Edwards Coordinates for Elliptic Curves, part 1

Tanja Lange

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

joint work with Daniel J. Bernstein

10.11.2007

Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.

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

Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.

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

is a commutative group with
$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$, where

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

- Polar coordinates and trigonometric identities readily show that the result is on the curve.
- Associativity of the addition boils down to associativity of addition of angles.
- Look, an addition law!
- But it’s not elliptic; index calculus work efficiently.

Now add on an elliptic curve

An elliptic curve:

Now add on an elliptic curve

An elliptic curve:

$$x^2 + y^2 = a^2(1 + x^2y^2)$$

Now add on an elliptic curve

$$x^2 + y^2 = a^2(1 + x^2y^2)$$

elliptic?

use $z = y(1 - a^2x^2)/a$ to obtain

$$z^2 = x^4 - (a^2 + 1/a^2)x^2 + 1.$$

Now add on an elliptic curve

Let k be a field with $2 \neq 0$ and let $a \in k$ with $a^5 \neq a$.
There is an – almost everywhere defined – operation on the set

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

as

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

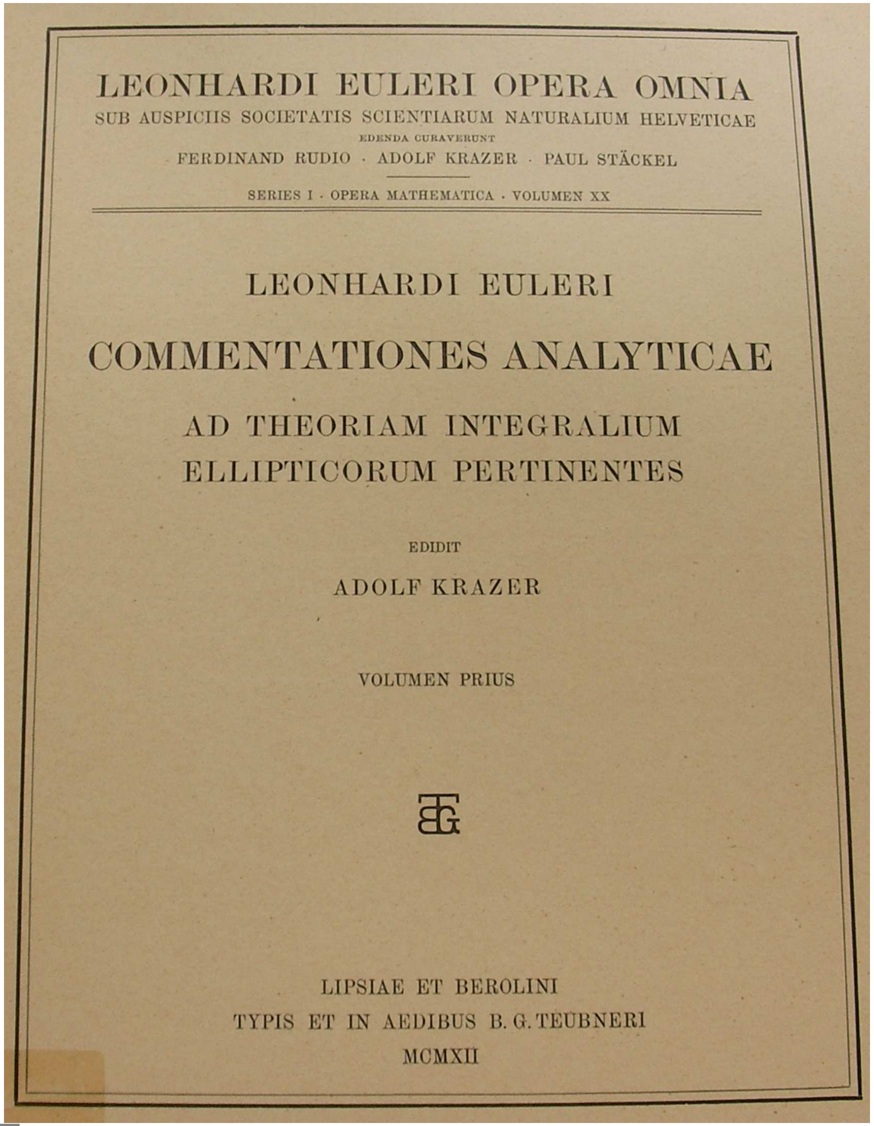
defined by the Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Numerators like in addition on circle!

Where do these curves come from?

Long, long ago . . .


LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
FERDINAND RUDIO · ADOLF KRAZER · PAUL STÄCKEL

SERIES I · OPERA MATHEMATICA · VOLUMEN XX

LEONHARDI EULERI

COMMENTATIONES ANALYTICAE

AD THEORIAM INTEGRALIUM
ELLIPTICORUM PERTINENTES

EDIDIT

ADOLF KRAZER

VOLUMEN PRIUS

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXII

Euler 1761

“ Observationes de Comparatione Arcuum Curvarum Irrectificabilium”

I. DE ELLIPSI

1. Sit quadrans ellipticus ABC (Fig. 1), cuius centrum in C, eiusque semiaxes ponantur $CA=1$ et $CB=c$; sumta ergo abscissa quacunque $CP=x$ erit applicata ei respondens $PM=y=c\sqrt{(1-xx)}$; cuius differentiale cum sit $dy=-\frac{cxdx}{\sqrt{(1-xx)}}$, erit abscissae $CP=x$ arcus ellipticus respondens

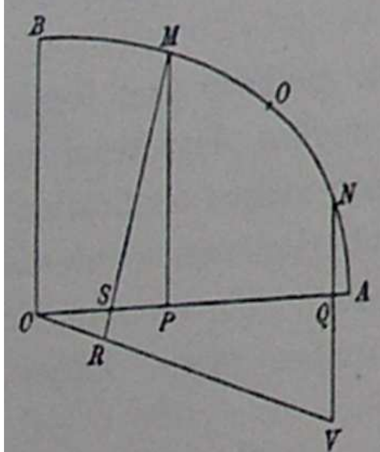


Fig. 1.

$$BM=\int\frac{dx\sqrt{(1-(1-cc)xx)}}{\sqrt{(1-xx)}}.$$

Ponatur brevitatis gratia $1-cc=n$, ut sit arcus

$$BM=\int dx\sqrt{\frac{1-nxx}{1-xx}},$$

$$\frac{1}{y^2}=\frac{1-nx^2}{1-x^2}\Leftrightarrow x^2+y^2=1+nx^2y^2.$$

Euler 1761

COROLLARIUM 3

43. Inventio ergo cordarum arcuum quorumvis multiplorum una cum cordis complementi ita se habebit:

Corda arcus	Corda complementi
simpli $= a$	simpli $= A$
dupli $= b = \dfrac{2aA}{1-aaAA}$	dupli $= \dfrac{AA-aa}{1+aaAA} = B$
tripli $= c = \dfrac{aB+bA}{1-abAB}$	tripli $= \dfrac{AB-ab}{1+abAB} = C$
quadrupli $= d = \dfrac{aC+cA}{1-acAC}$	quadrupli $= \dfrac{AC-ac}{1+acAC} = D$
quintupli $= e = \dfrac{aD+dA}{1-adAD}$	quintupli $= \dfrac{AD-ad}{1+adAD} = E$
etc.	etc.

Euler gives doubling and (special) addition for (a, A) on $a^2 + A^2 = 1 - a^2A^2$.

Gauss, posthumously

ELEGANTIORES INTEGRALIS $\int \frac{dx}{\sqrt{(1-x^4)}}$ PROPRIETATES.

[2.]

$$1 = ss + cc + sscc \quad \text{sive} \quad 2 = (1+ss)(1+cc) = (\tfrac{1}{ss}-1)(\tfrac{1}{cc} -$$

$$s = \sqrt{\frac{1-cc}{1+cc}}, \qquad c = \sqrt{\frac{1-ss}{1+ss}}$$

$$\sin\text{lemn}(a \pm b) = \frac{sc' \pm s'c}{1 \mp scs'c'}$$

$$\cos\text{lemn}(a \pm b) = \frac{cc' \mp ss'}{1 \pm ss'cc'}$$

$$\sin\text{lemn}(-a) = -\sin\text{lemn}\, a, \qquad \cos\text{lemn}(-a) = \cos\text{lemn}\, a$$

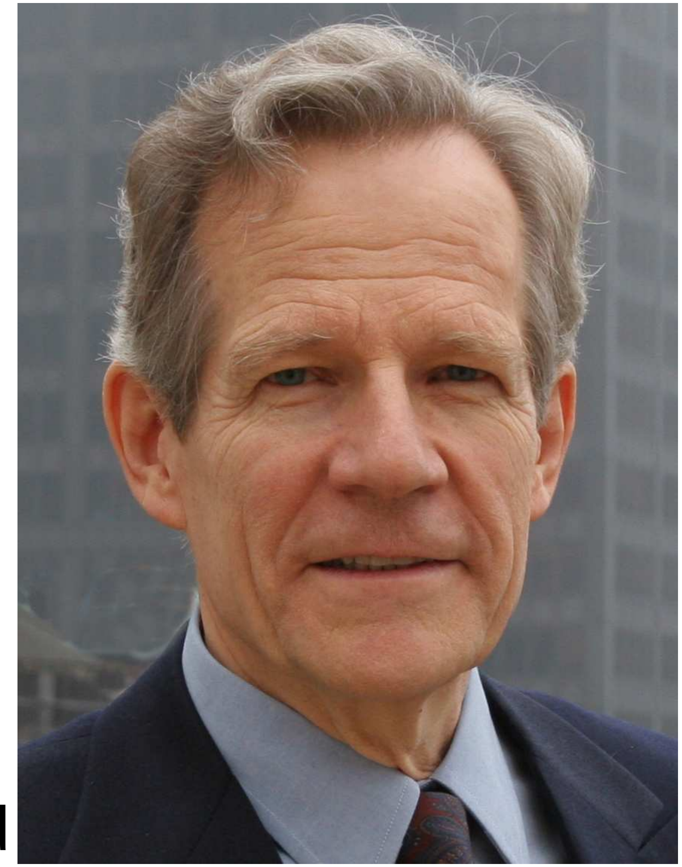
$$\sin\text{lemn}\, k\varpi = 0 \qquad \sin\text{lemn}(k+\tfrac{1}{2})\varpi = \pm 1$$

$$\cos\text{lemn}\, k\varpi = \pm 1 \qquad \cos\text{lemn}(k+\tfrac{1}{2})\varpi = 0$$

Gauss gives general addition for arbitrary points on

$$1 = s^2 + c^2 + s^2c^2.$$

Ex uno plura



- Harold M. Edwards, Bulletin of the AMS, **44**, 393–422, 2007
  $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
  describes an elliptic curve.
- Every elliptic curve can be written in this form – over some extension field.
- Ur-elliptic curve
  $$x^2 + y^2 = 1 - x^2y^2$$
  needs $\sqrt{-1} \in k$ transform.
- Edwards gives above-mentioned addition law for this generalized form, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization . . .

Edwards curves over finite fields

- We do not necessarily have $\sqrt{-1} \in k$! The example curve $x^2 + y^2 = 1 - x^2y^2$ from Euler and Gauss is not always an Edwards curve.
- Solution: change the definition of Edwards curves.
- Introduce further parameter d to cover more curves

$$x^2 + y^2 = c^2(1 + dx^2y^2), \; c, d \neq 0, dc^4 \neq 1.$$

- At least one of c, d small: if $c^4 d = \bar{c}^4 \bar{d}$ then $x^2 + y^2 = c^2(1 + dx^2y^2)$ and $x^2 + y^2 = \bar{c}^2(1 + \bar{d}x^2y^2)$ isomorphic.
  We can always choose $c = 1$ (and do so in the sequel).
- $\bar{c}^4\bar{d} = (c^4 d)^{-1}$ gives quadratic twist (might be isomorphic).

Addition on Edwards curves

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

- Neutral element is

Addition on Edwards curves

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

- Neutral element is $(0, 1)$, this is an affine point!

Addition on Edwards curves

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

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) =$

Addition on Edwards curves

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

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) = (-x_1, y_1)$.

Addition on Edwards curves

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

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2, $(\pm 1, 0)$ have order 4, so not every elliptic curve can be transformed to an Edwards curve over k — but every curve with a point of order 4 can!
- Our Asiacrypt 2007 paper makes explicit the birational equivalence between a curve in Edwards form and in Weierstrass form.
  See also our `newelliptic` page.

Nice features of the addition law

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

Nice features of the addition law

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

Nice features of the addition law

- $$P \oplus Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$
- $$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$$
- Addition law also works for doubling (compare that to curves in Weierstrass form!)
- Can show: denominator never 0 for non-square d.

Nice features of the addition law

- $P \oplus Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- Addition law also works for doubling (compare that to curves in Weierstrass form!)
- Can show: denominator never 0 for non-square d.

Explicit formulas for addition/doubling:

$$\begin{aligned} A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\ E &= (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D;\ F = d \cdot C \cdot D; \\ X_{P \oplus Q} &= A \cdot E \cdot (B - F);\ Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F); \\ Z_{P \oplus Q} &= (B - F) \cdot (B + F). \end{aligned}$$

Nice features of the addition law

- $P \oplus Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- Addition law also works for doubling (compare that to curves in Weierstrass form!)
- Can show: denominator never 0 for non-square d.

Explicit formulas for addition/doubling:

$$\begin{aligned} A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\ E &= (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D;\ F = d \cdot C \cdot D; \\ X_{P \oplus Q} &= A \cdot E \cdot (B - F);\ Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F); \\ Z_{P \oplus Q} &= (B - F) \cdot (B + F). \end{aligned}$$

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

Strongly unified group operations

- Addition formulas work also for doubling.
- Addition in Weierstrass form $y^2 = x^3 + a_4x + a_6$, involves computation

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\ (3x_1^2 + a_4)/(2y_1) & \text{else.} \end{cases}$$

  division by zero if first form is accidentally used for doubling.
- Strongly unified addition laws remove some checks from the code.
- Help against simple side-channel attacks. Attacker sees uniform sequence of identical group operations, no information on secret scalar given (assuming the field operations are handled appropriately).

Unified Projective coordinates

- Brier, Joye 2002
  Idea: unify how the slope is computed.
- improved in Brier, Déchène, and Joye 2004
- $$\lambda = \frac{(x_1+x_2)^2 - x_1x_2 + a_4 + y_1 - y_2}{y_1 + y_2 + x_1 - x_2}$$
  $$= \begin{cases} \frac{y_1-y_2}{x_1-x_2} & (x_1,y_1) \neq \pm(x_2,y_2) \\ \frac{3x_1^2+a_4}{2y_1} & (x_1,y_1) = (x_2,y_2) \end{cases}$$

  Multiply numerator & denominator by $x_1 - x_2$ to see this.
- Proposed formulae can be generalized to projective coordinates.
- Some special cases may occur, but with very low probability, e. g. $x_2 = y_1 + y_2 + x_1$. Alternative equation for this case.

Jacobi intersections

- Chudnovsky and Chudnovsky 1986; Liardet and Smart CHES 2001
- Elliptic curve given as intersection of two quadratics

$$s^2 + c^2 = 1 \text{ and } as^2 + d^2 = 1.$$

- Points $(S : C : D : Z)$ with $(s, c, d) = (S/Z, C/Z, D/Z)$.
- Neutral element is $(0, 1, 1)$.

$$\begin{aligned}
S_3 &= (Z_1C_2 + D_1S_2)(C_1Z_2 + S_1D_2) - Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\
C_3 &= Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\
D_3 &= Z_1D_1Z_2D_2 - aS_1C_1S_2C_2 \\
Z_3 &= Z_1C_2^2 + D_1S_2^2.
\end{aligned}$$

- Unified formulas need 13M + 2S + 1D.

Jacobi quartics

- Billet and Joye AAECC 2003

$$E_J : Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4.$$

$$\begin{aligned} X_3 &= X_1 Z_1 Y_2 + Y_1 X_2 Z_2 \\ Z_3 &= (Z_1 Z_2)^2 - \epsilon (X_1 X_2)^2 \\ Y_3 &= (Z_3 + 2\epsilon (X_1 X_2)^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) + \\ & \quad 2\epsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + Z_1^2 X_2^2). \end{aligned}$$

- Unified formulas need 10M+3S+D+2E
- Can have ϵ or δ small
- Needs point of order 2; for $\epsilon = 1$ the group order is divisible by 4.
- Some recent speed ups due to Duquesne and to Hisil, Carter, and Dawson.

Hessian curves

$$E_H : X^3 + Y^3 + Z^3 = cXYZ.$$

Addition: $P \neq \pm Q$

$$X_3 = X_2 Y_1^2 Z_2 - X_1 Y_2^2 Z_1$$
$$Y_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1$$
$$Z_3 = X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2$$

Doubling $P = Q \neq -P$

$$X_3 = Y_1(X_1^3 - Z_1^3)$$
$$Y_3 = X_1(Z_1^3 - Y_1^3)$$
$$Z_3 = Z_1(Y_1^3 - X_1^3)$$

- Curves were first suggested for speed
- Joye and Quisquater show

$$[2](X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) \oplus (Y_1 : Z_1 : X_1)$$

- Unified formulas need 12M.
- Doubling is done by an addition, but not automatically – only unified, not strongly unified.

Unified addition law

- Unified formulas introduced as countermeasure against side-channel attacks – but useful in general.
- Strongly unified addition laws indeed remove the check for $P \neq Q$ before addition.
- Some systems allow to omit the check $P \neq -Q$ before addition.
- Most systems still have exceptional cases.
- No surprise:
  "The smallest cardinality of a complete system of addition laws on E equals two."
  (Theorem 1 in Wieb Bosma, Hendrik W. Lenstra, Jr., J. Number Theory **53**, 229–240, 1995)
- Bosma/Lenstra give such system; similar to unified projective coordinates.

Complete addition law

- If d is not a square then Edwards addition law is complete: For $x_i^2 + y_i^2 = 1 + dx_i^2 y_i^2,\ i = 1, 2,$ always $dx_1x_2y_1y_2 \neq \pm 1$. Outline of proof:
  If $(dx_1x_2y_1y_2)^2 = 1$ then $(x_1 + dx_1x_2y_1y_2y_1)^2 = dx_1^2y_1^2(x_2 + y_2)^2$. Conclude that d is a square. But $d \neq \square$.
- 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.
- Bosma/Lenstra strikes over quadratic extension.
  “Pointless exceptional divisor!”

Fastest unified addition-or-doubling formula

System	Cost of unified addition-or-doubling
Projective	11M+6S+1D; see Brier/Joye ’03
Projective if $a_4 = -1$	13M+3S; see Brier/Joye ’02
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Jacobi quartic ($\epsilon = 1$)	10M+3S+1D; see Billet/Joye ’01
Hessian	12M; see Joye/Quisquater ’01
Edwards	10M+1S+1D

- Exactly the same formulae for doubling (no re-arrangement like in Hessian; no if-else)
- No exceptional cases if d is not a square.
- Operation counts as in Asiacrypt’07 paper.
- See EFD `hyperelliptic.org/EFD`.

What if we know that we double?

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

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

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right)$$

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

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

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

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

$$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

How about non-unified doubling?

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

$$= \left(\frac{2 x_1 y_1}{1 + d(x_1 y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1 y_1)^2} \right)$$

$$= \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right)$$

$$\begin{aligned} B &= (X_1 + Y_1)^2;\ C = X_1^2;\ D = Y_1^2;\ E = C + D;\ H = (c \cdot Z_1)^2; \\ J &= E - 2H;\ X_3 = c \cdot (B - E) \cdot J;\ Y_3 = c \cdot E \cdot (C - D);\ Z_3 = E \cdot J \end{aligned}$$

Inversion-free version needs 3M + 4S + 6A.

Very fast doubling formulae

System	Cost of doubling
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	7M+1S; see Hisil/Carter/Dawson '07
Doche/Icart/Kohel-3	2M+7S+2D; see Doche/Icart/Kohel '06
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi quartic	2M+6S+2D; see Hisil/Carter/Dawson '07
Jacobi intersection	3M+4S; see Liardet/Smart '01
Edwards	3M+4S;
Doche/Icart/Kohel-2	2M+5S+2D; see Doche/Icart/Kohel '06

- Edwards fastest for general curves, no D.
- Operation counts as in our Asiacrypt paper.

Fastest addition formulae

System	Cost of addition
Doche/Icart/Kohel-2	12M+5S+1D; see Doche/Icart/Kohel ’06
Doche/Icart/Kohel-3	11M+6S+1D; see Doche/Icart/Kohel ’06
Jacobian	11M+5S; EFD
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Projective	12M+2S; HECC
Jacobi quartic	10M+3S+1D; see Billet/Joye ’03
Hessian	12M; see Joye/Quisquater ’01
Edwards	10M+1S+1D

- EFD and full paper also contain costs for mixed addition (mADD) and re-additions (reADD).
- reADD: non-mixed ADD where one point has been added before and computations have been cached.

Single-scalar multiplication using NAF

System	1 DBL, 1/3 mADD
Projective	8M+6.67S+1D
Projective if $a_4 = -3$	10M+3.67S
Hessian	10.3M+1S
Doche/Icart/Kohel-3	4.33M+8.33S+2.33D
Jacobian	3.33M+9.33S+1D
Jacobian if $a_4 = -3$	5.33M+6.33S
Jacobi intersection	6.67M+4.67S+0.333D
Jacobi quartic	4.67M+7S+2.33D
Doche/Icart/Kohel-2	4.67M+6.33S+2.33D
Edwards	6M+4.33S+0.333D

For comparison: Montgomery arithmetic takes 5M+4S+1D per bit.

Signed width-4 sliding windows

These counts include the precomputations.

System	0.98 DBL, 0.17 reADD, 0.025 mADD, 0.0035 A
Projective	7.17M+6.28S+0.982D
Projective if $a_4 = -3$	9.13M+3.34S
Doche/Icart/Kohel-3	3.84M+7.99S+2.16D
Hessian	9.16M+0.982S
Jacobian	2.85M+8.64S+0.982D
Jacobian if $a_4 = -3$	4.82M+5.69S
Doche/Icart/Kohel-2	4.2M+5.86S+2.16D
Jacobi quartic	3.69M+6.48S+2.16D
Jacobi intersection	5.09M+4.32S+0.194D
Edwards	4.86M+4.12S+0.194D

Montgomery takes 5M+4S+1D per bit. Edwards solidly faster!

Inverted Edwards coordinates

- Latest news (Bernstein/Lange, to appear at AAECC 2007):
  inverted Edwards coordinates are even faster strongly unified system – but not complete.
- Using the representation $(X_1 : Y_1 : Z_1)$ for the affine point $(Z_1/X_1, Z_1/Y_1)$ ($X_1 Y_1 Z_1 \neq 0$) gives operation counts:
  - Doubling takes $3M + 4S + 1D$.
  - Addition takes $9M + 1S + 1D$.
- This saves $1M$ for each addition compared to standard Edwards coordinates.
- New speed leader: inverted Edwards coordinates.

Different coordinate systems

For coordinate systems we could find, the group law, operation counts (and improvements) for the explicit formulas, MAGMA-based proofs (sorry, not SAGE) of their correctness, lots of entertainment visit the

Explicit Formulas Database

`http://www.hyperelliptic.org/EFD`

Non-zero denominators

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

What if denominators are 0?

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Intuitive explanation:
The points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ are singular. They correspond to four points on the desingularization of the curve; but those four points are defined over $k(\sqrt{d})$.

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2$

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \end{aligned}$$

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \\ &= 1 + d x_1^2 y_1^2 = x_1^2 + y_1^2 \end{aligned}$$

Non-zero denominators

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $dx_1^2y_1^2(x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$\begin{aligned}(x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2 \\ &= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2.\end{aligned}$$

Non-zero denominators

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

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$(x_1 + \epsilon y_1)^2 = x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2$$
$$= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2.$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1 y_1 (x_2 + y_2))^2 \Rightarrow d = \square$

$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1 y_1 (x_2 - y_2))^2 \Rightarrow d = \square$

If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.