Shapes of Elliptic Curves

Daniel J. Bernstein
University of Illinois at Chicago
djb@cr.yp.to

Tanja Lange
Technische Universiteit Eindhoven
tanja@hyperelliptic.org

19.05.2008
Weierstrass curve

\[ y^2 = x^3 - 0.4x + 0.7 \]
Weierstrass curve

\[ y^2 = x^3 - 0.4x + 0.7 \]

The Weierstrass-turtle: old, trusted and slow. Warning: (picture) incomplete!
Jacobi quartic

\[ x^2 = y^4 - 1.9y^2 + 1 \]
Jacobi quartic

\[ x^2 = y^4 - 1.9y^2 + 1 \]

The Jacobi-quartic squid: can be extended to XXYZZR giant squid.
Hessian curve

\[ x^3 - y^3 + 1 = 0.3xy \]
Hessian curve

\[ x^3 - y^3 + 1 = 0.3xy \]

The Hessian-ray: uniform

but not strongly so
Edwards curve

\[ x^2 + y^2 = 1 - 300x^2y^2 \]
Edwards curve

\[ x^2 + y^2 = 1 - 300x^2y^2 \]

The Edwards starfish new, fast and complete!
The race – zoom on Weierstrass and Edwards
Weierstrass vs. Edwards I

Start!

D. J. Bernstein & T. Lange

cr.yp.to/papers.html – p.12
Weierstrass vs. Edwards II

Start!

1985

Weierstrass sets off, Edwards left behind sleeping

D. J. Bernstein & T. Lange

cr.yp.to/papers.html – p. 13
Weierstrass vs. Edwards III

1985

Weierstrass sets off, Edwards left behind sleeping

2007-Jan

Weierstrass has made some progress - finally Edwards wakes up.

D. J. Bernstein & T. Lange

cr.yp.to/papers.html - p. 14
Weierstrass vs. Edwards IV

2007-Jan

Weierstrass has made some progress — finally Edwards wakes up.

Feb

Exciting progress: Edwards about to overtake!!

D. J. Bernstein & T. Lange

cr.yp.to/papers.html – p. 15
Weierstrass vs. Edwards V

Feb

Exciting progress: Edwards about to overtake!!

Mar

And the winner is Edwards!

D. J. Bernstein & T. Lange

cr.yp.to/papers.html – p. 16
all competitors ...
All competitors I
All competitors II
All competitors III

1985

2007-Jan

D. J. Bernstein & T. Lange
cr.yp.to/papers.html – p. 20
All competitors IV
All competitors V

Feb

Mar

D. J. Bernstein & T. Lange

cr yp.to/papers.html – p. 22
Read the full story at:
hyperelliptic.org/EFD
One year passes . . .

. . . I feel so odd . . .

D. J. Bernstein & T. Lange

cr.yp.to/papers.html – p. 24
Exceptions, $2 \neq 0 \ldots$

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

$$(x_1, y_1), (x_2, y_2) \mapsto \left( \frac{x_1 y_2 + y_1 x_2}{c(1 + dx_1 x_2 y_1 y_2)}, \frac{y_1 y_2 - x_1 x_2}{c(1 - dx_1 x_2 y_1 y_2)} \right)$$

$x^2 + y^2 = a^2(1 + x^2 y^2)$, $a^5 \neq a$
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???
After extensive (finite) field studies . . .

(joint work with Reza Rezaeian Farashahi)

Assume $d_1, d_2 \in \mathbb{F}_{2^n}$, $d_1 \neq 0$, $\text{Tr}(d_2) = 1$. Then

$$d_1(x + y) + d_2(x + y)^2 = xy + xy(x + y) + x^2y^2$$

describes an elliptic curve.

(Curve shape is symmetric and has highest term $x^2y^2$ like 'classic' Edwards curves $x^2 + y^2 = 1 + dx^2y^2$.)

Neutral element is $(0, 0)$. Negative of $(x, y)$ is $(y, x)$.

The addition law on this curve is complete! It works for adding arbitrary points – doubling, adding negatives, adding the neutral element, . . .

Every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve.

D. J. Bernstein & T. Lange

[cr.yp.to/papers.html – p. 26]
Timeline (after some early aborts)

- February 13th, 2008: Binary Edwards curves born
- February 15th, 2008: Binary Edwards takes first steps
- February 15th, 2008: Binary Edwards curves are complete (!) for \(d_2 = 1\) and \(n\) odd.
- February 16th, 2008: Binary Edwards plays with \(d_1, d_2\)
- February 20th, 2008: Binary Edwards adds differentially
- February 29th, 2008: Binary Edwards reaches all ordinary curves
- March 31st, 2008: Intel announces support for binary Edwards curves (PCMULQDQ in Westmere)
- April 16th, 2008: Sun announces support for binary Edwards curves in Rock.
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 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.

<table>
<thead>
<tr>
<th>System</th>
<th>Cost of doubling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projective</td>
<td>7M+4S; see HEHCC</td>
</tr>
<tr>
<td>Jacobian</td>
<td>4M+5S; see HEHCC</td>
</tr>
<tr>
<td>Lopez-Dahab</td>
<td>3M+5S; Lopez-Dahab</td>
</tr>
<tr>
<td>Edwards</td>
<td>2M+6S; new, complete</td>
</tr>
<tr>
<td>Lopez-Dahab $a_2 = 1$</td>
<td>2M+5S; Kim-Kim</td>
</tr>
</tbody>
</table>

Explicit-Formulas Database

[www.hyperelliptic.org/EFD](http://www.hyperelliptic.org/EFD)

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