Binary Edwards Curves

Daniel J. Bernstein and Tanja Lange

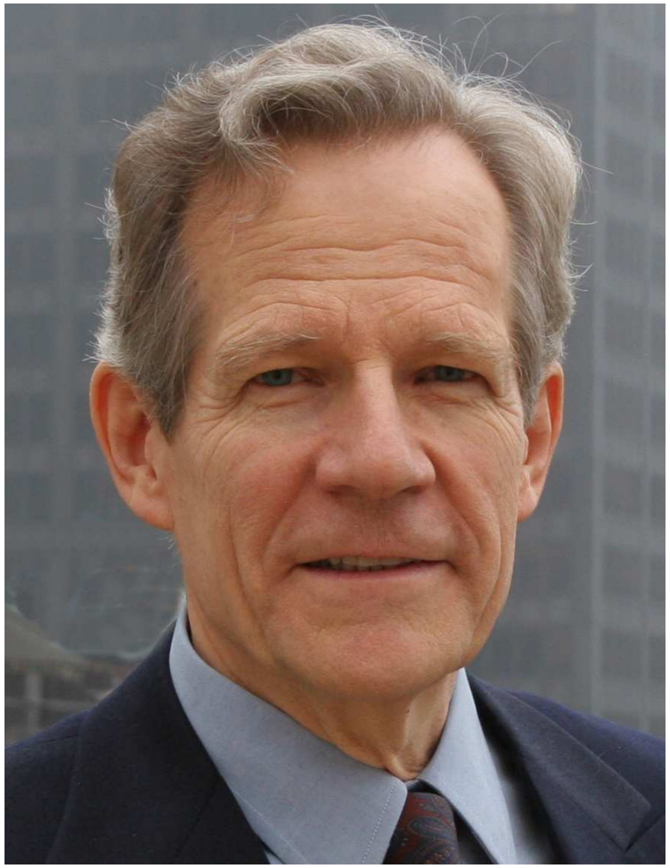
University of Illinois at Chicago and Technische Universiteit Eindhoven

djb@cr.yp.to tanja@hyperelliptic.org

09.05.2008

joint work with Reza Rezaeian Farashahi, Eindhoven

Harold M. Edwards



- Edwards generalized single example $x^2 + y^2 = 1 - x^2y^2$ by Euler/Gauss to whole class of curves.
- Shows that – after some field extensions – every elliptic curve over field k of odd characteristic is birationally equivalent to a curve of the form $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
- Edwards gives addition law for this generalized form, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization . . . in his paper Bulletin of the AMS, **44**, 393–422, 2007

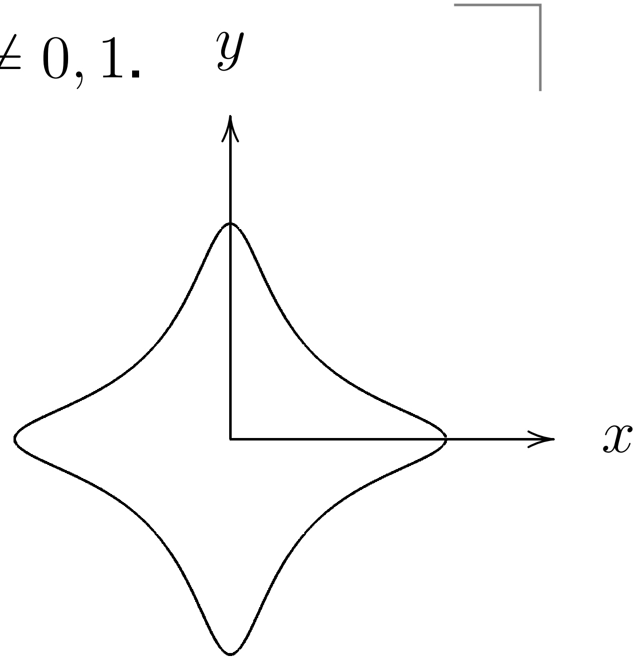
How to add on an Edwards curve

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

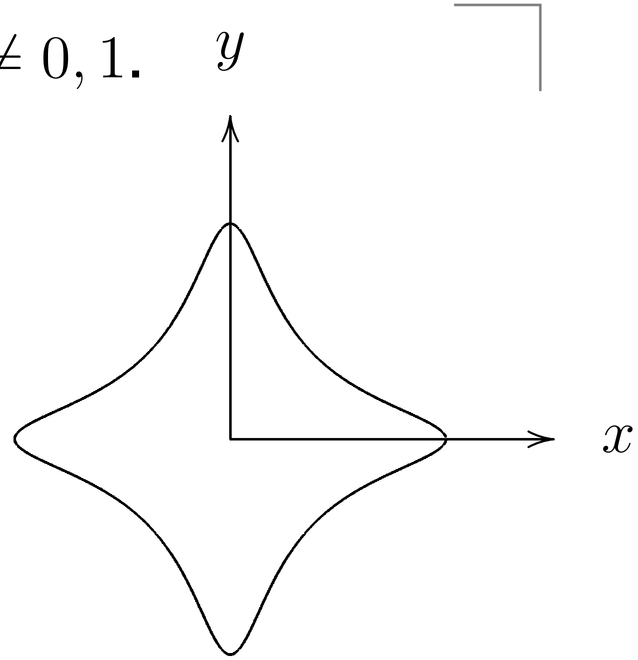


$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

How to add on an Edwards curve

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

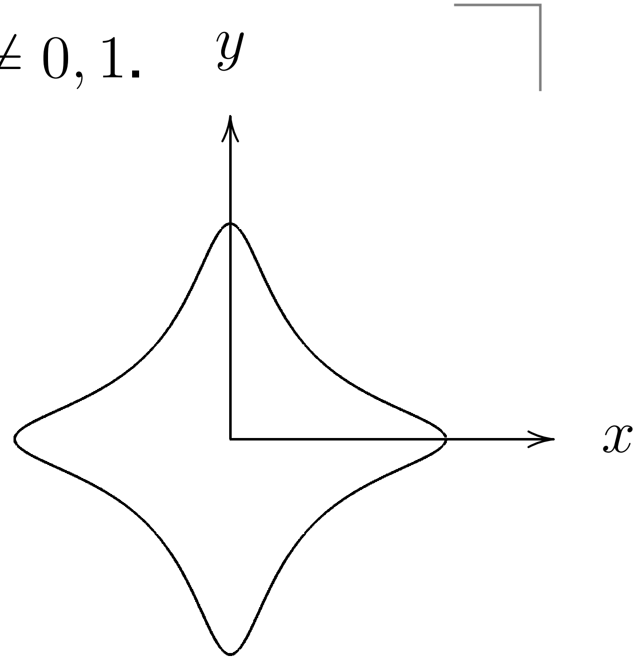
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

How to add on an Edwards curve

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 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 $(0, 1)$.

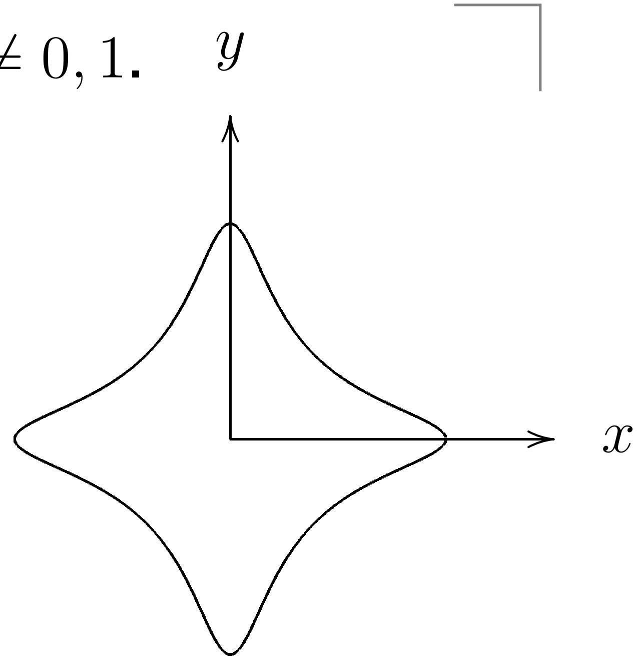
How to add on an Edwards curve

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



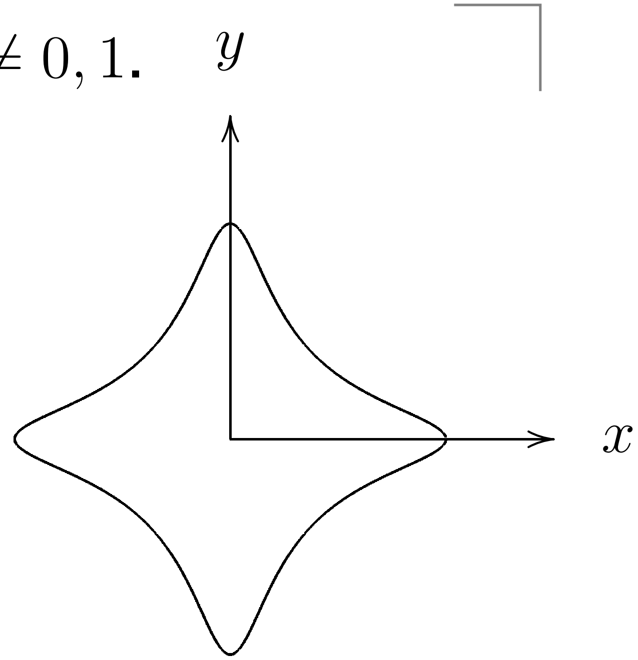
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) =$

How to add on an Edwards curve

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

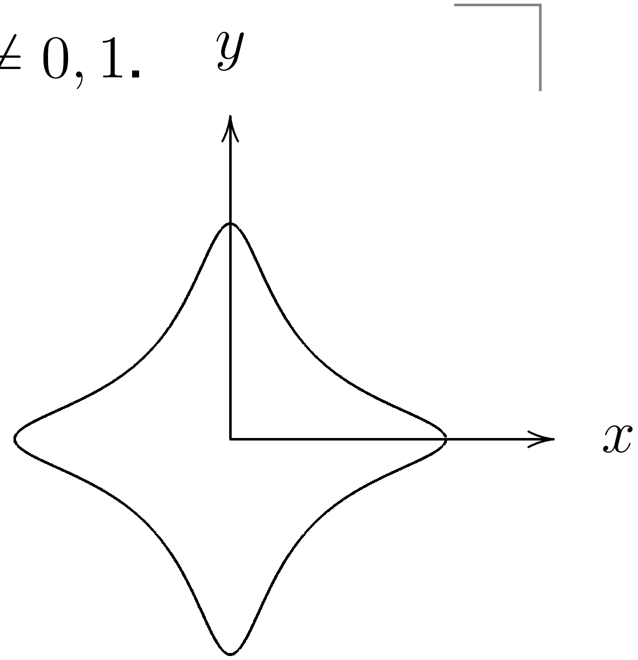
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.

How to add on an Edwards curve

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 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.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

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.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}\right)$.
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1}\right)$.

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.
- $$P + Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right).$$
- $$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right).$$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

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.
- $P + Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

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.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

Complete addition law

- If d is not a square in k, then there are no points at infinity on the blow-up of the curve.
- If d is not a square, the only exceptional points of the birational equivalence are P_∞ corresponding to $(0, 1)$ and $(0, 0)$ corresponding to $(0, -1)$.
- If d is not a square the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.

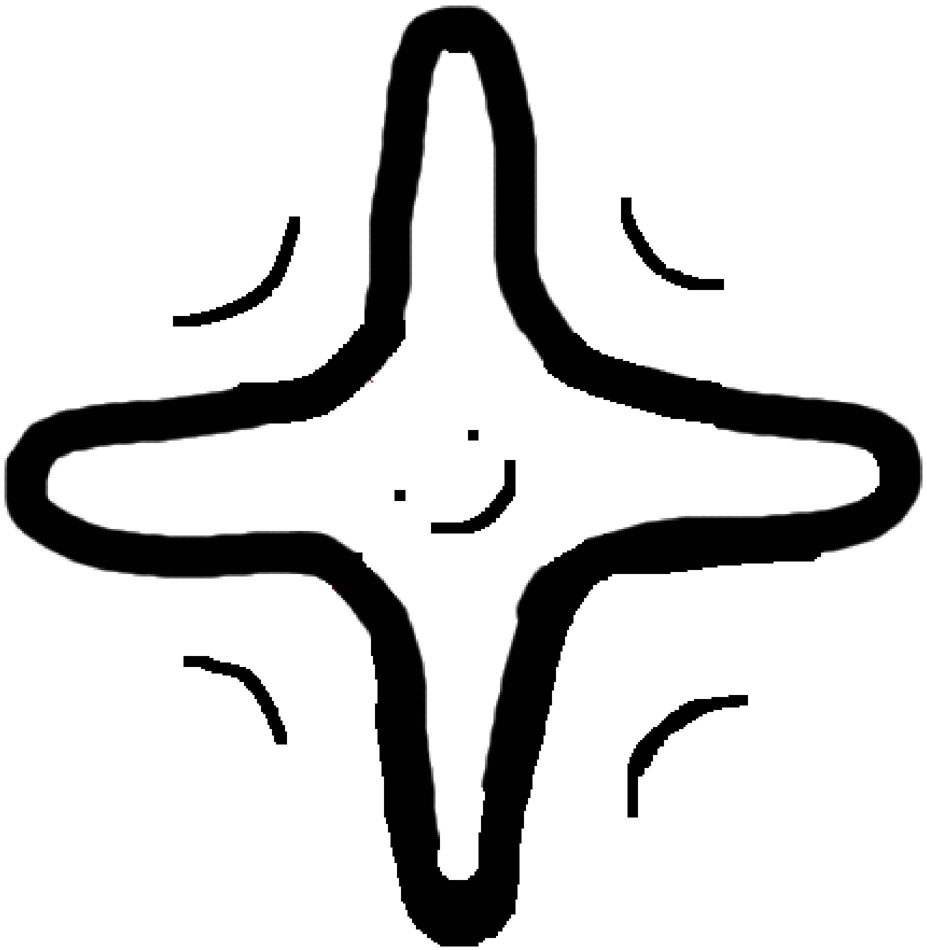
Fast addition law

- Very fast point addition 10M + 1S + 1D. (Even faster with Inverted Edwards coordinates.)
- 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`

  for the Explicit-Formulas Database.

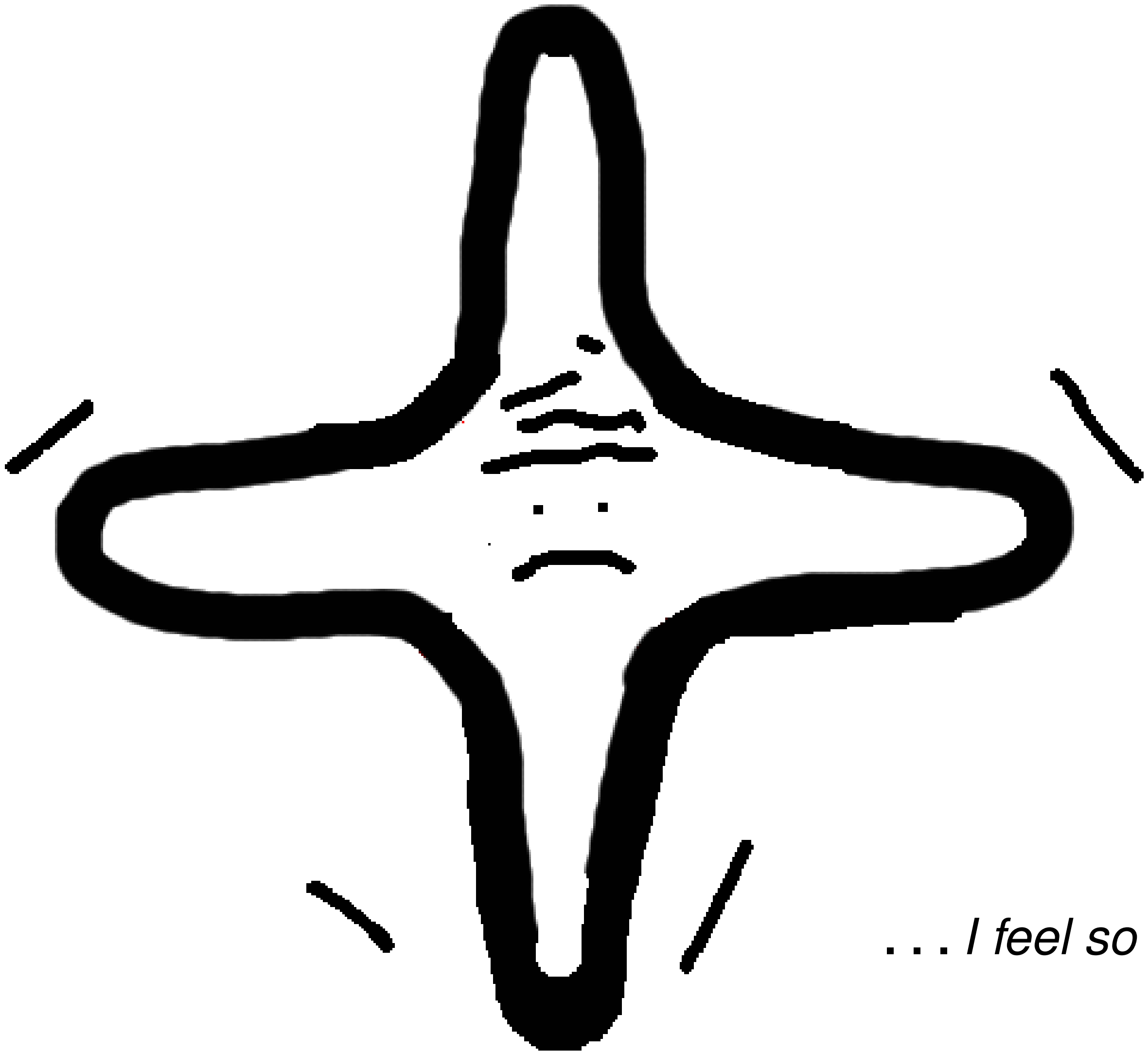
Edwards Curves – a new star(fish) is born



lecture circuit:

Hoboken
Turku
Warsaw
Fort Meade, Maryland
Melbourne
Ottawa (SAC)
Dublin (ECC)
Bordeaux
Bristol
Magdeburg
Seoul
Malaysia (Asiacrypt)
Madras
Bangalore (AAECC)
⋮
Madrid

One year passes . . .



. . . I feel so odd . . .

Exceptions, $2 \neq 0$ ...

Fix a field k of characteristic different from 2. Fix $c, d \in k$ such that $c \neq 0$, $d \neq 0$, and $dc^4 \neq 1$. Consider the *Edwards addition law*

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1 y_2 + y_1 x_2}{c(1 + d x_1 x_2 y_1 y_2)}, \frac{y_1 y_2 - x_1 x_2}{c(1 - d x_1 x_2 y_1 y_2)} \right)$$

$x^2 + y^2 = a^2(1 + x^2 y^2), a^5 \neq a$
describes an elliptic curve over
field k of odd characteristic.

Theorem 2.1. *Let k be a field in which $2 \neq 0$. Let E be an elliptic curve over k such that the group $E(k)$ has an element of order 4. Then*

How can there be an incomplete set of complete curves???

How to design a worthy binary partner?

Our wish-list early February 2008:

A binary Edwards curve should

- be elliptic.
- look like an Edwards curve.
- have a complete addition law.
- cover most (all?) ordinary binary elliptic curves.
- have an easy to compute negation.
- have efficient doublings.
- have efficient additions.

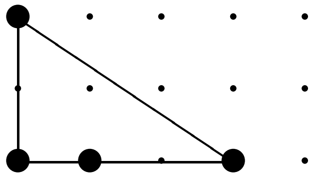
How to design a worthy binary partner?

Our wish-list early February 2008:

A binary Edwards curve should

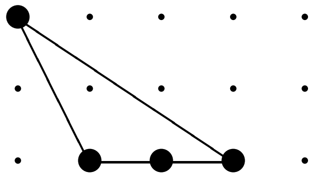
- be elliptic.
- look like an Edwards curve.
- have a complete addition law.
- cover most (all?) ordinary binary elliptic curves.
- have an easy to compute negation.
- have efficient doublings.
- have efficient additions.
- be found before the CHES deadline, February 29th.

Newton Polygons, odd characteristic



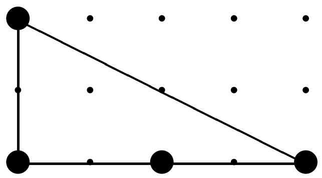
Short Weierstrass

$y^2 = x^3 + ax + b$



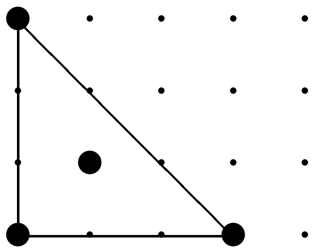
Montgomery

$by^2 = x^3 + ax^2 + x$



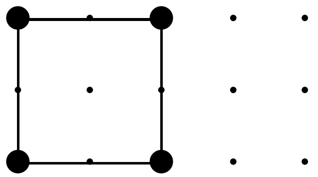
Jacobi quartic

$y^2 = x^4 + 2ax^2 + 1$



Hessian

$x^3 + y^3 + 1 = 3dxyz$



Edwards

$x^2 + y^2 = 1 + dx^2y^2$

The design choices

- Want x-degree ≤ 2, y-degree ≤ 2, i.e.

$$F(x, y) = \sum_{i=0}^{2} \sum_{j=0}^{2} a_{ij} x^i y^j .$$

- Want symmetric formulas, i.e. $a_{ij} = a_{ji}$.
- Want elliptic, i.e. $(1, 1)$ needs to be an interior point. This means $a_{22} \neq 0$ or $a_{12} = a_{21} \neq 0$.
- If $a_{22} = 0$ and $a_{12} = a_{21} \neq 0$ then there are three non-singular points at infinity $\Rightarrow$ addition law cannot be complete (for sufficiently large fields).
- Thus largest degree term $x^2 y^2$ (scale by a_{22}).

Binary Edwards curves?

$$a_{00} + a_{10}(x + y) + a_{11}xy + a_{20}(x^2 + y^2) + a_{21}xy(x + y) + x^2y^2$$

- Study projective equation
  $a_{00}Z^4 + a_{10}(X + Y)Z^3 + a_{11}XYZ^2 + a_{20}(X^2 + Y^2)Z^2 + a_{21}XY(X + Y)Z + X^2Y^2 = 0$
  to find points at infinity ($Z = 0$):
  $0 + X^2Y^2 = 0 \Rightarrow (1 : 0 : 0)$ and $(0 : 1 : 0)$.
- When are these points singular? (Then make sure that blow-up needs field extension.) Study $(1 : 0 : 0)$:

$$G(y, z) = a_{00}z^4+a_{10}(1+y)z^3+a_{11}yz^2+a_{20}(1+y^2)z^2+a_{21}y(1+y)z+y^2$$
$$G_y(y, z) = a_{10}z^3 + a_{11}z^2 + a_{21}z$$
$$G_z(y, z) = a_{10}(1 + y)z^2 + a_{21}y(1 + y)$$

Both derivatives vanish at $(0, 0)$, point is singular.

Blow-up

$a_{00}z^4 + a_{10}(1+y)z^3 + a_{11}yz^2 + a_{20}(1+y^2)z^2 + a_{21}y(1+y)z + y^2$
Use $y = uz$ to obtain
$a_{00}z^4 + a_{10}(1+uz)z^3 + a_{11}uz^3 + a_{20}(1+u^2z^2)z^2 + a_{21}u(1+uz)z^2 + u^2z^2$
and divide by z^2 to obtain

$$H(u,z) = a_{00}z^2 + a_{10}(1+uz)z + a_{11}uz + a_{20}(1+u^2z^2) + a_{21}u(1+uz) + u^2.$$

Points with $z = 0$ on blow-up:
$H(u,0) = a_{20} + a_{21}u + u^2$
Point is defined over k if $u^2 + a_{21}u + a_{20}$ is reducible.

Want that blow-up is defined only over quadratic extension, so in particular $a_{20}, a_{21} \neq 0$.
Then $H_u(u,z) = a_{10}z^2 + a_{11}z + a_{21}$ is nonzero in $z = 0$, so blow-up is non-singular.
Scale curve by $x \to a_{21}x, y \to a_{21}y$ to get $a_{21} = 1$.

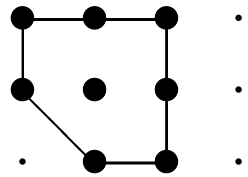
Some choices

$F(x, y) = a_{00} + a_{10}(x + y) + a_{11}xy + a_{20}(x^2 + y^2) + xy(x + y) + x^2y^2$
$F_x(x, y) = a_{10} + a_{11}y + y^2$
$F_y(x, y) = a_{10} + a_{11}x + x^2$
At most one of a_{10} and a_{00} can be 0.

Symmetry enforces that with (x, y) also (y, x) is on curve. Simplest possible negation: $-(x, y) = (y, x)$. There are other choices, several with surprisingly expensive negation.

We want an ordinary binary curve, i.e. one with a point of order 2. So there should be two points fixed under negation. Fixed points are (α, α) and $(\alpha + \sqrt{a_{11}}, \alpha + \sqrt{a_{11}})$, where $\alpha, \alpha + \sqrt{a_{11}}$ are the solutions of $a_{00} + a_{11}x^2 + x^4$.
To have two different solutions request $a_{11} \neq 0$.
Most convenient choices are $a_{00} = 0, a_{11} = 1$, neutral element $(0, 0)$, point of order 2 is $(1, 1)$.

Binary Edwards curves



Let $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$ then

$$E_{\mathrm{B},d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2,$$

is a binary Edwards curve with parameters d_1, d_2.
Map $(x, y) \mapsto (u, v)$ defined by

$$u = d_1(d_1^2 + d_1 + d_2)(x+y)/(xy + d_1(x+y)),$$
$$v = d_1(d_1^2 + d_1 + d_2)(x/(xy + d_1(x+y)) + d_1 + 1)$$

is a birational equivalence from E_{B,d_1,d_2} to the elliptic curve

$$v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4(d_1^4 + d_1^2 + d_2^2),$$

an ordinary elliptic curve in Weierstrass form.

Properties of binary Edwards curves

$$E_{\mathrm{B},d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2$$

- $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ with

$$x_3 = \frac{d_1(x_1+x_2) + d_2(x_1+y_1)(x_2+y_2) + (x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1 + (x_1+x_1^2)(x_2+y_2)},$$

$$y_3 = \frac{d_1(y_1+y_2) + d_2(x_1+y_1)(x_2+y_2) + (y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1 + (y_1+y_1^2)(x_2+y_2)}.$$

  if denominators are nonzero.
- Neutral element is $(0,0)$.
- $(1,1)$ has order 2.
- $-(x,y) = (y,x)$.
- $(x_1,y_1) + (1,1) = (x_1+1, y_1+1)$.

Edwards curves over finite fields

- Addition law for curves with $\mathrm{Tr}(d_2) = 1$ is complete.
- Denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero:
  If $x_2 + y_2 = 0$ then the denominators are $d_1 \neq 0$.
  Otherwise $d_1/(x_2 + y_2) = x_1 + x_1^2$ and

$$\frac{d_1}{x_2 + y_2} = \frac{d_1(x_2 + y_2)}{x_2^2 + y_2^2} = \frac{d_2(x_2^2 + y_2^2) + x_2 y_2 + x_2 y_2 (x_2 + y_2) + x_2^2 y_2^2}{x_2^2 + y_2^2}$$
$$= d_2 + \frac{x_2 y_2 + x_2 y_2 (x_2 + y_2) + y_2^2}{x_2^2 + y_2^2} + \frac{y_2^2 + x_2^2 y_2^2}{x_2^2 + y_2^2}$$
$$= d_2 + \frac{y_2 + x_2 y_2}{x_2 + y_2} + \frac{y_2^2 + x_2^2 y_2^2}{x_2^2 + y_2^2}$$

So $\mathrm{Tr}(d_2) = \mathrm{Tr}(x_1 + x_1^2) = 0$, contradiction.

Generality & doubling

- Every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve if $n \geq 3$. Proof uses counting argument and Hasse bound.
- Nice doubling formulas (use curve equation to simplify)

$$x_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)},$$

$$y_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)}$$

- In projective coordinates:
2M+ 6S+3D, where the 3D are multiplications by d_1, d_2/d_1, and d_2.

Operation counts

These curves are the first binary curves to offer complete addition laws. They are also surprisingly fast:

- ADD on binary Edwards curves takes 21M+1S+4D, mADD takes 13M+3S+3D.
- Latest results (today, 4 a.m.) ADD in 18M+2S+7D.
- Differential addition ($P+Q$ given P, Q, and $Q-P$) takes 8M+1S+2D; mixed version takes 6M+1S+2D.
- Differential addition+doubling (typical step in Montgomery ladder) takes 8M+4S+2D; mixed version takes 6M+4S+2D.

See our preprint (ePrint 2008/171) or

`cr.yp.to/papers.html#edwards2`

for full details, speedups for $d_1 = d_2$, how to choose small coefficients, affine formulas, . . .

Comparison with other doubling formulas

Assume curves are chosen with small coefficients.

System	Cost of doubling
Projective	7M+4S; see HEHCC
Jacobian	4M+5S; see HEHCC
Lopez-Dahab	3M+5S; Lopez-Dahab
Edwards	2M+6S; new, complete
Lopez-Dahab $a_2 = 1$	2M+5S; Kim-Kim

Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

for characteristic 2 is in preparation; our paper already has some speed-ups for Lopez-Dahab coordinates.

Happy End!