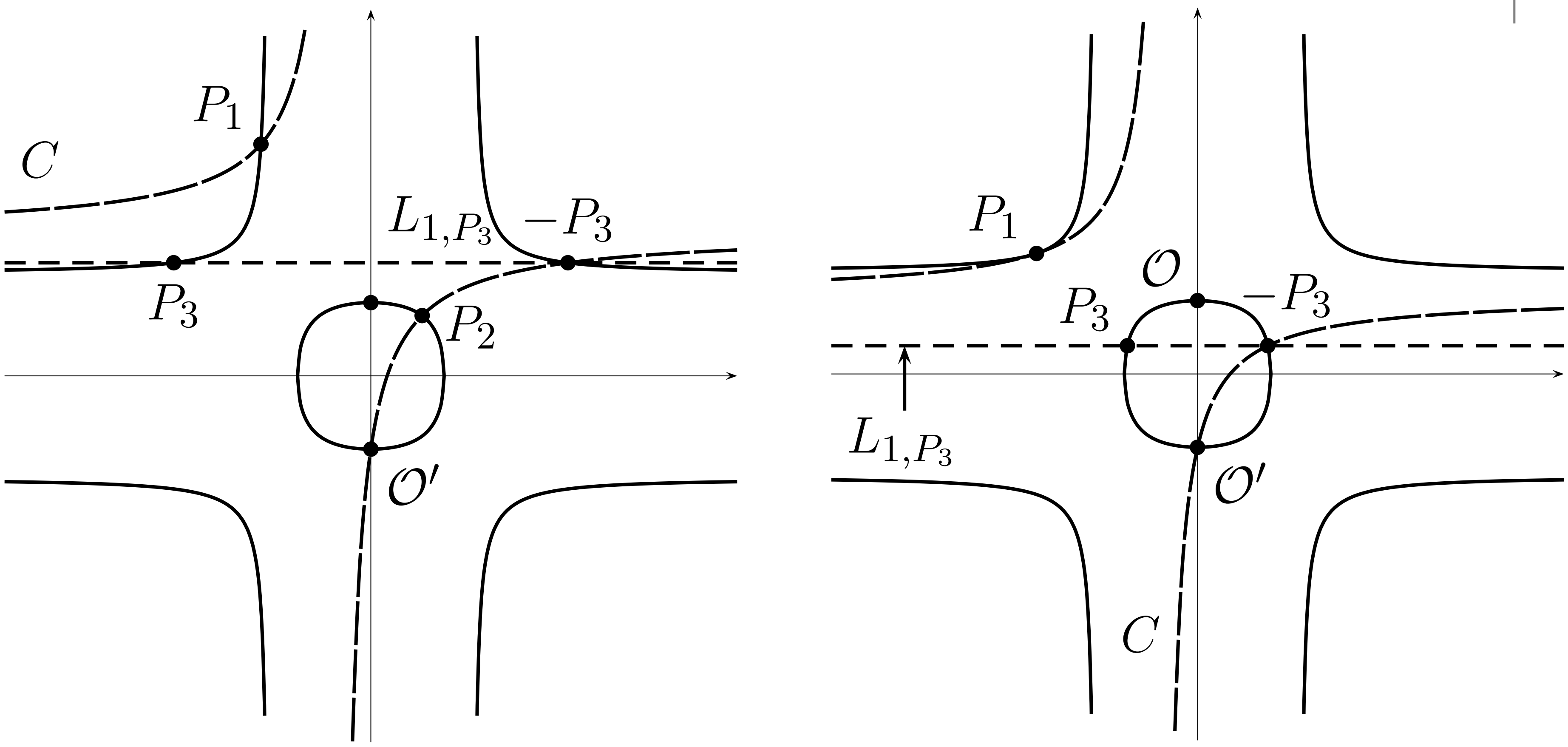
Addition and doubling over $\mathbb{R}$ for $d < 0$.

Pictures II



Addition and doubling over $\mathbb{R}$ for $d > 1$.

Pictures III



Addition and doubling over $\mathbb{R}$ for $0 < d < 1$.

What is this good for?

- Understanding the addition law.
- Efficient arithmetic

What is this good for?

- Understanding the addition law.
- Efficient arithmetic – not really.

What is this good for?

- Understanding the addition law.
- Efficient arithmetic – not really.
- Addition procedures are not complete. (Conic for addition is independent of curve while that for doubling needs tangent.)

What is this good for?

- Understanding the addition law.
- Efficient arithmetic – not really.
- Addition procedures are not complete. (Conic for addition is independent of curve while that for doubling needs tangent.)
- Pairings! Tate pairing (Florian Hess' talk):

$$(P, Q) \mapsto f_P(Q)^{(p^k-1)/r},$$

where $P \in E(\mathbb{F}_p)[r]$, E has embedding degree k with respect to r, and $\mathrm{div}(f_P) = rP - r\mathcal{O}$.

- Miller's algorithm computes $f_P(Q)$ iteratively using $g_{R,P}$.
- All sorts of tricks available to speed up computation of Tate pairing.

Miller function on twisted Edwards curve

- Common assumption k even; $\mathbb{F}_{p^k}$ constructed as $\mathbb{F}_{p^{k/2}}(\alpha)$, with $\alpha^2 = \delta \in \mathbb{F}_{p^{k/2}}$.
- Choose point Q in "smart" way: On twisted Edwards curves the quadratic twist affects the x-coordinate; choose $Q = (x_Q\alpha, y_Q)$.
- Compute

$$\frac{f_1}{l_1 l_2}(x_Q\alpha, y_Q) = \frac{c_{Z^2}(1+y_Q)+c_{XY}x_Q\alpha y_Q+c_{XZ}x_Q\alpha}{(Z_3 y_Q - Y_3)x_Q\alpha} = \frac{c_{Z^2}\frac{1+y_Q}{x_Q\delta}\alpha+c_{XY}y_Q+c_{XZ}}{Z_3 y_Q - Y_3},$$

in $2(k/2)\mathbf{m}$ over $\mathbb{F}_p$ given the coefficients c_{Z^2}, c_{XY}, c_{XY} and precomputed $\eta = \frac{1+y_Q}{x_Q\delta}$. Note that $Z_3 y_Q - Y_3 \in \mathbb{F}_{p^{k/2}}$.

- Computation of coefficients can share subexpressions with addition/doubling computation.

Comparison

	DBL	mADD	ADD
$\mathcal{J}$,	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m}_{\mathbf{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = -3$,	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = 0$,	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{E}$,	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m}_{\mathbf{a}}$	$12\mathbf{m} + 1\mathbf{m}_{\mathbf{a}}$	$14\mathbf{m} + 1\mathbf{m}_{\mathbf{a}}$

Comparison

	DBL	mADD	ADD
$\mathcal{J}$,	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m}_{\mathbf{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m}_{\mathbf{a_4}}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = -3$,	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$6\mathbf{m} + 5\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = 0$,	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$3\mathbf{m} + 8\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
$\mathcal{E}$,	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m}_{\mathbf{a}}$	$12\mathbf{m} + 1\mathbf{m}_{\mathbf{a}}$	$14\mathbf{m} + 1\mathbf{m}_{\mathbf{a}}$

Pairing friendly Edwards curves

Use the construction of generalized MNT curves with cofactor 4 given by S. Galbraith, J. McKee, and P. Valenca to construct curves with $k = 6$. We balance the size of the subgroup and the finite field (want non-trivial co-factor).

$$D = 7230,\ \lceil \log(n) \rceil = 165,\ \lceil \log(h) \rceil = 34,\ \lceil \log(p) \rceil = 201$$

$$\begin{aligned}
p &= 2051613663768129606093583432875887398415301962227490187508801,\\
n &= 448125454133085799139574382013313854347434423662 77,\\
h &= 7 \cdot 733 \cdot 2230663,\\
d &= 889556570662354157210639662153375862261205379822879716332449.
\end{aligned}$$

More curves and the explicit formulas in upcoming preprint.