Pairings on Edwards Curves

Tanja Lange

Technische Universiteit Eindhoven

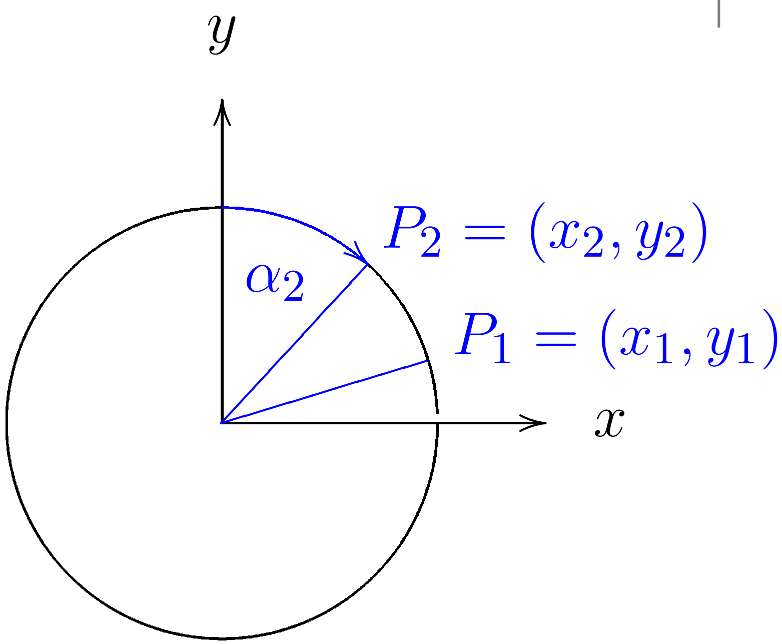
tanja@hyperelliptic.org

15.05.2009

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

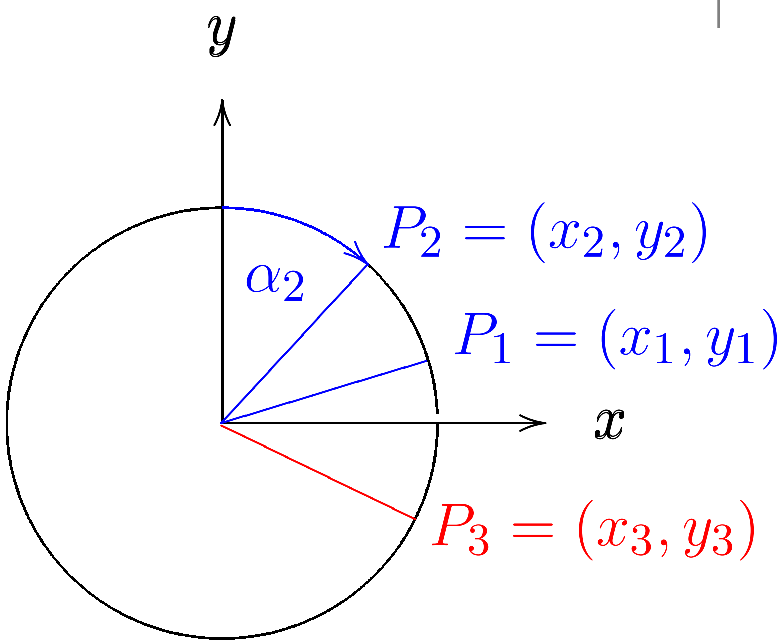
Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x, y) \in K \times K | x^2 + y^2 = 1\}$



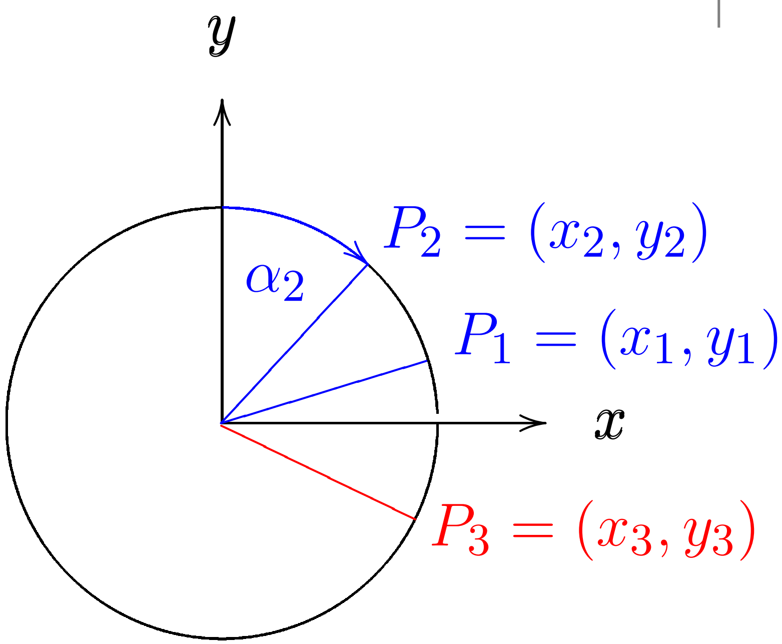
Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x,y) \in K \times K | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i), \; y_i = \cos(\alpha_i)$



Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x, y) \in K \times K | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i),\ y_i = \cos(\alpha_i)$



$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \end{aligned}$$

$$\begin{aligned} y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \end{aligned}$$

Addition of angles defines commutative group law
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Cryptography on the circle

- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R =$

Cryptography on the circle

- $(0,1)$ is at $\alpha = 0$. Then $(0,1) + Q = Q + (0,1) = Q$.
- $R = (0,-1)$ is at angle $180°$. Then $[2]R =(0,1)$.
- What is the order of $(1,0)$?

Cryptography on the circle

- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R =(0, 1)$.
- What is the order of $(1, 0)$? $[2](1, 0) = (0, -1)$.

Cryptography on the circle

- $(0, 1)$ is at $\alpha = 0$. Then $(0, 1) + Q = Q + (0, 1) = Q$.
- $R = (0, -1)$ is at angle $180°$. Then $[2]R =(0, 1)$.
- What is the order of $(1, 0)$? $[2](1, 0) = (0, -1)$.
- Negative of (x, y) is $(-x, y)$.
- These observations are clear from the angles on the circle, e.g. $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is at $45°$ and has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$?

Cryptography on the circle

- $(0,1)$ is at $\alpha = 0$. Then $(0,1) + Q = Q + (0,1) = Q$.
- $R = (0,-1)$ is at angle 180°. Then $[2]R =(0,1)$.
- What is the order of $(1,0)$? $[2](1,0) = (0,-1)$.
- Negative of (x,y) is $(-x,y)$.
- These observations are clear from the angles on the circle, e.g. $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is at 45° and has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$? Compute $[2]S$:

$x_3 = \frac{3}{5}\frac{4}{5} + \frac{4}{5}\frac{3}{5} = \frac{24}{25}, \; y_3 = \frac{4}{5}\frac{4}{5} - \frac{3}{5}\frac{3}{5} = \frac{7}{25}$

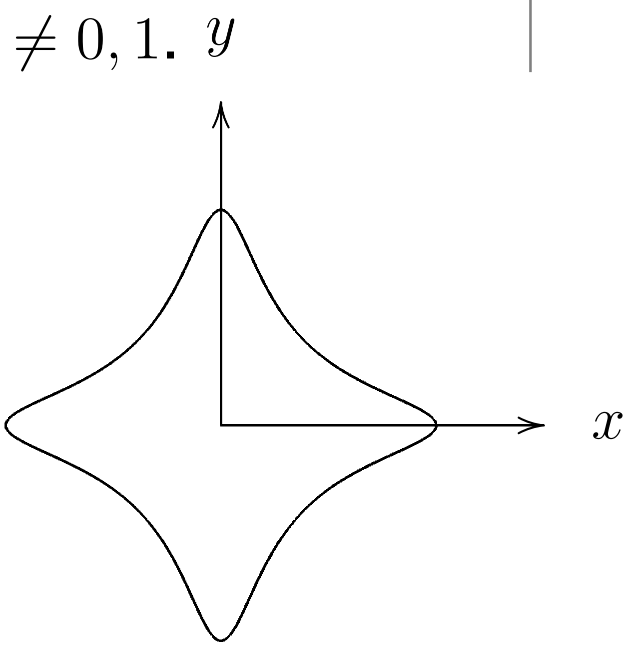
$[3]S = [2]S + S$: $x_3 = \frac{24}{25}\frac{4}{5} + \frac{7}{25}\frac{3}{5} = \frac{103}{125}, \; y_3 = \frac{7}{25}\frac{4}{5} - \frac{24}{25}\frac{3}{5} = \frac{-54}{125}$.

- For $p \equiv 3 \bmod 4$ the clock modulo p gives $T_2(\mathbb{F}_p)$.

Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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

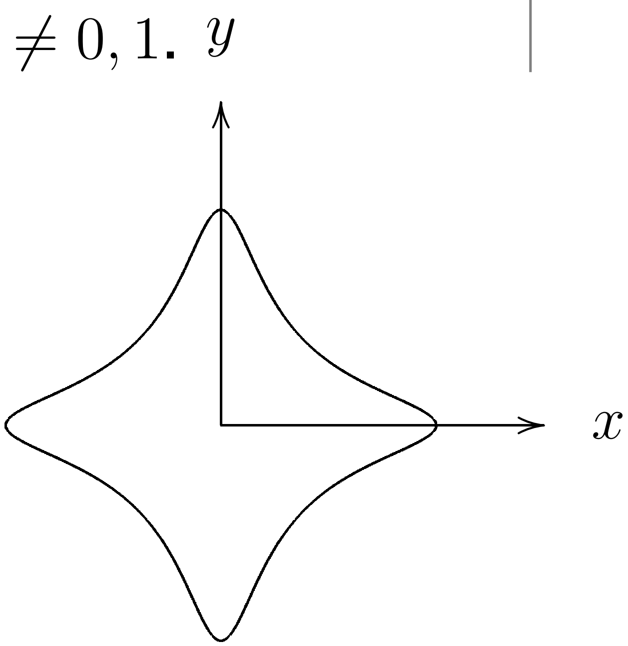


Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

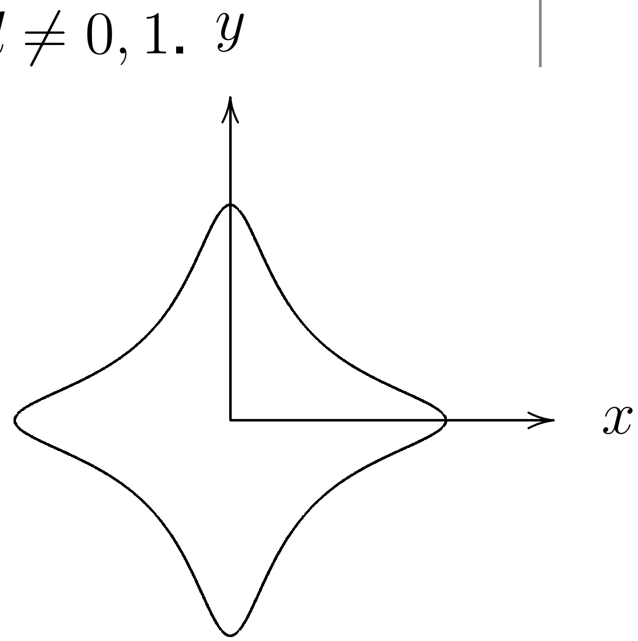
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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

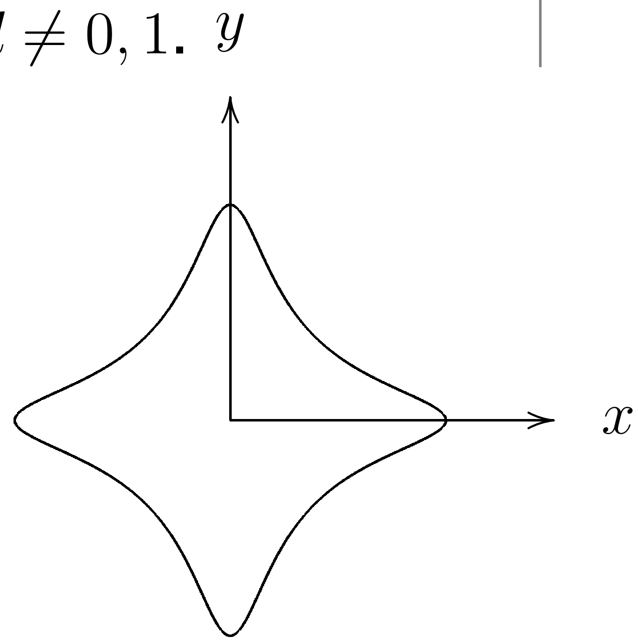
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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

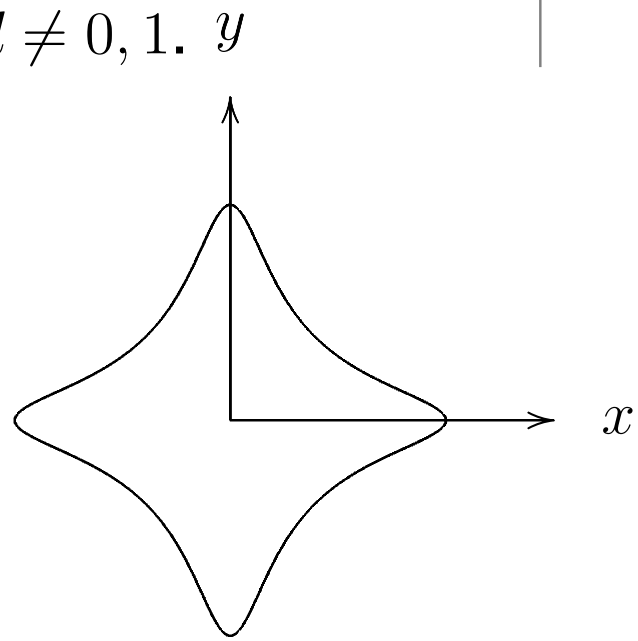
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).

Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on 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 $(0, 1)$ (like on circle).
- $-(x_1, y_1) =$

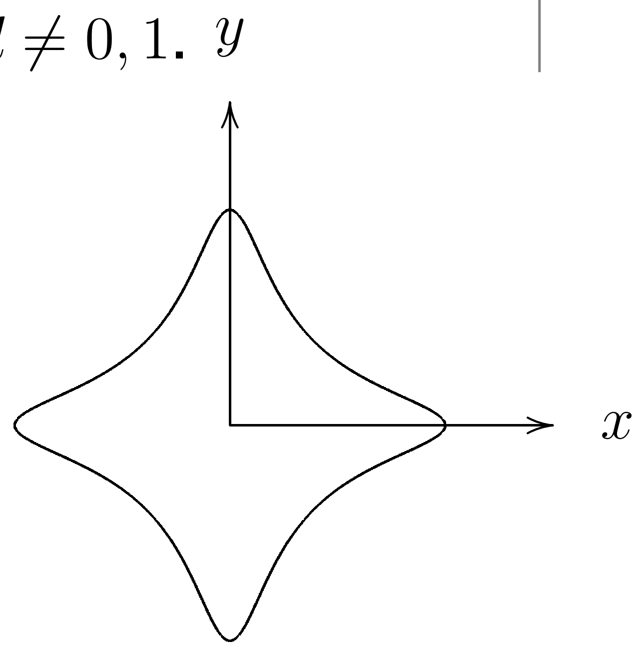
Now add on an elliptic curve

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

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

Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on 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 $(0, 1)$ (like on circle).
- $-(x_1, y_1) = (-x_1, y_1)$ (like on circle).

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.
- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$

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.
- $$P + Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$
- $$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$$

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.

Explicit formulas: addition

- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- Avoid inversions: Use $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ to represent $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$, i. e., $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for $\lambda \neq 0$.
- Addition formulas in projective coordinates:

$$\begin{aligned} A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\ E &= d \cdot C \cdot D;\ F = B - E;\ G = B + E; \\ X_3 &= A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D); \\ Y_3 &= A \cdot G \cdot (D - C); \\ Z_3 &= F \cdot G. \end{aligned}$$

- Needs 10M + 1S + 1D + 7A.

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

  Use curve equation $x^2 + y^2 = 1 + dx^2y^2$.

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
  $$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$
  $$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right)$$
$$= \left(\frac{2 x_1 y_1}{1 + d (x_1 y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d (x_1 y_1)^2} \right)$$
$$= \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right)$$
- Doubling formulas in projective coordinates:
$$\begin{aligned} B &= (X_1 + Y_1)^2;\ C = X_1^2;\ D = Y_1^2; \\ E &= C + D;\ H = Z_1^2;\ J = E - 2H; \\ X_3 &= (B - E) \cdot J;\ Y_3 = E \cdot (C - D);\ Z_3 = E \cdot J. \end{aligned}$$
- Needs 3M + 4S + 6A.

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`.

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.

Exceptional points of the map

- Points with $v(u+u_4)=0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1 - (4u_4^3/v_4^2)$.
- $u = -u_4$ is u-coordinate of a point iff

$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_4) \\ = \quad & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v = 0$ corresponds to $(0,0)$ which maps to $(0,-1)$ on Edwards curve and to solutions of $u^2 + (v_4^2/u_4^2 - 2u_4)u + u_4^2 = 0$. Discriminant is

$$(v_4^2/u_4^2 - 2u_4)^2 - 4u_4^2 = v_4^4 d,$$

  i. e., points defined over K iff d is a square.

Complete addition law

- Previous slide shows that for $d \neq \square$ in K all points of the Weierstrass curve map to the affine part of the Edwards curve; where we extend the map by $P_\infty \mapsto (0,1)$ and $(0,0) \mapsto (0,-1)$.
- Geometric description: The other missing points from the Weierstrass curve correspond to the blow-ups of $(1:0:0)$ and $(0:1:0)$ on the Edwards curve. They blow up to two points each on the desingularization of the curve. On both the Weierstrass and the Edwards side these points are defined over $K(\sqrt{d})$.
- Attention: Having no K-rational points at infinity does not guarantee that the formulas are complete:

$$(x_3, y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

is addition on Edwards curve . . . and fails for doublings.

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

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

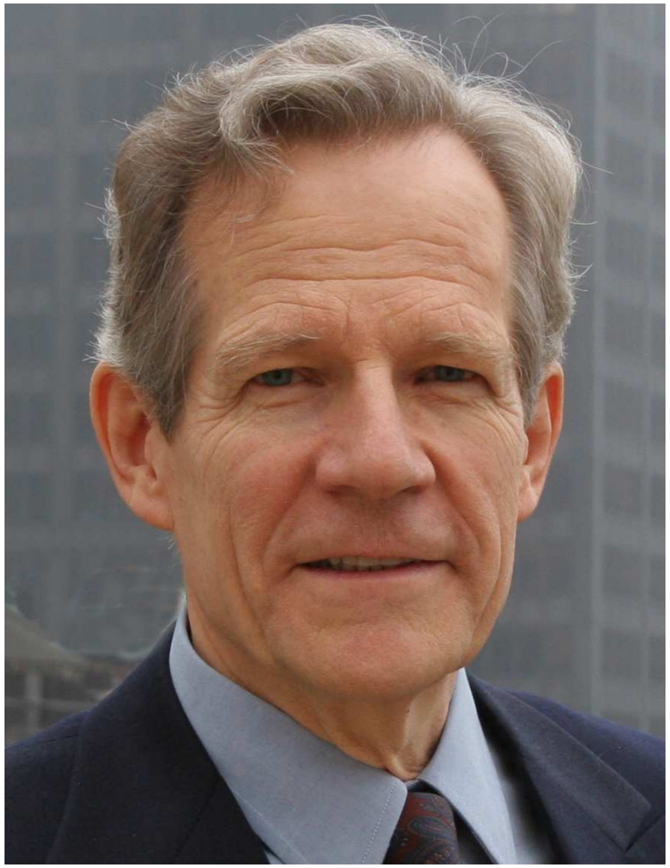
- Arithmetic complete only for $a = \square, d \neq \square$.
- Operation count same as Edwards (except for 1A in DBL and ADD).

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

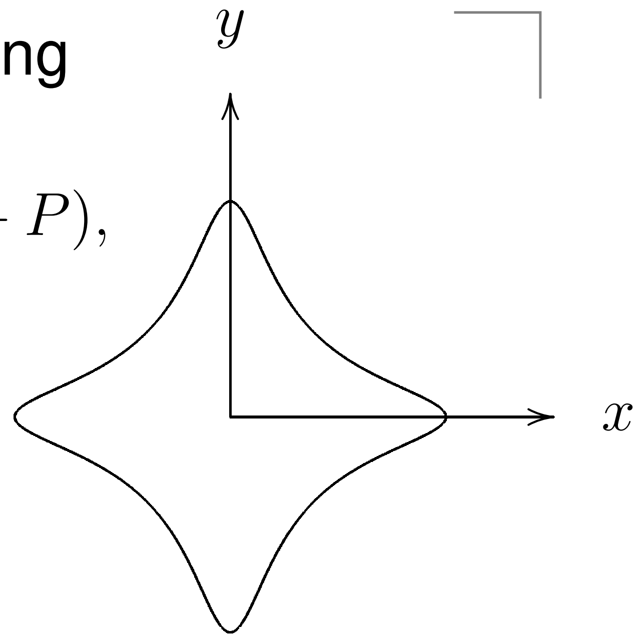
- The Gauss/Euler example ($d = -1$) is mentioned in some books.
- Edwards generalized this single example to whole class of curves;
- showed how to do arithmetic on this curve;
- gives several proofs of the addition law, e.g. algebraically; via holomorphic differentials; via algebraic variations.
- does not give any geometric interpretation.



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

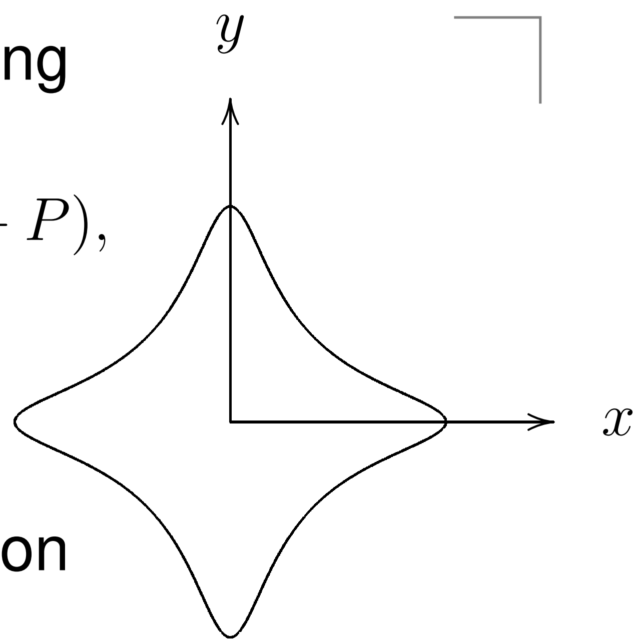
Geometric addition law

- 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; 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

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

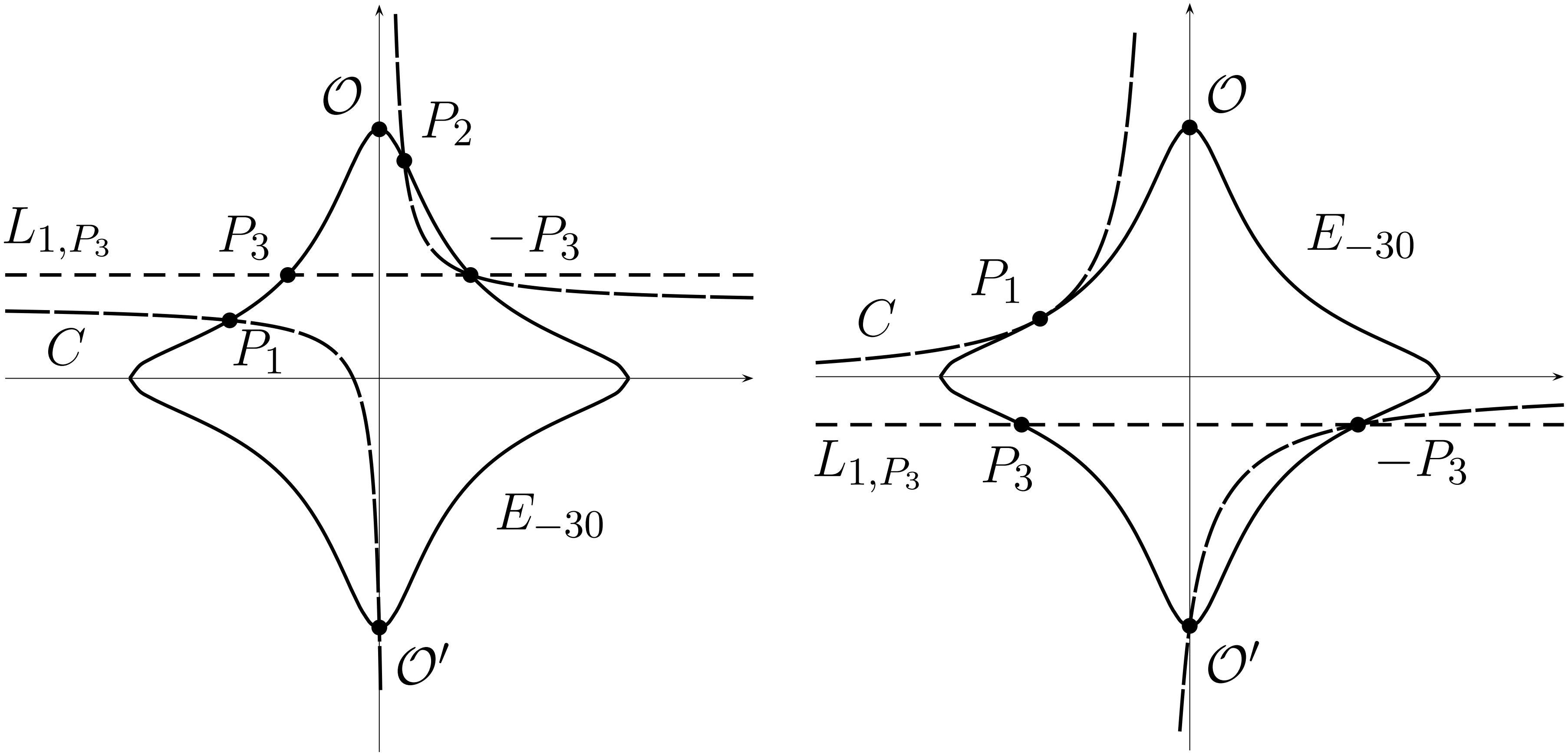
(b) If $P_1 \neq P_2 = \mathcal{O}'$, then

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

(c) If $P_1 = P_2$, then

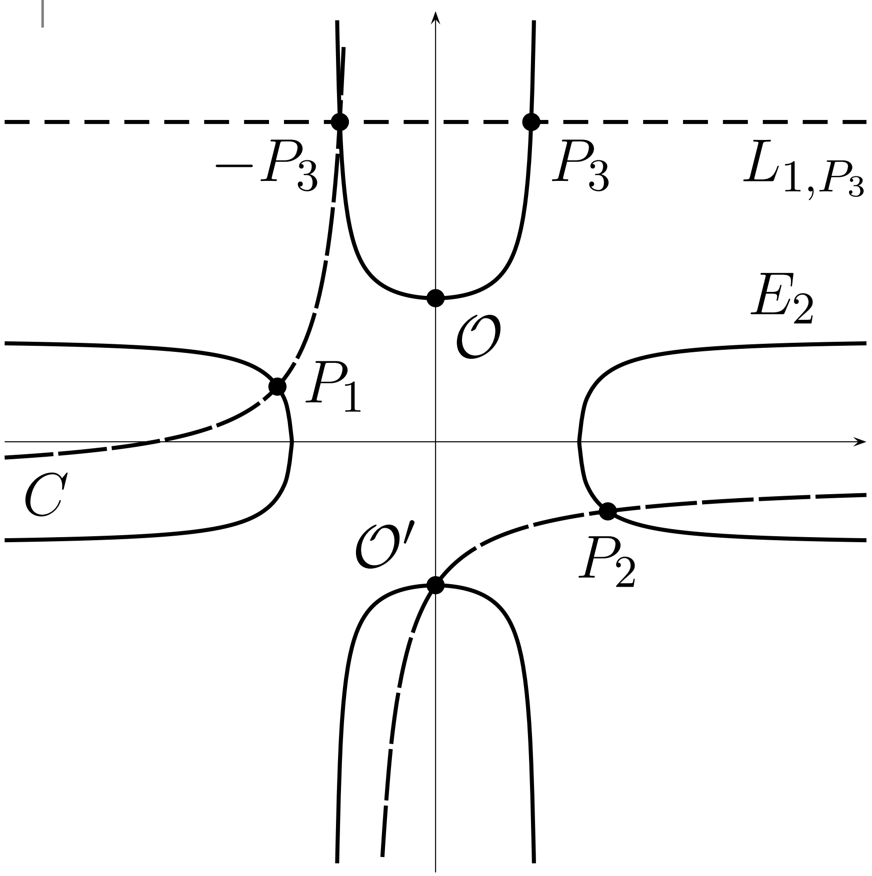
$$\begin{aligned}
c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\
c_{XY} &= dX_1^2Y_1 - Z_1^3, \\
c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2).
\end{aligned}$$

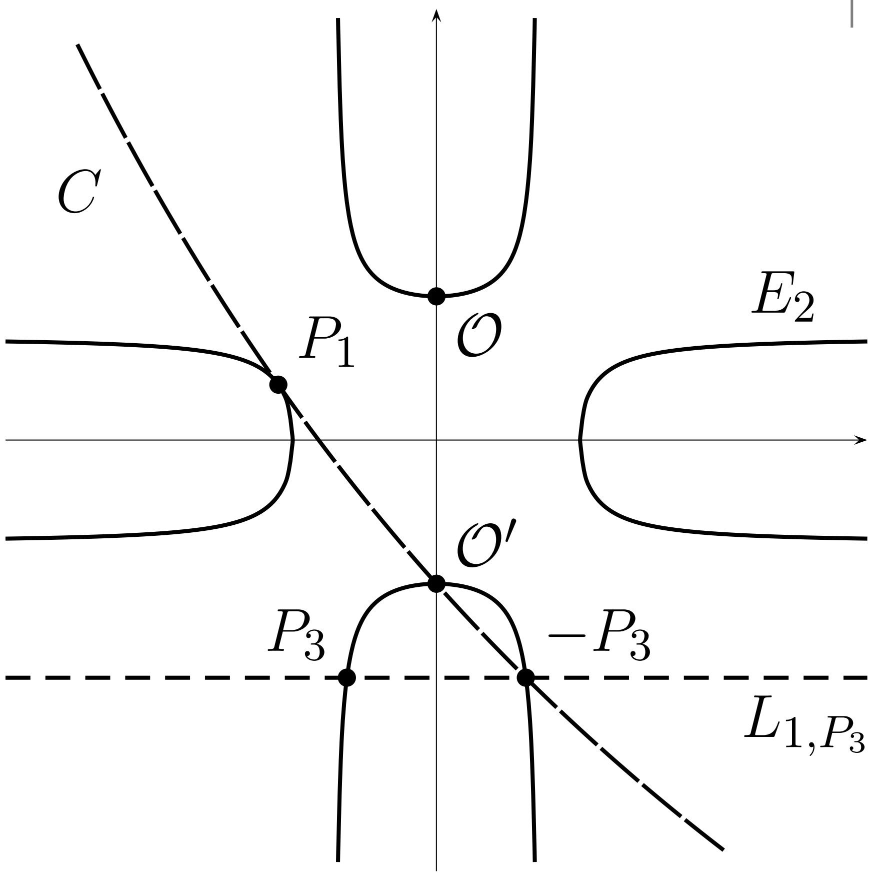
Pictures I



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

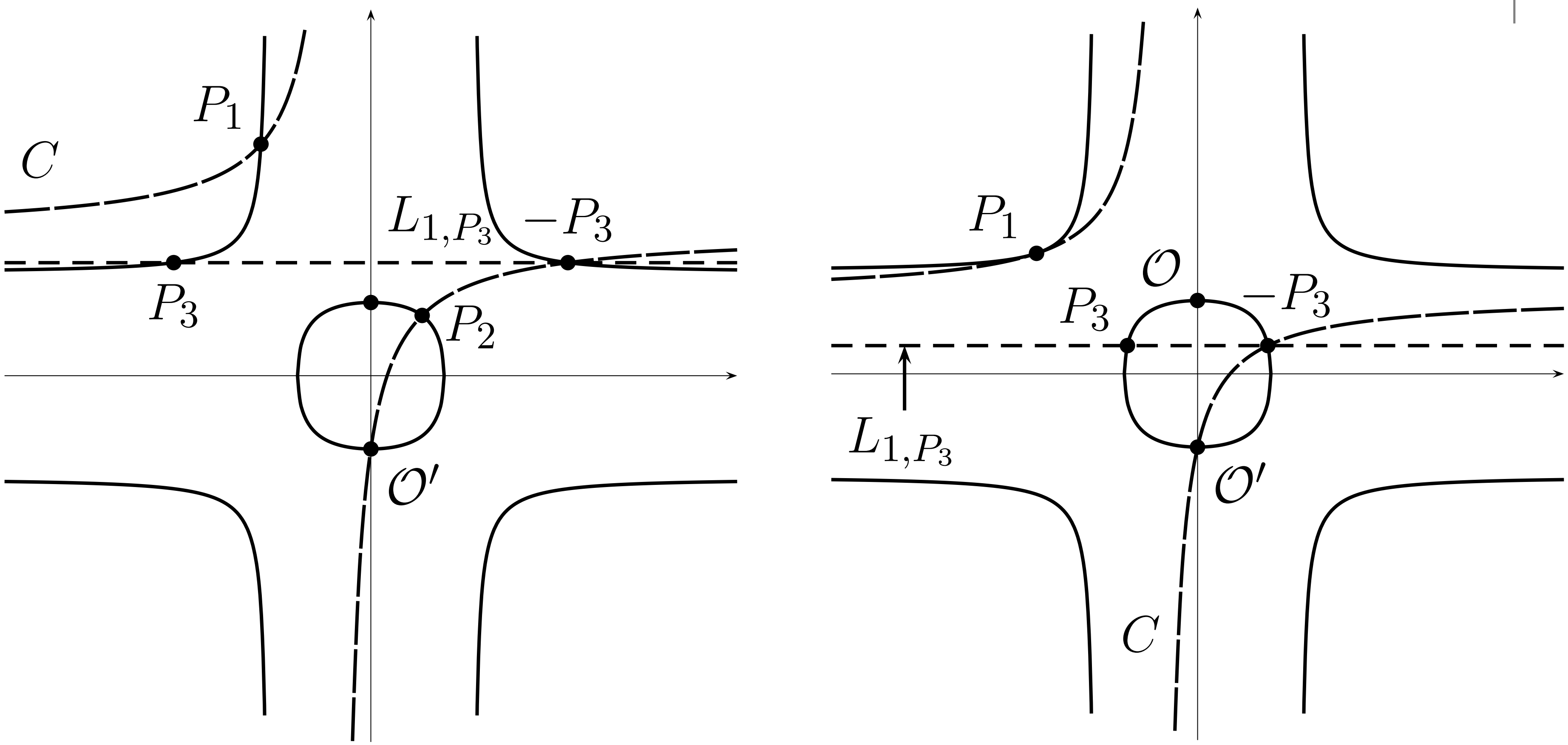
Pictures II





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:

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

  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.

Previous attempts

Das, Sarkar [Pairing 2008]:

- Map points to a curve in Weierstrass form using birational map and compute pairing there.
- Express functions $g_{R,R}$ and $g_{R,P}$ in the Miller loop by transformation to Montgomery form.
- Explicit formulas for supersingular curves with $k = 2$.

Ionica, Joux [Indocrypt 2008]:

- Compute Miller functions on a curve

$$v^2 u = (1 + du)^2 - 4u.$$

- Actually compute 4th power of the Tate pairing.
- Explicit formulas for even k.

Miller's algorithm

Let $k > 1$ be the embedding degree of E w.r.t. r,
$P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})$,
$r = (r_{l-1}, \ldots, r_1, r_0)_2$.
Compute the Tate pairing as:

1. $R \leftarrow P$, $f \leftarrow 1$
2. for $i = l - 2$ to 0 do
   (a) $f \leftarrow f^2 \cdot g_{R,R}(Q),\ R \leftarrow 2R$ //doubling step
   (b) if $r_i = 1$ then
   $f \leftarrow f \cdot g_{R,P}(Q),\ R \leftarrow R + P$ //addition step
3. $f \leftarrow f^{(p^k-1)/r}$

Miller function on twisted Edwards curves I

Assume an even embedding degree k.

- Represent $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$ where $\alpha^2 = \delta \in \mathbb{F}_{p^{k/2}}$.
- Use quadratic twist $E_{\delta a,\delta d}(\mathbb{F}_{p^{k/2}})$ to represent second pairing argument $Q = \psi(Q')$:

$$\begin{aligned} \psi : E_{\delta a,\delta d}(\mathbb{F}_{p^{k/2}}) &\rightarrow E_{a,d}(\mathbb{F}_{p^k}), \\ Q' = (x_0, y_0) &\mapsto (x_0\alpha, y_0). \end{aligned}$$

- Here $y_0 \in \mathbb{F}_{p^{k/2}}$ lies in a proper subfield of $\mathbb{F}_{p^k}$.
- In Miller's algorithm compute
  $f^2 \cdot g_{R,R}(\psi(Q'))$ (doubling step) and
  $f \cdot g_{R,P}(\psi(Q'))$ (addition step).

Miller function on twisted Edwards curves II

- Compute

$$\frac{h_1}{l_1 l_2}(x_0\alpha, y_0) = \frac{c_{Z^2}(1+y_0) + c_{XY}x_0\alpha y_0 + c_{XZ}x_0\alpha}{(Z_3 y_0 - Y_3)x_0\alpha} = \frac{c_{Z^2}\frac{1+y_0}{x_0\delta}\alpha + c_{XY}y_0 + c_{XZ}}{Z_3 y_0 - Y_3},$$

  where $(X_3 : Y_3 : Z_3)$ are the coord. of $[2]R$ or $R+P$,
- in $2(k/2)\mathbf{m}$ over $\mathbb{F}_p$ given the coefficients c_{Z^2}, c_{XY}, c_{XZ} and precomputed $\eta = \frac{1+y_0}{x_0\delta}$.
- Note that $Z_3 y_Q - Y_3 \in \mathbb{F}_{p^{k/2}}$. Discard it since final exponentiation maps it to 1 anyway.

Pairing-friendly Edwards curves

How to get Edwards curves with small embedding degree?

- Construct pairing-friendly curves in Weierstrass form and then transform to Edwards or twisted Edwards form.
- Only requirement is that the group order is a multiple of 4.
- If have a point of order 4, get plain Edwards curve.
- If not, get twisted Edwards curve. Can be transformed to plain Edwards form by using 2-isogenies.

Pairing-friendly Edwards curves

- Need curves with $4 \mid \#E(\mathbb{F}_p)$.
- Use generalized MNT construction for curves with cofactor 4 as done by Galbraith, McKee, Valença.
- Parameterizations for embedding degree $k = 6$ and cofactor 4.

Case	$q(\ell)$	$t(\ell)$	$n(\ell)$
1	$16\ell^2 + 10\ell + 5$	$2\ell + 2$	$4\ell^2 + 2\ell + 1$
2	$112\ell^2 + 54\ell + 7$	$14\ell + 4$	$28\ell^2 + 10\ell + 1$
3	$112\ell^2 + 86\ell + 17$	$14\ell + 6$	$28\ell^2 + 18\ell + 3$
4	$208\ell^2 + 30\ell + 1$	$-26\ell - 2$	$52\ell^2 + 14\ell + 1$
5	$208\ell^2 + 126\ell + 19$	$-26\ell - 8$	$52\ell^2 + 38\ell + 7$

Pairing-friendly Edwards curves

- First solve the norm equation

$$t(\ell)^2 - 4q(\ell) = -Dv^2.$$

- Case 1 in the table:

$$t(\ell) = 2\ell + 2,\ q(\ell) = 16\ell^2 + 10\ell + 5$$

  Transform equation into corresponding Pell equation by completing the square:

$$t(\ell)^2 - 4\,q(\ell) = -D\,y^2 \quad \Longleftrightarrow \quad x^2 - 15\,D\,y^2 = -44,$$

  where $x = 15\ell + 4$.

Pairing-friendly Edwards curves

- Constructed curves over $\mathbb{F}_p$ have order

$$\#E(\mathbb{F}_p) = 4hr$$

for a prime r and cofactor h.

- Since embedding degree is fixed to 6, balance the DLPs; ECRYPT report on key sizes suggests the following bitsizes:

r	p	p^6	h
160	208	1248	46
192	296	1776	102
224	405	2432	179
256	541	3248	283
512	2570	15424	2056

Examples

$D = 1$, $\lceil \log(n) \rceil = 363$, $\lceil \log(h) \rceil = 7$, $\lceil \log(p) \rceil = 371$

$$
\begin{aligned}
p &= 324289037284274348719606384560284091622819395824325759 45\\
&\quad 306321535594026280100199466816249589739372396374201691 41,\\
n &= 111057889480915872849180268685028798500965546515180054 60\\
&\quad 623832064312035897815509951488907964532000965993787241,\\
h &= 73,\\
d &= 162144518642137174359803192280142045811409697912162879 72\\
&\quad 65316076779701314005009973340812479486968619818710084571.
\end{aligned}
$$

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

$$
\begin{aligned}
p &= 2051613663768129606093583432875887398415301962227490187508801,\\
n &= 44812545413308579913957438201331385434743442366277,\\
h &= 7 \cdot 733 \cdot 2230663,\\
d &= 8895565706623541572106396621533758622612053798228797163324 49.
\end{aligned}
$$

Toy example in Barreto, Lynn, Scott with $k = 12$, $D = 13188099$.

Explicit formulas

- Use explicit formulas with extended Edwards coordinates by Hisil, et. al. [Asiacrypt 2008] for point doubling and addition in Miller's algorithm.
- Can reuse large parts of the computation for coefficients of the conic.
- Use even embedding degree and quadratic twist to represent second pairing argument Q, i.e. multiplications with coordinates x_Q and y_Q cost $k/2$ multiplications in $\mathbb{F}_p$.
- Compute conic coefficients in doubling step with $6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$, in addition step with $14\mathbf{m} + 1\mathbf{m_a}$ (mixed addition $12\mathbf{m} + 1\mathbf{m_a}$).

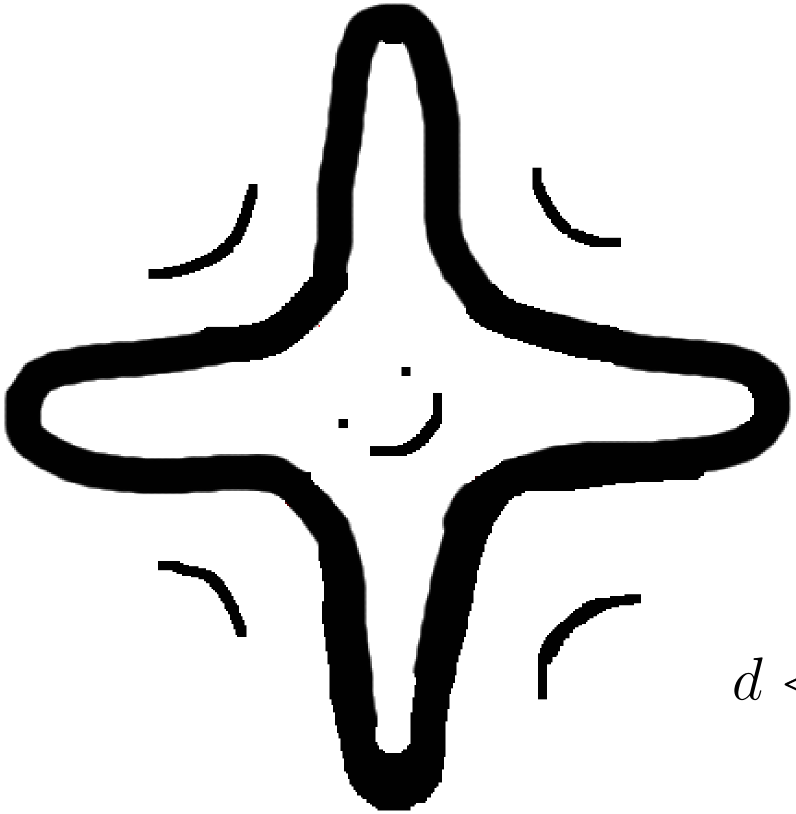
Comparison

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

Thank you for your attention!



$d < 0$, non-square!

Explicit formulas and more curve examples in preprint

`http://eprint.iacr.org/2009/155`