Elliptic-curve cryptography IV

Edwards curves and twisted Edwards curves

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

The Edwards addition law over $\mathbf{R}$

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

is a group law for the curve $x^2 + y^2 = 1 + dx^2 y^2$ for $d < 0$.

- Addition result is on curve. Not shown here, yet, but easy by computer.
- Addition law is associative. Not shown here, yet, but easy by computer.
- $(0, 1)$ is neutral element.
- $(x_1, y_1) + (-x_1, y_1) = (0, 1)$, so $-(x_1, y_1) = (-x_1, y_1)$.
- Addition law is commutative.

The Edwards addition law over $\mathbf{R}$

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

is a group law for the curve $x^2 + y^2 = 1 + dx^2y^2$ for $d < 0$.

- Addition result is on curve. Not shown here, yet, but easy by computer.
- Addition law is associative. Not shown here, yet, but easy by computer.
- $(0, 1)$ is neutral element.
- $(x_1, y_1) + (-x_1, y_1) = (0, 1)$, so $-(x_1, y_1) = (-x_1, y_1)$.
- Addition law is commutative.

For crypto want curves over $\mathbf{F}_p$. But our proof used $x^2 + y^2 > 0$. This is meaningless modulo p.

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$dx_1^2y_1^2(x_2^2 + y_2^2) = dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2$$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 \end{aligned}$$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2. \end{aligned}$$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$dx_1^2y_1^2(x_2^2 + y_2^2) = dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2$$
$$= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2.$$

$$\Downarrow$$

$$(x_1 + y_1\epsilon)^2 = x_1^2 + y_1^2 + 2x_1y_1\epsilon \stackrel{\Downarrow}{=} dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2$$
$$= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2.$$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2. \end{aligned}$$

$$\Downarrow$$

$$\begin{aligned} (x_1 + y_1\epsilon)^2 = x_1^2 + y_1^2 + 2x_1y_1\epsilon &\stackrel{\Downarrow}{=} dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2. \end{aligned}$$

$$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1y_1(x_2 + y_2))^2 \Rightarrow d = \square$$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2. \end{aligned}$$

$$\begin{aligned} (x_1 + y_1\epsilon)^2 = x_1^2 + y_1^2 + 2x_1y_1\epsilon &\overset{\Downarrow}{=} dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2. \end{aligned}$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1y_1(x_2 + y_2))^2 \Rightarrow d = \square$
$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1y_1(x_2 - y_2))^2 \Rightarrow d = \square$

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2. \end{aligned}$$

$$\Downarrow$$

$$\begin{aligned} (x_1 + y_1\epsilon)^2 = x_1^2 + y_1^2 + 2x_1y_1\epsilon &\stackrel{\Downarrow}{=} dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2. \end{aligned}$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1y_1(x_2 + y_2))^2 \Rightarrow d = \square$
$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1y_1(x_2 - y_2))^2 \Rightarrow d = \square$
If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.

Need new proof for denominators $\neq 0$

Also need a replacement condition for $d < 0$, assume p odd

Reminder: Denominators are $1 \pm dx_1x_2y_1y_2$.
Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$.
Let $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{\pm 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$.

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 = 1 + dx_1^2y_1^2 = x_1^2 + y_1^2. \end{aligned}$$

$$\Downarrow$$

$$\begin{aligned} (x_1 + y_1\epsilon)^2 = x_1^2 + y_1^2 + 2x_1y_1\epsilon &\stackrel{\Downarrow}{=} dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2. \end{aligned}$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1y_1(x_2 + y_2))^2 \Rightarrow d = \square$
$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1y_1(x_2 - y_2))^2 \Rightarrow d = \square$
If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.

No exceptions if d is not a square.

Edwards curves mod p

Choose an odd prime p. Choose a non-square $d \in \mathbf{F}_p$.

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

is a "complete Edwards curve", i.e., there are no exceptions.

There are roughly $p + 1$ pairs (x, y) over $\mathbf{F}_p$ on the Edwards curve.
$(0, 1)$ has order 1, $(0, -1)$ has order 2, and $(\pm 1, 0)$ have order 4.
All Edwards curves have order divisible by 4.
Points $(\pm b, \pm b)$ (if they exist) have order 8.

Edwards curves mod p

Choose an odd prime p. Choose a non-square $d \in \mathbf{F}_p$.

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

is a "complete Edwards curve", i.e., there are no exceptions.

There are roughly $p + 1$ pairs (x, y) over $\mathbf{F}_p$ on the Edwards curve.
$(0, 1)$ has order 1, $(0, -1)$ has order 2, and $(\pm 1, 0)$ have order 4.
All Edwards curves have order divisible by 4.
Points $(\pm b, \pm b)$ (if they exist) have order 8.

If we instead choose square $d \notin \{0, 1\}$:
curve is still elliptic, and addition mostly works,
but there are failure cases.

Edwards curves mod p

Choose an odd prime p. Choose a non-square $d \in \mathbf{F}_p$.

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

is a "complete Edwards curve", i.e., there are no exceptions.

There are roughly $p + 1$ pairs (x, y) over $\mathbf{F}_p$ on the Edwards curve.
$(0, 1)$ has order 1, $(0, -1)$ has order 2, and $(\pm 1, 0)$ have order 4.
All Edwards curves have order divisible by 4.
Points $(\pm b, \pm b)$ (if they exist) have order 8.

If we instead choose square $d \notin \{0, 1\}$:
curve is still elliptic, and addition mostly works,
but there are failure cases.

Failures often exploitable by attackers.
Safe implementation is more complicated.

Twisted Edwards curves

Let p be an odd prime. Let $a, d \in \mathbf{F}_p^*, a \neq d$.

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

is called a twisted Edwards curve.

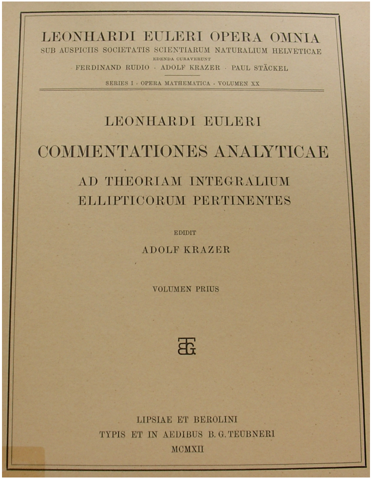
The addition law

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

is complete if a is a square and d is not.

Twisted Edwards curves cover more curves than Edwards curves ($a = 1$).
Group order is still divisible by 4. Points of order 4 need not exist.

Some history – going back to Euler



LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
FERDINAND RUDIO · ADOLF KRAZER · PAUL STÄCKEL
SERIES I · OPERA MATHEMATICA · VOLUMEN XX

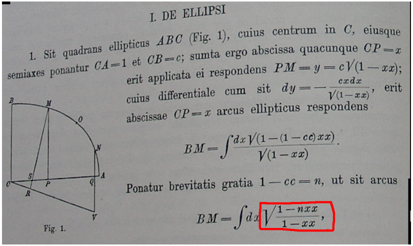
LEONHARDI EULERI
COMMENTATIONES ANALYTICAE
AD THEORIAM INTEGRALIUM
ELLIPTICORUM PERTINENTES

EDIDIT
ADOLF KRAZER

VOLUMEN PRIUS

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

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 $dy = -\frac{cx\,dx}{\sqrt{(1-xx)}}$, erit abscissae $CP = x$ arcus ellipticus respondens

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

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

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

Fig. 1.

$1/y = (1 - nx^2)/(1 - x^2)$
matches
$x^2 + y^2 = 1 + nx^2y^2$.

Gauss

Carl F. Gauss
(posthumously)

[2.]

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

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

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

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

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

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

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

General addition formulas for
$1 = s^2 + c^2 + s^2c^2$

Gauss and Edwards

Carl F. Gauss
(posthumously)

[2.]

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

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

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

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

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

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

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

General addition formulas for
$1 = s^2 + c^2 + s^2c^2$

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

Every elliptic curve
can be written as
$x^2 + y^2 = a^2(1 + x^2y^2)$,
for $a^5 \neq a$
over some extension field.

Edwards curves are cool!